Heterogene Einbruchs-Erkennungssysteme für Hochgeschwindigkeitsnetze

CASED

High-Speed Malware Collection in Netzwerken mittels rekonfigurierbarer Hardware (FPGAs)

Sascha Mühlbach

TECHNISCHE UNIVERSITÄT DARMSTADT
Fraunhofer SIT
h.da HOCHSCHULE DARMSTADT UNIVERSITY OF APPLIED SCIENCES
LOEWE – Landes-Offensive zur Entwicklung Wissenschaftlich-ökonomischer Exzellenz

Inhalt

- Motivation
- Honeypots: Funktion, Vorteile und Risiken
- Die MalCoBox: Ein hardwarebasierter Honeypot
- Details der Architektur
- Emulation verwundbarer Applikationen
- Demonstration

Motivation

CASED

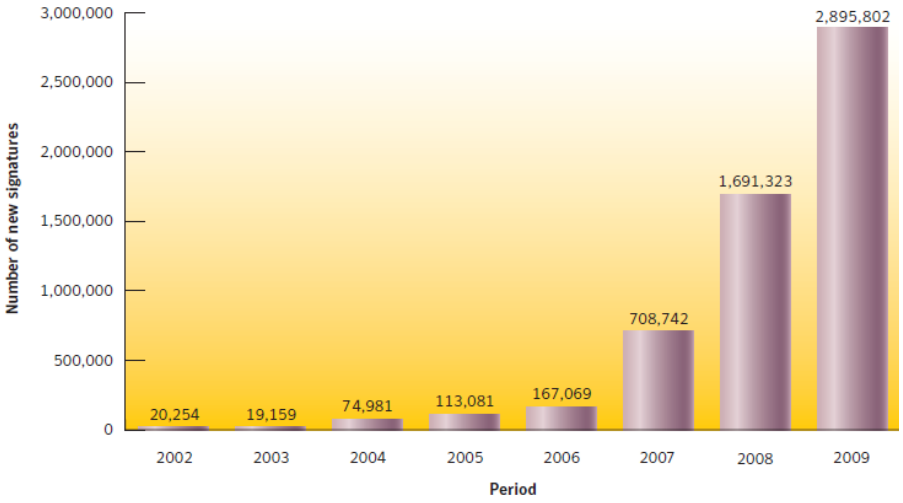
Malware

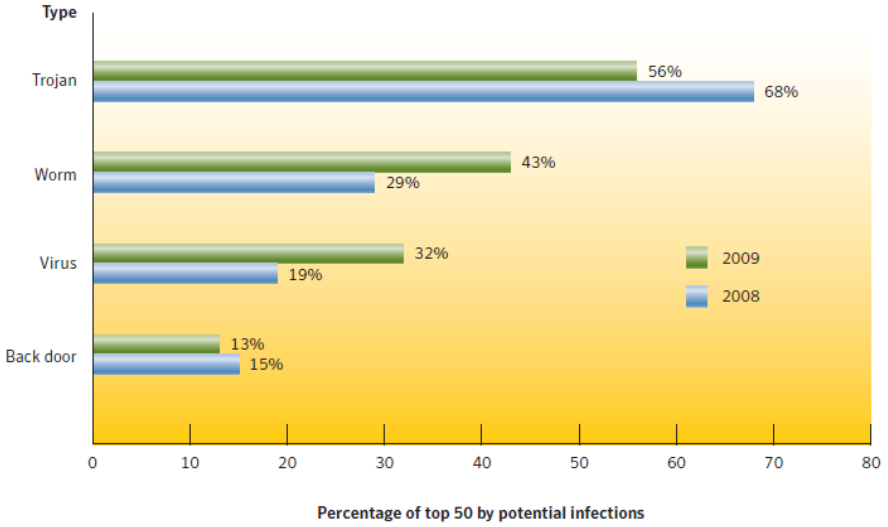
- gehört zu den größten Bedrohungen im Internet
- umfasst Schadprogramme wie Viren, Trojaner, Backdoors, Würmer etc.
- Ziel nicht mehr das Zerstören von Daten (wie oft bei Viren aus den 90ern), sondern das gezielte Ausspähen vertraulicher Informationen
  - Passwörter, Kreditkartendaten, Firmengeheimnisse
- hochentwickelte Malware erst bei Ausführung identifizierbar

verbreitet sich auf diversen Wegen

- über Schwachstellen in Netzwerkservern
- über Webseiten
- über Dokumente (PDF)

Malware - Fakten





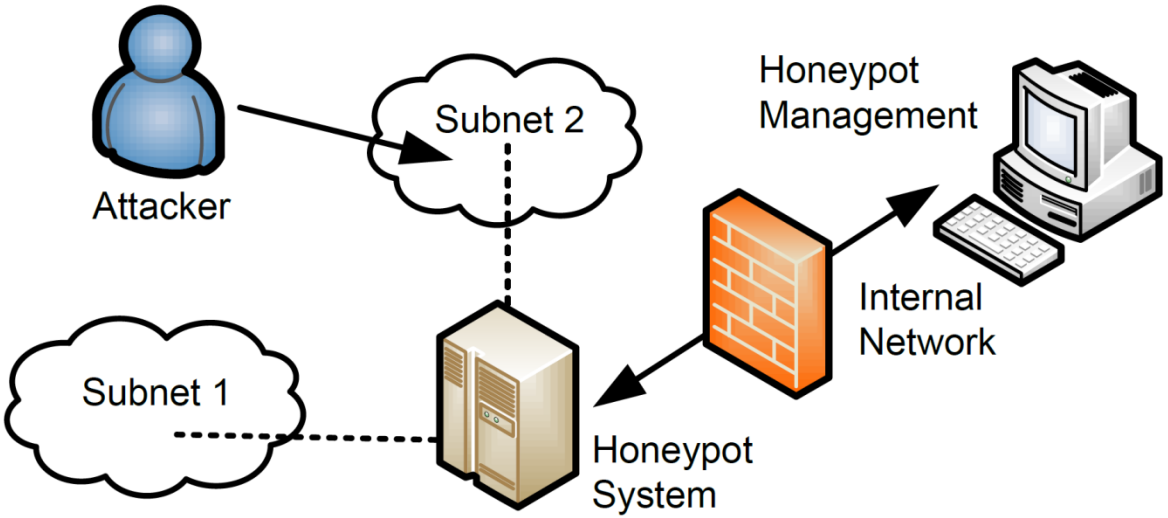
Rank	Propagation Mechanisms	2009 Percentage	2008 Percentage
1	File-sharing executables	72%	66%
2	File transfer, CIFS	42%	30%
3	File transfer, email attachment	25%	31%
4	Remotely exploitable vulnerability	24%	12%
5	File sharing , P2P	5%	10%
6	File transfer, HTTP, embedded URI, instant messenger	4%	4%
7	SQL	2%	3%
8	Back door, Kuang2	2%	3%
9	Back door, SubSeven	2%	3%
10	File sharing, data files	1%	1%

Table 18. Propagation mechanisms
Source: Symantec

Honeypots

Honeypots sind Netzwerksysteme mit dem Ziel, Angreifer anzulocken

- sind getrennt vom eigentlichen Netzwerk
- emulieren verwundbare Applikationen



Honeypots

CASED

Einsatzbereich

- **Forschung**: Auswertung der Angriffsmuster zur Entwicklung von Gegenmaßnahmen, Sammeln von Malware
- **Produktivsysteme**: als Ergänzung für IDS zur Meldung von Angriffsversuchen (Angreifer soll durch den Honeypot vom eigentlichen Netzwerk abgelenkt werden)

Herausforderungen

- **Risiko**: auf den Honeypots läuft Software -> Der Honeypot selber kann kompromittiert und für Angriffe auf andere Systeme missbraucht werden
- **Performance**: um möglichst viele Angreifer anzulocken, wird eine entsprechende Rechenleistung benötigt

-> Entwicklung eines hardwarebasierten Honeypots

MalCoBox

CASED

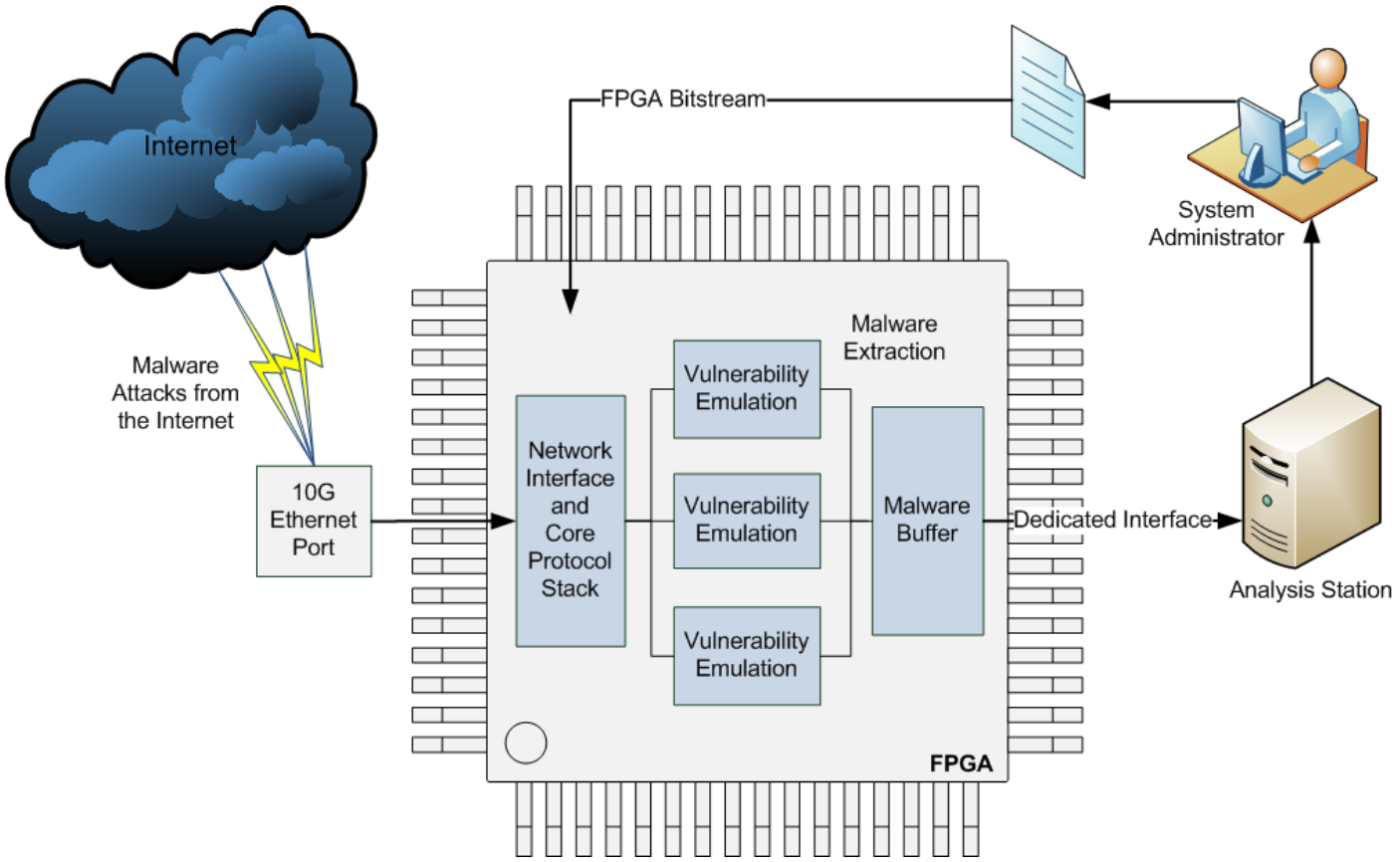
Hardwarebasierter Ansatz bietet Vorteile

- **Sicherheit:** Hardwarestrukturen lassen sich nicht von außen verändern
- **Performance:** Geschwindigkeiten im Bereich von 10Gbit/s sowie viele parallele Verbindungen sind durch dedizierte Hardware erreichbar
- **Benutzbarkeit:** System kann als Appliance ohne hohen Wartungsaufwand eingesetzt werden

MalCoBox: Malware Collection Box

- emuliert verwundbare Anwendungen, die für das Einschleusen von Malware ausgenutzt werden können
- extrahiert potentielle Malware aus einkommenden Anfragen und speichert diese für eine weitere Analyse
- ermöglicht die Abdeckung eines sehr großen IP-Adressbereichs bei einem Netzwerkdurchsatz von 10 Gbit/s

MalCoBox: Übersicht



MalCoBox: Designziele

CASED

mind. 10 Gbit/s

- 128 Bit Datenpfad bei 156.25 Mhz (10G Takt) ermöglicht 20 Gbit/s und bietet so genügend Spielraum für Variationen bei der Verarbeitungsgeschwindigkeit

flexibel erweiterbar

- neue Emulationen müssen sich einfach hinzufügen lassen (werden sich oft ändern)

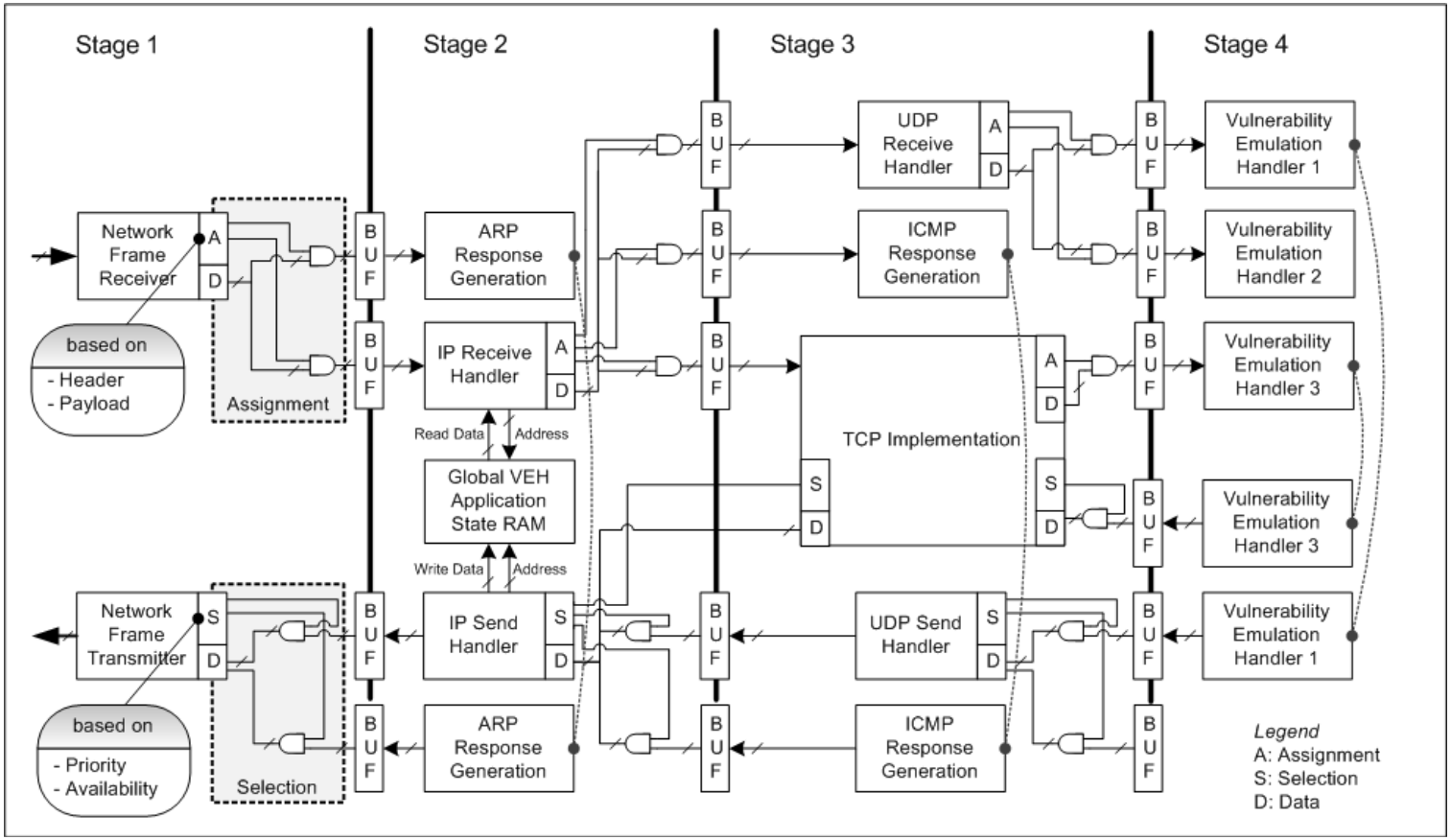
skalierbar (z.B. auf mehrere oder neue FPGAs)

- System soll nicht auf speziellen Technologieelementen aufbauen

möglichst zustandslose Verarbeitung

- Speicherung von Zuständen macht das Design komplex

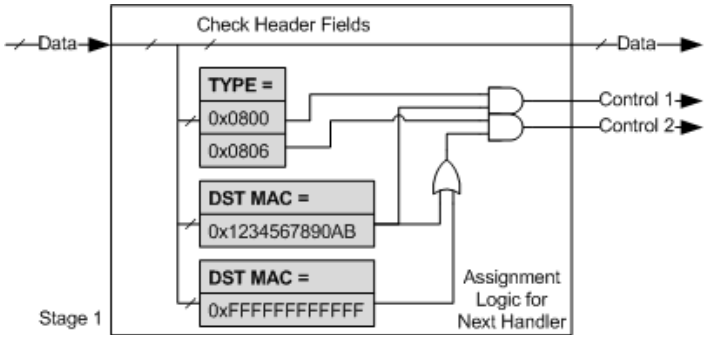
MalCoBox: Architektur



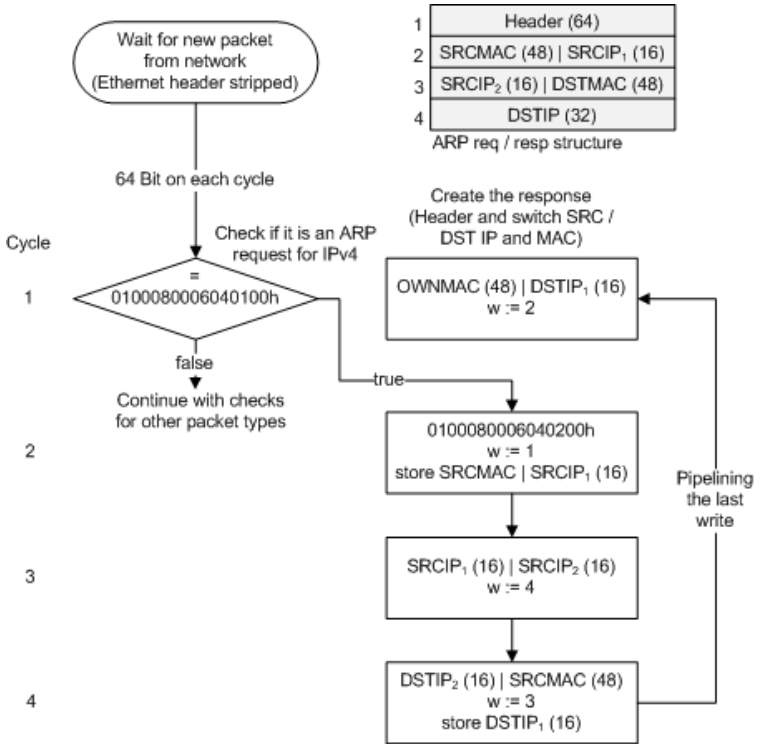
NetStage Architektur

MalCoBox: Architekturdetails

- Verteilung der Pakete auf die nächsten Handler mit flexiblen Regeln

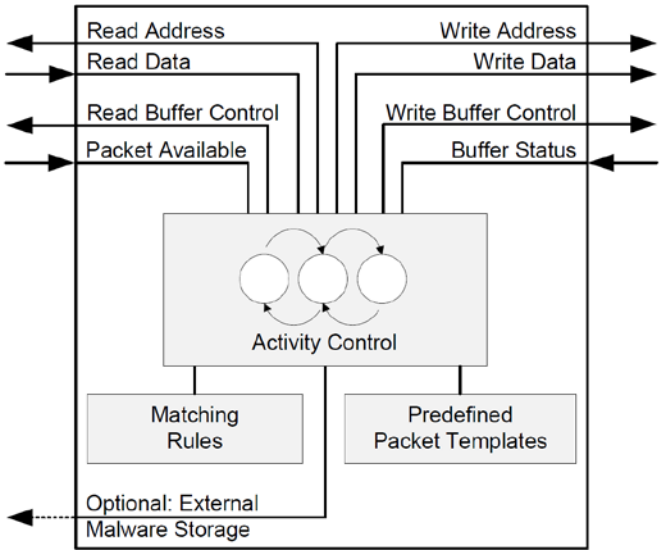


- Handler verarbeiten Paketdaten on-the-fly ohne Verzögerung (z.B. ARP Response)



Vulnerability Emulation Handler

- emulieren **spezielle Schwachstelle** einer Applikation
- **nur notwendige Funktionalität**, nicht das gesamte Protokoll
- bestehen aus einer **zentralen State-Machine und spezieller Hardware** für z.B.
  - Pattern Matching
  - Antwort-Templates
- reagieren nur auf **einkommende Pakete**
- besitzen **Verbindung zu einem Speicher-medium** für die Malware (PCIe oder NET)
  - inkl. eines Headers mit Zeitstempel, Logdaten und Emulationskennung



Vulnerability Emulation Handler

CASED

SIP (sipX Framework Buffer Overflow)

- Übermittlung eines CSeq-Wertes mit einer Länge von mehr als 20 Zeichen in einem INVITE Paket führt zu einem Buffer-Overflow
- Malware-Erkennung: Alles zwischen „CSeq: „ und „Max-Fo“ (Feldbegrenzer) > 20 Zeichen

Paket:

INVITE sip:LF@127.0.0.1 SIP/2.0

To: <sip:127.0.0.1:5060>

Via: SIP/2.0/UDP 127.0.0.1:8918

From: "LF"<sip:127.0.0.1:8918>

Call-ID: 125127.0.0.1

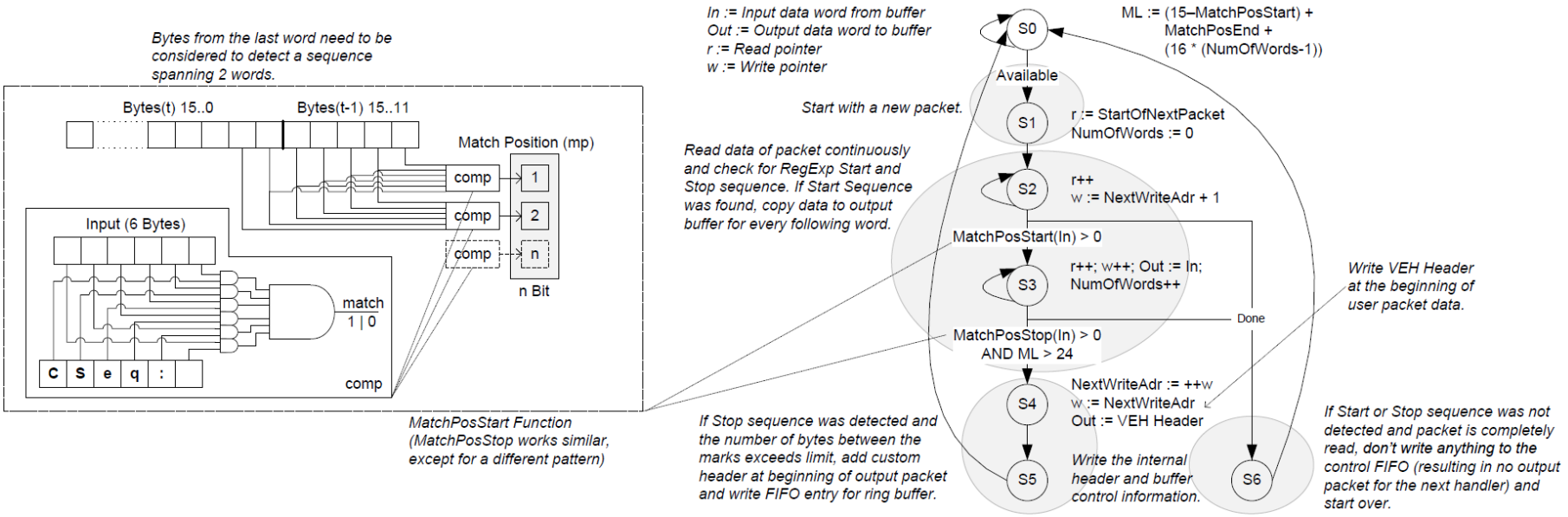
CSeq: **MALWAREMALWAREMALWARE**

Max-Forwards: 20

Vulnerability Emulation Handler

Implementierung der SIP-Schwachstelle

- 16 Byte wortparallele Match-Unit prüft Position des Start und End-Patterns
- Daten zwischen den beiden Markierungen werden kopiert



Vulnerability Emulation Handler

CASED

MS SQL Server 2000 Buffer Overflow (Slammer Wurm)

- Angreifer sendet Ping und prüft auf MS SQL Server -> MalCoBox antwortet
- Paket beginnend mit 0x04 enthält Malware Payload

Mail Server

- MalCoBox empfängt Mails an beliebige Adressaten und gibt sich als Open Relay aus
- Implementiert SMTP Dialog (normalerweise zustandsbehaftet, hier aber nicht zwingend nötig)
- Mails werden gespeichert (meistens SPAM, eventuell mit Malware)

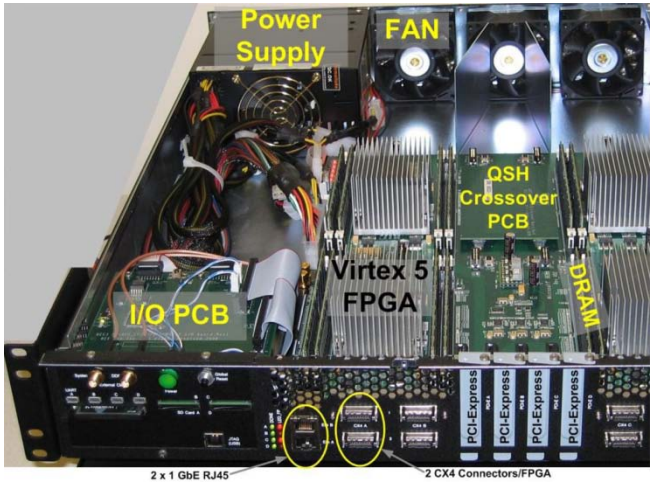
Web Server

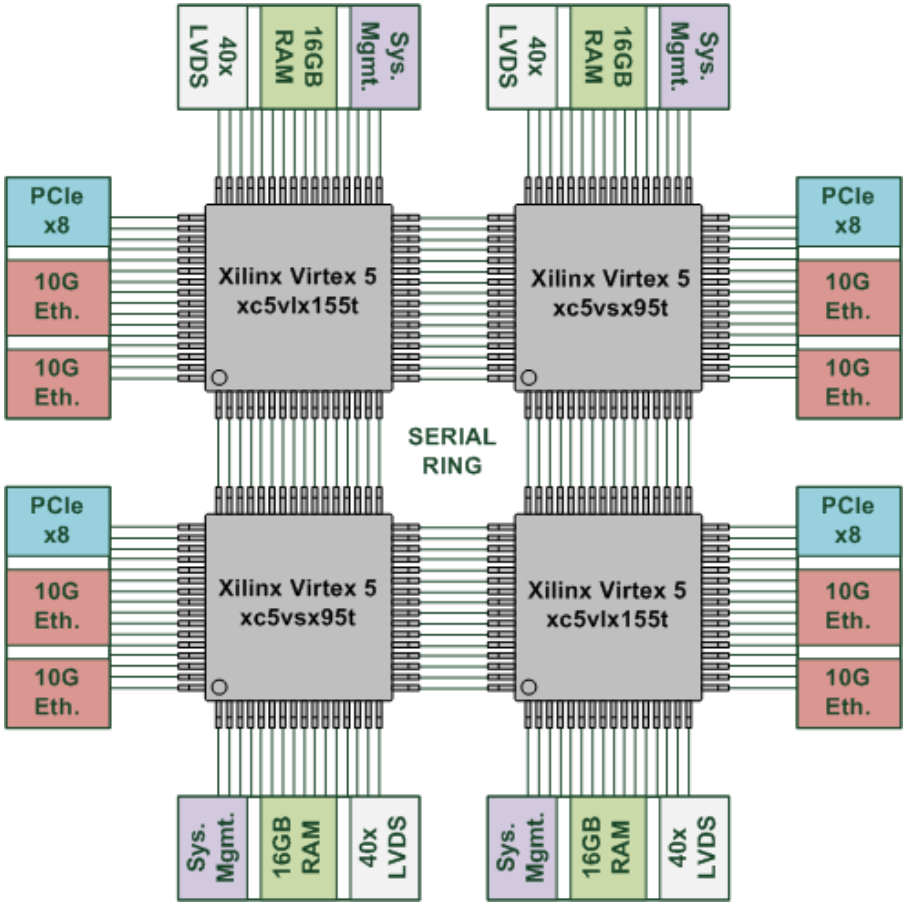
- MalCoBox antwortet auf GET-Anfragen mit vordefinierten Templates
- z.B. Emulation eines WebMail-Service
- Angriffsversuche können aufgezeichnet werden

Hardware

BeeCube BEE3

- 4 x Virtex5-FPGA
- 4 x PCI Express x8
- 8 x 10GBase-CX4 Ethernet
- 4 x 16GB DDR2-RAM





Zusammenfassung

MalCoBox: flexibler Hardware-Honeypot für das Sammeln von Malware

- sicher: keine Manipulation übers Netzwerk möglich (da nur Hardware)
- schnell: Hardwarebeschleunigung -> große Anzahl von Verbindungen bei 10G

Status:

- Basissystem der MalCoBox läuft auf der BEE3 (1 FPGA)
- Malware wird über Netzwerkport an Management-PC übertragen

Nächste Schritte:

- Entwickeln weiterer Vulnerability Emulation Handler (VHDL, Verilog)
- Entwicklung eines PCIe-Treibers für den Transfer der Malware auf die Management-Station sowie erweitertes Logging
- Test des Systems in einer realen Umgebung