

Results of threat analysis for a publishing system

Koen Buyens Johan Grégoire Sam Michiels
Bart De Win Wouter Joosen

Report CW475, Jan. 2007



Katholieke Universiteit Leuven
Department of Computer Science
Celestijnenlaan 200A – B-3001 Heverlee (Belgium)

Results of threat analysis for a publishing system

Koen Buyens Johan Grégoire Sam Michiels
Bart De Win Wouter Joosen

Report CW475, Jan. 2007

Department of Computer Science, K.U.Leuven

Abstract

This report contains the results of a threat modeling experiment for a next-generation digital publishing system that was developed within the context of the DigiNews research project. Threats have been elicited using two complementary techniques: (i) applying the STRIDE approach developed by Microsoft, and (ii) brainstorming driven by common security knowledge and privacy related regulations. The results of this experiment can be used, among others, to define the security requirements of the publishing system.

Contents

1	Introduction	2
2	Publishing architecture	3
3	Threat modeling	5
3.1	Technical elicitation and analysis	5
3.1.1	Step 1: Understand the attacker's view	5
3.1.2	Step 2: Characterize the security of the system	6
3.1.3	Step 3: Determine threats	10
3.2	Business elicitation and analysis	11
3.2.1	Collecting relevant information	11
3.2.2	Organizing a structured brainstorming activity	12
4	Discussion	12
5	Conclusion	13
A	Microsoft Threat Modelling	14
A.1	Understand the adversary's view	14
A.1.1	Entry points	14
A.1.2	Assets	20
A.1.3	Trust Levels	23
A.2	Characterize the security of the system	25
A.2.1	Define use scenario's	25
A.2.2	Identify assumptions and dependencies	25
A.2.3	Model the system	26
A.3	Define threats	42
A.3.1	Determine threats	42
A.3.2	Analyze threats	84
B	Brainstorming threat modeling	84
B.0.3	Collecting relevant information	84
B.0.4	Organizing a structured brainstorming activity	85

1 Introduction

Software security is not a "one-shot" activity. It requires the execution of a process that starts at the inception of the system and continues throughout the implementation, deployment, operation, and ends at the retirement of the system[3, 1]. This process is commonly referred to as full lifecycle management.

One of the key steps in the lifecycle of a secure system is risk assessment (or risk analysis), see Figure 1) – the *assessment of threats to, impacts on and vulnerabilities of information and information processing facilities and the likelihood of their occurrence*[4]. More formally stated: risk is defined as the complete set of scenarios S_i , the likelihood L_i and the consequences C_i of each scenario, that is the set of all triplets (S_i, L_i, C_i) [5]. The ultimate goal of risk assessment is to identify the scenarios with detrimental consequences and an unacceptable likelihood of occurring.

After the identification and assessment of the risks to which a system is subject, risks can be managed. Risk management conventionally encompasses risk assessment as a subprocess. While risk management can be broadly defined as the culture, processes and structures that are directed towards realizing potential opportunities whilst managing adverse effects[14], we will take a more IT-centric view: risk management is the process of identifying and controlling security risks that may affect information systems and this at an acceptable cost[4]. It allows IT managers to balance the operational and economic costs of protective measures[11]. It is a continual process of assessing and addressing risk throughout the life of the software that encompasses four subprocesses: asset identification, risk analysis, risk mitigation, and finally evaluation and assessment.

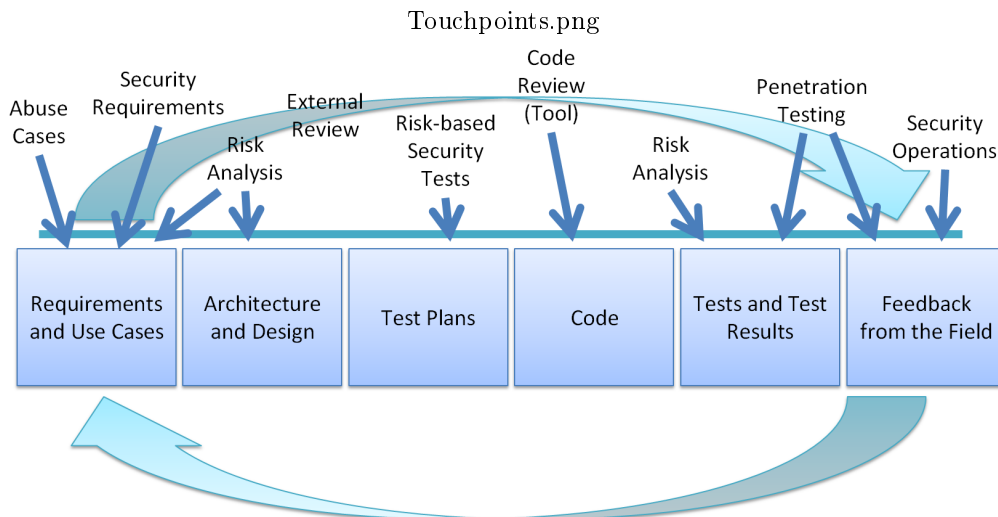


Figure 1: Security lifecycle according to build security in. Risk assessment is an important activity.

This report focuses on the first steps of risk analysis, namely the identification of threats to a publishing system. Two techniques have been applied to elicitate and analyze the risk to the system: the STRIDE method that was defined by Microsoft, which focuses on technical risks, and a brainstorming-based technique focusing on business-oriented risks. Both techniques have been applied to a publishing system developed in the context of the Diginews research project. It is our belief that the two techniques are complementary and that the application of both is useful in most cases.

The rest of this document is structured as follows. Section 2 briefly describes the particular case that was the subject of this experiment. Section 3 discusses the application of the two techniques for threat elicitation. Section 4 discusses the results to provide further insights into benefits and drawbacks of the techniques. Finally, Section 5 concludes our findings. The detailed results of the application of the two techniques are available in appendix.

2 Publishing architecture

This section describes a simplified version of the publishing system. A more elaborate version of the publishing system can be found in a report that describes the architecture of the system[6] and a report that provides an initial analysis of the system[13].

Figure 2 illustrates the overall structure of the publishing system. A subset of this publishing system is now described. The main features of the system are input management, content management, content distribution, and user management. In the architecture, the components responsible for these features are the following. An *Input Management System* (IMS) is used to annotate and prepare produced content to be stored in the Content Management System. The *Content Management System* (CMS) is responsible for storing and retrieving content items, and a *Service News Desk* is responsible for making content ready to be published. A *Service* (S) is utilized for distributing editions towards the media consumer and an *User Management System* (UMS) takes care of authenticating, authorizing, and accounting users that are using services of the publishing system.

The main actors involved in the publishing system are the input source, the advertiser, the media consumer, the service news desk worker, and the corporate news desk worker. The *input source* is the entity that produces content. This can be, for instance, an author, or a musician. The *advertiser* is the entity that produces advertisements. At the other end of the content consumption chain, the *media consumer* is the individual who wants to obtain and consume content. For example, a home user who wants to download and read the news of the day. The *service news desk worker* uses the publishing system to distribute finished content, and forms the bridge between consumers and producers.

In order to illustrate the functionality of the system, consider the following example scenario. Suppose that a *Media Consumer* wants to obtain the latest newspaper, which has a free book attached with it. In order to do this, he contacts the *Service Controller*, that has three successive tasks. First, the service controller obtains the media consumers credentials and sends them to the *User Management System*, which verifies these credentials. Second, it contacts the *Newspaper Service*, that obtains the newspaper from the *Content Management System*. Finally it forwards the reading material to the consumer.

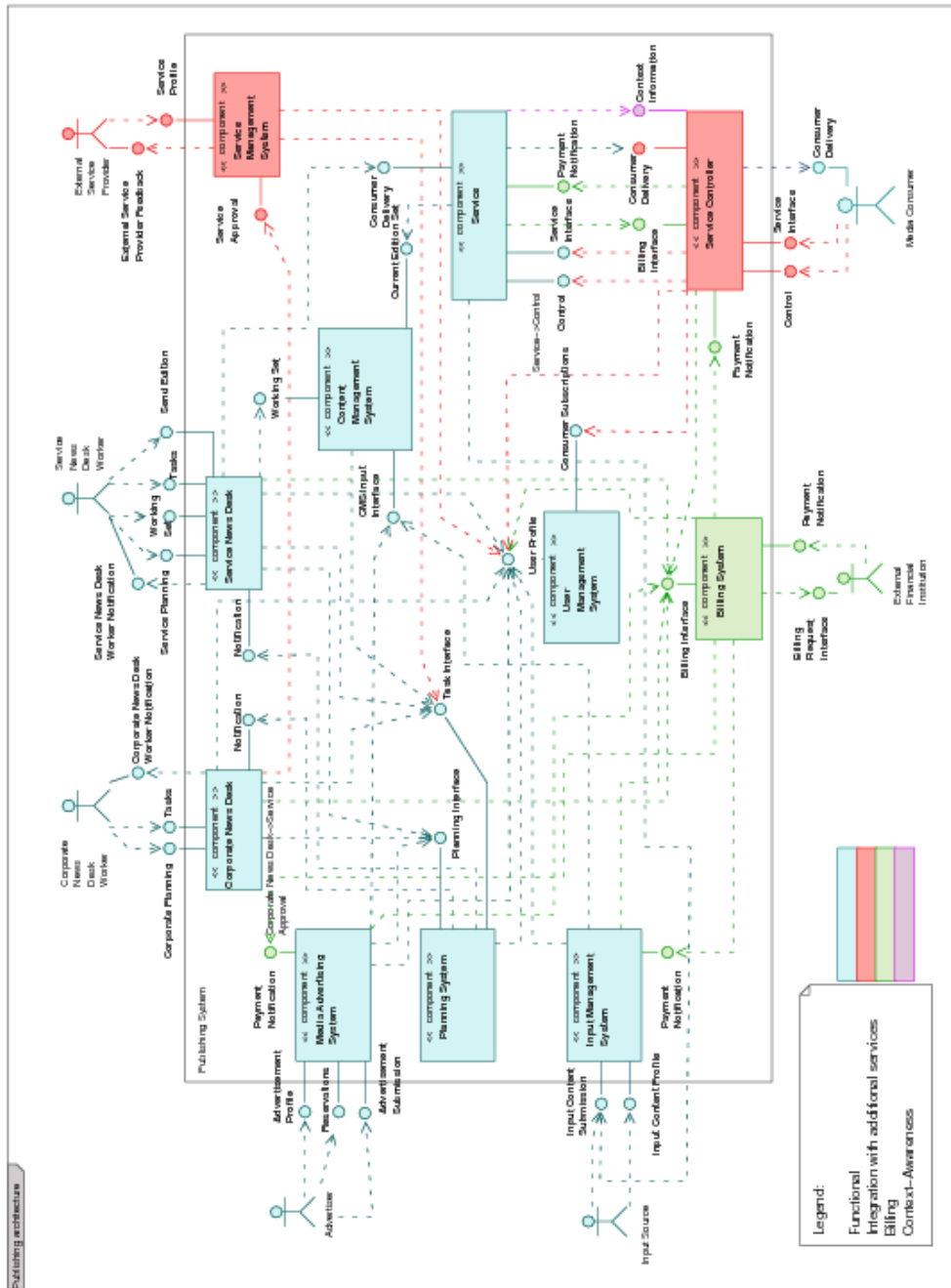


Figure 2: The complete publishing architecture.

Step 1 Understand the adversary's view

Identify Entry points Any location where data or control flow crosses the system's boundaries.

Identify Assets Anything that needs protection.

Identify Trust Levels Categorization of possible threat agents according to power.

Step 2 Characterize the security of the system

Define use scenario's Define how the system will be used, and how it won't be used in order to bound the threat modeling discussion.

Identify assumptions and dependencies External dependencies, security relevant information to users that interface with the system, information for the reader of the threat model, and assumptions under which the current threat model was made are identified.

Model the system by using dataflow diagrams.

Step 3 Determine threats

Determine threats Elicit and categorize threats using the STRIDE categories.

Analyze threats Decompose threats into threat trees and rate these threats by using DREAD.

Figure 3: Microsoft's threat modeling process.

3 Threat modeling

This section describes methods as well as results for identifying threats on the above described publishing system from two perspectives: (i) the application of Microsoft's threat modeling process[12] which focuses on the technical perspective, while (ii) a brainstorm activity on possible misuse of available use cases addresses the business perspective. In order to keep this section readable, only interesting results are highlighted; a detailed description (incl. results) of the application of each methodology has been included in appendix.

3.1 Technical elicitation and analysis

The main focus of Microsoft's threat modeling process[12] (see Figure 3) is the identification and prioritization of threats during the development phase of an application. It is based on the assumption that an application cannot be attacked unless the attacker can interact with it to compromise the information the application processes. The process consists of three high-level steps: (i) understanding the attackers view, (ii) characterizing the security of the system, and (iii) determining threats using the information identified in the previous steps. Each of these steps has logical substeps and do not have to be executed in a strictly linear way.

3.1.1 Step 1: Understand the attacker's view

The first step is to closely model the adversary's view. Understanding his view entails identifying (i) the application entry points, which also serve as entry points for attacks; (ii) the information the application processes (assets), that are subject to attack; and (iii) possible attackers who want to compromise the application and their power (trust levels).

Entry points are any locations where data passes between the (sub)system under review and the outside world, i.e. everything not belonging to the (sub)system. These points are the possible places where an adversary is able to interface with, and thus attack, the system. Examples are e.g.

a webpage with a contact form, a webservice, or an RPC call. In this experiment, identified entry points are organized in a hierarchical way. At the top level, an entry point is described as a general component of the publishing system, while at the lowest level¹ these are the interfaces of these components. Two types of entry points are distinguished, namely (i) internal entry points exposed by subcomponents to support internal system communication and (ii) entry points intended to be exposed to clients. Seven external top-level entry points were identified, including Corporate News Desk, Service News Desk, Media Advertising System, Input Management System, Billing System, Service Controller, and Service Management System. Internal top-level entry points complement these list with User Management System, Content Management System, and Planning System. Internal services have been included in this list as well.

Assets are the resources the system processes/has that the adversary might try to modify, steal, access or manipulate. Hence, assets are threat targets, and thus the basis for threats. These assets can be tangible, such as a credit card numbers. In this experiment, identified assets are divided in two types: (i) information, which is the business product; and (ii) infrastructure, which aids in the primary business model. Care was taken to a good selection of the granularity of assets: not too fine-grained and not too general (e.g. address of media consumer as asset) in order to keep the list of threats manageable, because similar information is grouped. Examples of information assets include Input, Consumer Behavior Information, and Corporate Planning. Examples of infrastructural assets are User Management System Server, and Media Consumer Device.

Trust levels represent the set of rights given to an external entity based on the system's knowledge of that entity. Trust levels group external entities according to their power into logical categories. They are applied at system entry points to safeguard assets. In this experiment, these entities correspond to users who access the publishing system, users and attackers of the infrastructure, and the identities of the running processes.

3.1.2 Step 2: Characterize the security of the system

Characterizing the security of the system involves (i) bounding the threat model, (ii) gathering information about dependencies that are critical to security, and (iii) understanding the internal workings of the system.

¹The methods of each interface have the same trust level as the interface. Hence, they are not included in the list of entry points.

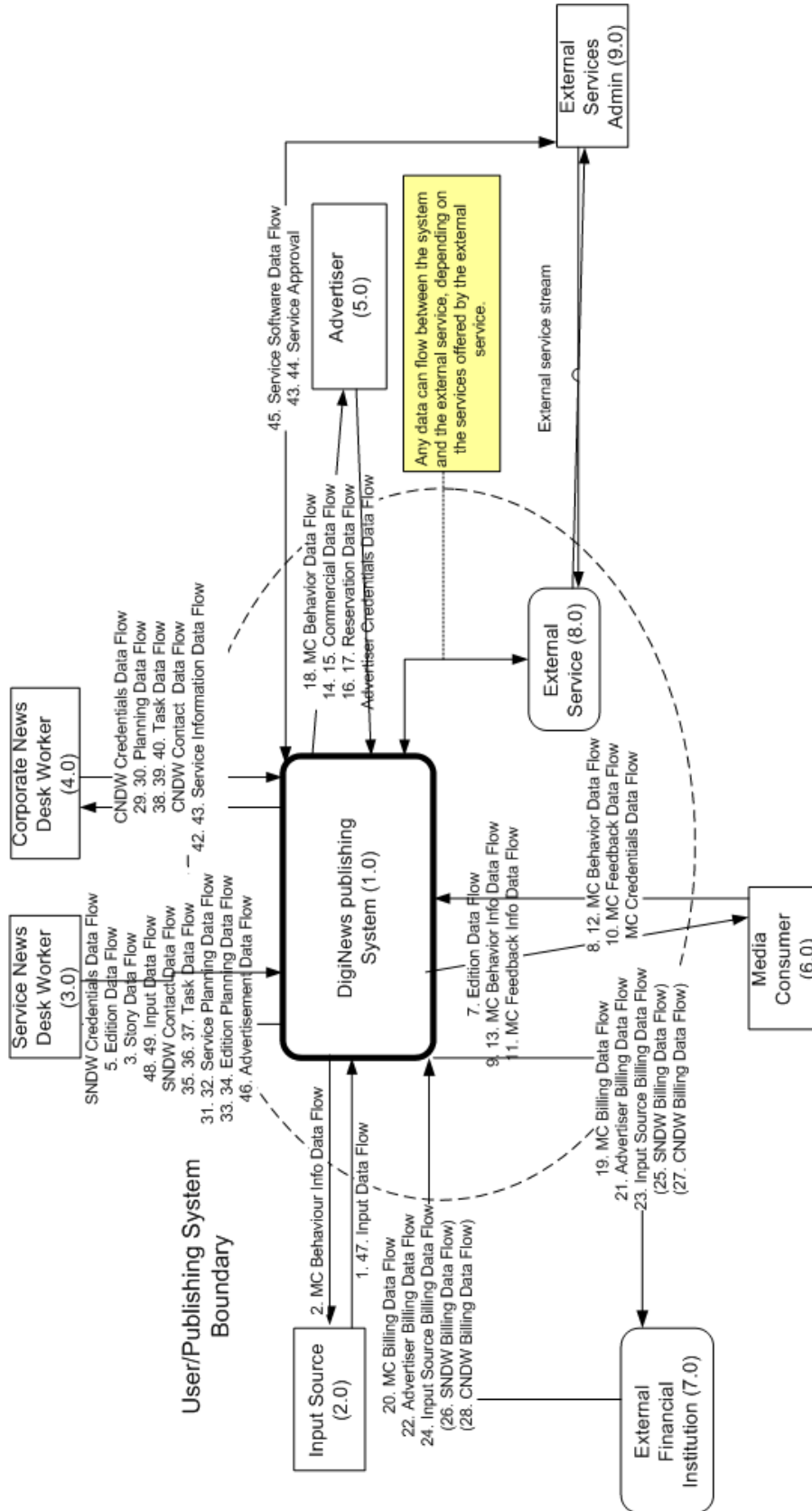


Figure 4: The context level dataflow diagram.

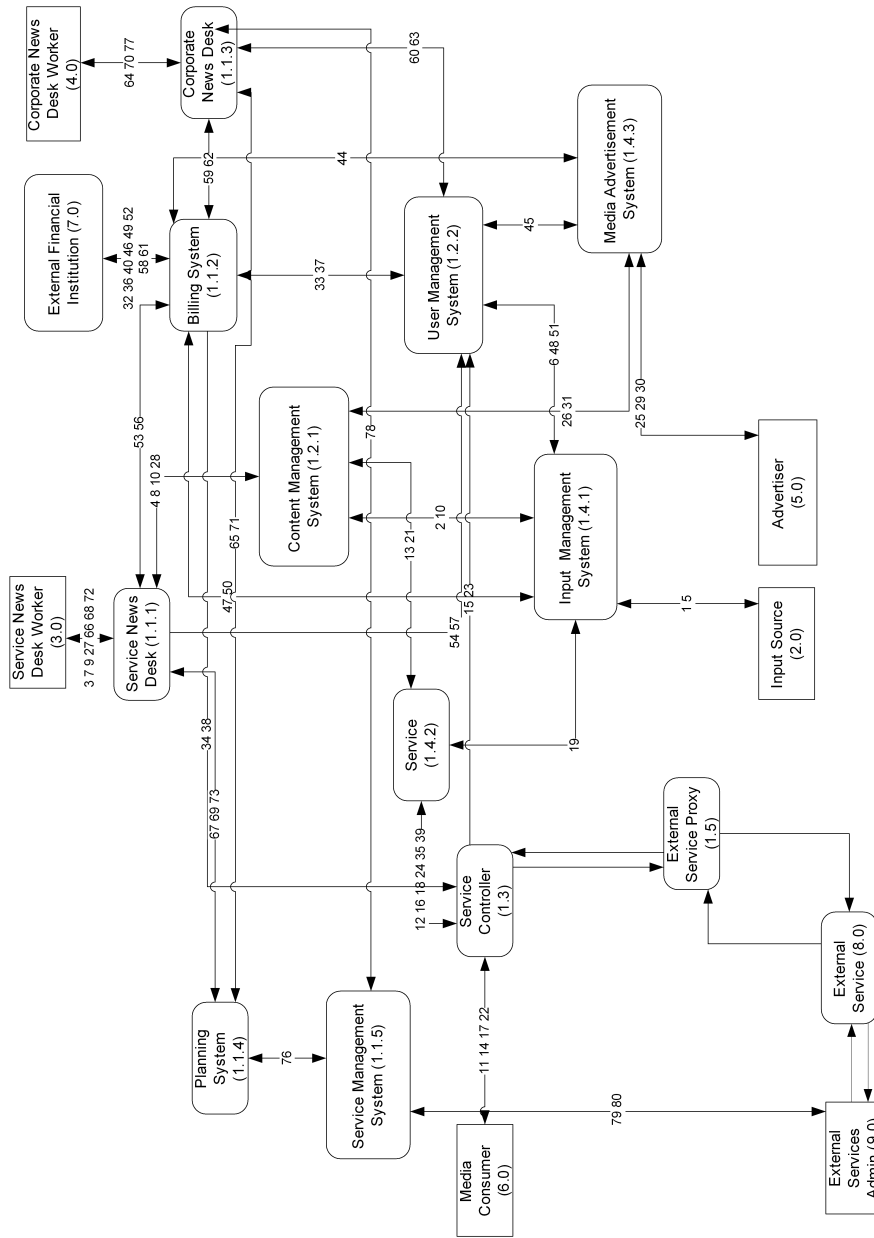


Figure 6: The level-2 dataflow diagram of the publishing system. Each number represents a data flow of an asset between two components. Trust boundaries are left out for clarity reasons.

The threat model can be bound by use scenario's, pointing out situations beyond the scope of the security architecture. These scenario's describe how the system is intended or *not* intended to be used. In other words, these scenario's *also* describe uses outside the safe use of the system, and can thus formulated in a more *negative* way. An example is *The Media Consumer Device is not designed to withstand attacks against the physical device.*

External dependencies document risks on other systems that also affect the security of the system being modeled. These dependencies are assumptions made about the usage or behavior of those other components or products. Inconsistencies can lead to security weaknesses. In this experiment, several external dependencies were identified. An example is *The publishing application depends on the security of the operating system(s) it runs on.*

A description of the internal working of the system aids in understanding the actions a system performs at a given entry point, and by consequence what an attacker might do at this given entry point. The internal working of the system is characterized by Data Flow Diagrams (DFDs). A DFD decomposes an application into processes (assets), (external) entities (entry points, assets), data stores (assets), data flows and privilege or trust boundaries (trust levels). This decomposition is iterative: starting from a rough DFD, each iteration adds refinements until a sufficient level of detail is acquired. In this experiment, Figure 4 depicts the top level dataflow diagram. This diagram contains the system itself as top-level process, the actors interacting with the system, trust boundaries, and elementary data flows. Figure 5 refines the top-level diagram and identifies the subsystems the actors are interacting with. Figure 6 refines the previous diagram and identifies all internal components of the system and their interactions.

3.1.3 Step 3: Determine threats

Threats are identified and analyzed in a systematic way by the (i) STRIDE and (ii) DREAD methods respectively. STRIDE is an acronym formed by the first letter of each of the following categories of threats:

1. *Spoofing* Faking an identify.
2. *Tampering* Compromising the integrity of data.
3. *Repudiation* Denying having performed an action, such as denying having purchased an item from an online shop.
4. *Information disclosure* Compromising the confidentiality of data.
5. *Denial of service* Compromising the availability of a service.
6. *Elevation of privilege* Illegally obtain more privileges.

The STRIDE method assigns the above-mentioned categories to the elements in the final DFD in order to identify classes of threats to which the elements may be vulnerable (see Table 1). Each combination of a STRIDE-threat and a threat target (DFD element) should be investigated in order to verify whether the threat is indeed a real threat. This investigation can be done by using attack trees. The threat should be kept if there is an attack path in the tree leading to the threat under investigation. Otherwise, the threat should be removed from the list of threats. In this experiment, STRIDE-threats were identified for the data-flow elements. Table 2 illustrates possible STRIDE-threats for a subset of these data-flow elements. An example threat tree for the *Spoofing Media Consumer Client*-threat can be found in Figure 7. The threat tree illustrates that it is indeed possible to spoof a media consumer client. By consequence the system is vulnerable for this threat. The verification whether the threat is indeed a real threat has been done for the subset of the threats, because this was monotonous and time-consuming. The authors assume that every threat has an attack path. By consequence, this leads to an explosion of possible threats (see Table 2) to the publishing system.

DREAD is then used to assess these potential vulnerabilities. DREAD is an acronym that defines the following five key attributes used to measure the criticality of a vulnerability: Damage

- 1 Spoofing Media Consumer client
 - 1.1 Falsify Media Consumer Client software
 - 1.2 Install falsified software on Client
 - 1.2.1 Obtain Media Consumer client software
 - 1.2.1.1 Media Consumer client software is available
 - 1.2.2 Install Media Consumer client software on Client
 - 1.3 Install falsified software on existing Media Consumer client
 - 1.3.1 Break into a Media Consumer house (or similar)
 - 1.3.2 Install falsified software

Figure 7: An example attack tree.

potential, Reproducibility, Exploitability, Affected users, and Discoverability. The application of DREAD is beyond the scope of this report.

	Process	Data Storage	Actor	Data Flow
Spoofing	x		x	
Tampering	x	x		x
Repudiation		x	x	x
Information Disclosure	x	x		x
Denial of Service	x	x		x
Elevation of Privilege	x			

Table 1: Possible combinations of STRIDE-threats and threat targets

	Spoofing	Tampering	Repudiation	Information Disclosure	DoS	Elevation of privilege
Data Flow Input		1	2	3	4	
MC Behavior		5	6	7	8	
Story		9	10	11	12	
Edition		13	14	15	16	
MC credentials		17	18	19	20	
MC behavior		21	22	23	24	

Table 2: A subset of the possible STRIDE threats in the experiment. Each number represents a possible threat.

3.2 Business elicitation and analysis

This section describes a structured brainstorming approach for identifying business threats. A business threat is defined as a threat that uses the functionality the system offers in way that is not conform with business policy or regulations and laws. The method the authors came up with consists of two high-level steps: (i) collecting relevant regulations, laws, and a description of the system, and (ii) organizing a structured brainstorming activity for identifying business abuses.

3.2.1 Collecting relevant information

The first step is to collect relevant information about the application domain. This information includes (i) regulations and legislations, and (ii) an inventory of use cases.

Applications in the e-commerce are subject to different regulations and legislations. These determine to a great extent the architectural security requirements and solutions of the system.

In this experiment, the following regulations may be applicable for a publishing platform: (i) Privacy legislation on usage and storage of personal data[8, 9, 10], (ii) E-transactions legislations and regulations[7], and (iii) Information Security Law. These regulations are summarized as follows:

1. Collecting: personal data can only be collected and processed by the provider if permitted by some law or if the individual has unambiguously given his consent.
2. Use: Data must not be processed for any purposes incompatible with those for which the data was initially collected. It cannot be transferred to third parties without agreement from the data subject. Security measures must be taken to protect the data against destruction or loss. It should not be kept longer than necessary for the purpose it was collected.
3. Access: Data should be accurate, complete and kept up-to-date. The customer must have access to any personal data concerning him/her that is being processed or kept. A request for correction or deletion of incorrect personal data must be granted. The customer must have the possibility to opt out.
4. Processing of personal preferences is usually prohibited, except for when the person who's information is to be processed has given his consent.

The use cases described in the analysis document[13] and the architecture document[6] were used.

3.2.2 Organizing a structured brainstorming activity

Brainstorming[2] is a group creativity technique that was designed to generate a large number of ideas for the solution of a problem. This process is based on 4 ideas. The participants should focus on *quantity*, because a higher number of ideas increases the chance that an effective solution is produced. *No criticism* creates the right atmosphere for generating *unusual ideas*, which may provide better solutions. The participants should also *combine and improve* the ideas of others.

During the brainstorming session(s), possible attacks were generated for the system. The authors tried to attack the system, which was seen as a *blackbox*, in any way they thought was possible. Documents describing the functionality of the system have been used as starting point.

Examples of abuses that were found are:

1. Bribe the News Desk Workers in order to give an edition before it is published.
2. Threat the user to use his device to subscribe to a service.
3. The people who implemented the system also implemented some backdoor, allowing them to access the system and all the sensitive information without any restriction

This unstructured method complements the abuses found in the previous section with environmental and business abuses.

4 Discussion

In this section, the applied methods for eliciting threats are compared in an informal way, and two alternative approaches for threat elicitation are described.

Microsoft's STRIDE methodology is a structured way for threat elicitation. This method examines all information data flowing from the actors to the system, and between subsystems. Since it is based on technical descriptions of a system (e.g., an architectural description), it finds most technical threats related to information assets. However, this methodology does not identify business threats. The business threat brainstorming process, on the other hand, focuses on identifying business related threats. Hence, it can be seen as a method that complements the threats found with STRIDE.

An alternative approach to enumerating threats related to information assets (technical threats) may start from the use cases of the system. This alternative approach consists of two steps for each use case. First, one has to identify the information assets and entities processing this information. These assets are the data the user provides to or obtains from the system. The entities are typically the main actor of the use case and the (sub)systems he is interacting with. Second, one has to identify ways to compromise this information by applying the STRIDE categories to the assets and processing entities. Experiments have shown that the threats that result from such analysis mostly correspond to the results obtained by applying the STRIDE approach.

A more structured approach for eliciting business threats extends the alternative approach for enumerating technical threats. For each identified asset and processing entity identify which regulations and laws are applicable. Afterwards, enumerate abuses based on these regulations. The following example illustrates this process. According to the privacy regulation, the address of a media consumer is indeed privacy-sensitive data. Therefore, the publisher is not allowed to e.g. collect this data without the consent of the media consumer, use this data for other than the agreed purposes (e.g. selling to a third party), or do not allow the media consumer to consult or modify this information. By consequence, a possible threat is *Spread the address of the media consumer*.

5 Conclusion

In this report two methods for enumerating threats (STRIDE, brainstorming) have been applied and analyzed in the context of a digital publishing case study. In summary, STRIDE requires a lot of work but identifies a significant number of threats. The brainstorming method complements the threats enumerated by STRIDE with environmental and business threats. In the future, this work can be used as input for the identification of security requirements of the publishing system, as well as for research on secure software engineering.

A Microsoft Threat Modelling

The main focus of Microsoft's threat modeling process[12] (see Figure 3) is the identification and prioritization of threats during the development phase of an application. Its based on the assumption that an application cannot be attacked unless the attacker can interact with it to compromise the information the application processes. The process consists of three high-level steps: (i) understanding the attackers view, (ii) characterizing the security of the system, and (iii) determining threats using the information identified in the previous steps. Each of these steps has logical substeps and do not have to be executed in a strictly linear way.

A.1 Understand the adversary's view

The first step is to closely model the adversary's view. Understanding his view entails identifying (i) the application entry points, which also serve as entry points for attacks; (ii) the information the application processes (assets), that are subject to attack; and (iii) possible attackers who compromise the application and their power (trust levels).

A.1.1 Entry points

Entry points are any location where data passes between the (sub)system under review and the outside world, i.e. everything not belonging to the (sub)system. These points are the possible places where an adversary is able to interface with, and thus attack, the system. Examples are e.g. a webpage with a contact form, a webservice, or an RPC call. In this experiment, identified entry points are organized in a hierarchical way. At the top level, an entry point is described as a general component of the publishing system, while at the lowest level² these are the interfaces of these components. Two types of entry points are distinguished, namely (i) internal entry points exposed by subcomponents to support internal system communication and (ii) entry points intended to be exposed to clients.

Tables 3 and 4 list the external and internal entry points and describes the interfaces through which external entities can interact with the components, either by direct interaction or by indirectly supplying it with data.

²The methods of each interface have the same trust level as the interface. Hence, they are not included in the list of entry points.

ID	Name	Description	Trust Level
All	Common	Administrator has access to the publishing system at all time.	(9) Administrator
1	Corporate News Desk	The component that is been used by the Corporate News Desk Workers.	(2) Corporate News Desk Worker
1.1	Corporate Planning	This interface is offered to the Corporate News Desk Worker to consult and/or adapt the planning of the corporate strategy.	(2) Corporate News Desk Worker
1.2	Tasks	This interface is used by a Corporate News Desk Worker to insert new tasks into the task system.	(2) Corporate News Desk Worker
2	Service News Desk	Every Service News Desk is responsible for one or more services and the editions that will be released by these services.	(3) Service News Desk Worker
2.1	Service Planning	This interface is offered to the Service News Desk Workers and will be used for the planning of a service and/or their editions.	(3) Service News Desk Worker
2.2	Working Set	This interface enables the Service News Desk Worker to access and use their Working Set. Each Service News Desk Worker has a Working Set, which contains all the content that he is currently working on.	(3) Service News Desk Worker
2.3	Tasks	This interface is used by a Service News Desk Worker to insert new tasks into the system.	(3) Service News Desk Worker
2.4	Send Edition	Once an edition is finished it might be necessary for the Service News Desk to push it towards the Media Consumer. This interface is used for that occasion.	(3) Service News Desk Worker
3	Media Advertisement System	This component is used by the Advertisers to submit new advertisements to the system in order to have them published.	(4) Advertiser
3.1	Advertisement Profile	This interface is used by the Advertiser to retrieve information about the advertisements he has submitted to the system.	(4) Advertiser
3.2	Reservations	Through this interface the Advertiser can request a list of available reservations, in order to be able	(4) Advertiser

3.3	Advertisement Submission	to pick one out for the submission of a new advertisement. The actual submission of advertisements is done through this interface.	(4) Advertiser
4.	Input Management System	The Input Management System is the component that handles incoming noncommercial content, such as articles or photographs, that is uploaded to the system by the Input Sources.	(5) Input Source
4.1	Input Content Submission	This interface is used by Input Sources to send in their content.	(5) Input Source
4.2	Input Content Profile	This interface is used by Input Sources to check the profile of the content sent in by them.	(5) Input Source
5.	Billing System	The Billing System is the component in the publishing system that keeps information about all payment methods, all External Financial Institutions, and pending payments.	(7) External Financial Institution
5.1	Payment Notification	This interface is used by the External Financial Institutions to notify the publisher when a payment transaction has been completed successfully.	(7) External Financial Institution
6.	Service Controller	This component is responsible for having control over services.	(1) Media Consumer
6.1	Control	This interface is offered to the Media Consumer for subscribing/unsubscribing to a service and to the system.	(1) Media Consumer
6.2	Service Interface	This interface is offered to the Media Consumer for browsing through editions, lists of editions, etc. It is also used to send viewing information and feedback from the Media Consumer to the Service.	(1) Media Consumer
7.	Service Management System	This component is responsible for the communication with the different service providers.	(2) Corporate News Desk Worker (6) External Service Provider
7.1	Service Profile	This interface is used to check and change the profile of a service.	(2) Corporate News Desk Worker (6) External Service Provider

Table 3: External entry points for the publishing system.

1.	Corporate News Desk	The component that is been used by the Corporate News Desk Workers.	(2) Corporate News Desk Worker (11) Planning Service Process (11) Corporate News Desk Service Process
1.1	Notification	This interface is used by the Planning System to notify a Corporate News Desk Worker of the addition of new tasks.	(2) Corporate News Desk Worker (11) Planning Service Process
2.	Service News Desk	Every Service News Desk is responsible for one or more services and the editions that will be released by these services.	(11) Corporate News Desk Service Process (3) Service News Desk Worker (11) Planning Service Process
2.1	Notification	This interface is generally used to notify the Service News Desk Workers of the addition of new tasks.	(11) Service News Desk Worker (11) Planning Service Process
3.	Media Advertisement System	This component is used by the Advertisers to submit new advertisements to the system in order to have them published.	(3) Service News Desk Worker (11) Planning Service Process (11) Service News Desk Process (4) Advertiser
3.1	Payment Notification	This interface is used by the Billing System to notify the Media Advertising System that the payment has been completed.	(4) Advertiser
4.	Input Management System	The Input Management System is the component that handles incoming noncommercial content, such as articles or photographs, that is uploaded to the system by the Input Sources.	(5) Input Source
4.1	Payment Notification	This interface is used by the Billing System to notify the Input Management System that the payment has been completed.	(5) Input Source
5.	Billing System	The Billing System is the component in the publishing system that keeps information about all payment methods, all External Financial Institutions, and pending payments.	(6) External Financial Institution
5.1	Billig Interface	This interface is used to request payments from users.	(6) External Financial Institution
6.	Service Controller	This component is responsible for having control over services.	(7) External Service Provider
6.1	Payment Notification	This interface is used by the Billing System to notify the Service Controller about the completion	(7) External Service Provider

6.2	Billing Interface	of a certain payment for a certain Service. This interface is used by the Service components to invoke the publishing system to request a payment from a certain user.	(7) External Service Provider
6.3	Consumer Delivery	This interface is used by each of the services to present information to the Media Consumer.	(1) Media Consumer (7) External Service Provider
6.4	Context Information	This interface is offered to the Services to request context information of a certain user.	(1) Media Consumer (7) External Service Provider
7.	Service Management System	This component is responsible for the communication with the different service providers.	(2) Corporate News Desk Worker (7) External Service Provider
7.1	Service Approval	This interface is used by the Corporate News Desk to approve newly requested services.	(2) Corporate News Desk Worker
8.	User Management System	The User Management System is the component that handles all information about all of the publisher's users, which are the Media Consumers, the Advertisers and the Input Sources.	(1) Media Consumer (9) Administrator (4) Advertiser (5) Input Source (2) Corporate News Desk Worker (3) Service News Desk Worker (8) External Service Provider (1) Media Consumer (9) Administrator (1) Media Consumer (9) Administrator
8.1	Consumer Subscriptions	This interface is used for handling everything that is subscription-related.	
8.2	User Profile	This interface is used for reading and changing the profile of a user.	
9.	Content Management System	All content, such as articles, photographs and advertisements are stored and organized centrally in the Content Management System. The interfaces of this component facilitate the lifecycle of stories.	
9.1	CMS Input Interface	New content (regular content and/or advertisements) is passed to the Content Management System via this interface.	
9.2	Working Set	After reception of new content, it will at some	

point be inserted in the Working Set of a certain Service News Desk Worker. This working set is the collection of all content that this Service News Desk Worker is currently working on. From then on this interface is used to work with that input in order to create a story out of it or include it in an edition.

Once an edition is finished and ready to be published, it will be marked as a current edition of a certain service. The Current Edition Set interface can then be used to retrieve this edition in an easy way.

This component is responsible for knowing the corporate strategy and making semi-automated decisions that are in accordance with this strategy. This interface is used to query and adapt the planning and/or strategies.

This interface is used by the different workers to offer tasks to the Planning System component.

The Service component serves as a representation for a service that is offered to the Media Consumer. This interface is used by a Service News Desk to trigger the release of an edition. It is a notification that a certain edition was added to the Current Edition Set.

This interface is used to notify the Service component of the completion of a certain payment. This interface is used by a Service News Desk to trigger the release of an edition.

Table 4: Internal entry points for the publishing system.

9.3	Current Edition Set	(11)Corporate News Desk Server process identity
10.	Planning System	(11)Corporate News Desk Server process identity
10.1	Planning Interface	(11)Service News Desk Server process identity
10.2	Task Interface	(1) Media Consumer
11.	Service	(11)X Server process identity
11.1	Consumer Delivery	(11)Service News Desk Server process identity
11.2	Payment Notification	(11)Billing System
11.3	Consumer Delivery	Server process identity (11)Service News Desk Server process identity

A.1.2 Assets

Assets are the resources the system processes/has that the adversary might try to modify, steal, access or manipulate. Hence, assets are threat targets, and thus the basis for threats. These assets can be tangible, such as a credit card numbers. In this experiment, identified assets are divided in two types: (i) information, which is the business product; and (ii) infrastructure, which aids in the primary business model. Care was taken to a good selection of the granularity of assets: not too fine-grained and not too general (e.g. address of media consumer as asset) in order to keep the list of threats manageable, because similar information is grouped.

- Information

1. **Edition**

An edition is an ordered and structured collection of stories and commercials. For instance, an edition can be a newspaper or a book or a free tutorial. We distinguish the following editions:

Edition limited in time, valuable : an edition can be limited in time. For instance news in a newspaper ages really fast. The day after, this newspaper is almost nothing worth. Who wants to read news of a few days old?

Edition limited in time, free : the publishing company gives sometimes editions away for free. For instance an extra edition is added to another paid edition.

Edition not limited in time, valuable : an edition that do not lose its value, even after a long time. For instance, a book of the brothers Grimm.

Edition not limited in time, free : an edition that does not lose its value, even after a long time, but was given away for free. For instance, an overview of the year 2001.

2. **Story**

A story is a finished publication which can be incorporated in editions. A story is built from story items and can be a combination of media types. We distinguish the following stories:

Story limited in time, valuable : a story can be limited in time and valuable. For instance news of the day (scoop) ages really fast, but is initially very valuable. However, the day after, it is almost nothing worth.

Story limited in time, invaluable : a story can be limited in time and invaluable. For instance, local news that has been published by several other publishing companies.

Story not limited in time, valuable : a story which do not lose its value, even after a long time. For instance, a picture of the collapsing Twin Towers.

Story not limited in time, invaluable : a story which is invaluable, even after long time. For instance, local news in a year overview.

3. **Input**

The terms input or raw input are used to specify the multi-media content coming from the sources. We assume all input is equally important, before passing the input verification task. After verifying and classification, input becomes a story.

4. **Commercial (Advertisement)**

Commercials are made by advertisers. Commercials are typically an important source of income for the publisher. The goal of the commercials is to convince the media consumers to buy the advertisers products or services. Publishing systems which support digital, multi-media content can offer commercials in different forms. An advertiser pays for the space and/or time the commercial appears. A long running commercial of an entire page is more valuable than a one time commercial of a quarter page. Commercials possibly contain a *description* of the product or service, *billing information* of the product or service and or *contact information* of the product or service.

5. Commercial Reservation

A Commercial reservation is a list of reservations of advertisements in e.g. an edition. This asset can be seen as a part of the edition planning.

6. Meta-data

Meta-data is added to input and advertisements and contains *Critical meta-data* such as validation information and *Non-critical meta-data* such as a description of the text. This asset can be seen as a subpart of the commercial asset and the input asset.

7. Customer information

The advertiser, input source, media consumer, financial institution and third party services are all customers of the publisher. By consequence, the publisher stores the following information of these parties:

Customer Contact : the contact information of a customer. This can be for instance an address, a telephone number, an e-mail address, etc.

Customer Billing : the billing information of a customer. This includes his bill or receipt, his account number, his credit card number, the total value of the goods ordered etc.

Customer Behavior : the behavior of a customer. For instance, for a consumer this includes his consumption behavior.

Note that one should make a distinction between the information of each party. The account number of a customer is less important than the account number of the publishing company.

8. Employee information

The service and corporate news desk workers are all working for the publisher. Because the publisher pays these parties, he stored for instance their account numbers:

Employee Contact : the contact information of an employee. This can be for instance an address, a telephone number, an e-mail address, etc.

Employee Billing : the billing information of the employee. This includes his loan, his account number, etc.

Employee behavior : the behavior of the employee. For instance, the tracking of every action an employee makes.

9. Task

A task is a piece of work assigned to an employee of the publishing company. There can be tasks for gathering content, modifying content or verifying content. It contains a *subject*, a *description*, *contact information* (such as addressee and possibly principal) and *timing information* (such as a deadline, date received and starting date). We are interested in the following tasks:

Input Verification Task : most important task. The employee who is assigned this task, verifies and categorizes the input.

Advertisement Verification Task

Other tasks : the other tasks

10. Planning

The planning for the different products is mostly pro-active. First a publisher strategy is defined by the corporate news desk. This will include the business goals of the publisher and a coarse-grained strategy for publishing on multiple services. Next, the service news desks define the strategy for their services. When the strategies are defined, the concrete service planning and edition planning are worked out by the service news desks. If someone influences the planning of a certain edition, news desk or corporate planning, the publisher will be influenced too. By changing the planning, a publishing company can evolve from a science related publishing company to a gossip publishing company. We distinguish the following planning assets (ordered by importance):

Corporate Planning**Service Planning****Edition Planning**

The planning contains a lot of information. The edition planning contains for instance the layout of the edition including color-schemes, advertisement placement etc.

- **Infrastructure**

The infrastructure aids the primary business model and consists mainly of hardware and software.

1. **Consumer devices:** The consumer devices are the devices used by the media consumers to consume content. It includes the hardware (e.g. a flexible screen) and the software (e.g. a webbrowser).
2. **Servers and environment:** The hardware that runs the services of the publisher. We distinguish:
 - Servers: hardware itself
 - Electricity: hardware is powered
 - Environment: humidity, temperature, etc.
 - Physical location: hardware is placed in a building.
3. **Publisher Clients:** the hardware of the news desk workers.
4. **Network connectivity:** connection between the publisher and its customers. We distinguish the following connections:
 - **Publisher-to-consumer channel** is used by the consumer to interact with the media consumer.
 - **Input-source-to-publisher** is used by the input source to submit input.
 - **Advertiser-to-publisher** is used by the publisher to interact with the advertiser.
 - **Publisher-to-third-party** is used by the publisher to interact with different service providers.
 - **Publisher-to-financial-institution** is used by the publisher to interact with the financial institution.
 - **Other** Channels which we do not influence. For instance the consumer-to-financial-institution.
5. **Services:** the services the publisher offers. We distinguish the following services:
 - **Input System:** imports input and offers statistics.
 - **Advertisement System:** imports advertisements and offers statistics.
 - **Planning System:** manages planning and tasks.
 - **Service News Desk:** interface towards the service news desk worker.
 - **Corporate News Desk:** interface towards the corporate news desk worker
 - **Content Management System:** stores all the content, including commercials, input, stories, etc.
 - **User Management System:** used to manage all the users of the system.
 - **Service:** each service from the service news desk can have a service.
6. **Employees:** employees keep the publishing company alive. We distinguish
 - **Corporate News Desk Workers:** manage the publishing company.
 - **Service News Desk Workers:** create editions, stories and input. E.g. reporters, lay-outers, etc.

A.1.3 Trust Levels

Trust levels represent the set of rights given to an external entity based on the system's knowledge of that entity. Trust levels group external entities according to their power into logical categories. They are applied at system entry points to safeguard assets. In this experiment, these entities correspond to users who access the publishing system, users and attackers of the infrastructure, and the identities of the running processes.

Table 5 lists the trust levels and describes privilege levels that are associated with entry points and assets.

ID	Name	Description
1	Media Consumer	A user who has login credentials that allow him/her to obtain editions, to submit viewing information, to manage their profile, etc.
2	Corporate News Desk Worker	The Corporate News Desk Worker is a person that works at the Corporate News Desk. He is offered the following functionalities: consult and adapt the planning of the corporate strategy, insert new tasks into the system, approving new services, etc.
3	Service News Desk Worker	A Service News Desk Worker is a person that works at the Service News Desk. He is offered the following functionalities: consult, create, and adapt the service planning, insert new tasks into the system, work with the offered content, send the finished edition to the Media Consumers, etc.
4	Advertiser	An Advertiser submits advertisements to the publishing system, by selecting a previously placed reservation or making a new one. He also has the option to check the profile of the advertisements uploaded by him (the number of views, . . .), etc.
5	Input Source	The Input Source submits new content to the publishing system, checks the profile of the content already sent in by him (the number of views, etc).
6	External Service Provider	The (external) Service Provider represents the person or company that wants to install a new Service component within the publisher's infrastructure, in order to offer new services. This person is offered the following functionalities: consulting and adapting the service profile.
7	External Financial Institution	This institution offers the publishing system the functionality to request payments from a certain person or to perform payments to a certain person.
8	Remote anonymous user	A user who has connected to the system, but has not yet provided legitimate credentials.
9	Administrator	The administrator can configure the publishing system, including data server, publishing platform, internal services, service controller, etc.
10	External Service Provider Provider Administrator	The administrator can configure the external service provider components.
11	X Server process identity	This depends on the deployment of the publishing system. Each component can be installed on a separate server, or can be deployed as recommended in the deployment diagram.

Table 5: The trust levels and privileges that are associated with entry points and assets

A.2 Characterize the security of the system

Characterizing the security of the system involves (i) bounding the threat model, (ii) gathering information about dependencies that are critical to security, and (iii) understanding the internal workings of the system.

A.2.1 Define use scenario's

The threat model can be bound by use scenario's, pointing out situations beyond the scope of the security architecture. These scenario's describe how the system is intended or *not* intended to be used. In other words, these scenario's *also* describe uses outside the safe use of the system, and can thus formulated in a more *negative* way. Table 6 lists the identified use scenarios for the application.

ID	Description
1	The Media Consumer Device is not designed to withstand attacks against the physical device.
2	The Advertiser is not designed to withstand attacks against the physical device.
3	The Input Source is not designed to withstand attacks against the physical device.
4	The publishing application will be connected via the Internet.
5	The MC device is connected to the publishing system in some way.
6	Communication between internal publishing components should be conducted over a private network.
7	The publishing platform, internal services, service controller, data server, external service proxies should be protected from direct access from the Internet by a firewall.

Table 6: Identified use scenarios for the publishing system

A.2.2 Identify assumptions and dependencies

External dependencies document risks on other systems that also affect the security of the system being modeled. These dependencies are assumptions made about the usage or behavior of those other components or products. Inconsistencies can lead to security weaknesses. Table 7 lists the identified external dependencies.

ID	Description
1	The publishing application depends on the security of the operating system(s) it runs on.
2	The publishing application depends on the external financial institution for payments.
3	The publishing application depends on the services external services provide. Weaknesses in these services shouldn't compromise other services or the publishing system.
4	The publishing application depends on the security of the (.NET) runtime libraries it uses.
5	The publishing application data components depends on the security of the database server it uses.
6	The publishing application depends on the security of the network between the internal publishing system components. If the network is compromised, sensitive data could be viewed or direct attacks on the internal components (including data components) could be made.

Table 7: External Dependencies the publishing system has on other components or products that can impact security.

A.2.3 Model the system

A description of the internal working of the system aids in understanding the actions a system performs at a given entry point, and by consequence what an attacker might do at this given entry point. The internal working of the system is characterized by Data Flow Diagrams (DFDs). A DFD decomposes an application into processes (assets), (external) entities (entry points, assets), data stores (assets), data flows and privilege or trust boundaries (trust levels). This decomposition is iterative: starting from a rough DFD, each iteration adds refinements until a sufficient level of detail is acquired. In this experiment, figure 8 depicts the top level dataflow diagram. This diagram contains the system itself as top-level process, the actors interacting with the system, trust boundaries, and elementary data flows. The data flows of this diagram are described in table 8.

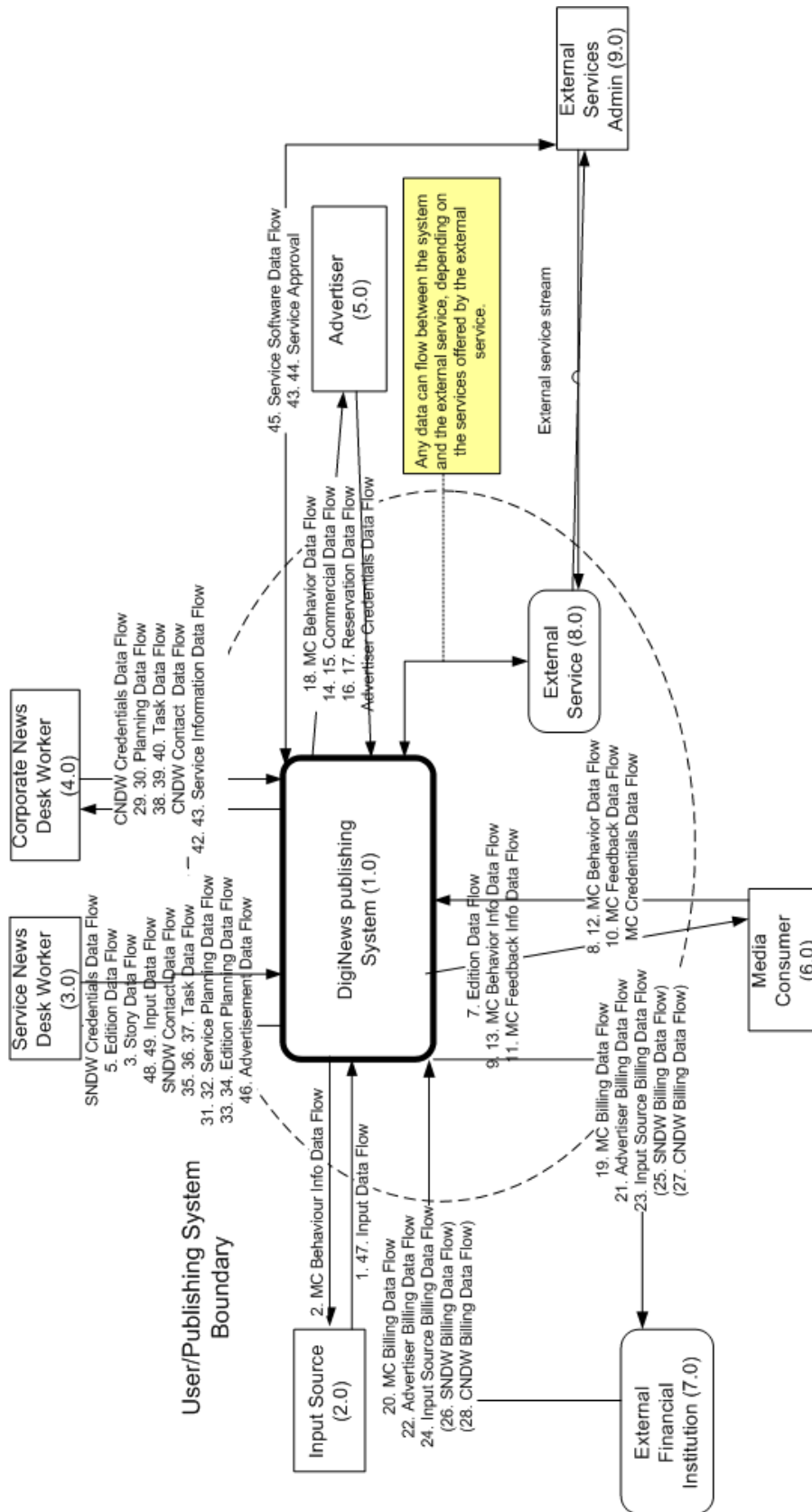


Figure 8: The context level dataflow diagram.

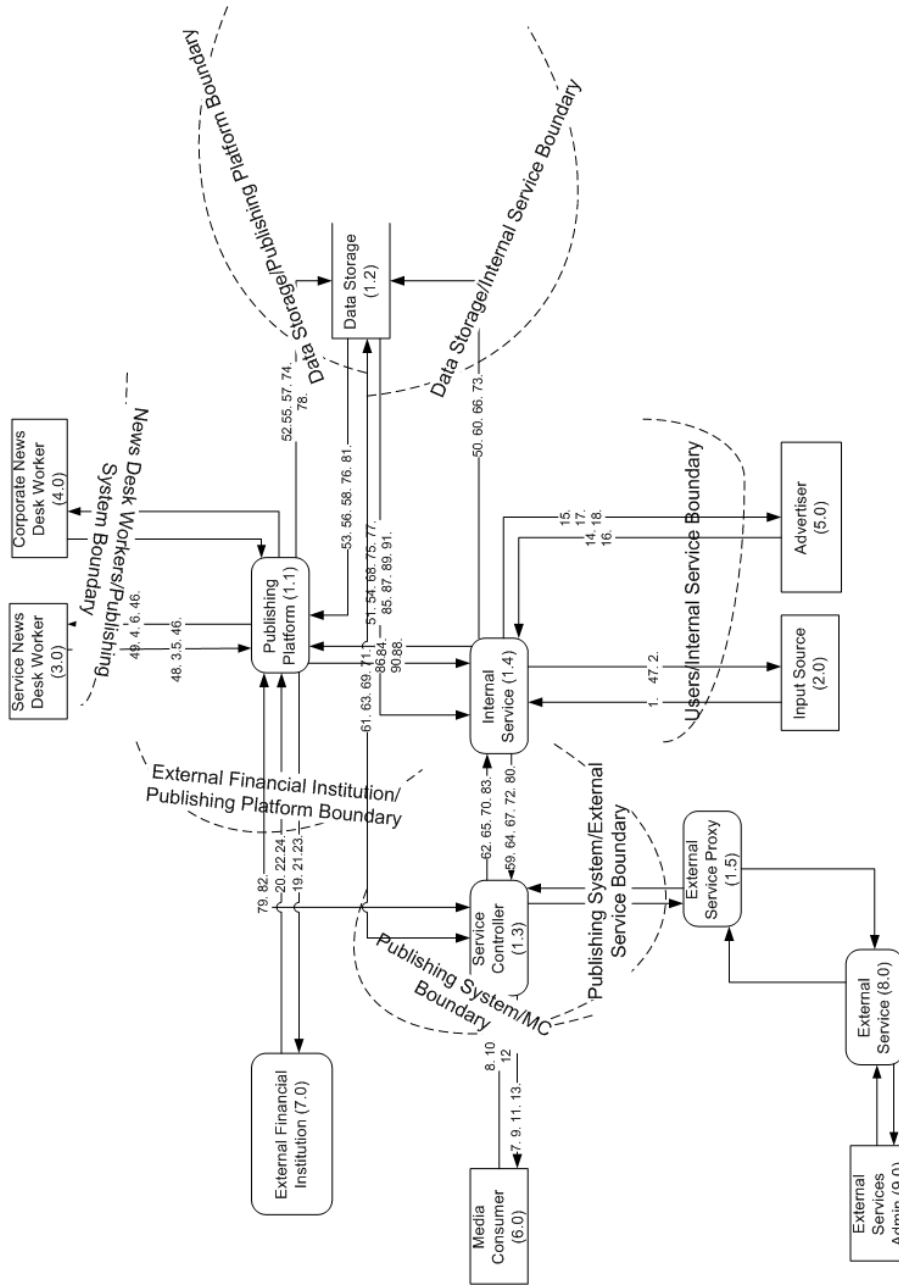


Figure 9: The level-1 dataflow diagram of the publishing system. Each number represents a data flow of an asset between two components.

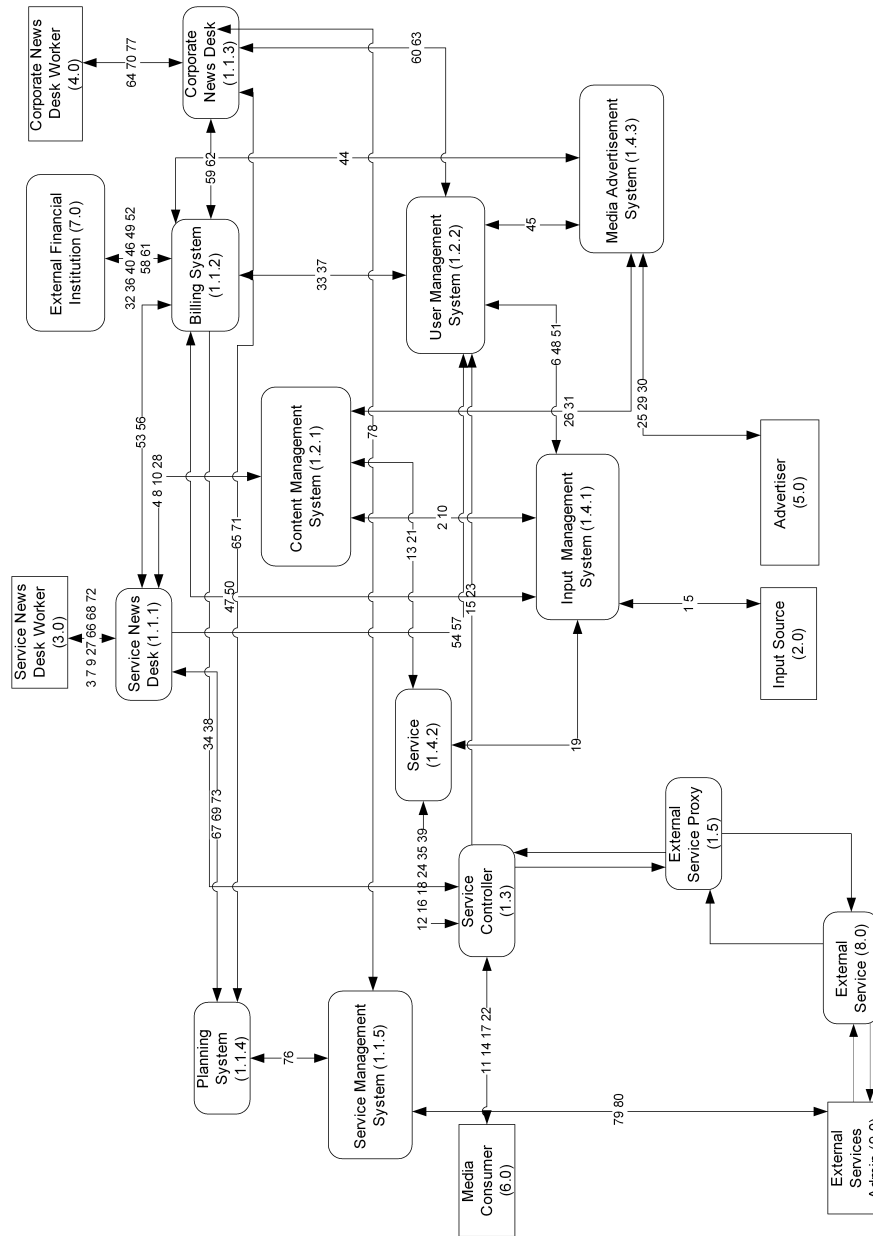


Figure 10: The level-2 dataflow diagram of the publishing system. Each number represents a data flow of an asset between two components. Trust boundaries are left out for clarity reasons.

Figure 10 shows the final level of detail. All internal communication is shown. Trust boundaries are left out for clarity reasons. Table 9 shows the details of the data flows. Communication between two components flowing into both directions are grouped.

In order to have a complete list of all threats, one should make the cross product of 1 and each of the elements of the data flow diagram.

Nr.	Name	From	To	Description (assets)
1	Input Data Flow	2.0 Input Source	1.0 Publishing System	This stream contains <i>input</i> submitted by the Input Source.
47	Input Data Flow	1.0 Publishing System	2.0 Input Source	This stream contains <i>input</i> submitted by the Input Source.
48	Input Data Flow	3.0 Service News Desk Worker	1.0 Publishing System	The Service News Desk Worker manipulates input data in order to create stories
49	Input Data Flow	1.0 Publishing System	3.0 Service News Desk Worker	The Service News Desk Worker manipulates input data in order to create stories
2	Media Consumer Anonymous Behavior Data Flow (Read Input Content Profile)	1.0 Publishing System	2.0 Input Source	This stream contains the input profile, which is <i>anonymous media consumer behavior information</i>
3	Story Data Flow	3.0 Service News Desk Worker	1.0 Publishing System	This stream contains <i>stories</i> which are created, read, or modified.
4	Story Data Flow	1.0 Content Management System	3.0 Service News Desk Worker	This stream contains <i>stories</i> which are created, read, or modified.
5	Edition Data Flow	3.0 Service News Desk Worker	1.0 Publishing System	This stream contains <i>editions</i> which are read, modified, or ready to be sent.
6	Edition Data Flow	1.0 Publishing System	3.0 Service News Desk Worker	This stream contains <i>editions</i> which are read, modified, or ready to be sent.
7	Edition Data Flow	1.0 Publishing System	6.0 Media Consumer	This stream contains editions
8	Media Consumer Behavior Information Data Flow	6.0 Media Consumer	1.0 Publishing System	<i>Media consumer behavior information (context information)</i> flows between the Media Consumer and the Publishing System.
9	Media Consumer Behavior Information Data Flow	1.0 Publishing System	6.0 Media Consumer	<i>Media consumer behavior information (context information)</i> flows between the Media Consumer and the Publishing System.
10	Media Consumer Feedback Data Flow	6.0 Media Consumer	1.0 Publishing System	This stream contains <i>feedback information</i> created by the Media Consumer.
11	Media Consumer Feedback Data Flow	1.0 Publishing System	6.0 Media Consumer	This stream contains <i>feedback information</i> created by the Media Consumer.

12	Media Consumer Behavior Data Flow	6.0 Media Consumer		This stream contains <i>Media Consumer behavior information</i> (viewing information).
13	Media Consumer Behavior Data Flow	1.0 Publishing System	6.0 Media Consumer	This stream contains <i>Media Consumer behavior information</i> (viewing information).
14	Advertisement Data Flow	5.0 Advertiser	1.0 Publishing System	This stream contains <i>Commercials</i> .
15	Advertisement Data Flow	1.0 Publishing System	5.0 Advertiser	This stream contains <i>Commercials</i> .
16	Reservation Data Flow	5.0 Advertiser	1.0 Publishing System	This stream contains <i>reservations for commercials</i> .
17	Reservation Data Flow	1.0 Publishing System	5.0 Advertiser	This stream contains <i>reservations for commercials</i> .
18	Media Consumer Behavior Information Data Flow	1.0 Publishing System	5.0 Advertiser	This stream contains <i>viewing information</i> (part of <i>advertisement profile</i>)
19	Media Consumer Billing Information Data Flow	1.0 Publishing System	7.0 External Financial Institution	This stream contains information about the <i>media consumers payments</i> (He has to pay for X).
20	Media Consumer Billing Information Data Flow	7.0 External Financial Institution	1.0 Publishing System	This stream contains information about the <i>media consumers payments</i> (Media Consumer Payment Notification).
21	Advertiser Billing Information Data Flow	1.0 Publishing System	7.0 External Financial Institution	<i>This stream contains information about the advertisers payments</i> (He has to pay for X).
22	Advertiser Billing Information Data Flow	7.0 External Financial Institution	1.0 Publishing System	This stream contains information about the advertiser <i>payments</i> (Advertiser Payment Notification).
23	Input Source Billing Information Data Flow	1.0 Publishing System	7.0 External Financial Institution	This stream contains input source <i>billing information</i> (request payment).
24	Input Source Billing Information Data Flow	7.0 External Financial Institution	1.0 Publishing System	This stream contains information about the input sources <i>payments</i> (Input Source Payment Notification).
25	Service News Desk Worker Billing Information Data Flow	1.0 Publishing System	7.0 External Financial Institution	This stream contains information about the <i>employees payments</i> (Employee payment)
26	Service News Desk Worker Billing Information Data Flow	7.0 External Financial Institution	1.0 Publishing System	This stream contains information about the employee payments.
27	Corporate News Desk Worker Billing Information Data Flow	1.0 Publishing System	7.0 External Financial Institution	This stream contains information about the employee payments.

28	Corporate News Desk Worker Billing Information Data Flow	7.0 External Financial Institution	1.0 Publishing System	This stream contains information about the <i>employees payments</i> (Employee payment)
29	Corporate Planning Data Flow	4.0 Corporate News Desk Worker	1.0 Publishing System	The Corporate News Desk Worker is able to modify, create, read and delete <i>corporate planning</i> schemes.
30	Corporate Planning Data Flow	1.0 Publishing System	4.0 Corporate News Desk Worker	The Corporate News Desk Worker is able to modify, create, read and delete <i>corporate planning</i> schemes.
31	Service Planning Data Flow	3.0 Service News Desk Worker	1.0 Publishing System	The Service News Desk Worker is able to modify, create, read and delete <i>service planning</i> schemes.
32	Service Planning Data Flow	1.0 Publishing System	3.0 Service News Desk Worker	The Service News Desk Worker is able to modify, create, read and delete <i>service planning</i> schemes.
33	Edition Planning Data Flow	3.0 Service News Desk Worker	1.0 Publishing System	The Service News Desk Worker is able to modify, create, read and delete <i>edition planning</i> schemes.
34	Edition Planning Data Flow	1.0 Publishing System	3.0 Service News Desk Worker	The Service News Desk Worker is able to modify, create, read and delete <i>edition planning</i> schemes.
35	Task Data Flow	1.0 Publishing System	4.0 Corporate News Desk Worker	This stream contains information about the <i>tasks</i> of a Corporate News Desk Worker (task notification).
36	Task Data Flow	1.0 Publishing System	4.0 Corporate News Desk Worker	This stream contains <i>tasks</i> of a Corporate News Desk Worker, because he is able to create, read, modify or delete them.
37	Task Data Flow	4.0 Corporate News Desk Worker	1.0 Publishing System	This stream contains <i>tasks</i> of a Corporate News Desk Worker, because he is able to create, read, modify or delete them.
38	Task Data Flow	1.0 Publishing System	3.0 Service News Desk Worker	This stream contains <i>tasks</i> of a Service News Desk Worker, because he is able to create, read, modify or delete them.
39	Task Data Flow	3.0 Service News Desk Worker	1.0 Publishing System	This stream contains <i>tasks</i> of a Service News Desk Worker, because he is able to create, read, modify or delete them.
40	Task Data Flow	1.0 Publishing System	3.0 Service News Desk Worker	This stream contains information about the <i>tasks</i> of a Service News Desk Worker (task notification).
41	Service Data Flow	9.0 External Service Provider	1.0 Publishing System	This streams contains <i>information about the external service provider</i> . (service proposal)

42	Service Task Data Flow	1.0 Publishing System	4.0 Corporate News Desk Worker	This stream contains <i>information about the external service provider</i> . (service proposal)
43	Service Approval Data Flow	4.0 Corporate News Desk Worker	1.0 Publishing System	This stream contains <i>information about the external service provider</i> . (service approval)
44	Service Approval Data Flow	1.0 Publishing System	9.0 External Service Provider	This stream contains <i>information about the external service provider</i> . (service approval)
45	Service Software Data Flow	9.0 External Service Provider	1.0 Publishing System	This stream contains the new service (or the proxy).

Table 8: A description of the dataflows for the toplevel diagram.

ID	Nr.	Name	Between		Description (assets)
1	1 47	Input Data Flow	2.0 Input Source	1.4.1 Input Management System	This stream contains <i>input</i> submitted by the Input Source.
2	50 51	Input Data Flow	1.4.1 Input Management System	1.2.1 Content Management System	This stream contains <i>input</i> submitted by the Input Source.
3	48 49	Input Data Flow	3.0 Service News Desk Worker	1.1.1 Service News Desk	The Service News Desk Worker manipulates input data in order to create stories
4	52 53	Input Data Flow	1.1.1 Service News Desk	1.2.1 Content Management System	The Service News Desk Worker manipulates input data in order to create stories
5	2	Media Consumer Anonymous Behavior Data Flow (Read Input Content Profile)	1.4.1 Input Management System	2.0 Input Source	This stream contains the input profile, which is <i>anonymous media consumer behavior information</i>
6	54	Media Consumer Anonymous Behavior Data Flow	1.2.2 User Management System	1.4.1 Input Management System	This stream contains the input profile, which is <i>anonymous media consumer behavior information</i>
7	3 4	Story Data Flow	3.0 Service News Desk Worker	1.1.1 Service News Desk	This stream contains <i>stories</i> which are created, read, or modified.
8	55 56	Story Data Flow	1.1.1 Service News Desk	1.2.1 Content Management System	This stream contains <i>stories</i> which are created, read, or modified.
9	5 6	Edition Data Flow	3.0 Service News Desk Worker	1.1.1 Service News Desk	This stream contains <i>editions</i> which are read, modified, or ready to be sent.
10	57 58	Edition Data Flow	1.1.1 Service News Desk	1.2.1 Content Management System	This stream contains <i>editions</i> which are read, modified, or ready to be sent.
11	7	Edition Data Flow	1.3 Service Controller	6.0 Media Consumer	This stream contains editions
12	59	Edition Data Flow	1.4.2 Service	1.3 Service Controller	This stream contains editions
13	60	Edition Data Flow	1.2.1 Content Management System	1.4.2 Service	This stream contains editions

14	8 9	Media Consumer Behavior Information Data Flow	6.0 Media Consumer	1.3 Service Controller	<i>Media consumer behavior information (context information)</i> flows between the Media Consumer and the Publishing System.
15	61 63	Media Consumer Behavior Information Data Flow	1.3 Service Controller	1.2.2 User Management System	<i>Media consumer behavior information (context information)</i> flows between the Media Consumer and the Publishing System.
16	62 64	Media Consumer Behavior Information Data Flow	1.3 Service Controller	1.4.2 Service	<i>Media consumer behavior information (context information)</i> flows between the Media Consumer and the Publishing System.
17	10 11	Media Consumer Feedback Data Flow	6.0 Media Consumer	1.3 Service Controller	This stream contains <i>feedback information</i> created by the Media Consumer.
18	65 67	Media Consumer Feedback Data Flow	1.3 Service Controller	1.4.2 Service	This stream contains <i>feedback information</i> created by the Media Consumer.
19	66	Media Consumer Feedback Data Flow	1.4.2 Service	1.4.1 Input Management System	This stream contains <i>feedback information</i> created by the Media Consumer.
20	100	Media Consumer Feedback Data Flow	1.4.1 Input Management System	1.2.1 Content Management System	This stream contains <i>feedback information</i> created by the Media Consumer.
21	68	Media Consumer Feedback Data Flow	1.2.1 Content Management System	1.4.2 Service	This stream contains <i>feedback information</i> created by the Media Consumer.
22	12 13	Media Consumer Behavior Information Data Flow	6.0 Media Consumer	1.3 Service Controller	This stream contains <i>Media Consumer behavior information</i> (viewing information).
23	69 71	Media Consumer Behavior Information Data Flow	1.3 Service Controller	1.2.2 User Management System	This stream contains <i>Media Consumer behavior information</i> (viewing information).
24	70	Media Consumer Behavior Information Data Flow	1.3 Service Controller	1.4.2 Service	This stream contains <i>Media Consumer behavior information</i> (viewing information).
25	14 15	Advertisement Data Flow	5.0 Advertiser	1.4.3 Media Advertisement System	This stream contains <i>Commercials</i> .

26	73 112	Advertisement Data Flow	1.4.3 Media Advertisement System	1.2.1 Content Management System	This stream contains <i>Commercials</i> .
27	46 46	Advertisement Data Flow	3.0 Service News Desk Worker 1.1.1 Service News Desk	1.1.1 Service News Desk	This stream contains <i>Commercials (to be included in a story)</i>
28	74 75 76	Advertisement Data Flow	1.1.1 Service News Desk	1.2.1 Content Management System	This stream contains <i>Commercials (to be included in a story)</i>
29	16 17	Reservation Data Flow	5.0 Advertiser	1.4.3 Media Advertisement System	This stream contains <i>reservations for commercials</i> .
30	18	Media Consumer Behavior Information Data Flow	1.4.3 Media Advertisement System	5.0 Advertiser	This stream contains <i>viewing information (part of advertisement profile)</i>
31	77	Media Consumer Behavior Information Data Flow	1.2.1 Content Management System	1.4.3 Media Advertisement System	This stream contains <i>viewing information (part of advertisement profile)</i>
32	19	Media Consumer Billing Information Data Flow	1.1.2 Billing System	7.0 External Financial Institution	This stream contains information about the <i>media consumers payments (He has to pay for X)</i> .
33	78	Media Consumer Billing Information Data Flow	1.1.2 Billing System	1.2.2 User Management System	This stream contains information about the <i>media consumers payments (He has to pay for X)</i> .
34	79	Media Consumer Billing Information Data Flow	1.3 Service Controller	1.1.2 Billing System	This stream contains information about the <i>media consumers payments (He has to pay for X)</i> .
35	80	Media Consumer Billing Information Data Flow	1.4.2 Service	1.3 Service Controller	This stream contains information about the <i>media consumers payments (He has to pay for X)</i> .
36	20	Media Consumer Billing Information Data Flow	7.0 External Financial Institution	1.1.2 Billing System	This stream contains information about the <i>media consumers payments (Media Consumer Payment Notification)</i> .
37	81	Media Consumer Billing Information Data Flow	1.2.2 User Management System	1.1.2 Billing System	This stream contains information about the <i>media consumers payments (He has to pay for X)</i> .
38	82	Media Consumer Billing Information Data Flow	1.1.2 Billing System	1.3 Service Controller	This stream contains information about the <i>media consumers payments (He has to pay for X)</i> .

39	83	Media Consumer Billing Information Data Flow	1.3 Service Controller	1.4.2 Service	This stream contains information about the <i>media consumers payments</i> (He has to pay for X).
40	21	Advertiser Billing Information Data Flow	1.1.2 Billing System	7.0 External Financial Institution	<i>This stream contains information about the advertisers payments</i> (He has to pay for X).
41	84	Advertiser Billing Information Data Flow	1.4.3 Media Advertisement System	1.1.2 Billing System	<i>This stream contains information about the advertisers payments</i> (He has to pay for X).
42	85	Advertiser Billing Information Data Flow	1.2.2 User Management System	1.4.3 Media Advertisement System	<i>This stream contains information about the advertisers payments</i> (He has to pay for X).
43	22	Advertiser Billing Information Data Flow	7.0 External Financial Institution	1.1.2 Billing System	This stream contains information about the advertiser <i>payments</i> (Advertiser Payment Notification).
44	86	Advertiser Billing Information Data Flow	1.1.2 Billing System	1.4.3 Media Advertisement System	This stream contains information about the advertiser <i>payments</i> (Advertiser Payment Notification).
45	87	Advertiser Billing Information Data Flow	1.4.3 Media Advertisement System	1.2.2 User Management System	This stream contains information about the advertiser <i>payments</i> (Advertiser Payment Notification).
46	23	Input Source Billing Information Data Flow	1.1.2 Billing System	7.0 External Financial Institution	This stream contains input source <i>billing information</i> (request payment).
47	88	Input Source Billing Information Data Flow	1.4.1 Input Management System	1.1.2 Billing System	This stream contains input source <i>billing information</i> (request payment).
48	89	Input Source Billing Information Data Flow	1.2.2 User Management System	1.4.1 Input Management System	This stream contains input source <i>billing information</i> (request payment).
49	24	Input Source Billing Information Data Flow	7.0 External Financial Institution	1.1.2 Billing System	This stream contains information about the input sources <i>payments</i> (Input Source Payment Notification).
50	90	Input Source Billing Information Data Flow	1.1.2 Billing System	1.4.1 Input Management System	This stream contains information about the input sources <i>payments</i> (Input Source Payment Notification).

51	91	Input Source Billing Information Data Flow	1.4.1 Input Management System	1.2.2 User Management System	This stream contains information about the input sources <i>payments</i> (Input Source Payment Notification).
52	25	Service News Desk Worker Billing Information Data Flow	1.1.2 Billing System	7.0 External Financial Institution	This stream contains information about the <i>employees payments</i> (Employee payment)
53	92	Service News Desk Worker Billing Information Data Flow	1.1.1 Service News Desk	1.1.2 Billing System	This stream contains information about the <i>employees payments</i> (Employee payment)
54	93	Service News Desk Worker Billing Information Data Flow	1.2.2 User Management System	1.1.1 Service News Desk	This stream contains information about the <i>employees payments</i> (Employee payment)
55	26	Service News Desk Worker Billing Information Data Flow	7.0 External Financial Institution	1.1.2 Billing System	This stream contains information about the employee payments.
56	94	Service News Desk Worker Billing Information Data Flow	1.1.2 Billing System	1.1.1 Service News Desk	This stream contains information about the employee payments.
57	95	Service News Desk Worker Billing Information Data Flow	1.1.1 Service News Desk	1.2.2 User Management System	This stream contains information about the employee payments.
58	27	Corporate News Desk Worker Billing Information Data Flow	1.1.2 Billing System	7.0 External Financial Institution	This stream contains information about the employee payments.
59	96	Corporate News Desk Worker Billing Information Data Flow	1.1.3 Corporate News Desk	1.1.2 Billing System	This stream contains information about the employee payments.
60	97	Corporate News Desk Worker Billing Information Data Flow	1.2.2 User Management System	1.1.3 Corporate News Desk	This stream contains information about the employee payments.
61	28	Corporate News Desk Worker Billing Information Data Flow	7.0 External Financial Institution	1.1.2 Billing System	This stream contains information about the <i>employees payments</i> (Employee payment)

62	98	Corporate News Desk Worker Billing Information Data Flow	1.1.2 Billing System	1.1.3 Corporate News Desk	This stream contains information about the <i>employees payments</i> (Employee payment)
63	99	Corporate News Desk Worker Billing Information Data Flow	1.1.3 Corporate News Desk	1.2.2 User Management System	This stream contains information about the <i>employees payments</i> (Employee payment)
64	29 30	Corporate Planning Data Flow	4.0 Corporate News Desk Worker	1.1.3 Corporate News Desk	The Corporate News Desk Worker is able to modify, create, read and delete <i>corporate planning</i> schemes.
65	101 102	Corporate Planning Data Flow	1.1.3 Corporate News Desk	1.1.4 Planning System	The Corporate News Desk Worker is able to modify, create, read and delete <i>corporate planning</i> schemes.
66	31 32	Service Planning Data Flow	3.0 Service News Desk Worker	1.1.1 Service News Desk	The Service News Desk Worker is able to modify, create, read and delete <i>service planning</i> schemes.
67	103 103	Service Planning Data Flow	1.1.1 Service News Desk	1.1.4 Planning System	The Service News Desk Worker is able to modify, create, read and delete <i>service planning</i> schemes.
68	33 34	Edition Planning Data Flow	3.0 Service News Desk Worker	1.1.1 Service News Desk	The Service News Desk Worker is able to modify, create, read and delete <i>edition planning</i> schemes.
69	104 105	Edition Planning Data Flow	1.1.1 Service News Desk	1.1.4 Planning System	The Service News Desk Worker is able to modify, create, read and delete <i>edition planning</i> schemes.
70	35 108	Task Data Flow	4.0 Corporate News Desk Worker	1.1.3 Corporate News Desk	This stream contains information about the <i>tasks</i> of a Corporate News Desk Worker (task notification).
71	106 107	Task Data Flow	1.1.3 Corporate News Desk	1.1.4 Planning System	This stream contains information about the <i>tasks</i> of a Corporate News Desk Worker (task notification).
72	39 40	Task Data Flow	3.0 Service News Desk Worker	1.1.1 Service News Desk	This stream contains <i>tasks</i> of a Service News Desk Worker, because he is able to create, read, modify or delete them.

73	110 109	Task Data Flow	1.1.1 Service News Desk	1.1.4 Planning System	This stream contains <i>tasks</i> of a Service News Desk Worker, because he is able to create, read, modify or delete them.
74	41	Service Data Flow	9.0 External Service Provider	1.1.5 Service Management System	This stream contains <i>information about the external service provider</i> . (service proposal)
75	111	Service Task Data Flow	1.1.5 Service Management System	1.1.4 Planning System	This stream contains <i>information about the external service provider</i> . (service proposal)
76	112	Service Task Data Flow	1.1.4 Planning System	1.1.3 Corporate News Desk	This stream contains <i>information about the external service provider</i> . (service proposal)
77	42	Service Task Data Flow	1.1.3 Corporate News Desk	4.0 Corporate News Desk Worker	This stream contains <i>information about the external service provider</i> . (service proposal)
78	43	Service Approval Data Flow	4.0 Corporate News Desk Worker	1.1.5 Service Management System	This stream contains <i>information about the external service provider</i> . (service approval)
79	44	Service Approval Data Flow	1.1.5 Service Management System	9.0 External Service Provider	This stream contains <i>information about the external service provider</i> . (service approval)
80	45	Service Software Data Flow	9.0 External Service Provider	1.1.5 Service Management System	This stream contains the new service (or the proxy).

Table 9: A description of the dataflows for the level-2 diagram with grouped two-way communication.

A.3 Define threats

Threats are identified and analyzed in a systematic way by the (i) STRIDE and (ii) DREAD methods respectively.

A.3.1 Determine threats

STRIDE is an acronym formed by the first letter of each of the following categories of threats:

1. *Spoofing* Faking an identify.
2. *Tampering* Compromising the integrity of data.
3. *Repudiation* Denying having performed an action, such as denying having purchased an item from an online shop.
4. *Information disclosure* Compromising the confidentiality of data.
5. *Denial of service* Compromising the availability of a service.
6. *Elevation of privilege* Illegally obtain more privileges.

The STRIDE method assigns the above-mentioned categories to the elements in the final DFD in order to identify classes of threats to which the elements may be vulnerable (see Table 1). Each combination of a STRIDE-threat and a threat target (DFD element) should be investigated in order to verify whether the threat is indeed a real threat. This investigation can be done by using attack trees. The threat should be kept if there is an attack path in the tree leading to the threat under investigation. Otherwise, the threat should be removed from the list of threats. In this experiment, STRIDE-threats were identified for the data-flow elements. The verification whether the threat is indeed a real threat has been done for the subset of the threats:

Spoofing

1. Spoofing Media Consumer client
 - (a) Falsify Media Consumer Client software
 - (b) Install falsified software on Client
 - i. Obtain Media Consumer client software
 - A. Media Consumer client software is available
 - ii. Install Media Consumer client software on Client
 - (c) Install falsified software on existing Media Consumer client
 - i. Break into a Media Consumer house (or similar)
 - ii. Install falsified software
2. Spoofing Service News Desk Server
 - (a) Falsify Service News Desk software
 - (b) Falsify Service News Desk server
 - i. Break into publishers server room
 - ii. Install falsified Service News Desk server
3. Spoofing Content Management System
 - (a) Falsify Content Management System software
 - (b) Falsify Content Management System server

- i. Break into publishers server room
 - ii. Install falsified Content Management System server
- 4. Spoofing News Paper Service Server
 - (a) Falsify News Paper Service software
 - (b) Falsify News Paper Service server
 - i. Break into publishers server room
 - ii. Install falsified News Paper Service server
- 5. Spoofing User Management System
 - (a) Falsify User Management System software
 - (b) Falsify User Management System server
 - i. Break into publishers server room
 - ii. Install falsified User Management System server
- 6. Spoofing Service Controller
 - (a) Falsify Service Controller software
 - (b) Falsify Service Controller server
 - i. Break into publishers server room
 - ii. Install falsified Service Controller server
- 7. Spoofing Input Management System
 - (a) Falsify Input Management System software
 - (b) Falsify Input Management System server
 - i. Break into publishers server room
 - ii. Install falsified Input Management System server
- 8. Spoofing Input Source Client
 - (a) Falsify Input Source Client software
 - (b) Install falsified software on Client
 - i. Obtain Input Source client software
 - A. Input Source client software is available
 - ii. Install falsified Input Source client software on Client
 - (c) Install falsified software on existing Input Source client
 - i. Break into a Input Source house (or similar)
 - ii. Install falsified software
- 9. Spoofing Service News Desk Worker Client
 - (a) Falsify Service News Desk Worker Client software
 - (b) Install falsified software on Client
 - i. Obtain Service News Desk Worker client software
 - A. Service News Desk Worker client software is available
 - ii. Install falsified Service News Desk Worker client software on Client

- (c) Install falsified software on existing Service News Desk Worker client
 - i. Break into a Service News Desk Worker house (or similar)
 - ii. Install falsified software
- 10. Spoofing Media Consumer
 - (a) Spoofing MC Client (see 1) (AND)
 - (b) Obtain MC credentials (AND)
 - i. Read media consumer credentials information
 - ii. Eavesdrop media consumer credentials data stream
 - iii. Guess media consumer credentials
 - iv. Another way
 - (c) Authenticate as Media Consumer on spoofed client
 - i. Do not ask for authentication at the Service Controller/Newspaper Service
- 11. Spoofing Input Source
 - (a) Spoofing Input Source Client (see 8) (AND)
 - (b) Obtain Input Source credentials (AND)
 - i. Read Input Source credentials information
 - ii. Eavesdrop Input Source credentials data stream
 - iii. Guess Input Source credentials
 - iv. Another way
 - (c) Authenticate as Input Source on spoofed client
 - i. Do not ask for authentication at Input Management System
- 12. Spoofing Service News Desk Worker
 - (a) Spoofing Service News Desk Worker Client (see 9) (AND)
 - (b) Obtain Service News Desk Worker credentials (AND)
 - i. Read Service News Desk Worker credentials information
 - ii. Eavesdrop Service News Desk Worker credentials data stream
 - iii. Guess Service News Desk Worker credentials
 - iv. Another way
 - (c) Authenticate as Service News Desk Worker on spoofed client
 - i. Do not ask for authentication at the Service News Desk

Tampering

- 1. Tamper with input
 - (a) by tampering at the Input Management System
 - i. Elevation of privileges at IMS (AND) (see 201)
 - ii. Obtain access to the input
 - A. No access control at the Input Management System
 - iii. Tamper with input data

- (b) by tampering at the Content Management System
 - i. Elevation of privileges at CMS (AND) (see 197)
 - ii. Obtain access to the input
 - A. No access control at the Content Management System
 - iii. Tamper with input data
 - (c) by tampering at the Service News Desk
 - i. Elevation of privileges at SND (see 196)
 - ii. Obtain access to input
 - A. No access control at the SND
 - iii. Tamper with input data
 - (d) by tampering at the Service News Desk Worker Client
 - i. Elevation of privileges at SNDW Client (see 203)
 - ii. Obtain access to input
 - A. No access control at the SNDW Client
 - iii. Tamper with input data
 - (e) by tampering with input data stream (see 32)
 - i. Break into publishing network infrastructure (AND)
 - ii. Tamper with IMS/CMS hardware
2. Tamper with user information
 3. Tamper with MC contact information
 - (a) by tampering at the User Management System
 - i. Elevation of privileges at the User Management System (see 199)
 - ii. Obtain access to the MC contact information
 - A. No access control at the User Management System
 - iii. Tamper with MC contact information
 - (b) by tampering at the Service Controller
 - i. Elevation of privileges at the Service Controller (see 200)
 - ii. Obtain access to the MC contact information
 - A. No access control at the Service Controller
 - iii. Tamper with MC contact information
 - (c) by tampering at the Media Consumer Client
 - i. Elevation of privileges at the MC Client (see 195)
 - ii. Obtain access to the MC contact information
 - A. No access control at the MC client
 - iii. Tamper with MC contact information
 - (d) by tampering at the Service News Desk
 - i. Elevation of privileges at the Service News Desk (see 196)
 - ii. Obtain access to the MC contact information
 - A. No access control at the SND
 - iii. Tamper with MC contact information
 - (e) by tampering at the Service News Desk Worker Client

- i. Elevation of privileges at the Service News Desk Worker Client (see 203)
 - ii. Obtain access to the MC contact information
 - A. No access control at the SNDW Client
 - iii. Tamper with MC contact information
 - (f) by tampering with the MC contact information data stream (see 35)
- 4. Tamper with MC behaviour information
 - (a) by tampering with the MC behaviour information at the Media Consumer Client
 - i. Elevation of privileges at the Media Consumer Client (see 195)
 - ii. Obtain access to the MC behaviour information
 - A. No access control at the Media Consumer Client
 - iii. Tamper with the MC behaviour information
 - (b) by tampering with the MC behaviour information at the Service Controller
 - i. Elevation of privileges at the Service Controller (see 200)
 - ii. Obtain access to the MC behaviour information
 - A. No access control at the Service Controller
 - iii. Tamper with the MC behaviour information
 - (c) by tampering with the MC behaviour information at the User Management System
 - i. Elevation of privileges at the User Management System (see 199)
 - ii. Obtain access to the MC behaviour information at the User Management System
 - A. No access control at the User Management System
 - iii. Tamper with the MC behaviour information
 - (d) by tampering with the MC behaviour information at the Input Management System
 - i. Elevation of privileges at the IMS (see 201)
 - ii. Obtain access to the MC behaviour information at the IMS
 - A. No access control at the IMS
 - iii. Tamper with the MC behaviour information
 - (e) by tampering with the MC behaviour information at the Input Source Client
 - i. Elevation of privileges at the IS Client (see 202)
 - ii. Obtain access to the MC behaviour information at the IS Client
 - A. No access control at the IS Client
 - iii. Tamper with the MC behaviour information
 - (f) by tampering with the MC behaviour information data stream (see 34)
- 5. Tamper with MC credentials
 - (a) by tampering with the MC credentials data at the Media Consumer Client
 - i. Elevation of privileges at the Media Consumer Client (see 195)
 - ii. Obtain access to the MC credentials data
 - A. No access control at the Media Consumer Client
 - iii. Tamper with the MC credentials
 - (b) by tampering with the MC credentials data information at the Service Controller
 - i. Elevation of privileges at the Service Controller (see 200)
 - ii. Obtain access to the MC credentials data

- A. No access control at the Service Controller
 - iii. Tamper with the MC credentials
 - (c) by tampering with the MC credentials data information at the User Management System
 - i. Elevation of privileges at the User Management System (see 199)
 - ii. Obtain access to the MC credentials data
 - A. No access control at the User Management System
 - iii. Tamper with the MC credentials
 - (d) by tampering with the MC credentials data stream (see 38)
- 6. Tamper with Service News Desk Worker contact information
 - (a) by tampering with the SNDW contact information at the SNDW client
 - i. Elevation of privileges at the Service News Desk Worker Client (see 203)
 - ii. Obtain access to the Service News Desk Worker contact information
 - A. No access control at the Service News Desk Worker Client
 - iii. Tamper with the Service News Desk Worker contact information
 - (b) by tampering with the SNDW contact information at the Service News Desk
 - i. Elevation of privileges at the Service News Desk (see 196)
 - ii. Obtain access to the Service News Desk Worker contact information
 - A. No access control at the Service News Desk
 - iii. Tamper with the Service News Desk Worker contact information
 - (c) by tampering with the SNDW contact information at the User Management System
 - i. Elevation of privileges at the User Management System (see 199)
 - ii. Obtain access to the Service News Desk Worker contact information
 - A. No access control at the User Management System
 - iii. Tamper with the Service News Desk Worker contact information
 - (d) by tampering with the SNDW contact information stream (see 37)
- 7. Tamper with Service News Desk Worker credentials
 - (a) by tampering with the SNDW credentials at the SNDW client
 - i. Elevation of privileges at the Service News Desk Worker Client (see 203)
 - ii. Obtain access to the Service News Desk Worker credentials
 - A. No access control at the Service News Desk Worker Client
 - iii. Tamper with the Service News Desk Worker credentials
 - (b) by tampering with the SNDW credentials at the Service News Desk
 - i. Elevation of privileges at the Service News Desk (see 196)
 - ii. Obtain access to the Service News Desk Worker credentials
 - A. No access control at the Service News Desk
 - iii. Tamper with the Service News Desk Worker credentials
 - (c) by tampering with the SNDW credentials at the User Management System
 - i. Elevation of privileges at the User Management System (see 199)
 - ii. Obtain access to the Service News Desk Worker credentials
 - A. No access control at the User Management System

- iii. Tamper with the Service News Desk Worker credentials
- (d) by tampering with the SNDW credentials stream (see 38)
- 8. Tamper with Input Source contact information
 - (a) by tampering with the Input Source Contact information at the Input Source Client
 - i. Elevation of privileges at the Input Source Client (see 202)
 - ii. Obtain access to the Input Source Contact information
 - A. No access control at the Input Source Client
 - iii. Tamper with the Input Source Contact information
 - (b) by tampering with the Input Source Contact information at the Input Management System
 - i. Elevation of privileges at the Input Management System (see 201)
 - ii. Obtain access to the Input Source Contact information
 - A. No access control at the Input Management System
 - iii. Tamper with the Input Source Contact information
 - (c) by tampering with the Input Source Contact information at the User Management System
 - i. Elevation of privileges at the User Management System (see 199)
 - ii. Obtain access to the Input Source Contact information
 - A. No access control at the User Management System
 - iii. Tamper with the Input Source Contact information
 - (d) by tampering with the Input Source Contact information stream (see 39)
- 9. Tamper with Input Source Credentials
 - (a) by tampering with the Input Source credentials at the Input Source Client
 - i. Elevation of privileges at the Input Source Client (see 202)
 - ii. Obtain access to the Input Source credentials
 - A. No access control at the Input Source Client
 - iii. Tamper with the Input Source credentials
 - (b) by tampering with the Input Source Credentials at the Input Management System
 - i. Elevation of privileges at the Input Management System (see 201)
 - ii. Obtain access to the Input Source credentials
 - A. No access control at the Input Management System
 - iii. Tamper with the Input Source credentials
 - (c) by tampering with the Input Source Credentials at the User Management System
 - i. Elevation of privileges at the User Management System (see 199)
 - ii. Obtain access to the Input Source credentials
 - A. No access control at the User Management System
 - iii. Tamper with the Input Source credentials
 - (d) by tampering with the Input Source Credentials stream (see 40)
- 10. Tamper with edition
 - (a) by tampering with the edition at the Service News Desk Worker Client

- i. Elevation of privileges at the Service News Desk Worker Client (see 203)
 - ii. Obtain access to the edition
 - A. No access control at the Service News Desk Worker Client
 - iii. Tamper with the edition
 - (b) by tampering with the edition at the Service News Desk
 - i. Elevation of privileges at the Service News Desk (see 196)
 - ii. Obtain access to the edition
 - A. No access control at the Service News Desk
 - iii. Tamper with the edition
 - (c) by tampering with the edition at the Content Management System
 - i. Elevation of privileges at the Content Management System (see 197)
 - ii. Obtain access to the edition
 - A. No access control at the Content Management System
 - iii. Tamper with the edition
 - (d) by tampering with the edition at the Newspaper Service
 - i. Elevation of privileges at the Newspaper Service (see 198)
 - ii. Obtain access to the edition
 - A. No access control at the Newspaper Service
 - iii. Tamper with the edition
 - (e) by tampering with the edition at the Service Controller
 - i. Elevation of privileges at the Service Controller (see 200)
 - ii. Obtain access to the edition
 - A. No access control at the Service Controller
 - iii. Tamper with the edition
 - (f) by tampering with the edition at the Media Consumer Client
 - i. Elevation of privileges at the Media Consumer Client (see 195)
 - ii. Obtain access to the edition
 - A. No access control at the Media Consumer Client
 - iii. Tamper with the edition
 - (g) by tampering with the Edition Data Stream (see 41)
11. Tamper with edition, limited in time, valuable (see 22)
 12. Tamper with edition, limited in time, not valuable (see 22)
 13. Tamper with edition, not limited in time, valuable (see 22)
 14. Tamper with edition, not limited in time, not valuable (see 22)
 15. Tamper with story
 - (a) by tampering with the story at the Service News Desk Worker Client
 - i. Elevation of privileges at the Service News Desk Worker Client (see 203)
 - ii. Obtain access to the story
 - A. No access control at the Service News Desk Worker Client
 - iii. Tamper with the story

- (b) by tampering with the story at the Service News Desk
 - i. Elevation of privileges at the Service News Desk (see 196)
 - ii. Obtain access to the story
 - A. No access control at the Service News Desk
 - iii. Tamper with the story
 - (c) by tampering with the story at the Content Management System
 - i. Elevation of privileges at the Content Management System (see 197)
 - ii. Obtain access to the story
 - A. No access control at the Content Management System
 - iii. Tamper with the story
 - (d) by tampering with the Story Data Stream (see 46)
16. Tamper with story, limited in time, valuable (see 28)
 17. Tamper with story, limited in time, not valuable (see 28)
 18. Tamper with story, not limited in time, valuable (see 28)
 19. Tamper with story, limited in time, not valuable (see 28)
 20. Tamper with input data stream
 - (a) by tampering as man in the middle
 - i. as man in the middle between Input Source Client and Input Management System
 - A. Communication between Input Source Client and Input Management System is susceptible for tampering by man in the middle
 - ii. as man in the middle between Input Management System and Content Management System
 - A. Communication between Input Management System and Content Management System is susceptible for tampering by man in the middle
 - iii. as man in the middle between Content Management System and Service News Desk
 - A. Communication between Content Management System and Service News Desk is susceptible for tampering by man in the middle
 - iv. as man in the middle between Service News Desk and Service News Desk Worker tool
 - A. Communication between Service News Desk and Service News Desk Worker tool is susceptible for tampering by man in the middle
 - (b) At the Input Source Client
 - i. Elevation of privileges of the IS client (see 202)
 - ii. Tamper with Input Data Stream
 - (c) At the Input Management System
 - i. Elevation of privileges at Input Management System (see 201)
 - ii. Tamper with Input Data Stream
 - (d) At the Content Management System
 - i. Elevation of privileges at the Content Management System (see 197)
 - ii. Tamper with Input Data Stream
 - (e) At the Service News Desk

- i. Elevation of privileges at the Service News Desk (see 196)
 - ii. Tamper with Input Data Stream
 - (f) At the Service News Desk Worker Client
 - i. Elevation of privileges at the Service News Desk Worker Client (see 203)
 - ii. Tamper with Input Data Stream
- 21. Tamper with the User Information Data Stream
- 22. Tamper with the Media Consumer Behaviour Information Data Stream
 - (a) by tampering as man in the middle
 - i. as man in the middle between Media Consumer Client and Service Controller
 - A. Communication between Media Consumer Client and Service Controller is susceptible for tampering by man in the middle
 - ii. as man in the middle between Service Controller and User Management System
 - A. Communication between Service Controller and User Management System is susceptible for tampering by man in the middle
 - iii. as man in the middle between User Management System and Input Management System
 - A. Communication between User Management System and Input Management System is susceptible for tampering by man in the middle
 - iv. as man in the middle between Input Management System and Input Source client
 - A. Communication between Input Management System and Input Source client is susceptible for tampering by man in the middle
 - (b) At the Media Consumer Client
 - i. Elevation of privileges at the Media Consumer Client (see 195)
 - ii. Tamper with Media Consumer Behaviour Information Data Stream
 - (c) At the Service Controller
 - i. Elevation of privileges at the Service Controller (see 200)
 - ii. Tamper with Media Consumer Behaviour Information Data Stream
 - (d) At the User Management System
 - i. Elevation of privileges at the User Management System (see 199)
 - ii. Tamper with Media Consumer Behaviour Information Data Stream
 - (e) At the Input Management System
 - i. Elevation of privileges at the Input Management System (see 201)
 - ii. Tamper with Media Consumer Behaviour Information Data Stream
 - (f) At the Input Source client
 - i. Elevation of privileges at the Input Source Client (see 202)
 - ii. Tamper with Media Consumer Behaviour Information Data Stream
- 23. Tamper with the Media Consumer Contact Information Data Stream
 - (a) by tampering as man in the middle
 - i. as man in the middle between Media Consumer Client and Service Controller
 - A. Communication between Media Consumer Client and Service Controller is susceptible for tampering by man in the middle

- ii. as man in the middle between Service Controller and User Management System
 - A. Communication between Service Controller and User Management System is susceptible for tampering by man in the middle
 - iii. as man in the middle between User Management System and Service News Desk
 - A. Communication between User Management System and Service News Desk is susceptible for tampering by man in the middle
 - iv. as man in the middle between Service News Desk Worker Client and Service News Desk
 - A. Communication between Service News Desk Worker Client and Service News Desk is susceptible for tampering by man in the middle
 - (b) At the Media Consumer Client
 - i. Elevation of privileges at the MC Client (see 195)
 - ii. Tamper with MC contact information data stream
 - (c) At the Service Controller
 - i. Elevation of privileges at the Service Controller (see 200)
 - ii. Tamper with MC contact information data stream
 - (d) At the User Management System
 - i. Elevation of privileges at the UMS (see 199)
 - ii. Tamper with MC contact information data stream
 - (e) At the Service News Desk
 - i. Elevation of privileges at the SND (see 196)
 - ii. Tamper with MC contact information data stream
 - (f) At the Service News Desk Worker Client
 - i. Elevation of privileges at the SNDWC (see 203)
 - ii. Tamper with MC contact information data stream
- 24. Tamper with the Media Consumer Credentials Information Data Stream
 - (a) by tampering as man in the middle
 - i. as man in the middle between Media Consumer Client and Service Controller
 - A. Communication between Media Consumer Client and Service Controller is susceptible for tampering by man in the middle
 - ii. as man in the middle between Service Controller and User Management System
 - A. Communication between Service Controller and User Management System is susceptible for tampering by man in the middle
 - iii. as man in the middle between Service Controller and Newspaper Service
 - A. Communication between Service Controller and Newspaper Service is susceptible for tampering by man in the middle
 - (b) At the Media Consumer Client
 - i. Elevation of privileges at the MC Client (see 195)
 - ii. Tamper with MC credentials information data stream
 - (c) At the Service Controller
 - i. Elevation of privileges at the Service Controller (see 200)
 - ii. Tamper with MC credentials information data stream
 - (d) At the User Management System

- i. Elevation of privileges at the UMS (see 199)
 - ii. Tamper with MC credentials information data stream
 - (e) At the Newspaper Service
 - i. Elevation of privileges at the Newspaper Service (see 198)
 - ii. Tamper with MC credentials information data stream
- 25. Tamper with the Service News Desk Worker Contact Information Data Stream
 - (a) by tampering as man in the middle
 - i. as man in the middle between News Desk Worker Client and Service News Desk
 - A. Communication between News Desk Worker Client and Service News Desk is susceptible for tampering by man in the middle
 - ii. as man in the middle between Service News Desk and User Management System
 - A. Communication between Service News Desk and User Management System is susceptible for tampering by man in the middle
 - (b) At the Service News Desk Worker Client
 - i. Elevation of privileges at the SNDW Client (see 203)
 - ii. Tamper with Service News Desk Worker Contact Information data stream
 - (c) At the Service News Desk
 - i. Elevation of privileges at the SND (see 196)
 - ii. Tamper with Service News Desk Worker Contact Information data stream
 - (d) At the User Management System
 - i. Elevation of privileges at the UMS (see 199)
 - ii. Tamper with Service News Desk Worker Contact Information data stream
- 26. Tamper with the Service News Desk Worker Credentials Information Data Stream
 - (a) by tampering as man in the middle
 - i. as man in the middle between News Desk Worker Client and Service News Desk
 - A. Communication between News Desk Worker Client and Service News Desk is susceptible for tampering by man in the middle
 - ii. as man in the middle between Service News Desk and User Management System
 - A. Communication between Service News Desk and User Management System is susceptible for tampering by man in the middle
 - (b) At the Service News Desk Worker Client
 - i. Elevation of privileges at the SNDW Client (see 203)
 - ii. Tamper with SNDW Credentials information data stream
 - (c) At the Service News Desk
 - i. Elevation of privileges at the SND (see 196)
 - ii. Tamper with SNDW Credentials information data stream
 - (d) At the User Management System
 - i. Elevation of privileges at UMS (see 199)
 - ii. Tamper with SNDW Credentials information data stream
- 27. Tamper with the Input Source Contact Information Data Stream

- (a) by tampering as man in the middle
 - i. as man in the middle between Input Source Client and Input Management System
 - A. Communication between Input Source Client and Input Management System is susceptible for tampering by man in the middle
 - ii. as man in the middle between Input Management System and User Management System
 - A. Communication between Input Management System and User Management System is susceptible for tampering by man in the middle
 - (b) At the Input Source Client
 - i. Elevation of privileges at the IS Client (see 202)
 - ii. Tamper with IS contact information data stream
 - (c) At Input Management System
 - i. Elevation of privileges at IMS (see 201)
 - ii. Tamper with IS contact information data stream
 - (d) At the User Management System
 - i. Elevation of privileges at the UMS (see 199)
 - ii. Tamper with IS contact information data stream
28. Tamper with the Input Source Credentials Information Data Stream
- (a) by tampering as man in the middle
 - i. as man in the middle between Input Source Client and Input Management System
 - A. Communication between Input Source Client and Input Management System is susceptible for tampering by man in the middle
 - ii. as man in the middle between Input Management System and User Management System
 - A. Communication between Input Management System and User Management System is susceptible for tampering by man in the middle
 - (b) At the Input Source Client
 - i. Elevation of privileges at the IS Client (see 202)
 - ii. Tamper with IS credentials information data stream
 - (c) At the Input Management System
 - i. Elevation of privileges at IMS (see 201)
 - ii. Tamper with IS credentials information data stream
 - (d) At the User Management System
 - i. Elevation of privileges at the UMS (see 199)
 - ii. Tamper with IS credentials information data stream
29. Tamper with Edition Stream
- (a) by tampering as man in the middle
 - i. as man in the middle between Service News Desk Worker Client and Service News Desk
 - A. Communication between Service News Desk Worker Client and Service News Desk is susceptible for tampering by man in the middle
 - ii. as man in the middle between Service News Desk and Content Management System

- A. Communication between Service News Desk and Content Management System is susceptible for tampering by man in the middle
 - iii. as man in the middle between Content Management System and Newspaper Service
 - A. Communication between Content Management System and Newspaper Service is susceptible for tampering by man in the middle
 - iv. as man in the middle between Newspaper Service and Service Controller
 - A. Communication between Newspaper Service and Service Controller is susceptible for tampering by man in the middle
 - v. as man in the middle between Service Controller and Media Consumer Client
 - A. Communication between Service Controller and Media Consumer Client is susceptible for tampering by man in the middle
 - (b) At the Service News Desk Worker Client
 - i. Elevation of privileges at the SNDW Client (see 203)
 - ii. Tamper with edition stream
 - (c) At the Service News Desk
 - i. Elevation of privileges at the SND (see 196)
 - ii. Tamper with edition stream
 - (d) At the Content Management System
 - i. Elevation of privileges at the CMS (see 197)
 - ii. Tamper with edition stream
 - (e) At the Newspaper Service
 - i. Elevation of privileges at the Newspaper Service (see 198)
 - ii. Tamper with edition stream
 - (f) At the Service Controller
 - i. Elevation of privileges at the Service Controller (see 200)
 - ii. Tamper with edition stream
 - (g) At the Media Consumer Client
 - i. Elevation of privileges at the MC Client (see 195)
 - ii. Tamper with edition stream
30. Tamper with Edition, limited in time, valuable Stream (see 41)
31. Tamper with Edition, limited in time, not valuable Stream (see 41)
32. Tamper with Edition, not limited in time, valuable Stream (see 41)
33. Tamper with Edition, not limited in time, not valuable stream (see 41)
34. Tamper with Story Stream
- (a) by tampering as man in the middle
 - i. as man in the middle between Service News Desk Worker Client and Service News Desk
 - A. Communication between Service News Desk Worker Client and Service News Desk is susceptible for tampering by man in the middle
 - ii. as man in the middle between Service News Desk and Content Management System
 - A. Communication between Service News Desk and Content Management System is susceptible for tampering by man in the middle

- (b) At the Content Management System
 - i. Elevation of privileges at the CMS (see 197)
 - ii. Tamper with story stream
- (c) At the Service News Desk
 - i. Elevation of privileges at the SND (see 196)
 - ii. Tamper with story stream
- (d) At the Service News Desk Worker Client
 - i. Elevation of privileges at the SNDW Client (see 203)
 - ii. Tamper with story stream
- 35. Tamper with Story, limited in time, valuable Stream (see 46)
- 36. Tamper with Story, limited in time, not valuable Stream (see 46)
- 37. Tamper with Story, not limited in time, valuable Stream (see 46)
- 38. Tamper with Story, not limited in time, not valuable stream (see 46)
- 39. Tamper with MC client
 - (a) Elevation of privileges at Media Consumer client (see 195)
 - (b) Have access to MC client software/memory
 - i. No access control at the MC client
 - (c) Tamper MC client software image/memory
- 40. Tamper with Service News Desk
 - (a) Elevation of privileges at Service News Desk (see 196)
 - (b) Have access to Service News Desk software/memory
 - i. No access control at the Service News Desk
 - (c) Tamper Service News Desk software image/memory
- 41. Tamper with Content Management System
 - (a) Elevation of privileges at Content Management System (see 197)
 - (b) Have access to Content Management System software/memory
 - i. No access control at the Content Management System
 - (c) Tamper Content Management System software image/memory
- 42. Tamper with Newspaper Service
 - (a) Elevation of privileges at Newspaper Service (see 198)
 - (b) Have access to Newspaper Service software/memory
 - i. No access control at the Newspaper Service
 - (c) Tamper Newspaper Service software image/memory
- 43. Tamper with User Management System
 - (a) Elevation of privileges at User Management System (see 199)
 - (b) Have access to User Management System software/memory

- i. No access control at the User Management System
 - (c) Tamper User Management System software image/memory
- 44. Tamper with Service Controller
 - (a) Elevation of privileges at Service Controller (see 200)
 - (b) Have access to Service Controller software/memory
 - i. No access control at the Service Controller
 - (c) Tamper Service Controller software image/memory
- 45. Tamper with Input Management System
 - (a) Elevation of privileges at Input Management System (see 201)
 - (b) Have access to Input Management System software/memory
 - i. No access control at the Input Management System
 - (c) Tamper Input Management System software image/memory
- 46. Tamper with Input Source Client
 - (a) Elevation of privileges at Input Source Client (see 202)
 - (b) Have access to Input Source Client software/memory
 - i. No access control at the Input Source Client
 - (c) Tamper Input Source Client software image/memory
- 47. Tamper with Service News Desk Worker Client
 - (a) Elevation of privileges at Service News Desk Worker Client (see 203)
 - (b) Have access to Service News Desk Worker Client software/memory
 - i. No access control at the Service News Desk Worker Client
 - (c) Tamper Service News Desk Worker Client software image/memory

Repudiation

1. Repudiation of actions on input
 - (a) Removal of input (see 13)
 - (b) Approval of input (see 13)
 - (c) Modification of input (see 13)
 - (d) Viewing of input (see 101)
 - (e) Making input unavailable (see 148)
2. Repudiation of actions on user information
3. Repudiation of actions on Media Consumer contact information
 - (a) Removal of Media Consumer Contact information (see 15)
 - (b) Modification of Media Consumer Contact information (see 15)
 - (c) Viewing Media Consumer Contact Information (see 103)

- (d) Making Media Consumer Contact information unavailable (see 150)
- 4. Repudiation of actions on Media Consumer behaviour information
 - (a) Removal of Media Consumer Behaviour information (see 16)
 - (b) Modification of Media Consumer Behaviour information (see 16)
 - (c) Viewing Media Consumer Behaviour Information (see 104)
 - (d) Making Media Consumer Behaviour information unavailable (see 151)
 - (e) Submitting Media Consumer Behaviour information
- 5. Repudiation of actions on Media Consumer credentials
 - (a) Removal of Media Consumer Credentials (see 17)
 - (b) Modification of Media Consumer Credentials (see 17)
 - (c) Viewing Media Consumer Credentials (see 105)
 - (d) Making Media Consumer Credentials unavailable (see 152)
- 6. Repudiation of actions on Service News Desk Worker contact information
 - (a) Removal of Service News Desk Worker Contact information (see 18)
 - (b) Modification of Service News Desk Worker Contact information (see 18)
 - (c) Viewing Service News Desk Worker Contact Information (see 106)
 - (d) Making Service News Desk Worker Contact information unavailable (see 153)
- 7. Repudiation of actions on Service News Desk Worker credentials
 - (a) Removal of Service News Desk Worker Credentials (see 19)
 - (b) Modification of Service News Desk Worker Credentials (see 19)
 - (c) Viewing Service News Desk Worker Credentials (see 107)
 - (d) Making Service News Desk Worker Credentials unavailable (see 154)
- 8. Repudiation of actions on Input Source Contact information
 - (a) Removal of Input Source Contact information (see 20)
 - (b) Modification of Input Source Contact information (see 20)
 - (c) Viewing Input Source Contact Information (see 108)
 - (d) Making Input Source Contact information unavailable (see 155)
- 9. Repudiation of actions on Input Source credentials
 - (a) Removal of Input Source Credentials (see 21)
 - (b) Modification of Input Source Credentials (see 21)
 - (c) Viewing Input Source Credentials (see 109)
 - (d) Making Input Source Credentials unavailable (see 156)
- 10. Repudiation of actions on edition
 - (a) Removal of edition (see 22)
 - (b) Modification of edition (see 22)
 - i. Composition of edition (see 22)

- ii. Lay-out of edition (see 22)
 - (c) Viewing edition (see 110)
 - (d) Making edition unavailable (see 155)
- 11. Repudiation of actions on edition, limited in time, valuable (see 69)
- 12. Repudiation of actions on edition, limited in time, not valuable (see 69)
- 13. Repudiation of actions on edition, not limited in time, valuable (see 69)
- 14. Repudiation of actions on edition, not limited in time, not valuable (see 69)
- 15. Repudiation of actions on story
 - (a) Removal of story (see 27)
 - (b) Modification of story (see 27)
 - (c) Viewing story (see 115)
 - (d) Making story unavailable (see 162)
- 16. Repudiation of actions on story, limited in time, valuable (see 74)
- 17. Repudiation of actions on story, limited in time, not valuable (see 74)
- 18. Repudiation of actions on story, not limited in time, valuable (see 74)
- 19. Repudiation of actions on story, not limited in time, not valuable (see 74)
- 20. Repudiation of actions on input data stream
 - (a) Make input data stream unavailable (see 167)
 - (b) Remove input from input data stream (see 32)
 - (c) Add input to input data stream (see 32)
 - (d) Modification of input in input data stream (see 32)
- 21. Repudiation of actions on user information stream
 - (a) Make user data stream unavailable (see 168)
 - (b) Remove user information from user information data stream (see 33)
 - (c) Add user information to user information data stream (see 33)
 - (d) Modification of user information in user information data stream (see 33)
- 22. Repudiation of actions on MC behaviour information stream (see 80)
- 23. Repudiation of actions on MC contact information stream (see 80)
- 24. Repudiation of actions on MC credentials information stream (see 80)
- 25. Repudiation of actions on SNDW contact information stream (see 80)
- 26. Repudiation of actions on SNDW credentials information stream (see 80)
- 27. Repudiation of actions on IS contact information stream (see 80)
- 28. Repudiation of actions on IS credentials information stream (see 80)
- 29. Repudiation of actions in edition stream

- (a) Make edition data stream unavailable (see 176)
 - (b) Remove edition information from edition information data stream (see 41)
 - (c) Add edition information to edition information data stream (see 41)
 - (d) Modification of edition information in edition information data stream (see 41)
30. Repudiation of actions on edition, limited in time, valuable, stream (see 88)
31. Repudiation of actions on edition, limited in time, not valuable, stream (see 88)
32. Repudiation of actions on edition, not limited in time, valuable, stream (see 88)
33. Repudiation of actions on edition, not limited in time, not valuable, stream (see 88)
34. Repudiation of actions on story data stream
- (a) Make story data stream unavailable (see 181)
 - (b) Remove story information from story data stream (see 46)
 - (c) Add story information to story data stream (see 46)
 - (d) Modification of story in story data stream (see 46)
35. Repudiation of actions on story, valuable, limited in time, stream (see 93)
36. Repudiation of actions on story, valuable, not limited in time, stream (see 93)
37. Repudiation of actions on story, not valuable, limited in time, stream (see 93)
38. Repudiation of actions on story, not valuable, not limited in time, stream (see 93)
39. Repudiation of actions from the Input Source
- (a) Repudiation of actions on input (see 60)
 - (b) Repudiation of actions on MC behaviour information (see 63)
 - (c) Repudiation of actions on IS contact information (see 67)
 - (d) Repudiation of actions on IS credentials information (see 68)
40. Repudiation of actions from the Media Consumer
- (a) Repudiation of actions on MC behaviour information (see 63)
 - (b) Repudiation of actions on MC contact information (see 62)
 - (c) Repudiation of actions on MC credentials (see 64)
 - (d) Repudiation of actions on editions (see 69)
41. Repudiation of actions from the Service News Desk Worker
- (a) Repudiation of actions on SNDW contact information (see 65)
 - (b) Repudiation of actions on SNDW credentials information (see 66)
 - (c) Repudiation of actions on edition (see 69)
 - (d) Repudiation of actions on input (see 60)
 - (e) Repudiation of actions on story (see 74)
 - (f) Repudiation of actions on MC contact information (see 62)
 - (g) Repudiation of actions on MC behaviour information (see 63)
 - (h) Repudiation of actions on MC credentials (see 64)
 - (i) Repudiation of actions on IS contact information (see 67)
 - (j) Repudiation of actions on IS credentials (see 68)

Information disclosure

1. Information disclosure of input
 - (a) information disclosure at the Input Management System
 - i. Elevation of privileges at IMS (AND) (see 201)
 - ii. Obtain access to the input
 - A. No access control at the Input Management System
 - (b) information disclosure at the Content Management System
 - i. Elevation of privileges at CMS (AND) (see 197)
 - ii. Obtain access to the input
 - A. No access control at the Content Management System
 - (c) information disclosure at the Service News Desk
 - i. Elevation of privileges at SND (see 196)
 - ii. Obtain access to input
 - A. No access control at the SND
 - (d) information disclosure at the Service News Desk Worker Client
 - i. Elevation of privileges at SNDW Client (see 203)
 - ii. Obtain access to input
 - A. No access control at the SNDW Client
 - (e) By physical information disclosure of input
 - i. Break into the server room of the publisher
 - ii. Input information disclosure from hardware
2. Information disclosure of user information
3. Information disclosure of MC contact information
 - (a) information disclosure of MC contact information at the User Management System
 - i. Elevation of privileges at the User Management System (see 199)
 - ii. Obtain access to the MC contact information
 - A. No access control at the User Management System
 - (b) information disclosure of MC contact information at the Service Controller
 - i. Elevation of privileges at the Service Controller (see 200)
 - ii. Obtain access to the MC contact information
 - A. No access control at the Service Controller
 - (c) information disclosure at the Media Consumer Client
 - i. Elevation of privileges at the MC Client (see 195)
 - ii. Obtain access to the MC contact information
 - A. No access control at the MC client
 - (d) information disclosure at the Service News Desk
 - i. Elevation of privileges at the Service News Desk (see 196)
 - ii. Obtain access to the MC contact information
 - A. No access control at the SND
 - (e) information disclosure at the Service News Desk Worker Client

- i. Elevation of privileges at the Service News Desk Worker Client (see 203)
 - ii. Obtain access to the MC contact information
 - A. No access control at the SNDW Client
 - (f) By physical information disclosure of MC contact information
 - i. Break into the server room of the publisher
 - ii. MC contact information disclosure from hardware
- 4. Information disclosure of MC behaviour information
 - (a) Information disclosure of MC behaviour information at the Media Consumer Client
 - i. Elevation of privileges at the Media Consumer Client (see 195)
 - ii. Obtain access to the MC behaviour information
 - A. No access control at the Media Consumer Client
 - (b) Information disclosure of MC behaviour information at the Service Controller
 - i. Elevation of privileges at the Service Controller (see 200)
 - ii. Obtain access to the MC behaviour information
 - A. No access control at the Service Controller
 - (c) Information disclosure of MC behaviour information at the User Management System
 - i. Elevation of privileges at the User Management System (see 199)
 - ii. Obtain access to the MC behaviour information at the User Management System
 - A. No access control at the User Management System
 - (d) Information disclosure of MC behaviour information at the Input Management System
 - i. Elevation of privileges at the IMS (see 201)
 - ii. Obtain access to the MC behaviour information at the IMS
 - A. No access control at the IMS
 - (e) Information disclosure of MC behaviour information at the Input Source Client
 - i. Elevation of privileges at the IS Client (see 202)
 - ii. Obtain access to the MC behaviour information at the IS Client
 - A. No access control at the IS Client
 - (f) By physical information disclosure of MC behaviour information
 - i. Break into the server room of the publisher
 - ii. MC behaviour information disclosure from hardware
- 5. Information disclosure of MC credentials
 - (a) Information disclosure of MC credentials data at the Media Consumer Client
 - i. Elevation of privileges at the Media Consumer Client (see 195)
 - ii. Obtain access to the MC credentials data
 - A. No access control at the Media Consumer Client
 - (b) Information disclosure of MC credentials data information at the Service Controller
 - i. Elevation of privileges at the Service Controller (see 200)
 - ii. Obtain access to the MC credentials data
 - A. No access control at the Service Controller
 - (c) Information disclosure of MC credentials data information at the User Management System

- i. Elevation of privileges at the User Management System (see 199)
 - ii. Obtain access to the MC credentials data
 - A. No access control at the User Management System
- 6. Information disclosure of SNDW contact information
 - (a) Information disclosure of SNDW contact information at the SNDW client
 - i. Elevation of privileges at the Service News Desk Worker Client (see 203)
 - ii. Obtain access to the Service News Desk Worker contact information
 - A. No access control at the Service News Desk Worker Client
 - (b) Information disclosure of SNDW contact information at the Service News Desk
 - i. Elevation of privileges at the Service News Desk (see 196)
 - ii. Obtain access to the Service News Desk Worker contact information
 - A. No access control at the Service News Desk
 - (c) Information disclosure of SNDW contact information at the User Management System
 - i. Elevation of privileges at the User Management System (see 199)
 - ii. Obtain access to the Service News Desk Worker contact information
 - A. No access control at the User Management System
- 7. Information disclosure of SNDW credentials
 - (a) Information disclosure of SNDW credentials at the SNDW client
 - i. Elevation of privileges at the Service News Desk Worker Client (see 203)
 - ii. Obtain access to the Service News Desk Worker credentials
 - A. No access control at the Service News Desk Worker Client
 - (b) Information disclosure of SNDW credentials at the Service News Desk
 - i. Elevation of privileges at the Service News Desk (see 196)
 - ii. Obtain access to the Service News Desk Worker credentials
 - A. No access control at the Service News Desk
 - (c) Information disclosure of SNDW credentials at the User Management System
 - i. Elevation of privileges at the User Management System (see 199)
 - ii. Obtain access to the Service News Desk Worker credentials
 - A. No access control at the User Management System
- 8. Information disclosure of IS contact information
 - (a) Information disclosure of IS Contact information at the Input Source Client
 - i. Elevation of privileges at the Input Source Client (see 202)
 - ii. Obtain access to the Input Source Contact information
 - A. No access control at the Input Source Client
 - (b) Information disclosure of IS Contact information at the Input Management System
 - i. Elevation of privileges at the Input Management System (see 201)
 - ii. Obtain access to the Input Source Contact information
 - A. No access control at the Input Management System
 - (c) Information disclosure of IS Contact information at the User Management System
 - i. Elevation of privileges at the User Management System (see 199)

- ii. Obtain access to the Input Source Contact information
 - A. No access control at the User Management System
- 9. Information disclosure of IS credentials
 - (a) Information disclosure of IS credentials at the Input Source Client
 - i. Elevation of privileges at the Input Source Client (see 202)
 - ii. Obtain access to the Input Source credentials
 - A. No access control at the Input Source Client
 - (b) Information disclosure of IS Credentials at the Input Management System
 - i. Elevation of privileges at the Input Management System (see 201)
 - ii. Obtain access to the Input Source credentials
 - A. No access control at the Input Management System
 - (c) Information disclosure of IS Credentials at the User Management System
 - i. Elevation of privileges at the User Management System (see 199)
 - ii. Obtain access to the Input Source credentials
 - A. No access control at the User Management System
- 10. Information disclosure of edition
 - (a) Information disclosure of edition at the Service News Desk Worker Client
 - i. Elevation of privileges at the Service News Desk Worker Client (see 203)
 - ii. Obtain access to the edition
 - A. No access control at the Service News Desk Worker Client
 - (b) Information disclosure of edition at the Service News Desk
 - i. Elevation of privileges at the Service News Desk (see 196)
 - ii. Obtain access to the edition
 - A. No access control at the Service News Desk
 - (c) Information disclosure of edition at the Content Management System
 - i. Elevation of privileges at the Content Management System (see 197)
 - ii. Obtain access to the edition
 - A. No access control at the Content Management System
 - (d) Information disclosure of edition at the Newspaper Service
 - i. Elevation of privileges at the Newspaper Service (see 198)
 - ii. Obtain access to the edition
 - A. No access control at the Newspaper Service
 - (e) Information disclosure of edition at the Service Controller
 - i. Elevation of privileges at the Service Controller (see 200)
 - ii. Obtain access to the edition
 - A. No access control at the Service Controller
 - (f) Information disclosure of edition at the Media Consumer Client
 - i. Elevation of privileges at the Media Consumer Client (see 195)
 - ii. Obtain access to the edition
 - A. No access control at the Media Consumer Client

11. Information disclosure of edition, limited in time, valuable (see 110)
12. Information disclosure of edition, limited in time, not valuable (see 110)
13. Information disclosure of edition, not limited in time, valuable (see 110)
14. Information disclosure of edition, not limited in time, not valuable (see 110)
15. Information disclosure of story
 - (a) Information disclosure of story at the Service News Desk Worker Client
 - i. Elevation of privileges at the Service News Desk Worker Client (see 203)
 - ii. Obtain access to the story
 - A. No access control at the Service News Desk Worker Client
 - (b) Information disclosure of story at the Service News Desk
 - i. Elevation of privileges at the Service News Desk (see 196)
 - ii. Obtain access to the story
 - A. No access control at the Service News Desk
 - (c) Information disclosure of story at the Content Management System
 - i. Elevation of privileges at the Content Management System (see 197)
 - ii. Obtain access to the story
 - A. No access control at the Content Management System
16. Information disclosure of story, limited in time, valuable (see 115)
17. Information disclosure of story, limited in time, not valuable (see 115)
18. Information disclosure of story, not limited in time, valuable (see 115)
19. Information disclosure of story, not limited in time, not valuable (see 115)
20. Information disclosure of input data stream
21. Tamper with input data stream
 - (a) Information disclosure of input data stream as eavesdropper
 - i. as eavesdropper between Input Source Client and Input Management System
 - A. Communication between Input Source Client and Input Management System is susceptible for eavesdropping
 - ii. as eavesdropper between Input Management System and Content Management System
 - A. Communication between Input Management System and Content Management System is susceptible for eavesdropping
 - iii. as eavesdropper between Content Management System and Service News Desk
 - A. Communication between Content Management System and Service News Desk is susceptible for eavesdropping
 - iv. as eavesdropper between Service News Desk and Service News Desk Worker tool
 - A. Communication between Service News Desk and Service News Desk Worker tool is susceptible for eavesdropping
 - (b) At the Input Source Client
 - i. Elevation of privileges of the IS client (see 202)
 - ii. Eavesdrop Input Data Stream

- (c) At the Input Management System
 - i. Elevation of privileges at Input Management System (see 201)
 - ii. Eavesdrop Input Data Stream
 - (d) At the Content Management System
 - i. Elevation of privileges at the Content Management System (see 197)
 - ii. Eavesdrop Input Data Stream
 - (e) At the Service News Desk
 - i. Elevation of privileges at the Service News Desk (see 196)
 - ii. Eavesdrop Input Data Stream
 - (f) At the Service News Desk Worker Client
 - i. Elevation of privileges at the Service News Desk Worker Client (see 203)
 - ii. Eavesdrop Input Data Stream
22. Information disclosure of user information data stream
23. Information disclosure of MC behaviour information data stream
- (a) Information disclosure of MC behaviour information data stream as eavesdropper
 - i. as eavesdropper between Media Consumer Client and Service Controller
 - A. Communication between Media Consumer Client and Service Controller is susceptible for eavesdropping
 - ii. as eavesdropper between Service Controller and User Management System
 - A. Communication between Service Controller and User Management System is susceptible for eavesdropping
 - iii. as eavesdropper between User Management System and Input Management System
 - A. Communication between User Management System and Input Management System is susceptible for eavesdropping
 - iv. as eavesdropper between Input Management System and Input Source client
 - A. Communication between Input Management System and Input Source client is susceptible for eavesdropping
 - (b) At the Media Consumer Client
 - i. Elevation of privileges at the Media Consumer Client (see 195)
 - ii. Eavesdrop Media Consumer Behaviour Information Data Stream
 - (c) At the Service Controller
 - i. Elevation of privileges at the Service Controller (see 200)
 - ii. Eavesdrop Media Consumer Behaviour Information Data Stream
 - (d) At the User Management System
 - i. Elevation of privileges at the User Management System (see 199)
 - ii. Eavesdrop Media Consumer Behaviour Information Data Stream
 - (e) At the Input Management System
 - i. Elevation of privileges at the Input Management System (see 201)
 - ii. Eavesdrop Media Consumer Behaviour Information Data Stream
 - (f) At the Input Source client
 - i. Elevation of privileges at the Input Source Client (see 202)
 - ii. Eavesdrop Media Consumer Behaviour Information Data Stream

24. Information disclosure of MC contact information data stream

- (a) Information disclosure of MC contact information data stream as eavesdropper
 - i. As eavesdropper between Media Consumer Client and Service Controller
 - A. Communication between Media Consumer Client and Service Controller is susceptible for eavesdropping
 - ii. As eavesdropper between Service Controller and User Management System
 - A. Communication between Service Controller and User Management System is susceptible for eavesdropping
 - iii. As eavesdropper between User Management System and Service News Desk
 - A. Communication between User Management System and Service News Desk is susceptible for eavesdropping
 - iv. As eavesdropper between Service News Desk Worker Client and Service News Desk
 - A. Communication between Service News Desk Worker Client and Service News Desk is susceptible for eavesdropping
- (b) At the Media Consumer Client
 - i. Elevation of privileges at the MC Client (see 195)
 - ii. Eavesdrop MC contact information data stream
- (c) At the Service Controller
 - i. Elevation of privileges at the Service Controller (see 200)
 - ii. Eavesdrop MC contact information data stream
- (d) At the User Management System
 - i. Elevation of privileges at the UMS (see 199)
 - ii. Eavesdrop MC contact information data stream
- (e) At the Service News Desk
 - i. Elevation of privileges at the SND (see 196)
 - ii. Eavesdrop MC contact information data stream
- (f) At the Service News Desk Worker Client
 - i. Elevation of privileges at the SNDWC (see 203)
 - ii. Eavesdrop MC contact information data stream

25. Information disclosure of MC credentials data stream

- (a) Information disclosure of MC credentials information data stream as eavesdropper
 - i. As eavesdropper between Media Consumer Client and Service Controller
 - A. Communication between Media Consumer Client and Service Controller is susceptible for eavesdropping
 - ii. As eavesdropper between Service Controller and User Management System
 - A. Communication between Service Controller and User Management System is susceptible for eavesdropping
 - iii. As eavesdropper between Service Controller and Newspaper Service
 - A. Communication between Service Controller and Newspaper Service is susceptible for tampering eavesdropping
- (b) At the Media Consumer Client
 - i. Elevation of privileges at the MC Client (see 195)

- ii. Eavesdrop MC credentials information data stream
 - (c) At the Service Controller
 - i. Elevation of privileges at the Service Controller (see 200)
 - ii. Eavesdrop MC credentials information data stream
 - (d) At the User Management System
 - i. Elevation of privileges at the UMS (see 199)
 - ii. Eavesdrop MC credentials information data stream
 - (e) At the Newspaper Service
 - i. Elevation of privileges at the Newspaper Service (see 198)
 - ii. Eavesdrop MC credentials information data stream
- 26. Information disclosure of SNDW contact information data stream
 - (a) Information disclosure of SNDW contact information data stream as eavesdropper
 - i. As eavesdropper between News Desk Worker Client and Service News Desk
 - A. Communication between News Desk Worker Client and Service News Desk is susceptible for eavesdropping
 - ii. As eavesdropper between Service News Desk and User Management System
 - A. Communication between Service News Desk and User Management System is susceptible for eavesdropping
 - (b) At the Service News Desk Worker Client
 - i. Elevation of privileges at the SNDW Client (see 203)
 - ii. Eavesdrop Service News Desk Worker Contact Information data stream
 - (c) At the Service News Desk
 - i. Elevation of privileges at the SND (see 196)
 - ii. Eavesdrop Service News Desk Worker Contact Information data stream
 - (d) At the User Management System
 - i. Elevation of privileges at the UMS (see 199)
 - ii. Eavesdrop Service News Desk Worker Contact Information data stream
- 27. Information disclosure of SNDW credentials data stream
 - (a) Information disclosure of SNDW credentials data stream as eavesdropper
 - i. As eavesdropper between News Desk Worker Client and Service News Desk
 - A. Communication between News Desk Worker Client and Service News Desk is susceptible for eavesdropping
 - ii. As eavesdropper between Service News Desk and User Management System
 - A. Communication between Service News Desk and User Management System is susceptible for eavesdropping
 - (b) At the Service News Desk Worker Client
 - i. Elevation of privileges at the SNDW Client (see 203)
 - ii. Eavesdrop SNDW Credentials information data stream
 - (c) At the Service News Desk
 - i. Elevation of privileges at the SND (see 196)
 - ii. Eavesdrop SNDW Credentials information data stream

- (d) At the User Management System
 - i. Elevation of privileges at UMS (see 199)
 - ii. Eavesdrop SNDW Credentials information data stream
28. Information disclosure of IS contact information data stream
- (a) Information disclosure of IS contact information data stream as eavesdropper
 - i. As eavesdropper between Input Source Client and Input Management System
 - A. Communication between Input Source Client and Input Management System is susceptible for eavesdropping
 - ii. As eavesdropper between Input Management System and User Management System
 - A. Communication between Input Management System and User Management System is susceptible for eavesdropping
 - (b) At the Input Source Client
 - i. Elevation of privileges at the IS Client (see 202)
 - ii. Eavesdrop IS contact information data stream
 - (c) At Input Management System
 - i. Elevation of privileges at IMS (see 201)
 - ii. Eavesdrop IS contact information data stream
 - (d) At the User Management System
 - i. Elevation of privileges at the UMS (see 199)
 - ii. Eavesdrop IS contact information data stream
29. Information disclosure of IS credentials data stream
- (a) Information disclosure of IS credentials information data stream as eavesdropper
 - i. As eavesdropper between Input Source Client and Input Management System
 - A. Communication between Input Source Client and Input Management System is susceptible for eavesdropping
 - ii. As eavesdropper between Input Management System and User Management System
 - A. Communication between Input Management System and User Management System is susceptible for eavesdropping
 - (b) At the Input Source Client
 - i. Elevation of privileges at the IS Client (see 202)
 - ii. Eavesdrop IS credentials information data stream
 - (c) At the Input Management System
 - i. Elevation of privileges at IMS (see 201)
 - ii. Eavesdrop IS credentials information data stream
 - (d) At the User Management System
 - i. Elevation of privileges at the UMS (see 199)
 - ii. Eavesdrop IS credentials information data stream
30. Information disclosure of edition data stream
- (a) Information disclosure of edition data stream as eavesdropper
 - i. As eavesdropper between Service News Desk Worker Client and Service News Desk

- A. Communication between Service News Desk Worker Client and Service News Desk is susceptible for eavesdropping
 - ii. As eavesdropper between Service News Desk and Content Management System
 - A. Communication between Service News Desk and Content Management System is susceptible for eavesdropping
 - iii. As eavesdropper between Content Management System and Newspaper Service
 - A. Communication between Content Management System and Newspaper Service is susceptible for eavesdropping
 - iv. As eavesdropper between Newspaper Service and Service Controller
 - A. Communication between Newspaper Service and Service Controller is susceptible for eavesdropping
 - v. As eavesdropper between Service Controller and Media Consumer Client
 - A. Communication between Service Controller and Media Consumer Client is susceptible for eavesdropping
 - (b) At the Service News Desk Worker Client
 - i. Elevation of privileges at the SNDW Client (see 203)
 - ii. Eavesdrop edition stream
 - (c) At the Service News Desk
 - i. Elevation of privileges at the SND (see 196)
 - ii. Eavesdrop edition stream
 - (d) At the Content Management System
 - i. Elevation of privileges at the CMS (see 197)
 - ii. Eavesdrop edition stream
 - (e) At the Newspaper Service
 - i. Elevation of privileges at the Newspaper Service (see 198)
 - ii. Eavesdrop edition stream
 - (f) At the Service Controller
 - i. Elevation of privileges at the Service Controller (see 200)
 - ii. Eavesdrop edition stream
 - (g) At the Media Consumer Client
 - i. Elevation of privileges at the MC Client (see 195)
 - ii. Eavesdrop edition stream
31. Information disclosure of edition, limited in time, valuable data stream (see 130)
32. Information disclosure of edition, limited in time, not valuable data stream (see 130)
33. Information disclosure of edition, not limited in time, valuable data stream (see 130)
34. Information disclosure of edition, not limited in time, not valuable data stream (see 130)
35. Information disclosure of story
- (a) Information disclosure of story data stream as eavesdropper
 - i. As eavesdropper between Service News Desk Worker Client and Service News Desk
 - A. Communication between Service News Desk Worker Client and Service News Desk is susceptible for eavesdropping

- ii. As eavesdropper between Service News Desk and Content Management System
 - A. Communication between Service News Desk and Content Management System is susceptible for eavesdropping
 - (b) At the Content Management System
 - i. Elevation of privileges at the CMS (see 197)
 - ii. Eavesdrop story stream
 - (c) At the Service News Desk
 - i. Elevation of privileges at the SND (see 196)
 - ii. Eavesdrop story stream
 - (d) At the Service News Desk Worker Client
 - i. Elevation of privileges at the SNDW Client (see 203)
 - ii. Eavesdrop story stream
- 36. Information disclosure of story, limited in time, valuable data stream (see 135)
- 37. Information disclosure of story, limited in time, not valuable data stream (see 135)
- 38. Information disclosure of story, not limited in time, valuable data stream (see 135)
- 39. Information disclosure of story, limited in time, not valuable data stream (see 135)
- 40. Information disclosure of MC client
 - (a) Elevation of privileges at MC client (see 195)
 - (b) Obtain access to software image/memory
 - i. No access control at MC Client
 - (c) Reverse engineering of MC Client
 - i. In order to know how the MC Client works
 - ii. In order to know whether the MC Client contains secret information
- 41. Information disclosure of Service News Desk
 - (a) Elevation of privileges at SND (see 196)
 - (b) Obtain access to software image/memory
 - i. No access control at SND
 - (c) Reverse engineering of SND
 - i. In order to know how the SND works
 - ii. In order to know whether the SND contains secret information
- 42. Information disclosure of Content Management System
 - (a) Elevation of privileges at CMS (see 197)
 - (b) Obtain access to software image/memory
 - i. No access control at CMS
 - (c) Reverse engineering of CMS
 - i. In order to know how the CMS works
 - ii. In order to know whether the CMS contains secret information
- 43. Information disclosure of Newspaper Service

- (a) Elevation of privileges at Newspaper Service (see 198)
 - (b) Obtain access to software image/memory
 - i. No access control at Newspaper Service
 - (c) Reverse engineering of Newspaper Service
 - i. In order to know how the Newspaper Service works
 - ii. In order to know whether the Newspaper Service contains secret information
44. Information disclosure of User Management System
- (a) Elevation of privileges at UMS (see 199)
 - (b) Obtain access to software image/memory
 - i. No access control at UMS
 - (c) Reverse engineering of UMS
 - i. In order to know how the UMS works
 - ii. In order to know whether the UMS contains secret information
45. Information disclosure of Service Controller
- (a) Elevation of privileges at Service Controller (see 200)
 - (b) Obtain access to software image/memory
 - i. No access control at Service Controller
 - (c) Reverse engineering of Service Controller
 - i. In order to know how the Service Controller works
 - ii. In order to know whether the Service Controller contains secret information
46. Information disclosure of Input Management System
- (a) Elevation of privileges at IMS (see 201)
 - (b) Obtain access to software image/memory
 - i. No access control at IMS
 - (c) Reverse engineering of IMS
 - i. In order to know how the IMS works
 - ii. In order to know whether the IMS contains secret information
47. Information disclosure of IS client
- (a) Elevation of privileges at IS Client (see 202)
 - (b) Obtain access to software image/memory
 - i. No access control at IS Client
 - (c) Reverse engineering of IS Client
 - i. In order to know how the IS Client works
 - ii. In order to know whether the IS Client contains secret information
48. Information disclosure of SNDW Client
- (a) Elevation of privileges at SNDW Client (see 203)
 - (b) Obtain access to software image/memory
 - i. No access control at SNDW Client
 - (c) Reverse engineering of SNDW Client
 - i. In order to know how the SNDW Client works
 - ii. In order to know whether the SNDW Client contains secret information

DoS

1. DoS attack on input (making input unavailable for SNDW)
 - (a) DoS-attack on IMS (see 193)
 - (b) DoS attack on UMS (see 190)
 - (c) DoS attack on IS Client (see 193)
 - (d) DoS-attack on SND (see 187)
 - (e) DoS attack on SNDW Client (see 194)
 - (f) DoS attack on input data stream (see 167)
 - (g) Physical attack on input
 - i. Break into publisher server room (AND)
 - ii. Damage IMS hardware
 - iii. Damage UMS hardware
 - iv. Break into IS office (AND)
 - v. Damage ISC hardware
 - vi. Break into Service News Desk Worker office (AND)
 - vii. Damage SNDWC hardware
2. DoS attack on user information
3. DoS attack on MC contact information
 - (a) DoS-attack on MC Client (see 186)
 - (b) DoS-attack on Service Controller (see 191)
 - (c) DoS-attack on UMS (see 190)
 - (d) DoS-attack on SND (see 187)
 - (e) DoS-attack on SNDWC (see 194)
 - (f) DoS-attack on MC contact information data stream (see 169)
 - (g) Physical attack on MC contact information
 - i. Break into publisher server room (AND)
 - ii. Damage Service Controller hardware
 - iii. Damage UMS hardware
 - iv. Damage SND hardware
 - v. Break into Service News Desk Worker office (AND)
 - vi. Damage SNDWC hardware
 - vii. Break into MC house (AND)
 - viii. Damage MCC hardware
4. DoS attack on MC behaviour information
 - (a) DoS-attack on MC Client (see 186)
 - (b) DoS-attack on Service Controller (see 191)
 - (c) DoS-attack on UMS (see 190)
 - (d) DoS-attack on IMS (see 192)
 - (e) DoS-attack on ISC (see 193)
 - (f) DoS-attack on MC behaviour information data stream (see 170)

- (g) Physical attack on MC behaviour information
 - i. Break into publisher server room (AND)
 - ii. Damage Service Controller hardware
 - iii. Damage UMS hardware
 - iv. Damage IMS hardware
 - v. Break into IS office (AND)
 - vi. Damage ISC hardware
 - vii. Break into MC house (AND)
 - viii. Damage MCC hardware
- 5. DoS attack on MC credentials information
 - (a) DoS-attack on MCC (see 186)
 - (b) DoS-attack on Service Controller (see 191)
 - (c) DoS-attack on UMS (see 190)
 - (d) DoS-attack on MC credentials information data stream (see 171)
 - (e) Physical attack on MC credentials information
 - i. Break into publisher server room (AND)
 - ii. Damage Service Controller hardware
 - iii. Damage UMS hardware
 - iv. Break into MC house (AND)
 - v. Damage MCC hardware
- 6. DoS attack on SNDW contact information
 - (a) DoS-attack on SNDWC (see 194)
 - (b) DoS-attack on SND (see 187)
 - (c) DoS-attack on UMS (see 190)
 - (d) DoS-attack on SNDW contact information data stream (see 172)
 - (e) Physical attack on SNDW contact information
 - i. Break into publisher server room (AND)
 - ii. Damage SND hardware
 - iii. Damage UMS hardware
 - iv. Break into Service News Desk Worker office (AND)
 - v. Damage SNDWC hardware
- 7. DoS attack on SNDW credentials information
 - (a) DoS-attack on SNDWC (see 194)
 - (b) DoS-attack on SND (see 187)
 - (c) DoS-attack on UMS (see 190)
 - (d) DoS-attack on SNDW contact information data stream (see 172)
 - (e) Physical attack on SNDW contact information
 - i. Break into publisher server room (AND)
 - ii. Damage SND hardware
 - iii. Damage UMS hardware
 - iv. Break into Service News Desk Worker office (AND)

- v. Damage SNDWC hardware
8. DoS attack on IS contact information
 - (a) DoS-attack on ISC (see 193)
 - (b) DoS-attack on IMS (see 192)
 - (c) DoS-attack on UMS (see 190)
 - (d) DoS-attack on SND (see 187)
 - (e) DoS-attack on SNDWC (see 194)
 - (f) Physical attack on IS contact information
 - i. Break into publisher server room (AND)
 - ii. Damage IMS hardware
 - iii. Damage UMS hardware
 - iv. Damage SND hardware
 - v. Break into Service News Desk Worker office (AND)
 - vi. Damage SNDWC hardware
 - vii. Break into Input Source office (AND)
 - viii. Damage ISC hardware
 9. DoS attack on IS credentials information
 - (a) DoS-attack on ISC (see 193)
 - (b) DoS-attack on IMS (see 192)
 - (c) DoS-attack on UMS (see 190)
 - (d) Physical attack on IS contact information
 - i. Break into publisher server room (AND)
 - ii. Damage IMS hardware (OR)
 - iii. Damage UMS hardware
 - iv. Break into Input Source office (AND)
 - v. Damage ISC hardware
 10. DoS attack on edition
 - (a) DoS-attack on CMS
 - (b) DoS-attack on SND (see 187)
 - (c) DoS-attack on SNDWC (see 194)
 - (d) DoS-attack on Newspaper Service (see 189)
 - (e) DoS-attack on Service Controller (see 191)
 - (f) DoS-attack on MCC (see 186)
 - (g) Physical attack on edition
 - i. Break into publisher server room (AND)
 - ii. Damage CMS hardware
 - iii. Damage SND hardware
 - iv. Damage Newspaper Service hardware
 - v. Damage Service Controller hardware
 - vi. Break into Service News Desk Worker office (AND)
 - vii. Damage SNDWC hardware

- viii. Break into Media Consumer house (AND)
 - ix. Damage MCC hardware
- 11. DoS attack on edition, limited in time, valuable (see 158)
- 12. DoS attack on edition, limited in time, not valuable (see 158)
- 13. DoS attack on edition, not limited in time, valuable (see 158)
- 14. DoS attack on edition, not limited in time, not valuable (see 158)
- 15. DoS attack on story
 - (a) DoS-attack on SNDWC
 - (b) DoS-attack on SND
 - (c) DoS-attack on CMS
 - (d) Physical attack on story
 - i. Break into publisher server room (AND)
 - ii. Damage SND hardware
 - iii. Damage CMS hardware
 - iv. Break into SNDW office (AND)
 - v. Damage SNDWC hardware
- 16. DoS attack on story, limited in time, valuable (see 163)
- 17. DoS attack on story, limited in time, not valuable (see 163)
- 18. DoS attack on story, not limited in time, not valuable (see 163)
- 19. DoS attack on story, not limited in time, valuable (see 163)
- 20. DoS attack on input data stream (make data stream impossible)
 - (a) DoS-attack on ISC (see 193)
 - (b) DoS-attack on IMS (see 192)
 - (c) DoS-attack on CMS (see 189)
 - (d) DoS-attack on SND (see 187)
 - (e) DoS-attack on SNDWC (see 194)
 - (f) DoS-attack on communication
 - i. Interrupt or modify communication between ISC and IMS as man in the middle
 - A. Communication between ISC and IMS is susceptible for man in the middle
 - ii. Interrupt or modify communication between IMS and CMS as man in the middle
 - A. Communication between IMS and CMS is susceptible for man in the middle
 - iii. Interrupt or modify communication between SND and CMS as man in the middle
 - A. Communication between SND and CMS is susceptible for man in the middle
 - iv. Interrupt or modify communication between SNDWC and SND as man in the middle
 - A. Communication between SNDWC and SND is susceptible for man in the middle
- 21. DoS attack on user information stream
- 22. DoS attack on MC contact information stream

- (a) DoS-attack on MCC (see 186)
 - (b) DoS-attack on Service Controller (see 191)
 - (c) DoS-attack on UMS (see 190)
 - (d) DoS-attack on SND (see 187)
 - (e) DoS-attack on SNDWC (see 194)
 - (f) DoS-attack on communication
 - i. Interrupt or modify communication between MCC and Service Controller as man in the middle
 - A. Communication between MCC and Service Controller is susceptible for man in the middle
 - ii. Interrupt or modify communication between Service Controller and UMS as man in the middle
 - A. Communication between Service Controller and UMS is susceptible for man in the middle
 - iii. Interrupt or modify communication between SND and UMS as man in the middle
 - A. Communication between SND and UMS is susceptible for man in the middle
 - iv. Interrupt or modify communication between SNDWC and SND as man in the middle
 - A. Communication between SNDWC and SND is susceptible for man in the middle
23. DoS attack on MC behaviour information stream
- (a) DoS-attack on MCC (see 186)
 - (b) DoS-attack on Service Controller (see 191)
 - (c) DoS-attack on UMS (see 190)
 - (d) DoS-attack on IMS (see 192)
 - (e) DoS-attack on ISC (see 193)
 - (f) DoS-attack on communication
 - i. Interrupt or modify communication between MCC and Service Controller as man in the middle
 - A. Communication between MCC and Service Controller is susceptible for man in the middle
 - ii. Interrupt or modify communication between Service Controller and UMS as man in the middle
 - A. Communication between Service Controller and UMS is susceptible for man in the middle
 - iii. Interrupt or modify communication between IMS and UMS as man in the middle
 - A. Communication between IMS and UMS is susceptible for man in the middle
 - iv. Interrupt or modify communication between IMS and ISC as man in the middle
 - A. Communication between IMS and ISC is susceptible for man in the middle
24. DoS attack on MC credentials information stream
- (a) DoS-attack on MCC (see 186)
 - (b) DoS-attack on Service Controller (see 191)
 - (c) DoS-attack on UMS (see 190)
 - (d) DoS-attack on communication

- i. Interrupt or modify communication between MCC and Service Controller as man in the middle
 - A. Communication between MCC and Service Controller is susceptible for man in the middle
 - ii. Interrupt or modify communication between Service Controller and UMS as man in the middle
 - A. Communication between Service Controller and UMS is susceptible for man in the middle
- 25. DoS attack on SNDW contact information stream
 - (a) DoS-attack on UMS (see 190)
 - (b) DoS-attack on SND (see 187)
 - (c) DoS-attack on SNDWC (see 194)
 - (d) DoS-attack on communication
 - i. Interrupt or modify communication between SND and UMS as man in the middle
 - A. Communication between SND and UMS is susceptible for man in the middle
 - ii. Interrupt or modify communication between SNDWC and SND as man in the middle
 - A. Communication between SNDWC and SND is susceptible for man in the middle
- 26. DoS attack on SNDW credentials information stream
 - (a) DoS-attack on UMS (see 190)
 - (b) DoS-attack on SND (see 187)
 - (c) DoS-attack on SNDWC (see 194)
 - (d) DoS-attack on communication
 - i. Interrupt or modify communication between SND and UMS as man in the middle
 - A. Communication between SND and UMS is susceptible for man in the middle
 - ii. Interrupt or modify communication between SNDWC and SND as man in the middle
 - A. Communication between SNDWC and SND is susceptible for man in the middle
- 27. DoS attack on IS contact information stream
 - (a) DoS-attack on UMS (see 190)
 - (b) DoS-attack on IMS (see 192)
 - (c) DoS-attack on ISC (see 193)
 - (d) DoS-attack on communication
 - i. Interrupt or modify communication between IMS and UMS as man in the middle
 - A. Communication between IMS and UMS is susceptible for man in the middle
 - ii. Interrupt or modify communication between IMS and ISC as man in the middle
 - A. Communication between IMS and ISC is susceptible for man in the middle
- 28. DoS attack on IS credentials information stream
 - (a) DoS-attack on UMS (see 190)
 - (b) DoS-attack on IMS (see 192)

- (c) DoS-attack on ISC (see 193)
 - (d) DoS-attack on communication
 - i. Interrupt or modify communication between IMS and UMS as man in the middle
 - A. Communication between IMS and UMS is susceptible for man in the middle
 - ii. Interrupt or modify communication between IMS and ISC as man in the middle
 - A. Communication between IMS and ISC is susceptible for man in the middle
29. DoS attack on edition stream
- (a) DoS-attack on CMS (see 188)
 - (b) DoS-attack on SND (see 187)
 - (c) DoS-attack on SNDWC (see 194)
 - (d) DoS-attack on Newspaper Service (see 189)
 - (e) DoS-attack on Service Controller (see 191)
 - (f) DoS-attack on MCC (see 186)
 - (g) DoS-attack on communication
 - i. Interrupt or modify communication between CMS and SND as man in the middle
 - A. Communication between CMS and SND is susceptible for man in the middle
 - ii. Interrupt or modify communication between SND and SNDWC as man in the middle
 - A. Communication between SND and SNDWC is susceptible for man in the middle
 - iii. Interrupt or modify communication between CMS and Newspaper Service as man in the middle
 - A. Communication between CMS and Newspaper Service is susceptible for man in the middle
 - iv. Interrupt or modify communication between Newspaper Service and Service Controller as man in the middle
 - A. Communication between Newspaper Service and Service Controller is susceptible for man in the middle
 - v. Interrupt or modify communication between Service Controller and MCC as man in the middle
 - A. Communication between Service Controller and MCC is susceptible for man in the middle
30. DoS attack on edition, limited in time, valuable, information stream (see 177)
31. DoS attack on edition, limited in time, not valuable, information stream (see 177)
32. DoS attack on edition, not limited in time, valuable, information stream (see 177)
33. DoS attack on edition, not limited in time, not valuable, information stream (see 177)
34. DoS attack on story information stream
- (a) DoS-attack on CMS (see 188)
 - (b) DoS-attack on SND (see 187)
 - (c) DoS-attack on SNDWC (see 194)
 - (d) DoS-attack on communication
 - i. Interrupt or modify communication between CMS and SND as man in the middle

- A. Communication between CMS and SND is susceptible for man in the middle
 - ii. Interrupt or modify communication between SND and SNDWC as man in the middle
 - A. Communication between SND and SNDWC is susceptible for man in the middle
- 35. DoS attack on story, limited in time, valuable, information stream (see 183)
- 36. DoS attack on story, limited in time, not valuable, information stream (see 183)
- 37. DoS attack on story, not limited in time, valuable, information stream (see 183)
- 38. DoS attack on story, not limited in time, not valuable, information stream (see 183)
- 39. DoS attack on MC client
 - (a) Power off MCC
 - i. Elevation of privileges on MCC (AND) (see 195)
 - ii. Power off MCC
 - (b) Overload MCC with requests
 - i. by a DoS on the Service Controller, which redirects the requests to the MCC
 - ii. by a man in the middle who generates requests or an eavesdropper who replays requests
 - A. between Service Controller and MCC
Communication between SC and MCC is susceptible for man-in-the-middle/eavesdropping
- 40. DoS attack on Service News Desk
 - (a) Power off SND
 - i. Elevation of privileges on SND (AND) (see 196)
 - ii. Power off SND
 - (b) Overload SND with requests
 - i. by a DoS on the SNDWC, which redirects the requests to the SND
 - ii. by a DoS on the IMS, which redirects notifications towards the SND
 - iii. by a man in the middle who generates requests or an eavesdropper who replays requests
 - A. between IMS and SND
 - B. between SNDWC and SND
- 41. DoS attack on Content Management System
 - (a) Power off CMS
 - i. Elevation of privileges on CMS (AND) (see 197)
 - ii. Power off CMS
 - (b) Overload CMS with requests
 - i. by a DoS on the IMS, which redirects input towards the CMS
 - ii. by a DoS on the SND, which redirects requests to the CMS
 - iii. by a DoS on the Newspaper Service, which obtains content from the CMS
 - iv. by a DoS on the Service Controller, which redirects requests to the Newspaper Service
 - v. by a DoS on the MCC, which redirects requests to the Service Controller

- 42. DoS attack on Newspaper Service
 - (a) Power off Newspaper Service
 - i. Elevation of privileges on Newspaper Service (AND) (see 198)
 - ii. Power off Newspaper Service
 - (b) Overload Newspaper Service
 - i. by a DoS on the Service Controller, which requests editions from the Newspaper Service
 - ii. by a DoS on the MCC, which requests editions via the Service Controller
 - iii. by a DoS on the CMS, which notifies the Newspaper Service when new content arrives
 - iv. by a DoS on the UMS, which pushes user credentials towards the Newspaper Service
 - v. by a DoS on the Service Controller, which pushes user login information towards the UMS
 - vi. by a Dos on the MMC, which redirects requests to the Service Controller
- 43. DoS attack on User Management System
 - (a) Power off UMS
 - i. Elevation of privileges on UMS (AND) (see 190)
 - ii. Power off UMS
 - (b) Overload UMS
 - i. by a DoS on the SND, which redirects user information requests to the UMS
 - ii. by a DoS on the IMS, which redirects user information requests to the UMS
 - iii. by a DoS on the Newspaper Service, which redirects on
- 44. DoS attack on Service Controller
 - (a) Power off Service Controller
 - i. Elevation of privileges on Service Controller (UMS) (see 200)
 - ii. Power off Service Controller
 - (b) Overload Service Controller
 - i. by a DoS on the Newspaper Service, which pushes editions to MCC, via the Service Controller
 - ii. by a DoS on the MCC, which requests content/requests, submits user information via the Service Controller
- 45. DoS attack on Input Management System
 - (a) Power off IMS
 - i. Elevation of privileges on IMS (see 201)
 - ii. Power off IMS
 - (b) Overload IMS
 - i. by a DoS on the IMC, which redirects requests towards the IMS
- 46. DoS attack on IS client
 - (a) Power off ISC
 - i. Elevation of privileges on ISC (see 202)

- ii. Power off ISC
 - (b) Overload ISC
 - i. by a DoS on the IMS, which sends user information towards the IMS
 - ii. by a DoS on the UMS, which sends user information towards the IMS
47. Dos attack on SNDW Client
- (a) Power off SNDWC
 - i. Elevation of privileges on SNDWC (see 203)
 - ii. Power off SNDWC
 - (b) Overload SNDWC
 - i. by a DoS on SND, which redirects requests towards SNDWC
 - ii. by a DoS on IMS, which sends notifications towards SND
 - iii. by a DoS on UMS, which sends user information towards SND
 - iv. by a DoS on CMS, which sends content towards SND

Elevation of privileges

1. Elevation of privileges on MC client
 - (a) by exploiting a software hole via communication
 - i. As eavesdropper
 - ii. As man in the middle
 - (b) by obtaining physical entrance
2. Elevation of privileges on Service News Desk
 - (a) by exploiting a software hole via communication between SND and SNDWC
 - i. As eavesdropper
 - ii. Ad man in the middle
 - (b) by exploiting a software hole via communication between IMS and SND
 - i. As eavesdropper
 - ii. Ad man in the middle
 - (c) by exploiting a software hole via communication between UMS and SND
 - i. As eavesdropper
 - ii. Ad man in the middle
 - (d) by exploiting a software hole via communication between CMS and SND
 - i. As eavesdropper
 - ii. Ad man in the middle
 - (e) by obtaining physical entrance
3. Elevation of privileges on Content Management System
 - (a) by exploiting a software hole via communication between IMS and CMS
 - i. As eavesdropper
 - ii. Ad man in the middle

- (b) by exploiting a software hole via communication between SND and CMS
 - i. As eavesdropper
 - ii. Ad man in the middle
 - (c) by exploiting a software hole via communication between NS and CMS
 - i. As eavesdropper
 - ii. Ad man in the middle
 - (d) by obtaining physical entrance
4. Elevation of privileges on Newspaper Service
- (a) by exploiting a software hole via communication between CMS and NS
 - i. As eavesdropper
 - ii. Ad man in the middle
 - (b) by exploiting a software hole via communication between SC and NS
 - i. As eavesdropper
 - ii. Ad man in the middle
 - (c) by obtaining physical entrance
5. Elevation of privileges on User Management System
- (a) by exploiting a software hole via communication between SC and UMS
 - i. As eavesdropper
 - ii. Ad man in the middle
 - (b) by exploiting a software hole via communication between IMS and UMS
 - i. As eavesdropper
 - ii. Ad man in the middle
 - (c) by exploiting a software hole via communication between SND and UMS
 - i. As eavesdropper
 - ii. Ad man in the middle
 - (d) by obtaining physical entrance
6. Elevation of privileges on Service Controller
- (a) by exploiting a software hole via communication between UMS and SC
 - i. As eavesdropper
 - ii. Ad man in the middle
 - (b) by exploiting a software hole via communication between NS and SC
 - i. As eavesdropper
 - ii. Ad man in the middle
 - (c) by exploiting a software hole via communication between MCC and SC
 - i. As eavesdropper
 - ii. Ad man in the middle
 - (d) by obtaining physical entrance
7. Elevation of privileges on Input Management System

- (a) by exploiting a software hole via communication between ISC and IMS
 - i. As eavesdropper
 - ii. Ad man in the middle
 - (b) by obtaining physical entrance
8. Elevation of privileges on IS Client
- (a) by exploiting a software hole via communication
 - i. As eavesdropper
 - ii. As man in the middle
 - (b) by obtaining physical entrance
9. Elevation of privileges on SNDW Client
- (a) by exploiting a software hole via communication
 - i. As eavesdropper
 - ii. As man in the middle
 - (b) by obtaining physical entrance

A.3.2 Analyze threats

DREAD is then used to assess these potential vulnerabilities. DREAD is an acronym that defines the following five key attributes used to measure the criticality of a vulnerability: Damage potential, Reproducibility, Exploitability, Affected users, and Discoverability. The application of DREAD is beyond the scope of this report..

B Brainstorming threat modeling

This section describes a structured brainstorming approach for identifying business threats. A business threat is defined as a threat that uses the functionality the system offers in way that is not conform with business policy or regulations and laws. The algorithm the authors came up with consists of two high-level steps: (i) collecting relevant regulations, laws, and a description of the system, and (ii) organizing a structured brainstorming activity for identifying business abuses.

B.0.3 Collecting relevant information

The first step is to collect relevant information about the application domain. This information includes (i) regulations and legislations, and (ii) an inventory of use cases.

Applications in the e-commerce are subject to different regulations and legislations. These determine to a great extent the architectural security requirements and solutions of the system. In this experiment, the following regulations may be applicable for a publishing platform: (i) Privacy legislation on usage and storage of personal data[8, 9, 10], (ii) E-transactions legislations and regulations[7], and (iii) Information Security Law. These regulations are summarized as follows:

1. Collecting: personal data can only be collected and processed by the provider if permitted by some law or if the individual has unambiguously given his consent.
2. Use: Data must not be processed for any purposes incompatible with those for which the data was initially collected. It cannot be transferred to third parties without agreement from the data subject. Security measures must be taken to protect the data against destruction or loss. It should not be kept longer than necessary for the purpose it was collected.

3. Access: Data should be accurate, complete and kept up-to-date. The customer must have access to any personal data concerning him/her that is being processed or kept. A request for correction or deletion of incorrect personal data must be granted. The customer must have the possibility to opt out.
4. Processing of personal preferences is usually prohibited, except for when the person who's information is to be processed has given his consent.

The use cases described in the analysis document[13] and the architecture document[6] were used.

B.0.4 Organizing a structured brainstorming activity

Brainstorming[2] is a group creativity technique that was designed to generate a large number of ideas for the solution of a problem. This process is based on 4 ideas. The participants should focus on *quantity*, because a higher number of ideas increases the chance that an effective solution is produced. *No criticism* creates the right atmosphere for generating *unusual ideas*, which may provide better solutions. The participants should also *combine and improve* the ideas of others.

During the brainstorming session(s), possible attacks were generated for the system. The authors tried to attack the system, which was seen as a *blackbox*, in any way they thought was possible. Documents describing the functionality of the system have been used as starting point. The resulting list is the following.

1. Steal the users device to subscribe to a service.
2. Bribe the user to use his device to subscribe to a service.
3. Threat the user to use his device to subscribe to a service.
4. Mislead the user to use his device to subscribe to a service.
5. Steal the users identity. (note: depends on the used identification mechanism. When the system uses biometrics, one could cut off the victims finger)
6. Friendly ask the user if he want to subscribe to a certain service.
e.g.: An under age person could ask his friend of age to subscribe to a 18+ service.
7. Steal a server by breaking into the building.
8. Steal a server by bribing the security guards.
9. Steal a server by using a Kalashnikov.
10. Steal a server by misleading the security guards.
11. Gain physical access to the terminal/workstation of a news desk worker —terminal hijacking.
12. Phone a news desk worker to get a list of subscribed clients by misleading him.
e.g. saying you are someone else
13. Phone a corporate news desk worker to get his login and password by misleading him.
e.g. saying you are an admin and that the corporate news desk worker should change his password
14. Threat an employee to get the wanted information.
15. Bribe a corporate news desk worker to adapt the corporate strategy. *e.g.: a key-logger to obtain someones planning*
16. The people who implemented the system also implemented some backdoor, allowing them to access the system and all the sensitive information without any restriction.

17. Everyone from the corporate news desk dies due to a plane crash.
18. Someone posing as a visitor and is left running around the offices on his own.
19. Steal someone's pre-paid access card to gain free access.
20. An external service provider feeds the system with garbage characters and succeeds in instantiating a fatal error.
21. Get your friends to constantly refresh a page to slow down the system.
22. Provide the system with false / malicious input when input is requested.
e.g.: insert a script when asked to enter your name
23. Take employees hostage.
24. Physically shoot a server in order to disable it.
25. Disable electrical grid.
26. Virus injection.
e.g.: a virus that infects all media devices, rendering them inoperable.
A virus that infects servers in order to obtain certain information
27. Disable the publisher's internet connection. This will effectively cut off any services relying on the internet.
28. Read a monitor (CRT) from outside the building based on radiation.
29. Disrupt the communication between the publisher and the billing provider. This will disable the system from doing any kind of payments or payment requests.
30. Prevent employees from entering the building where they work.
31. Install a packet sniffer on a communication to line to intercept information.
32. Allow a teenager to subscribe to a 18+ service (business abuse).
33. Make it impossible to unsubscribe from a service (business) *e.g.: to have someone else pay for it, in the case of a pay-per-view business model*
34. Spread an edition (to other consumers).(business)
35. Send an edition to the wrong media consumers (business)
36. Store non-anonymous search requests without the media consumers consent (business)
37. Collect viewing information without media consumer's consent. (business)
38. Do not allow the media consumer to remove his viewing information (business)
39. Do not allow the media consumer to view his viewing information (business)
40. Use the viewing information or other than intended purposes (business)
41. Collect context information without the media consumer's consent (business)
42. Do not allow the media consumer to view his context information (business)
43. Do not allow the media consumer to remove his context information (business)
44. Use the context information for other than intended purposes (business)
45. Do not verify input (when it has to) (business).

46. Multiple input sources input the same bogus content. (business)
47. Submit input with personal preferences. (business)
48. Do not use anonymized results (business)
49. Give a list of outstanding reservations to the wrong advertiser. (business)
50. Do not verify commercials when it has to (business). Possible (mainly business) abuses are:
51. Perform the wrong checks on the input (business).
52. Allow not allowed stories. (business)
53. Do not check if the input really came from the claimed source (business).
54. Do not verify the contents of the input (business).
55. Remove the input when it is not a duplicate/unuseful (business).
56. Tag the input with false information (business).
57. Assign an input verification task to the wrong input (business).
58. Assign an input verification task to a wrong member of the news desk (business).
59. Do not check the input. (business)
60. Do not perform several checks on the commercial. (business)
61. Do not assign a commercial verification task (business).
62. Allow the commercial even when it is not conform the reservation (business).
63. Do not allow the commercial even when it is conform the reservation (business).
64. Do not perform the reservation conformity check (business).
65. Do not perform the authentication of the source check (business).
66. Do not tag the commercial (business).
67. Falsely tag the commercial (business).

References

- [1] S. Barnum and M. Gegick. Build security in – Design principles.
- [2] M. Diel and W. Stroebe. Productivity loss in brainstorming groups: Toward the solution of a riddle. *Journal of Personality & Social Psychology*, 53(3):497–509, 1987.
- [3] M. Howard and S. Lipner. *The Security Development Lifecycle*. Microsoft Press, 2006.
- [4] ISO/IEC. 17799:2000 - information technology - code of practice for information security management.

-
- [5] S. Kaplan. The words of risk analysis. *Risk Analysis*, 17 (4):407–417, 1997.
 - [6] D. V. Landuyt, J. Grégoire, S. Michiels, E. Truyen, and W. Joosen. Modelling digital publishing: architecture report. Technical report, K.U.Leuven, Dept. of Computer Science, Leuven, Belgium, Dec. 2005.
 - [7] T. E. Parliament and the Council. Directive 1999/93/ec of the european parliament and of the council of 13 december 1999 on a community framework for electronic signatures, Dec 1999.
 - [8] E. Parliament and the Council. Directive 95/46/ec of the european parliament and of the council of 24 october 1995 on the protection of individuals with regard to the processing of personal data and on the free movement of such data, October 1995.
 - [9] T. E. Parliament and the Council. Directive 2002/22/ec of the european parliament and of the council of 7 march 2002 on universal service and users’ rights relating to electronic communications networks and services (universal service directive), March 2002.
 - [10] T. E. Parliament and the Council. Directive 2002/58/ec of the european parliament and of the council of 12 july 2002 concerning the processing of personal data and the protection of privacy in the communications sector (directive on privacy and electronic communications), Jul 2002.
 - [11] G. Stoneburner, A. Goguen, and A. Feringa. Risk management guide for information technology systems.
 - [12] F. Swiderski and W. Snyder. *Threat Modeling*. Microsoft Professional, 2004.
 - [13] K. Vandebroek, S. Michiels, E. Truyen, and W. Joosen. Modelling digital publishing. Technical report, K.U.Leuven, Dept. of Computer Science, Leuven, Belgium, July 2005.
 - [14] S. A. N. Zealand. Risk management as/nzs 4360:2004, 2004.