Notices

- Lab 3 Phase 1 Due 23:59 Friday March 1
Today’s Lecture

• Intrusion Detection
Intruders

• Two most widely known threats to security are:
  – **Intruders**: Humans with malicious / mischievous intent
  – **Malware**: Software with malicious / mischievous intent

• Classes of **Intruder**:
  – **Masquerader**
    • Likely to be an outsider
    • Unauthorized person who penetrates a system to exploit a legitimate account
  – **Misfeasar**
    • Generally an insider
    • Legitimate user who misuses privileges
  – **Clandestine User**
    • Can be either insider or outsider
    • Individual who seizes supervisory control to evade auditing and access controls or to suppress audit collection
Examples of Intrusion

• Remote super-user compromise
• Web site defacement
• Cracking passwords
• Copying databases of valuable information
• Viewing sensitive data without authorization
• Running a packet sniffer / port scanner
• Distributing pirated software
• Using an unsecured phone/tablet to access internal network
• Impersonating an member of staff to get information
• Using an unattended workstation
Hackers

• Typically **motivated** by **thrill** of access and/or **status**
  – Hacking community is a strong meritocracy
  – Status is determined by level of competence

• Arguably benign intruders, but they consume resources and reduce performance for legitimate users

• **Intrusion detection systems** (IDSs) and **intrusion prevention systems** (IPSs) are designed to help counter hacker threats
  – Can restrict remote logons to specific IP addresses
  – Can use virtual private network technology (VPN)

• Intruder problem led to establishment of **computer emergency response teams** (CERTs)
Security Engineer Intern, CERT job

FACEBOOK  MENLO PARK, CA

JOB DESCRIPTION

Summary:

Facebook's Computer Emergency Response Team is seeking a threat analyst intern to help us in our ongoing mission to understand, identify, and isolate threats to our corporate and production systems. You will be the first line of defense for Facebook's infrastructure. You will advance Facebook's mission of making the world more open and connected by quickly identifying and analyzing threats that aim to collect sensitive/proprietary information or disrupt our business. You will both analyze incoming threats as well as build tools that will help shape our analysis processes to help our mission. We are looking for a candidate who is passionate about hunting bad guys, analyzing their malware, and willing to think outside the box and help create novel methods and tools to make their lives hard. This position is located in Menlo Park, CA and will begin in Summer 2018.
Software Engineer, Security
Google
Software Engineering
Mountain View, CA, United States

Note: By applying to this position your application is automatically submitted to the following locations: San Francisco, CA, USA; Kirkland, WA, USA; New York, NY, USA; Seattle, WA, USA; Mountain View, CA, USA

Google's software engineers develop the next-generation technologies that change how billions of users connect, explore, and interact with information and one another. Our products need to handle information at massive scale, and extend well beyond web search. We're looking for engineers who bring fresh ideas from all areas, including information retrieval, distributed computing, large-scale system design, networking and data storage, security, artificial intelligence, natural language processing, UI design and mobile; the list goes on and is growing every day. As a software engineer, you will work on a specific project critical to Google's needs with opportunities to switch teams and projects as you and our fast-paced business grow and evolve. We need our engineers to be versatile, display leadership qualities and be enthusiastic to take on new problems across the full-stack as we continue to push technology forward.

You are a skilled software engineer who enjoys security and/or privacy work and is an expert in systems security, applications security, network security, data protection and infrastructure privacy, cryptography or automated malware analysis. You are a security and/or privacy researcher who thrives on addressing real world problems and likes to code.

In this role, you will focus on security or privacy for components of our systems, such as client devices, networking equipment and server infrastructure, with an emphasis on threats from all sources. You will be building large-scale systems to protect Google's users including, for example, hardening our core infrastructure, detecting intrusion attempts, or preventing malware across various platforms.

At Google, our users come first, and the Systems Infrastructure team is at the heart of that promise. We build the technologies that transform the way we think about doing business. Whether working on our cloud systems, researching the latest in computer technology or keeping Google's internal systems humming, Googlers and users alike rely on us to keep things running. We're back-end experts: protecting your privacy and ensuring your security.

Responsibilities

• Design and apply advanced security techniques.
• Develop advanced security and cryptographic systems.
• Build large-scale detection systems.

Qualifications

Minimum qualifications:
• BS degree in computer science or equivalent practical experience.
• Experience with one or more general purpose programming languages including but not limited to: Java, C/C++, C#, Objective C, Python, JavaScript, or Go.
• Experience in applications security, cryptography, network security, systems security or malware analysis.
Hacker Modus Operandi

- Select a target using IP lookup tools such as NSLookup, dig, etc.
- Scan network for accessible services using tools such as NMAP
- Identify potentially vulnerable services (pcAnywhere, etc.)
- Brute force or dictionary attack passwords
- Install remote administration tool
- Wait for administrator to log on and capture their password
- Use that password to access remainder of network
Criminal Modus Operandi

- Organized groups of hackers are a real threat
  - Corporation / government / loosely affiliated gangs
  - Meet in “dark net” forums
  - Common targets are credit card files on e-commerce sites

- Criminal hackers usually have specific targets
  - Once victim’s systems are penetrated, they act quickly and get out

- IDS / IPS can be used but less effective

- Hence sensitive data should *always* be encrypted
Cyber Criminal Patterns of Behaviour

• Act quickly and precisely to make their activities difficult to detect
• Exploit perimeter via **vulnerable ports**
• Use **Trojan horses** to leave back doors for re-entry
• Use **sniffers** and **key loggers** to capture passwords
• Do not stick around until they get noticed
Internal Threats

• Arguably the most difficult to detect and prevent

• Employees have access and systems knowledge

• May be motivated by revenge/entitlement
  – Employment was terminated
  – Taking customer lists when moving to a competitor
  – Taking confidential information / code to start own company

• DS / IPS can be useful but also need:
  – Enforcement of least privilege
  – Log monitoring
  – Strong authentication
  – Enforceable legal redress
Uber Knew Its Self-Driving Guru Had Taken Google's Trade Secrets, Report Says


The blockbuster legal battle between Uber and Google's self-driving spinoff company, Waymo, hinges on two questions. One: Did former Google engineer and self-driving car whiz Anthony Levandowski swipe documents containing valuable Google intellectual property and bring them to his own startup, which would be acquired by Uber just months later for a reported $680 million? And two: Did Uber executives, including now-ousted CEO Travis Kalanick, conspire with Levandowski to do it, then use that intellectual property to advance their own technology?

Uber Is Paying About $245 Million to Settle a Major Lawsuit With Google

(SAN FRANCISCO) — Uber is settling a lawsuit filed by Google's autonomous car unit alleging that the ride-hailing service ripped off self-driving car technology.

Both sides in the case issued statements confirming the settlement Friday morning in the midst of a federal court trial in the case.

Google's Waymo unit says Uber agreed to take steps to make sure Waymo technology isn't used in Uber's autonomous vehicles. Waymo says Uber also agreed to pay about $245 million.

Uber's CEO says in a printed statement that the company doesn't believe trade secrets made their way from Waymo to Uber. He also says Uber is taking steps to make sure its self-driving vehicle research represents only Uber's work.
Internal Threat Patterns of Behaviour

• Create network accounts for themselves and their friends
• Access accounts and applications they wouldn’t normally use for their daily jobs
• E-mail former and prospective employers
• Conduct furtive instant-messaging chats / WhatsApp conversations
• Visit web sites that cater to disgruntled employees
• Perform large downloads and file copying
• Access the network during off hours
The Internet Security Glossary RFC2828

- **Security Intrusion**: A security event, or a combination of multiple security events, that constitutes a security incident in which an intruder gains, or attempts to gain, access to a system (or system resource) without having authorization to do so.

- **Intrusion Detection**: A security service that monitors and analyzes system events for the purpose of finding, and providing real-time or near real-time warning of, attempts to access system resources in an unauthorized manner.
Cybersecurity Hype: Is the Industry Delivering on its Promise?

Kirsten Bay President and CEO, Cyber adAPT

Every week we see more headlines in the press about new cyber-attacks and security vulnerabilities affecting millions of consumers and businesses around the world.

Massive data protection scandals such as Equifax – where 143 million individuals' personal data were exposed in a hack that could have been prevented by a simple patch – now seem to happen on a worryingly regular basis.

Meanwhile, the cybersecurity industry seems to be sitting pretty, with business revenues in the sector growing by an estimated 11% every year. A recent report from Cybersecurity Ventures forecast that global spending on cybersecurity is expected to exceed $1 trillion between 2017 and 2021. Given the ongoing list of high-profile security breaches, is the cybersecurity industry really offering its customers value for money?

The statistics would suggest that it is not. The number of businesses falling victim to attacks rose by 21% in the US last year, and doubled in the UK in the past two years. Figures show that there were 918 data breaches compromising 1.9 billion data records in the first six months of 2017, up 164% compared to 2016.
Intrusion Detection Systems

• An **intrusion detection system** (IDS) can analyze system use and network traffic patterns and react to anomalous patterns
  – However, often there is nothing wrong but an unusual volume of activity and/or network requests

• Note that an IDS is **inherently reactive**
  – The attack has already begun when the IDS takes effect
Intrusion Detection Systems

• Components:
  – **Sensors**: Collect data
  – **Analysers**: Determine if intrusion has occurred
  – **User Interface**: View alerts and control system behaviour
    • Or plugin for Enterprise Management Systems (EMSs)

• Types:
  – **Host-based**: Monitors characteristics of a single host for suspicious activity
  – **Network-based**: Monitors network traffic and analyzes network, transport, and application protocols to identify suspicious activity

• Main Principle:
  – **Assume intruder behavior differs from legitimate users**
  – Overlap in behaviors causes problems
IDS Errors

• Two types of errors
  – **False negatives**: a genuine attack is not detected.
  – **False positives**: harmless behavior is misclassified as an attack.
  – Which do we think is a bigger problem?

• An intrusion detection system is:
  – **Accurate**: if it detects all genuine attacks;
  – **Precise**: if it never reports legitimate behavior as an attack

• It is relatively easy to make an IDS that is either accurate *or* precise
  – It’s hard (if not impossible) to make one that’s both
IDS Errors

• An undetected attack might lead to severe problems but frequent false alarms lead to the system being disabled or ignored
  — Security Principle? Psychological Acceptability

• A perfect IDS would be both accurate and precise

• But statistically, attacks are rare events

• Yet most IDSs suffer from the base-rate fallacy...
Base-Rate Fallacy

• Suppose that only 1% of traffic are actually attacks, and the detection accuracy of your IDS is 90% - what does that mean?
  – IDS classifies a genuine attack as an attack with probability 0.9
  – IDS classifies a valid connection as an attack with probability 0.1

• What is the probability that a connection flagged as an attack is not really an attack, i.e. a false positive?

• **Bayes’ Theorem:**

\[
p(\text{attack}|\text{detect}) = \frac{p(\text{detect}|\text{attack})p(\text{attack})}{p(\text{detect})} \\
= \frac{p(\text{detect}|\text{attack})p(\text{attack})}{p(\text{detect}|\text{attack})p(\text{attack}) + p(\text{detect}|\text{ok})p(\text{ok})} \\
p(\text{attack}) = 0.01 \\
p(\text{ok}) = 0.99 \\
p(\text{detect}|\text{attack}) = 0.9 \quad \text{(true positive)} \\
p(\text{detect}|\text{ok}) = 0.1 \quad \text{(false positive)} \\
p(\text{detect}) = p(\text{detect}|\text{attack})p(\text{attack}) + p(\text{detect}|\text{ok})p(\text{ok}) \\
p(\text{detect}) = 0.9 \times 0.01 + 0.1 \times 0.99 = 0.009 + 0.099 = 0.108 \\
p(\text{attack}|\text{detect}) = \frac{0.9 \times 0.01}{0.108} = 0.083333
\]

• i.e. there is an approximately **92% chance that a raised alarm is false!**

• False negatives and false positives are **both** bad for an IDS
  – An IDS must be very accurate or suffer from the base rate fallacy
  – An IDS with too many errors becomes useless

IDS Requirements / Desirable Attributes

- Run **continually**
- Be **fault tolerant**
- **Resist subversion**
- Impose a **minimal overhead** on system
- **Adapt** to changes in systems and users
- **Scale** to monitor large numbers of systems
- Provide **graceful degradation of service**
- Support **dynamic reconfiguration**
Host Based IDS

• Monitors activity to detect suspicious behavior
  – Primary purpose is to detect intrusions, log suspicious events, and send alerts
  – Can detect both external and internal intrusions

• Anomaly Detection
  – Threshold breach:
    • Counting the occurrences of a specific event type over a time interval
  – Profile based:
    • Learn activity patterns of each user
    • Detect changes in the behavior of individual accounts

• Signature Detection
  – (Attempt to) define a set of rules or attack patterns that can be used to decide that a given behavior is that of an intruder
Audit Records (log files)

- **Native:**
  - Multiuser operating systems include accounting software that collects information on user activity
  - Advantage is that no additional collection software is needed
  - Disadvantage is that records may not contain the needed information or in a convenient form

- **IDS Specific:**
  - Collection facility that generates records containing only information required by the IDS
  - Advantage is that it could be made vendor independent and ported to a variety of systems
  - Disadvantage is the extra overhead of having, in effect, two accounting packages running on one machine
## IDS Metrics: Login & Session Activity

<table>
<thead>
<tr>
<th>Metric</th>
<th>Model</th>
<th>Detects</th>
</tr>
</thead>
<tbody>
<tr>
<td>Login Frequency by Day &amp; Time</td>
<td>Mean &amp; standard deviation</td>
<td>Out of hours logins</td>
</tr>
<tr>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td></td>
<td></td>
<td></td>
</tr>
</tbody>
</table>
# IDS Metrics: Command & Program Execution

<table>
<thead>
<tr>
<th>Metric</th>
<th>Model</th>
<th>Detects</th>
</tr>
</thead>
<tbody>
<tr>
<td>Execution Frequency</td>
<td>Mean &amp; standard deviation</td>
<td>Intruders using unusual commands to investigate system, or successful by legitimate user who has gained access to privileged commands</td>
</tr>
</tbody>
</table>
## IDS Metrics : File Access

<table>
<thead>
<tr>
<th>Metric</th>
<th>Model</th>
<th>Detects</th>
</tr>
</thead>
<tbody>
<tr>
<td>CRUD (Create Read Update Delete) frequency</td>
<td>Mean &amp; standard deviation</td>
<td>Masquerading or unusual activity (e.g. file sharing) by authorised user</td>
</tr>
</tbody>
</table>
Signature Detection

Rule Based Anomaly Detection
- Historical audit records are analyzed to identify usage patterns
- Rules are generated that describe those patterns
- Current behavior is matched against the set of rules
- Does not require knowledge of security vulnerabilities within the system
- But… a large database of rules is needed

Rule Based Penetration Identification
- Key feature is the use of rules for identifying known penetrations or penetrations that would exploit known weaknesses
- Rules can also be defined that identify suspicious behavior
- Typically rules are specific to the machine and operating system
Distributed Host-Based IDS

**Diagram Description:**
- **Management Module (MM):** Located at the bottom left, connects to the Internet and acts as a central management hub.
- **Agent Module (AM):** Distributed throughout the network, monitoring and reporting on network activities.
- **Internet:** Central hub connecting all nodes, facilitating data and information exchange.

The diagram illustrates a network topology with multiple nodes, each connected to the Internet, and managed by a central management module.
Distributed Host-Based IDS

- Raw OS Audit Information
- Filters
- Host Audit Log
- Detection Logic
- Rules & Knowledge Base
- Agent Protocol
- Agent Module
- Alerts
- MM
- Responses / Updates
Network-Based IDS (NIDS)

• Monitors traffic at **selected points on a network**
• Examines traffic **packet by packet** in real or close to real time
• May examine **network, transport, and/or application-level** activity
• Comprised of:
  – A number of sensors
  – One or more servers for NIDS management functions
  – One or more management consoles
    • Or plugins to EMSs
**NIDS Sensor Deployment**

**Inline:**
Inserted into a network segment so that the traffic it is monitoring must pass through the sensor

**Passive:**
Monitors a *copy* of network traffic

Traffic Monitoring - No IP Ethernet Promiscuous Mode

To management interface over IP
Intrusion Detection Techniques

• **Signature detection**
  – at application, transport, network layers; unexpected application services, policy violations

• **Anomaly detection**
  – denial of service attacks, scanning, worms

• **When a sensor detects a potential violation it sends an alert and logs information related to the event**
  – Used by analysis module to refine intrusion detection parameters and algorithms
  – Security administrators can use this information to design prevention techniques
Honeypots

- **Decoy systems** designed to:
  - Lure a potential attacker away from critical systems
  - Collect information about the attacker’s activity
  - Encourage the attacker to stay on the system long enough for administrators to respond

- Filled with **fabricated information** that a legitimate user of the system wouldn’t access

- Resource that has **no production value**
  - Incoming communication is most likely a probe, scan, or attack
  - Outbound communication suggests the system has been compromised

- Once hackers are within the network, administrators can **observe their behavior** to figure out defenses
Honeypot Deployment

The Internet
Simplified NIDS Template

- Real-time packet capture and rule analysis
- Easily deployed on nodes
- Small memory and CPU footprint
- Easily configured
## Simplified NIDS Rules

<table>
<thead>
<tr>
<th>Action</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>Alert</td>
<td>Generate an alert and log the packet</td>
</tr>
<tr>
<td>Log</td>
<td>Log the packet</td>
</tr>
<tr>
<td>Pass</td>
<td>Ignore the packet</td>
</tr>
<tr>
<td>Activate</td>
<td>Alert then turn on another dynamic rule</td>
</tr>
<tr>
<td>Dynamic</td>
<td>Remain idle until activated then log</td>
</tr>
</tbody>
</table>
Intrusion Detection : Summary

• It’s complex
• It’s expensive
• It’s riddled with false-positives
• But it does catch intruders!
• Worth it if (and only if) your threat model demands it
Next Lectures

- Cloud Security