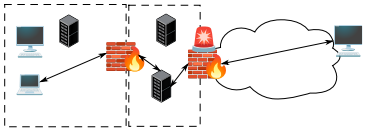
CSci 4271W
Development of Secure Software Systems
Day 16: Intrusion detection, midterm 2 review

Stephen McCamant (he/him)
University of Minnesota, Computer Science & Engineering

Based in large part on slides originally by Prof. Nick Hopper

Network intrusion detection

NIDSes augment the "perimeter defense" approach to network security with a "burglar alarm"



Suspicious traffic triggers the alarm, prompting a response

NIDS characteristics

NIDSes can be classified/evaluated by:

Error rates	Against typical traffic?
Search type	Known intrusions or unknown behavior?
Type of sensors	Host and/or network?
Evasion	Failures against targeted attacks?

Error rates

A false positive error is when a non-intrusion raises an alarm:

- Squirrel chews through sensor cable
- Printer driver scans subnet for printer
- User mistypes password three times

A false negative is when an intrusion does not raise an alarm.

False Positive Rate (FPR) = #FPs / #Normal Events

False Negative Rate (FNR) = #FNs / #Intrusions

Base rate problems

Suppose the BCI network has 10M network flows/day, and 100 flows are attacks.

If BCNIDS has a 0.1% FPR, then:

- How many false alarms per day?
- What fraction of alarms are FPs?

Even with 0% FNR, what FPR is needed to equally balance FPs and TPs?

Base rate problems

Suppose the BCI network has 10M network flows/day, and 100 flows are attacks.

If BCNIDS has a 0.1% FPR, then:

- How many false alarms per day? 10K
- What fraction of alarms are FPs?

Even with 0% FNR, what FPR is needed to equally balance FPs and TPs?

Base rate problems

Suppose the BCI network has 10M network flows/day, and 100 flows are attacks.

If BCNIDS has a 0.1% FPR, then:

- How many false alarms per day? 10K
- What fraction of alarms are FPs? >99.9%

Even with 0% FNR, what FPR is needed to equally balance FPs and TPs?

Signature matching IDS

The misuse detection problem is to find behavior matching known intrusions. Basic strategy:

- Collect many examples of known attacks.
- Divide them into groups matching a signature.
- Match new flows against these signatures.

Example rule (Snort): `alert tcp any any -> myip 21 (content: "site exec"; content:"%"; msg:"site exec buffer overflow attempt";)`

Anomaly detection

Anomaly detection tries to identify "normal" traffic patterns.

Traffic that does not fit these patterns causes an alarm.

- Advantage: more robust to slight attack changes
- Disadvantage: people do crazy things on the Internet

IDS tradeoffs

	Signature	Anomalies
FPs:	low	high
New attacks:	missed	"sounds fishy"
Need to know:	existing attacks	normal traffic
	+ automated extraction	– delayed response
	– easy to evade	– mimic attacks
		– changes in normal

Network-based NIDSes

Monitoring for "network" attacks: DoS, protocol/application bugs, worms, viruses and software.

Example: port scanning. Signature is multiple connections to the same network in short time period.

Examples of "what can go wrong" include fragmentation, volume of network data, "low and slow" attacks, etc.

Example: Snort 

Snort is a signature-based portable open-source NIDS with millions of downloads/installs (including at UMN OIT)

It scans packet logs, matching connections against sigs

Snort signatures are extended regular expressions that should match many variants of an attack, for example:

```
alert tcp any any -> [a.b.0.0/16,c.d.e.0/24] 80
(msg:"WEB-ATTACKS conf/httpd.conf attempt"; nocase; sid:1373;
flow:to_server,established; content:"conf/httpd.conf"; [...] )
```

Example: Zeek

Zeek (formerly "Bro") is a "policy-based" NIDS that uses scripts to monitor connection protocol state.

Zeek logs "connection events" specific to the protocols for each connection, e.g. TCP handshake, SSH authentication, SSH records, SSH shutdown, TCP shutdown.

Scripts can alert when known attacks are detected or when unusual protocol states occur.

Outline

Intrusion detection

Announcements intermission

Midterm information and review

Upcoming assignments

- Homework 4 (mostly networking) due tonight
  - Putting it off until after the midterm is not recommended
- Midterm 2 is this Thursday, 3/27
- Project part 2 will be coming out this week

Outline

Intrusion detection

Announcements intermission

Midterm information and review

Midterm 2 information

- In class (normal time and place) this Thursday
- Open book, open notes, any paper materials OK, but no electronics
- Pencil or erasable pen recommended
- Structure:
  - 3 homework-like questions (50 points total), one defensive programming
  - 10 short-answer questions (50 points total)

Midterm 2 topics

- Authentication (3 factors, attacks, defenses)
- Access control (subjects, objects, UNIX)
- Protection (isolation, MAC, sandboxing, containers)
- Network basics: layers, protocols
- Network threats
- Network perimeter defense

Kahoot game

- Go to `kahoot.it` in a web browser
- Your player name can be a pseudonym