

Automated Protection of End-Systems Against Known Attacks

Andreas Hess and Niels Karowski



Telecommunication Networks Group
Technische Universität Berlin

Motivation

- Increasing number of threats:
 - **48%** increase in new malware threats in 2005 over previous year (Sophos annual threat management report)
- Known viruses/attacks still do harm:
 - The Internet worm **Netsky-P**, spotted for the first time in **March 2004**, is still responsible for **15,7%** of all registered virus incidents.
 - **4781 Code Red** worms spotted in **4 days** at TU-Berlin
- Increasing propagation speed of self-distributing attacks (e.g. Slammer, Code Red)

- Need for an **automated protection in the networks**
- Network-based Intrusion Prevention System:
 - Difficulty of **scalability** - network traffic is delayed
 - etc.

Our Approach

Network-based and Intelligent Protection of Networks Against Known Attacks using Programmable Routers

- Creation of an intrusion prevention overlay network:
 - Distributed and demand driven supervision (requires knowledge about the resources to be protected)
 - Efficient operation
 - To block harmful traffic security services must be placed between attacker and potential victim

Why Programmable Routers?

1. Relieves the strain on end-users and administrators of continuously having to deal with security updates and configuration issues
2. No modification of end-systems
3. Ability to evolve over time
4. No single point of failure - attack resistance
5. Allows the intelligent distribution of required intrusion prevention functionalities: better flexibility to cope with today's QoS requirements

Intrusion Prevention System (IPS) - Events

- **Alarm / true positive:**

an IPS correctly identifies an attack which would do harm to the targeted system

- **False positive:**

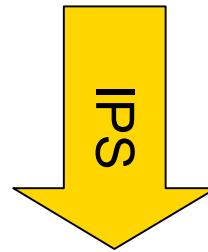
- An IPS thinks that the inspected network traffic belongs to an ongoing attack although current activity is benign
- An IPS correctly identifies an attack but the attack is non-threatening or not applicable to the site

- **False negative:**

a non-event and thus not correlated to an alarm indicating that IPS failed to identify an applicable attack

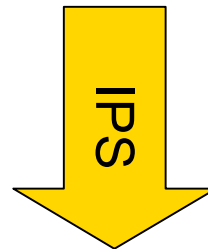
IPS and False Positives

1.) **Benign traffic** is identified as an attack



Legitimate communications are interrupted!

2.) **Non-threatening attack** is identified as an attack



- Increases the number of **non-relevant** alarms
- Reduces the **efficiency** of the IPS

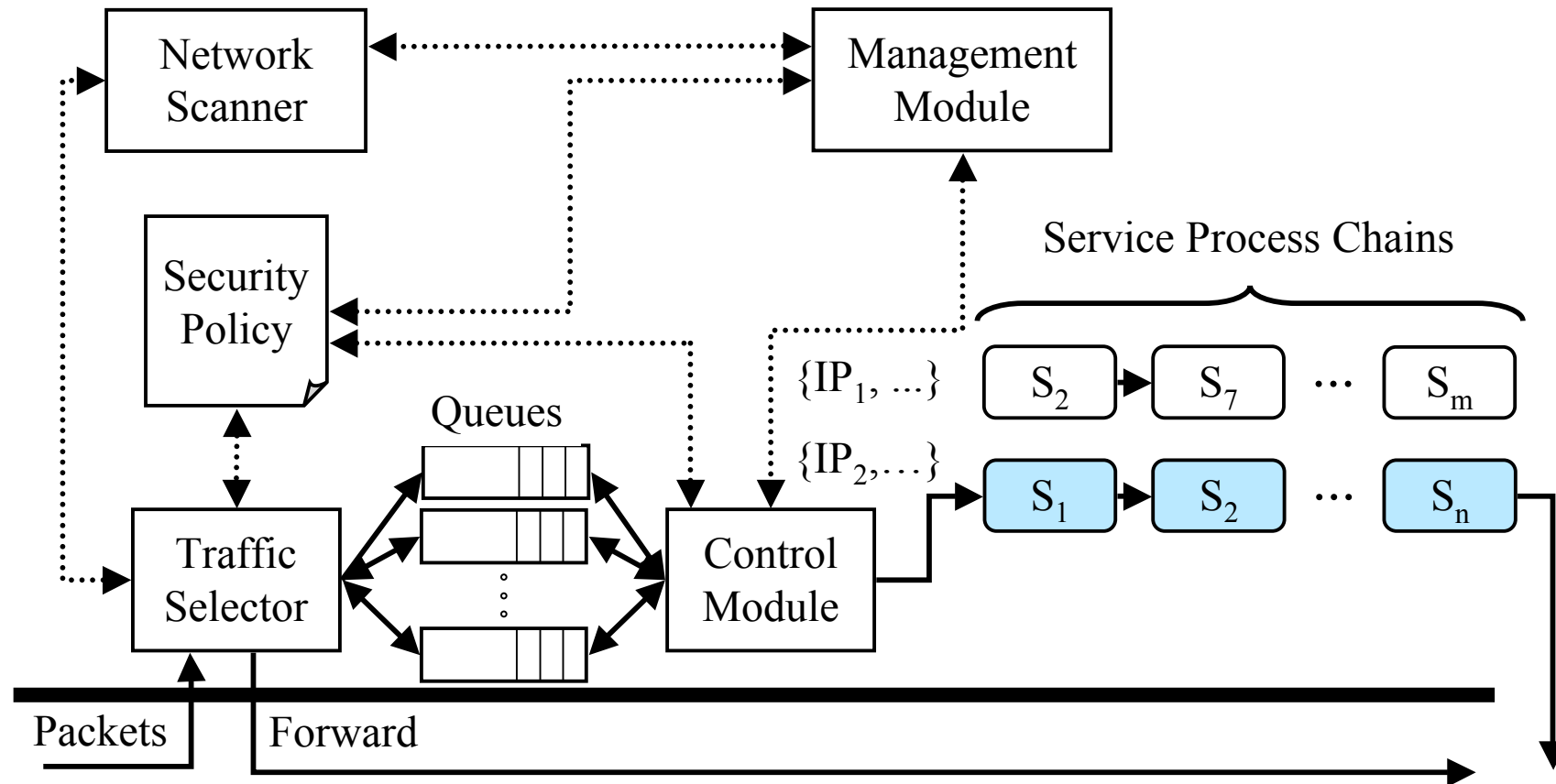
Demand-Driven Intrusion Prevention

- Most attacks require the existence of one or multiple concrete vulnerabilities to succeed:
 - *Code Red* → Buffer Overflow Vulnerability of Microsoft's Internet Information Server (IIS)
 - *Slammer* → Buffer Overflow Vulnerability of Microsoft's SQL Server
- **Approach**: flows to an end-system are only analyzed by intrusion prevention services that protect against attacks that could actually harm it:
 - Reduces the amount of checks to be performed per packet
 - Reduces the false positive rate.

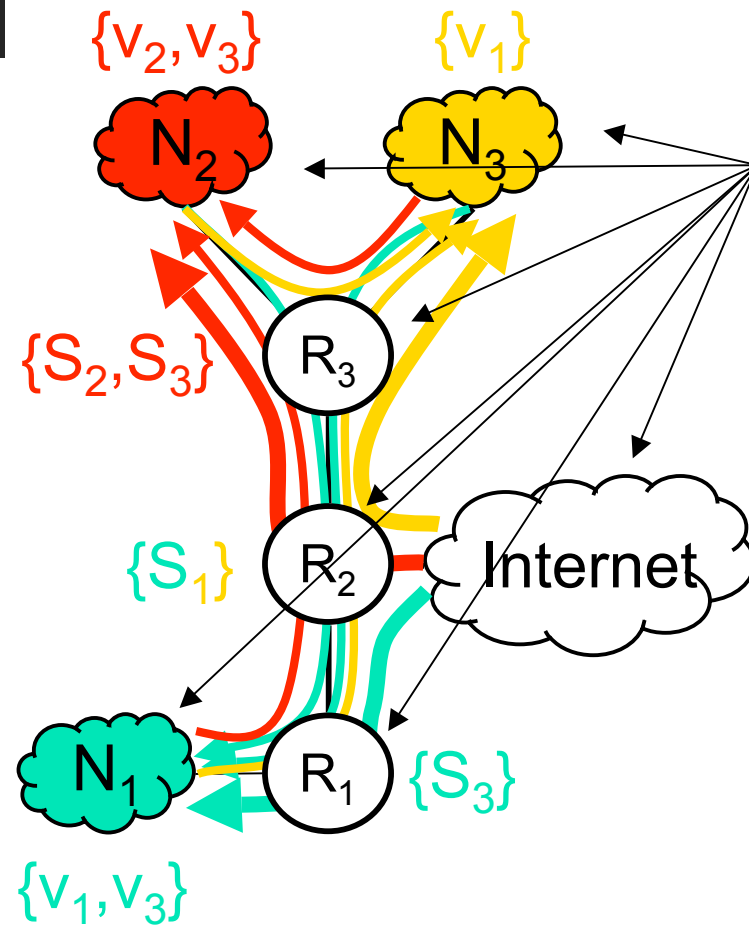
$$1 - \prod_{i=1}^N (1 - p_i), \quad 0 \leq p_i \leq 1$$

IPS Architecture

Flexible **I**ntrusion **D**etection and **R**esponse system
on **A**ctive **N**etworks



An Example Scenario



Identification of the IP topology

Identification of the vulnerabilities

Measurement of traffic loads

Calculation of optimal security service distribution

Configuration of nodes

Gathering Vulnerability Knowledge

Active Scanning	Passive Fingerprinting	Cooperation
<p data-bbox="376 517 875 691">Sending of specifically crafted packets (non-intrusive/intrusive)</p> <p data-bbox="443 743 875 959">Knowledge of the network is as current as the latest scan</p> <p data-bbox="443 1042 808 1155">Regularly and on on-demand</p>	<p data-bbox="958 580 1384 628">Sniffing the network</p> <p data-bbox="1066 826 1279 874">Duration?</p> <p data-bbox="920 1023 1420 1177">Continuously to identify new destination addresses</p>	<p data-bbox="1532 523 1906 683">Providing the information to the analysis tool</p> <p data-bbox="1509 799 1928 900">Requires a consent with users!</p>

Creation of Security Services

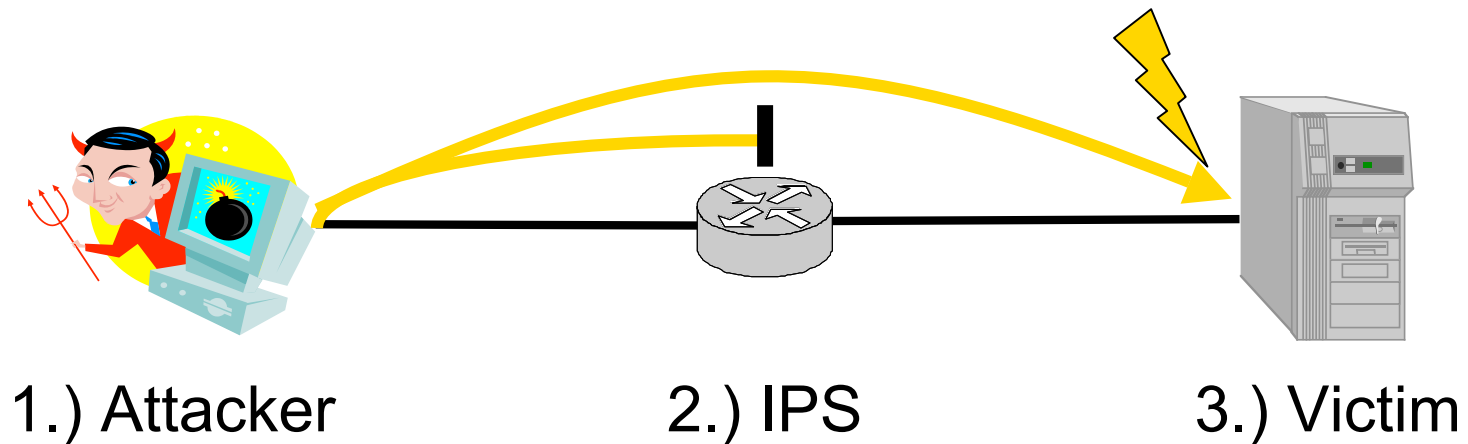
A security service provides protection against attacks exploiting a concrete vulnerability.

Identification of vulnerabilities:

- The Common Vulnerabilities and Exposures List (CVE)
 - MS-Security Bulletin ID (vulnerabilities related to Microsoft)
 - Bugtraq-ID (BID)
 - Information Assurance Vulnerability Alert (IAVA)
 - ...
- ➔ None of them is exhaustive!
- ➔ How to assess the risk of a vulnerability?

A Case Study

- **Attacker:** Metasploit-framework
- **Fidran:**
 - Nessus-3.02
 - Security services based on Snort attack signature database
 - CVE-specific intrusion prevention services
 - Application-specific intrusion prevention services
- **Victim:** Windows-XP, SP1, IIS



19 CVE-vulnerabilities and 1 other:

- CVE-2003-0717: Messenger Service
- CVE-2003-0818: ASN.1 parsing vulnerabilities
- CVE-2003-0715, CVE-2003-0528, CVE-2003-0605: RPC interface buffer overrun (exploited by Blaster)

→ Multiple CVE-specific IPS services contain the same set of attack signatures

→ In total 11 security services

→ Reduction of attack signatures (886 to 2 for CVE-2003-0715 ...)

→ But: No protection of vulnerable LSASS service possible

Discussion

The quality of the protection is limited by the availability of adequate protection mechanisms and the capability of the network scanner to accurately identify security holes.

False negative: the scanner fails to identify security holes. An active scanner is only able to identify vulnerabilities that are connected to a port.

→ No protection!

False positive: the scanner identifies non-existing vulnerabilities

→ Installation of superfluous intrusion prevention services

!Need for a Standardized Vulnerability Reporting!

▪ **Future:** Vulnerability Signatures allows an exact matching between vulnerabilities and attacks!