Intrusion Detection / Prevention Systems

HISTORY – DEFINITION - CLASSIFICATION

Learning outcome

- LO1: Understand how a generic intrusion detection system (by Dorothy Denning) works [1]
- LO2: Recognize anomaly intrusion detection and misuse intrusion detection [1]
- LO3: Recognize insertion, evasion and denial of service attacks against IDS [2,3]
- LO4: Tell difference between IPS and IDS

Further reading

1. Kumar, S., & Spafford, E. H. (1994). An application of pattern matching in intrusion detection: read section 3.1, 3.2, 3.11
2. Ptacek, T. H., & Newsham, T. N. (1998). *Insertion, evasion, and denial of service: Eluding network intrusion detection*. Secure Networks inc Calgary Alberta.: read section 2.2, 3.1, 3.2, 3.3
3. Stephen Northcutt, Judy Novak. Network Intrusion Detection, Third Edition. Sams Publishing 2002 : read chapter 8, page 147-150

What is network intrusion and examples?

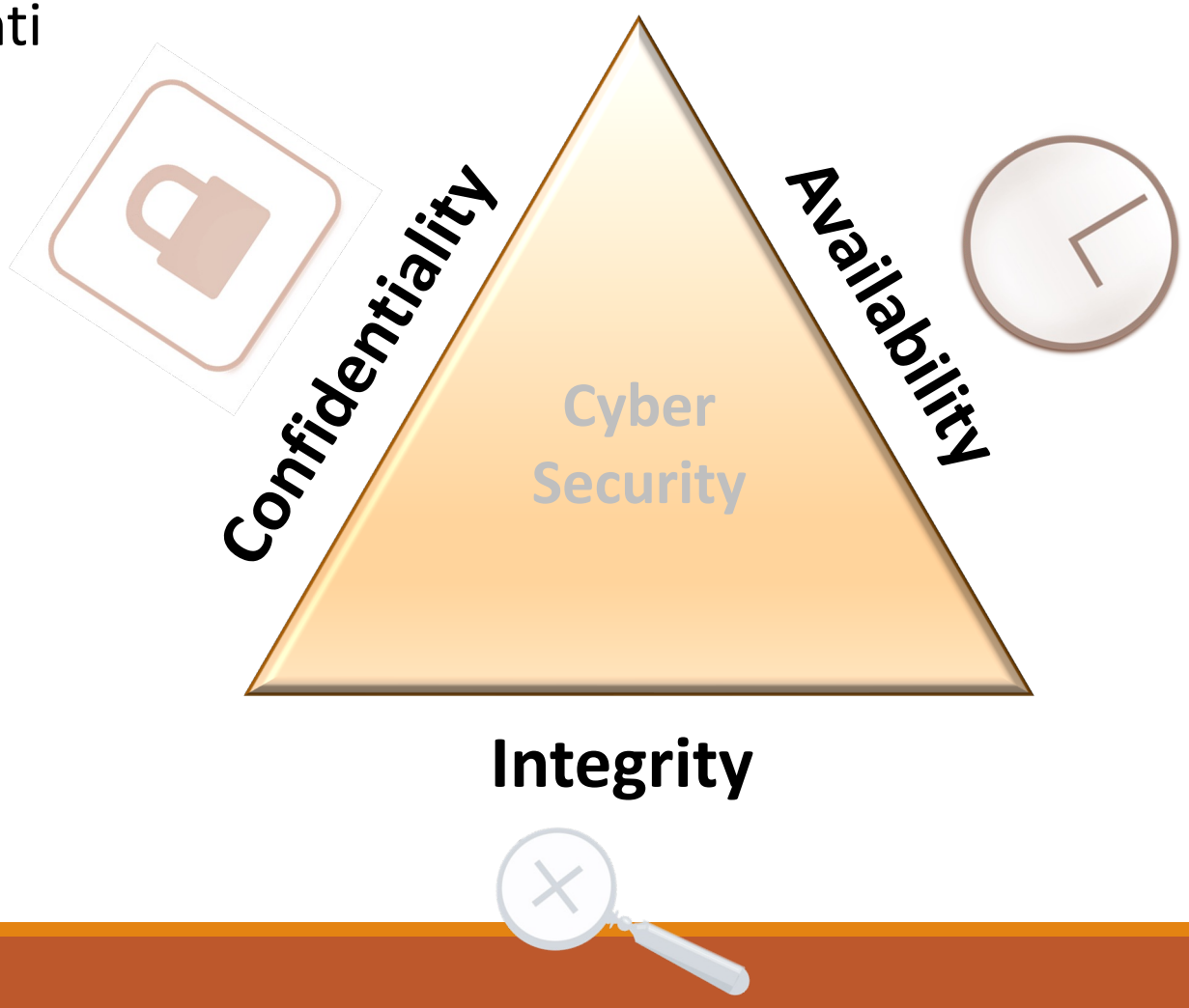
Google

menti

Cybersecurity requirements

The CIA triad

menti



Example

An ATM has tools that cover all three principles of the triad:

- It provides **confidentiality** by requiring two-factor authentication (both a physical card and a PIN code) before allowing access to data
- The ATM and bank software enforce data **integrity** by ensuring that any transfers or withdrawals made via the machine are reflected in the accounting for the user's bank account
- The machine provides **availability** because it's in a public place and is accessible even when the bank branch is closed

CIA triad - Example 1

- Menti,
- Identify which principle in CIA triad address the following loss:

“A rejected contract programmer, intent on sabotage, removed the name of a data file from the file directories in a credit union’s computer. Users of the computer and the data file no longer had the file available to them because the computer operating system recognizes the existence of information available for users only if it is named in the file directories. The credit union was shut down for two weeks while another programmer was brought in to find and correct the problem so that the file would be available. The perpetrator was eventually convicted of computer crime.” [Source: “Toward a new framework for information security”]

CIA triad - Example 2

- Menti
- Identify which principle in CIA triad address the following loss:

“We have discovered that between April 17 and April 19, 2011, certain PlayStation Network and Qriocity service user account information was compromised in connection with an illegal and unauthorized intrusion into our network.

Although we are still investigating the details of this incident, we believe that an unauthorized person has obtained the following information that you provided: name, address (city, state, zip), country, email address, birthdate, PlayStation Network/Qriocity password and login, and handle/PSN online ID....”

CIA triad - Example 3

- Menti
- Identify which principle in CIA triad address the following loss:

In 2016, the hackers breached the systems of the World Anti-Doping Agency and released the medical data of many famous athletes. However, investigators discovered that much of this data was altered before release. [Source: https://www.zettaset.com/blog/data-integrity-attacks-data-manipulation-more-dangerous]

Intrusion attempt

Deliberate unauthorized attempt to:

- access information (confidentiality)
- manipulate information (integrity)
- render a system unreliable or unusable (availability)

History of Intrusion Detection

1980

James P. Anderson

- Automated audit trail review
- Automated collection of information for review by security personnel
- Reduction of irrelevant records

1987

Dorothy Denning

- Generic Intrusion Detection Model

Setting the Scene

- “Greater reliance on the computer as a data processing and decision making tool in sensitive functional areas”
- “ … the need to realize economies by consolidating ADP resources thereby integrating or co-locating previously separate data processing operations” (ADP is automatic data processing)
- “ … the emergence of complex resource sharing computer systems providing users with capabilities for sharing data and processes with other users”
- “ … the extension of resource sharing concepts to networks of computers”
- “ .. The slowly growing recognition of security inadequacies of currently available computer systems”
- “Most of the efforts to date to provide computer security have been centred in environments where all persons coming in contact with the systems share a common clearance … effort has been directed to providing procedural controls … and proper marking of information found in the system.”

James P. Anderson “Computer Security Technology Planning Study” Oct 1972

Assumption

Exploitation of a system's vulnerabilities involves abnormal use of the system; therefore, security violations could be detected from abnormal patterns of system usage.

Ref: Dorothy Denning

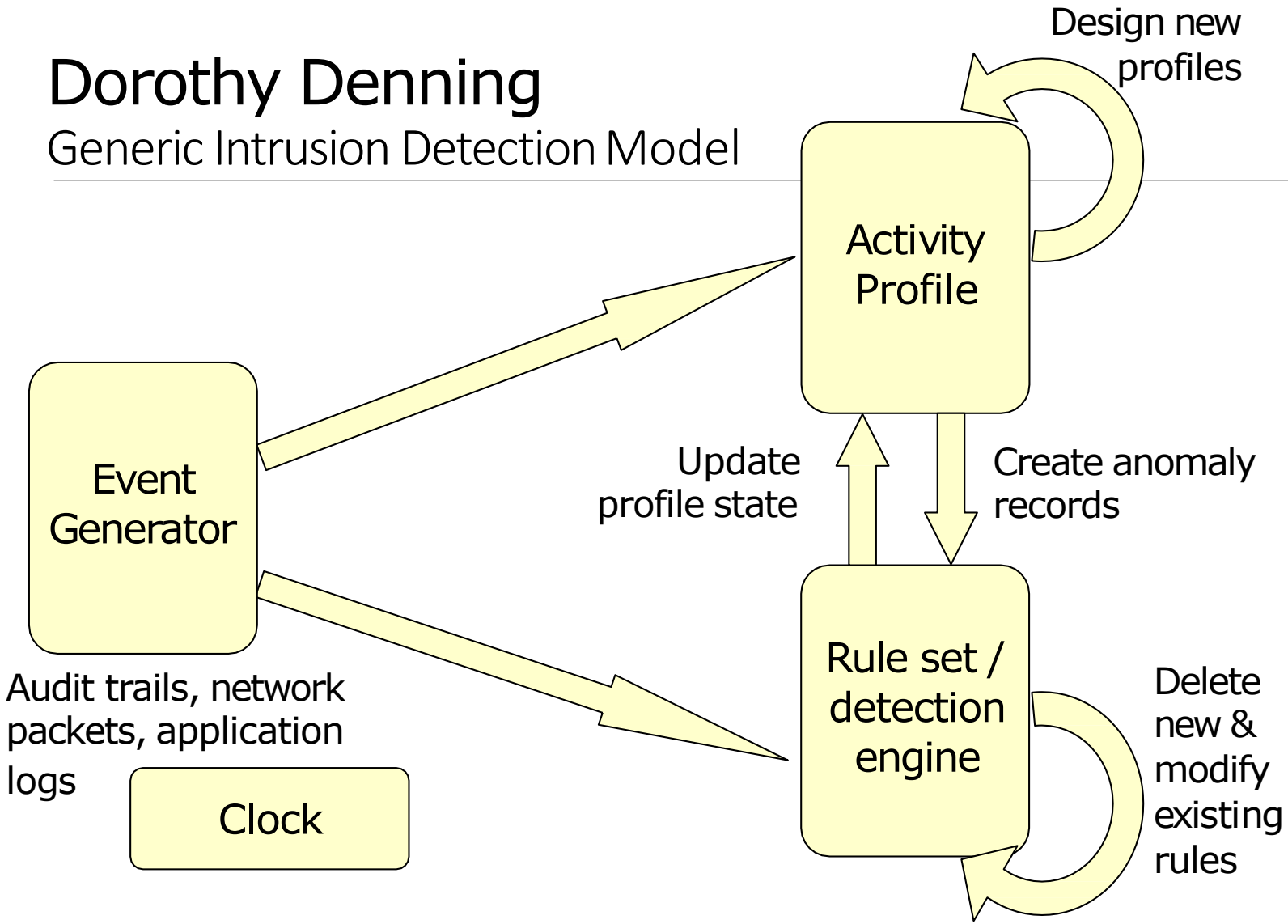
Example

menti

1. Someone attempting to break into a system might generate an abnormally high rate of password failures with respect to a single account or the system as a whole.
2. Someone logging into a system through an unauthorized account and password might have a different login time, location, or connection type from that of the account's legitimate user.
3. Intruder might spend most of his time browsing through directories and executing system status commands, whereas the legitimate user might concentrate on editing or compiling and linking programs.

Dorothy Denning

Generic Intrusion Detection Model



Source: section 3.11, Kumar, Sandeep, and Eugene H. Spafford. "An application of pattern matching in intrusion detection." (1994).

Design a generic IDS to detect

(menti) Ex1: Someone attempting to break into a system might generate an abnormally high rate of password failures with respect to a single account or the system as a whole.

Ex2: Someone logging into a system through an unauthorized account and password might have a different login time, location, or connection type from that of the account's legitimate user.

(menti) Ex3: Intruder might spend most of his time browsing through directories and executing system status commands, whereas the legitimate user might concentrate on editing or compiling and linking programs.

Example 1: Someone attempting to break into a system might generate an abnormally high rate of password failures with respect to a single account or the system as a whole.

1. Event: (date time, subject (account), log in , which system)

(28/2/22 7am, Alice, log in, database D): fail

(28/2/22 7.05am, Alice, log in, database D): fail

(28/2/22 7.30am, Alice, log in, database D): fail

(28/2/22 8.00am, Alice, log in, databased D): fail

…

(Event generator: logging system of the database management system)

2. Activity profile:

(subject (account), log in, which system, the number of password failure)

(Alice, log in, database D, 3 times failed)

3. Rule set/ detection engine

If fail log in over 3 times, send a notification to the administrator

At 7.30: Receive: (Alice, log in, database D, 3 times failed) -> no action

At 8: receive (Alice, log in, database D, 4 times failed) -> sends a notification to the administrator

Update rule: If fail log in over 4 times in the evening, send a notification to the administrator

-> change in activity profile

(subject (account), log in, which system, the number of password failure in the evening)

Example 2: Someone logging into a system through an unauthorized account and password might have a different login time, location, or connection type from that of the account's legitimate user

Event: (subject (who logs in), object (which system), log in, date time, location, connection type)

Example: (Alice, Microsoft active directory, log in, 11pm, server room, wired connection)

(Alice, Microsoft active directory, log in, 1am, office room, wireless connection)

Activity profile: : (subject (who logs in), object (which system), log in, date time, location, connection type, role of the subject)

Rule: If non-administrator accesses the server room, it may be an intrusion attempt -> send notification to the network administrator

What is an Intrusion Detection System (IDS)?

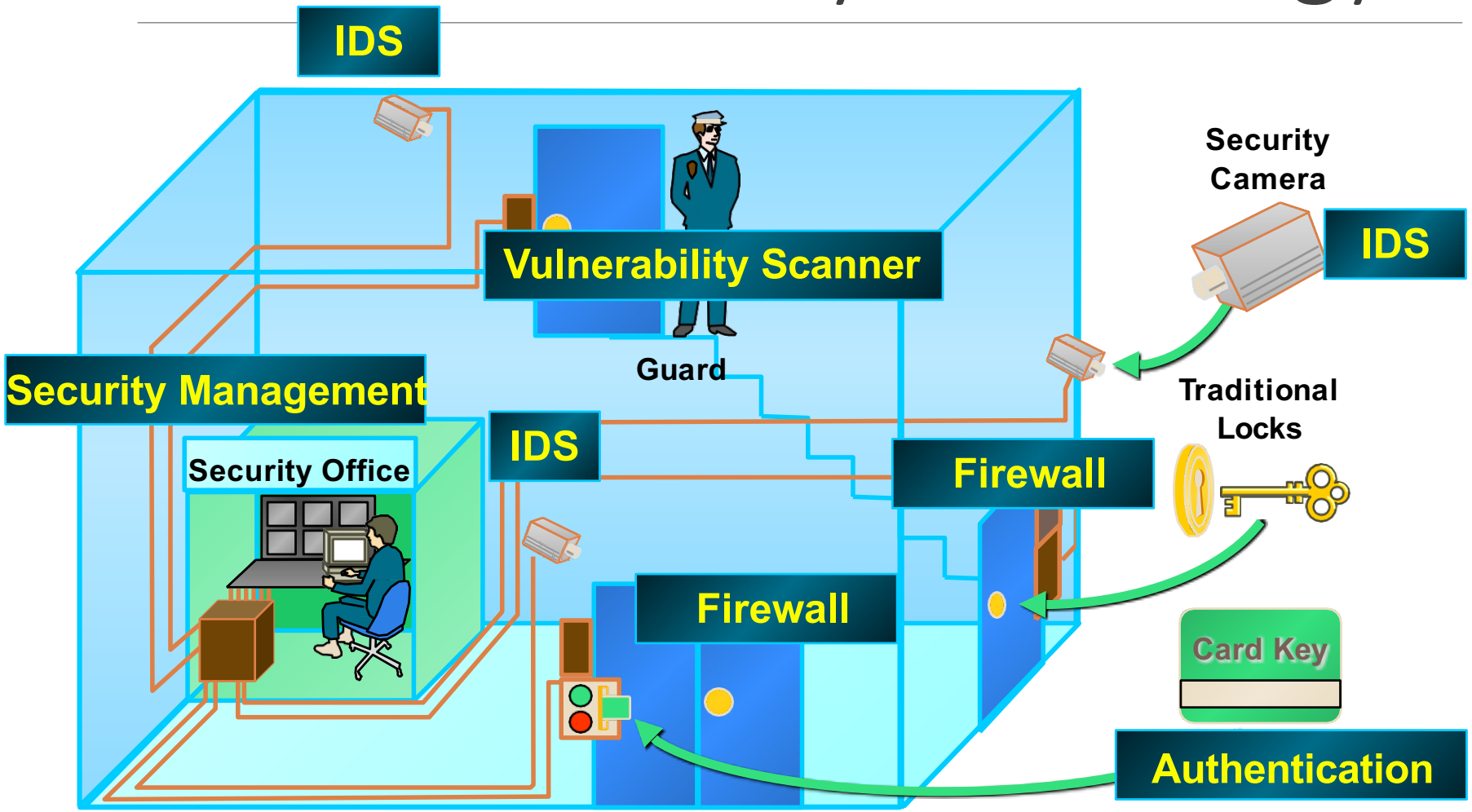




Intrusion Detection System (IDS) is a software or hardware product that monitors the events occurring in a computer system or network and analyses them for signs of intrusions

Intrusions are defined as attempts to compromise the confidentiality, integrity, availability, or to bypass the security mechanisms of a host or network.

Network Security: An analogy



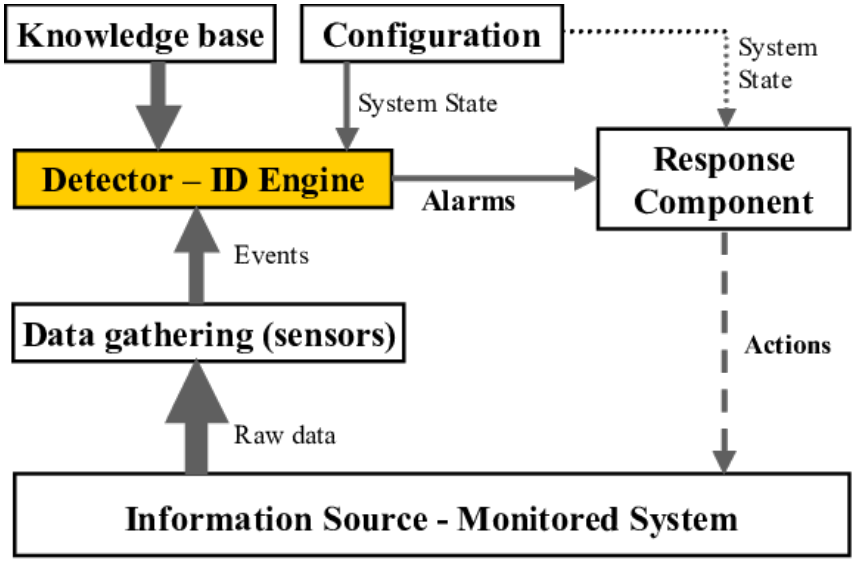
IDS Classification

IDS can be classified according to three factors:

the source from which they collect data for analysis.

the detection mechanism by which the collected data is then analysed in order to detect potential intrusions.

the response mechanisms which are triggered as a result of generated alerts



Types of IDSs

Host-based IDS (HIDS)

Utilizes two types of information sources, operating system audit trails, and system logs

Network-based IDS (NIDS)

Examines network traffic. Often consist of single purpose sensors that run in stealth mode

Hybrid IDS

Combines two or more of the sources above

Which threats can HIDS or NIDS identify?

menti

NIDS in broadcast network

Broadcast networks: the information packets are broadcast to everyone on that portion of the network, and only the intended recipient copies them off the network and responds.

The intrusion detection device can be located on a segment and passively "sniff' traffic involving all hosts on the subnet to look for attack signatures

Sensor S 1 operates on the uplink to the remainder of the network. Sensors S2 and S3 monitor all traffic broadcast on their respective legs of the network.

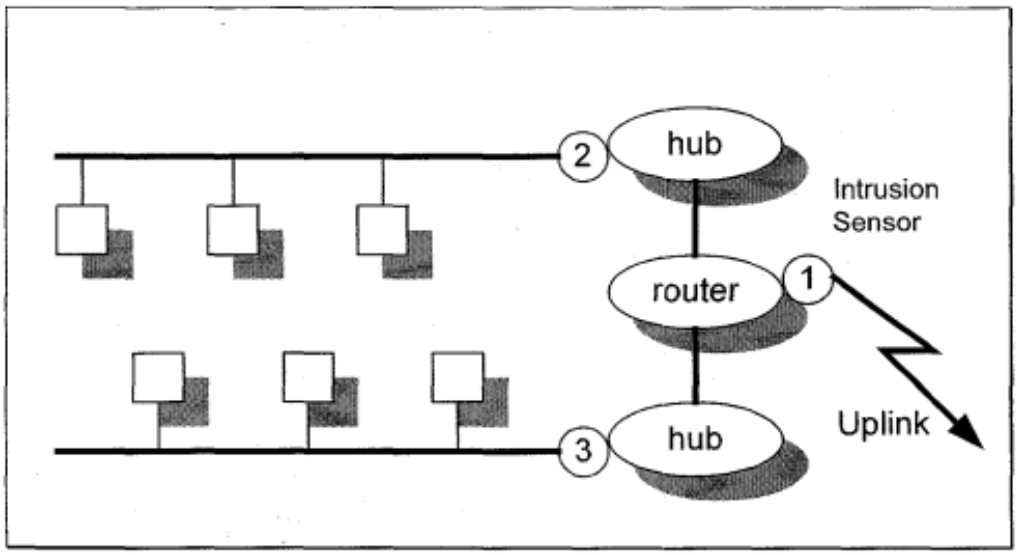


Figure 3: Broadcast network, with intrusion sensors

Source: Tarman, T. D., & Witzke, E. L. (2001, February). Intrusion detection considerations for switched networks. In *Enabling Technologies for Law Enforcement and Security* (Vol. 4232, pp. 85-92). SPIE.16

NIDS in switched network

Switched networks (such as ATM) use point-to-point physical connections between switches and end systems to deliver information packets directly to the destination

Sensor S1 operates on the link from this sub-net to the remainder of the network. Sensors S2, S3, S4, and S7 monitor links between switches. Sensors S5, S6, and S8 monitor links between switches and particular end systems

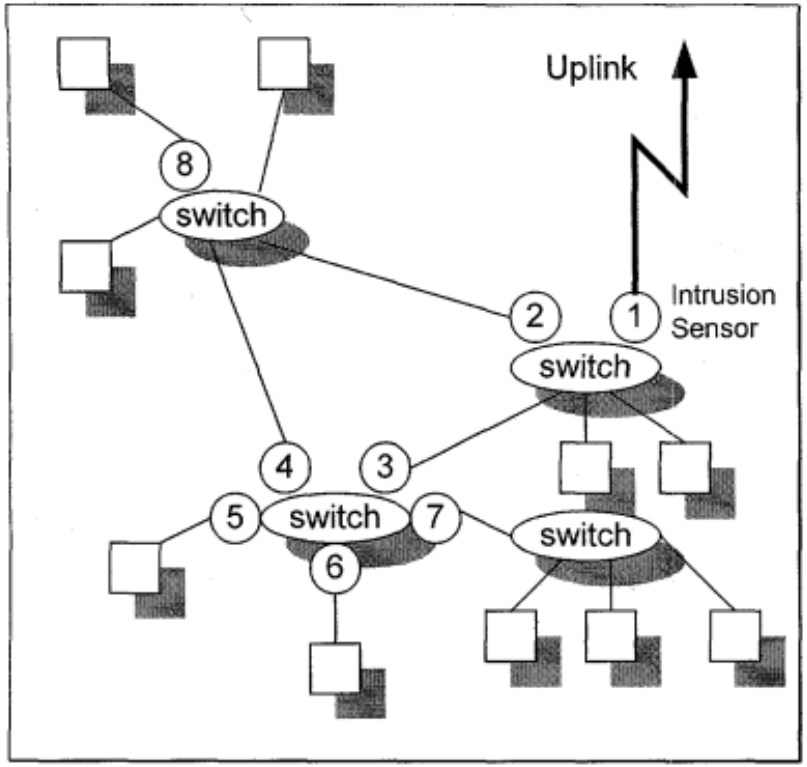
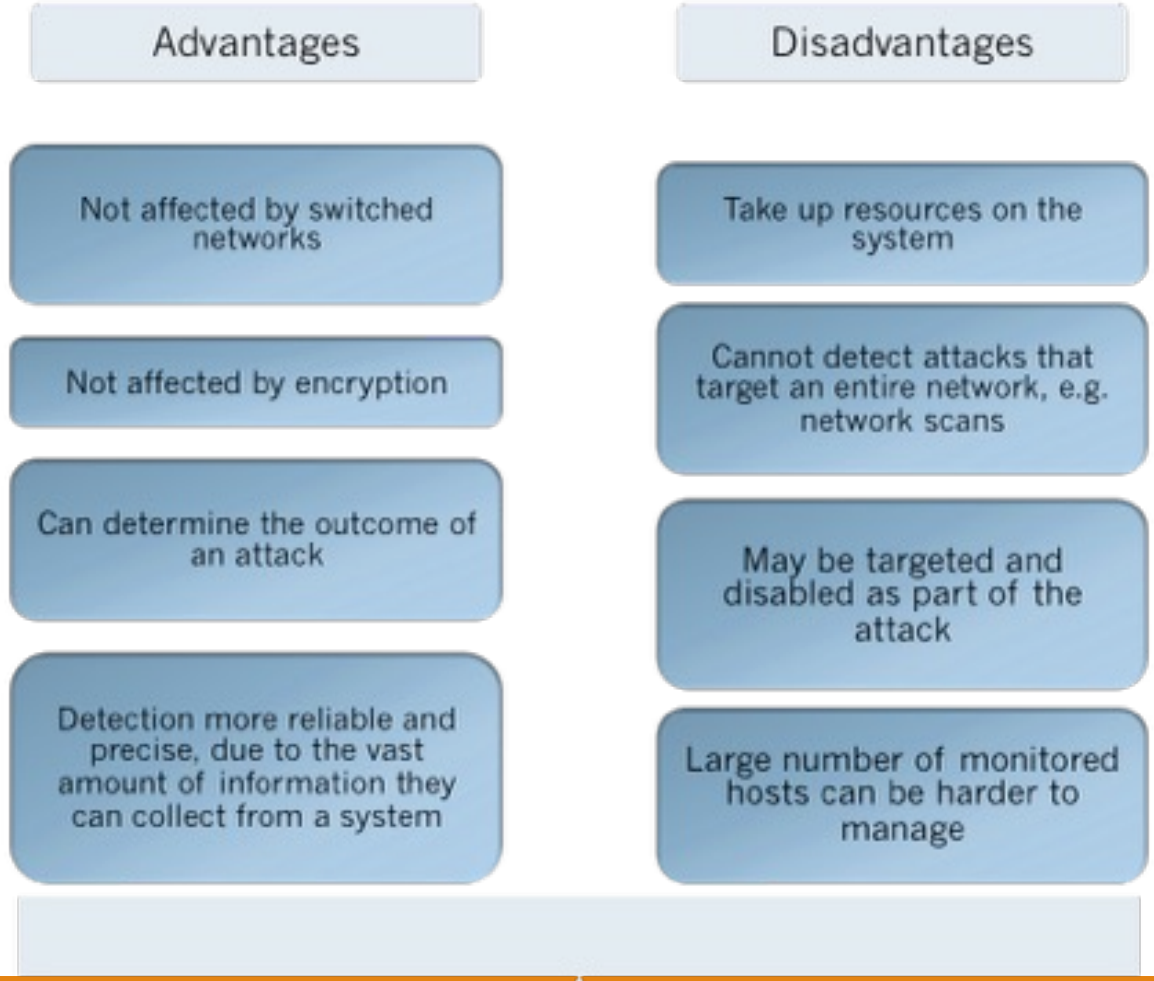


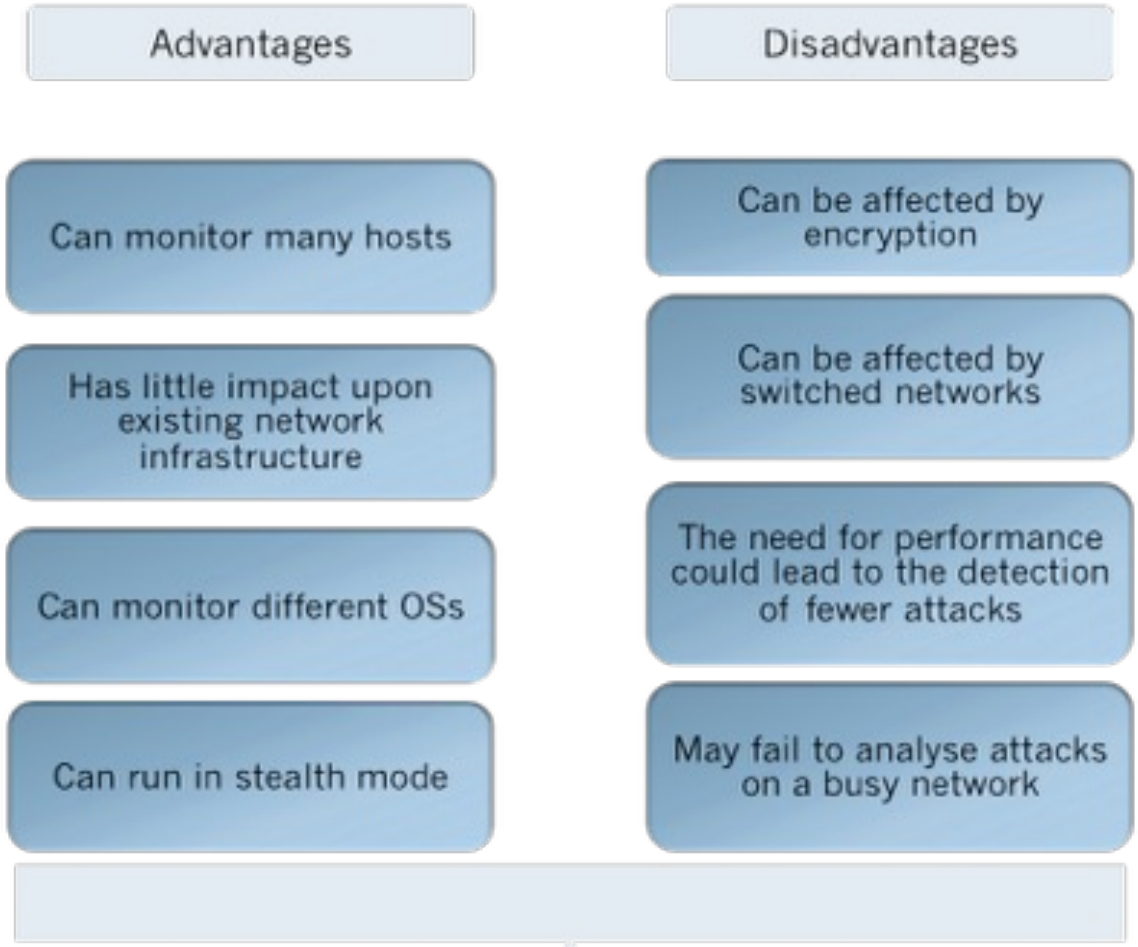
Figure 2: Switched network, with intrusion detection

Source: Tarman, T. D., & Witzke, E. L. (2001, February). Intrusion detection considerations for switched networks. In *Enabling Technologies for Law Enforcement and Security* (Vol. 4232, pp. 85-92). SPIE.16

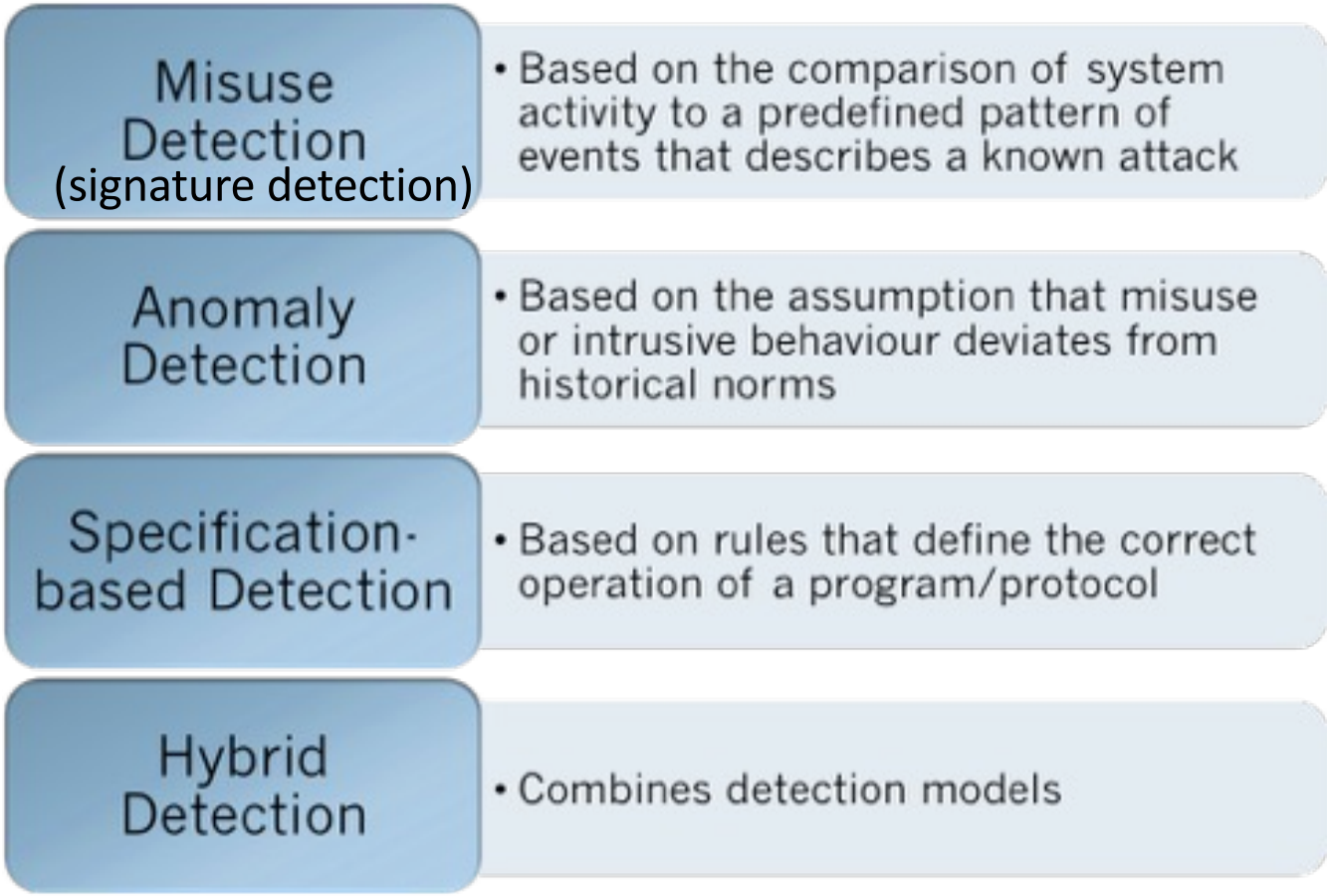
Host-based IDS (HIDS)



Network-based IDS (NIDS)



Detection Methods



Misuse or anomaly detection

Menti

Example 1: Suppose a particular user typically logs in around 10 a.m., reads mail, performs database transactions, takes a break between noon and 1 p.m., has very few file access errors, and so on. If the system notices that this same user logs in at 3 a.m., starts using compilers and debugging tools, and has numerous file access errors, it will flag this activity as suspicious.

Example 2: A system contains attack descriptions (or “signatures”) and match them against the audit data stream, looking for evidence of known attacks. One such attack, for example, would occur if someone created a symbolic link to a Unix system’s password file and executed a privileged application that accesses the symbolic link. If the system notices, it will flag this activity as suspicious.

Which can misuse/anomaly detection identify?

menti

Detection Comparisons

Anomaly Detection
☒Prone to false alarms
☒Often require extensive training periods
☑ Can often detect new and not previously known attacks
☑ Can serve as source of information for misuse detectors

Misuse Detection
☑Better at detecting attacks without generating overwhelming number of false alarms
☑Do not require training
☒Must be updated with signatures of new attacks
☒Could fail to detect variants of already defined attacks

Response Mechanisms

Passive

Aim to notify other parties about the occurrence of an incident, and then rely on them to take further action

E.g. Alert administrator/SSO via email, pop-up window, pager, SMS, report to central network management console via SNMP traps

Most IDSs support these options

Active

Aim to counter the incident that has occurred

Active or passive response

menti

Improving Detection

INSERTION – EVASION – DENIAL OF SERVICE-OBFUSCATION

Can detection be defeated?

How can you fool a network IDS and avoid detection?

Insertion: IDS accepts a packet that the destination rejects

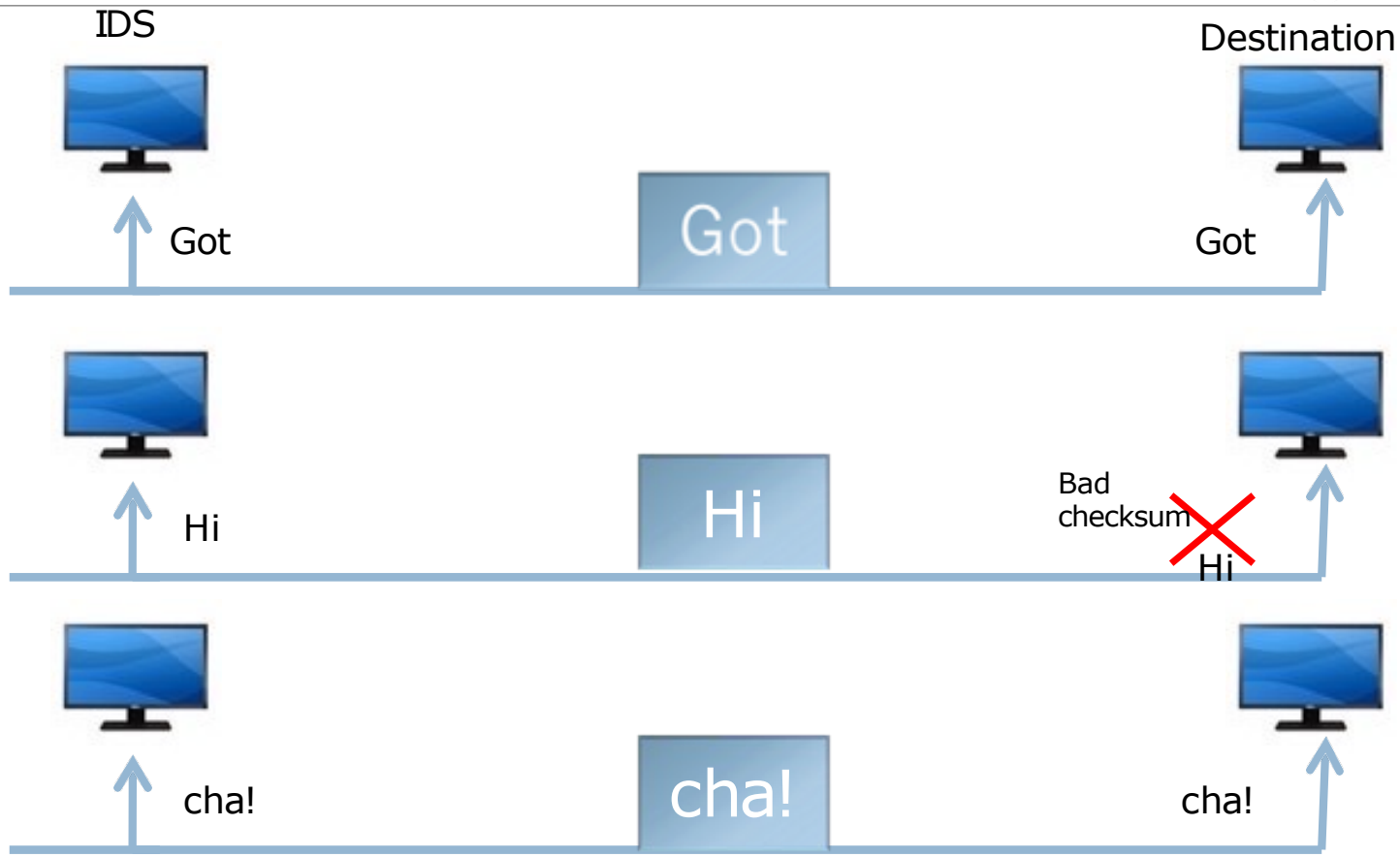
Evasion: Destination host accepts a packet that the IDS rejects

Denial of Service: The IDS is overwhelmed with traffic and is unable to analyse new packets

Source: Stephen Northcutt, Judy Novak - Network Intrusion Detection (2002, Sams), chapter 8, Insertion and Invasion attacks; or

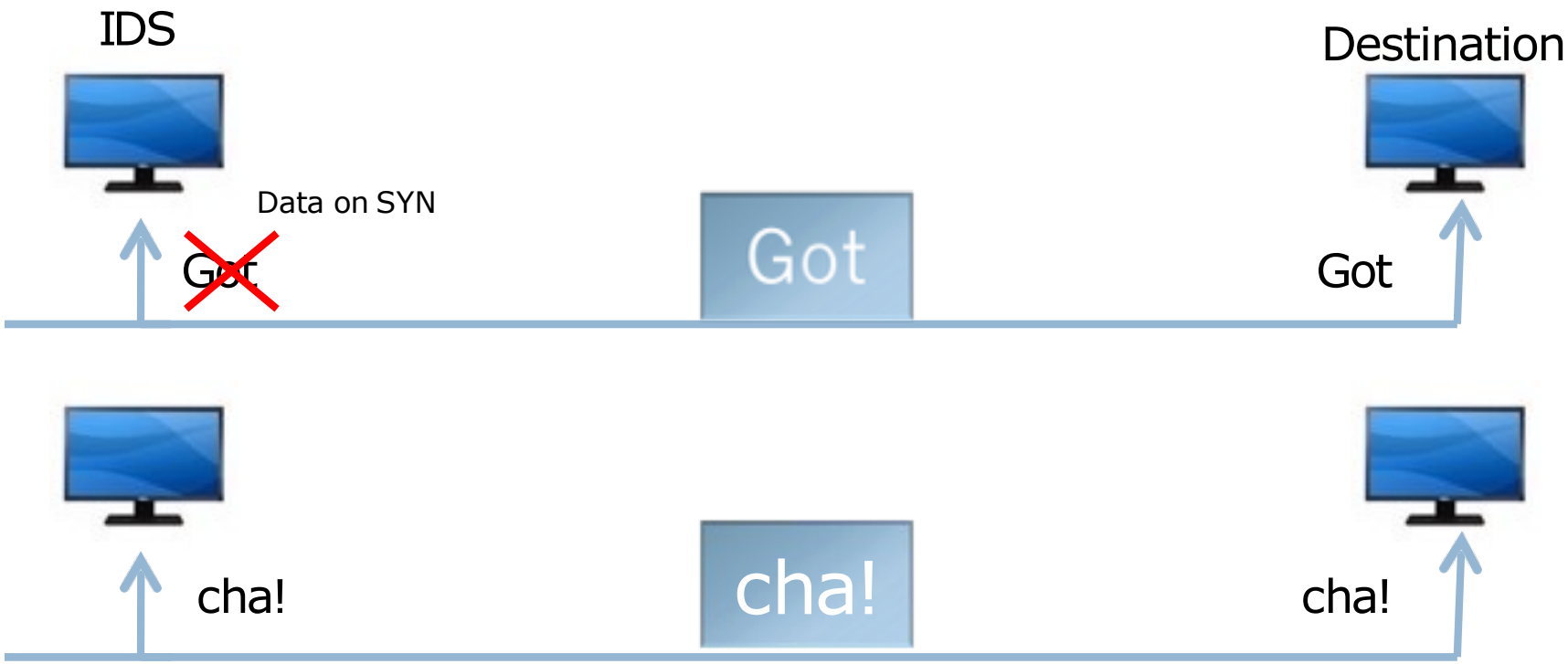
"Insertion, Evasion and Denial of Service", paper by Ptacek, Newsham (1998)

Insertion



IDS sees: GotHicha!
Destination sees: Gotcha!

Evasion

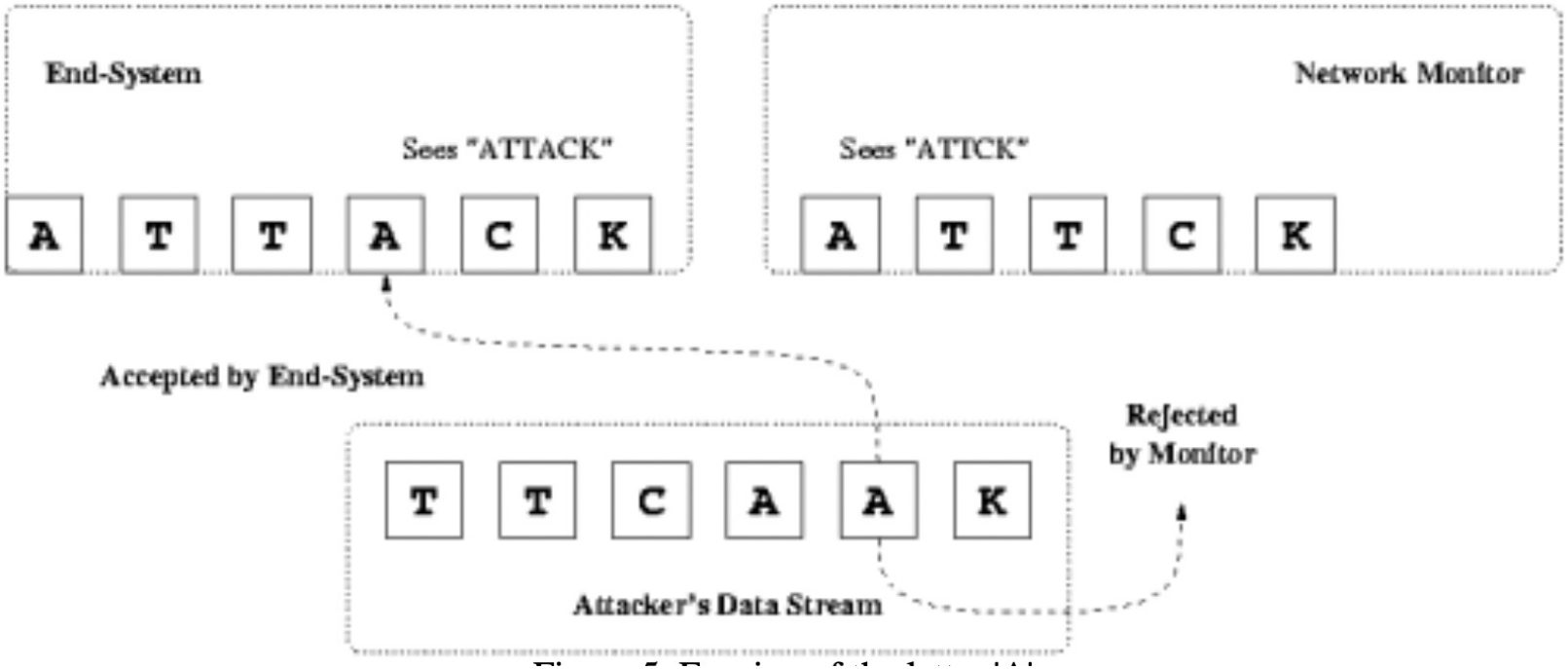


IDS sees: cha!
Destination sees: Gotcha!

What type of attack?

Menti

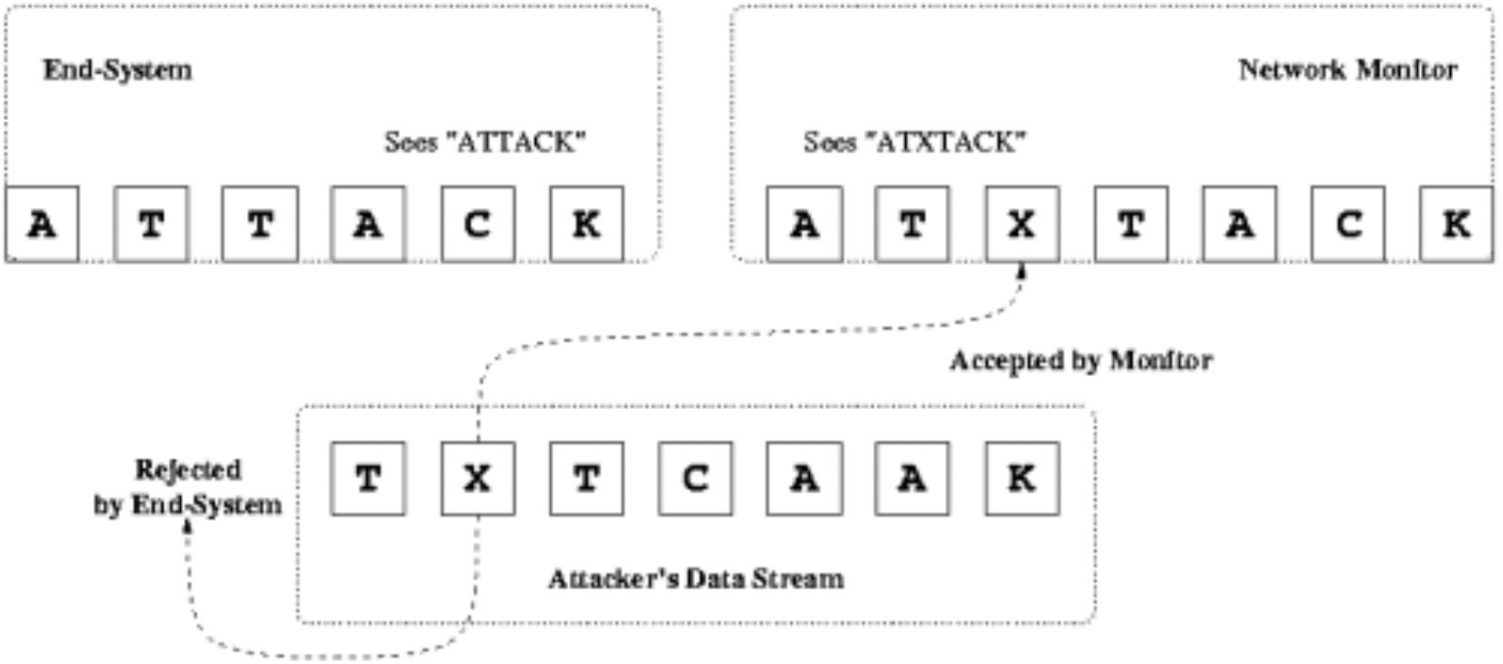
Example 1



What type of attack

Menti

Example 2



What type of attack

Menti

Example 3

“The attacker used several networks to spoof 167 Mpps (millions of packets per second) to 180,000 exposed CLDAP, DNS, and SMTP servers, which would then send large responses to us.”

String Obfuscation

Obfuscating strings at application level

For example, all the URLs below are the same

http://www.plymouth.ac.uk/cgi-bin/phf

http://www.plymouth.ac.uk/cgi-bin/./phf

http://www.plymouth.ac.uk/cgi-bin%63%67%69%2d%62%69%6e/phf

http://www.plymouth.ac.uk//cgi-bin//phf

If the IDS cannot decode protocols, it can be evaded

String Obfuscation Example

Code exploit (javascript)

```
var launcher = new ActiveXObject("WScript.Shell");
launcher.Run("C:\malware.exe");
```

IDS detection rule

```
alert tcp any any -> any 80 (content: "WScript.Shell"; content:
".Run|22|malware.exe"; distance: 0; within 100; msg: "malware.exe executed by
javascript";)
```

Deceive IDS by string obfuscation

String concatenation

```
var a = "cript.Sh";
var b = ".e";
var launcher = new ActiveXObject("WS" + a + "ell");
launcher.Run("C:\mal" + "ware" + b + "xe");
```

String Obfuscation Example

Deceive IDS by string obfuscation

String replacement

```
var launcher = new ActiveXObject("WxxSxcxrxixpxtx.xSxhxexlxlx".replace(/x/g,
""));
launcher.Run("C:\mGlwGrP.PxP".replace(/G/g, "a").replace(/P/g, "e")) ;
```

String encoding

```
var hexString = "x57x53x63x72x69x70x74x2ex53x68x65x6cx6c";
var octString = "1037213413415514115416714116214556145170145"
var launcher = new ActiveXObject(hexString);
launcher.Run(octString);
```

Find 1 evasion technique

Read
https://nmap.org/book/man-bypass-firewalls-ids.html
https://medium.com/@IamLucif3r/top-10-firewall-ids-evasion-techniques-cb1e1cc06f24

menti

Intrusion Prevention Systems

COUNTERING – TERMINATING – NIPS – HIPS

Automated responses

Automated response is increasingly important in order to cope with modern IT environments

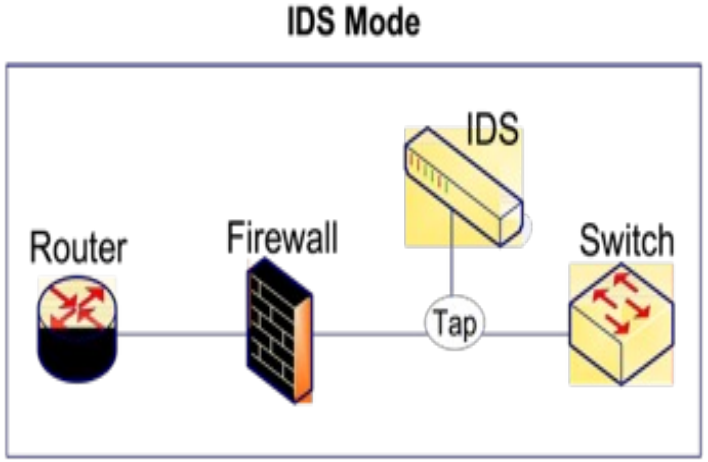
Large systems can receive a large number of attacks

Implementing automated response solutions is far from perfect

Countering intrusions

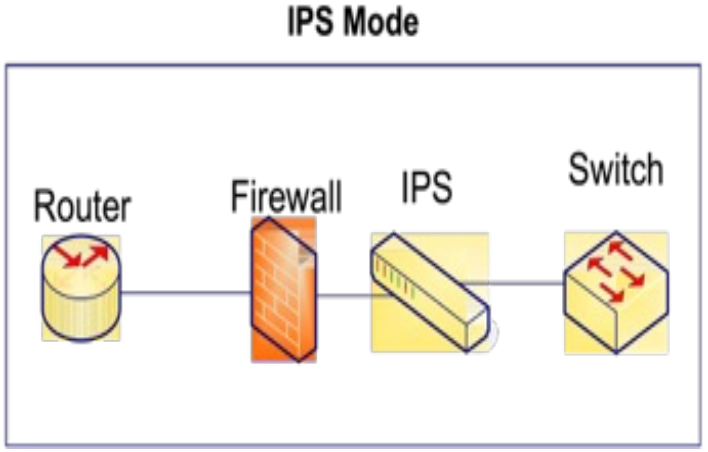
Intrusion Detection Systems (IDS)

- Monitor networks, looking for indications of malicious activity
- Have mainly passive responses



Intrusion Prevention Systems (IPS)

- Positioned inline
- Can respond in real-time
- Proactively block detected attacks



Network-based Intrusion Prevention Systems (NIPS)

Content-based IPS

- Can be thought of as the intersection of firewall with IDS capabilities
- Like firewalls, it uses at least 2 network interfaces (internal, external)
  - Packets appearing at either interface are passed to the detection engine
  - Malicious packets and subsequent traffic are discarded
  - Acceptable packets are forwarded to the second interface

Rate-based IPS

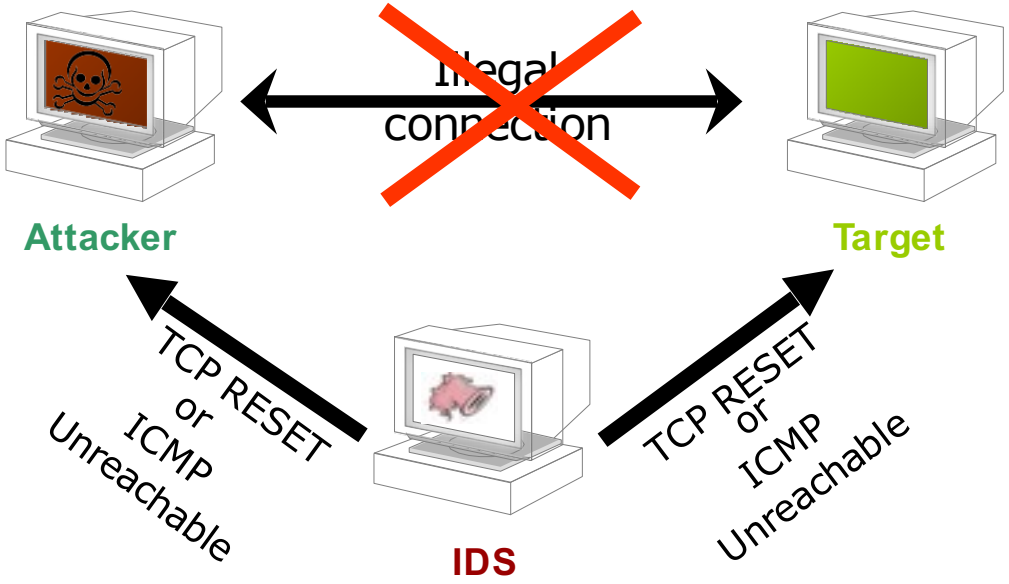
- Also known as Attack Mitigators
- Monitor traffic flows instead of packet content
- Look for anomalies that could indicate Denial of Service attacks (DoS, DDoS) or scan attempts

Source" Fuchsberger, Andreas. "Intrusion detection systems and intrusion prevention systems." *Information Security Technical Report* 10.3 (2005): 134-139.

Terminating a Session

An IDS can terminate a session by sending TCP RESET or ICMP Unreachable error messages to one or both ends of a session

An IPS can **block** the attack before it reaches its destination



Network-based Intrusion Prevention Systems (NIPS)

Advantages

- ☑ Can prevent attacks before they reach their destination
- ☑ Easier to manage than HIPS

Disadvantages

- ☒ Requires careful planning, as it can have significant impact on existing network infrastructure
- ☒ Can be targeted as part of an attack

Host-based Intrusion Prevention Systems (HIPS)

Operate above the OS kernel and services

Intercept all requests to the system

Monitor all system-API calls and block the ones that would result in malicious behaviour

Usually incorporate application-level protection by inspecting data streams and the environment specific to an application (e.g. web server)

Host-based Intrusion Prevention Systems (HIPS)

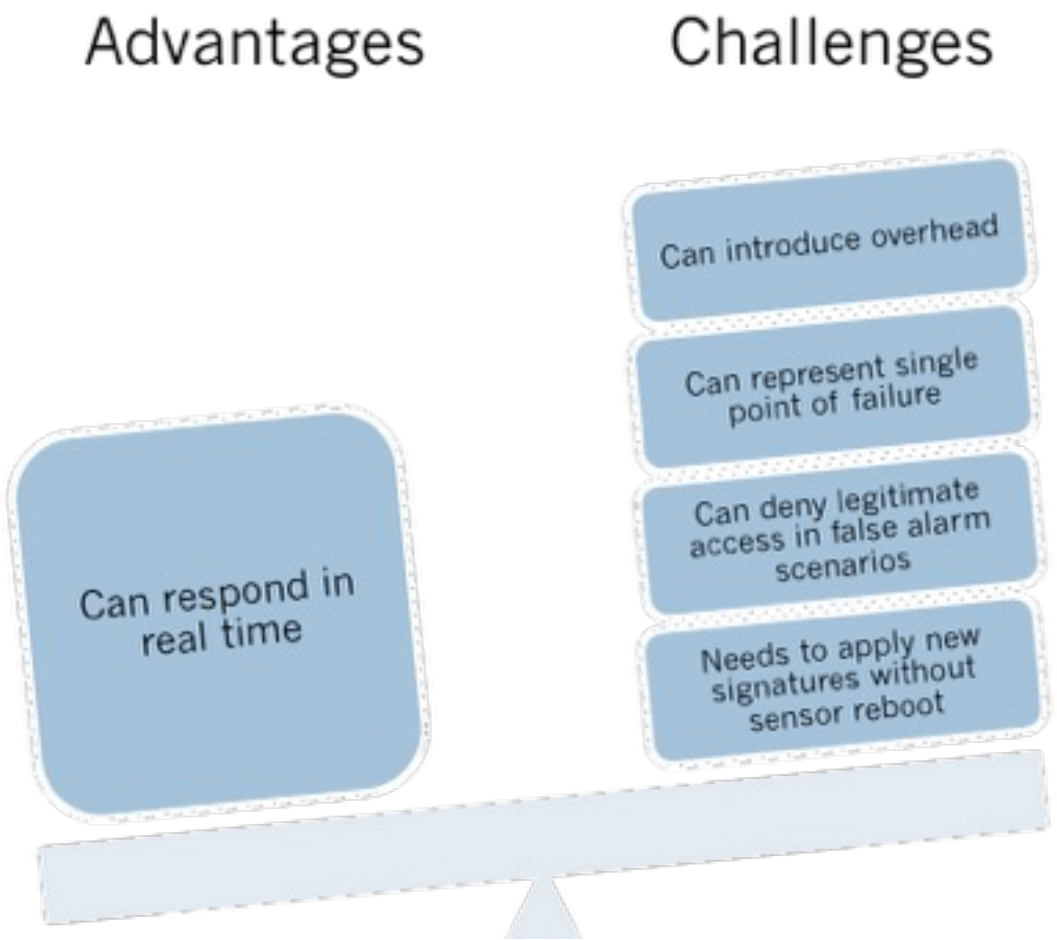
Advantages

- ☑ Usually performs misuse and anomaly detection

Disadvantages

- ☒ Future OS upgrades could cause problems
- ☒ Since it intercepts all system requests, it could inflict significant performance degradation on the system

Intrusion Prevention Pro/Cons



Addressing IPS challenges …

Single-point of failure

- Use a back-up IPS (fail-over)
  - expensive
- Redirect traffic around the IPS
  - provides no protection against attacks
- Pre-configure IPS to run with minimum capabilities, allowing all traffic to pass (fail-open)
  - provides no protection against attacks

False alarms

- Respond only to alarms with high certainty
  - Can be applicable to only a small set of alarms
  - Signature quality is paramount at reducing false alarms

In an IPS world …

Survey by Infonetics (2008)

- 169 security professionals managing IPS
- Targeted large enterprises with average company size 9,400 employees
- Aims to investigate experiences of customers using IPS

Findings

- IPS are often used in IDS mode to passively monitor traffic
- When used in-line, 50% of the time filters not always applied in blocking mode
- It can take even a year for users to gain confidence in an IPS and use it in in-line blocking mode

1 Messmer. 2008. "Intrusion prevention systems still not used full throttle: survey", Network World Magazine

Conclusions

The need for timely response has led to the emergence of IPS

IDS and IPS have different roles –one cannot replace another

Performance, reliability, and the risk of denying legitimate services are the main challenges for IPS

Combining output from different security tools (including IPS) can enhance detection and response

Emergence of Security Information and Event Management (SIEM)

Intrusion Detection is a very challenging area that can be enhanced by combining different approaches

Intrusion Response is equally challenging that requires effective context-aware detection

Thank You