**SafeCard**
A Gigabit Intrusion Prevention System on the network card

Willem de Bruijn, Asia Slowinska, Tomas Hruby,
Kees van Reeuwijk, Li Xu, and Herbert Bos
wdb@few.vu.nl
Vrije Universiteit Amsterdam

**Maximise Detection Rate:** Combine orthogonal detection vectors in a single pipelined application

- Header-based Filtering
- TCP Stream Reassembly
- Pattern Matching
- Protocol Deconstruction
- Behavioral Detection

**Maximise Performance:**
- Only deconstruct headers for active applications
- Compile matching engine to assembly
- Reassemble TCP streams in-place
- Employ specialised hardware

**Ruler**
Fast Regular Expression Matching

more expressive than string-matching through repetition, alternation protocol header support

faster than traditional regex-engines generalisation of Aho-Corasick compiled, not interpreted to embedded hardware

**Streamline**
Employ Specialised Hardware

**Prospector**
Block polymorphic attacks through Protocol Deconstruction

Check maximum bufferlength
Application-specific information

**Behavioral Detection**
flow-based accounting
aggregate information
statistical aggregation

**Signs**
flows/sec
address entropy
out-of-order arrival
overlapping segments

**Zero-Copy TCP**
Scrub malicious traffic

- Ethernet Frames
tcp 80
- tcp 22

Combine information from all stages to minimise false positives and false negatives