“Cyber attack”

Spooky!
Today’s Lecture:

What actually happens in these “cyber attacks”?

What can enterprises do to protect themselves?
What is an “Enterprise”? 

Enterprise: a company / organization / institution 

- The collection of machines, employees, and digital assets (e.g., datasets) that are owned by one such entity

Companies

- Google
- Walmart
- Microsoft

Organizations & Institutions (Government, Nonprofit, etc.)

- American Red Cross
- Chicago Public Schools
What is “Enterprise Security”?

(Software / tech companies)
How do we keep our customers & software secure?
“Product Security”, “AppSec”, “Trust & Safety”

Enterprise Security
How do we keep our company’s digital assets secure?

- Corporate Machines / Devices
- Money & Trade Secrets
- Datasets
- Software Products / Public Websites
- User Interactions / Hate & Harassment
- User Accounts / Login
Outline

• What is enterprise security?

• Structure of enterprise networks & basic defenses

• Attacks on enterprises

• Common enterprise defenses
What do enterprises look like?

**Enterprise network:** the set of all devices & digital assets an enterprise owns
- Laptops, servers, cloud services, datasets, etc.
- (Outside this class: can also refer to just the networking infrastructure & configuration)

Huge variation in how enterprises networks are structured
- **On-premise (old-school):** company physically owns all machines
- **Cloud hosted:** servers & services hosted in the cloud-providers (company’s systems & data lives in cloud VMs or services)
- **Hybrid:** some systems & services hosted on-prem and some hosted in cloud
Example: (Simplified) Enterprise Network

Production Services / Public web(s)ite servers

Networking Servers (DNS, DHCP, etc.)
Basic Enterprise Security

Basic idea: only **authorized employees** allowed to access internal resources.
Basic Enterprise Security: Border Firewalls

Firewall: all connections to/from external IPs go through gateway w/ specific access policies
- Most internal machines “invisible” to outside
- Outbound connections typically have more relaxed (fewer) restrictions
Basic Enterprise Security: User Authentication

- Machines & services require users to login/authenticate with valid credentials
- Typically have a central authentication database & service (e.g., Active Directory)
Example: (Simplified) Enterprise Network

Public Internet

Directory & Auth Servers (e.g., Active Directory)

Networking Servers (DNS, DHCP, etc.)

Production Services / Public web/site servers
Outline

• What is enterprise security?

• Structure of enterprise networks & basic defenses

• Attacks on enterprises

• Common enterprise defenses
Common types of enterprise attacks

• Data breach & Theft
Common types of enterprise attacks

• Data breach & Theft
• Denial of Service: [D]DoS
• Destruction & Defacement

Pennsylvania courts resume business after weekend DDoS attack

Pennsylvania state courts officials said they've resumed work after their website was knocked offline by a distributed denial-of-service attack over the weekend.

Compromise of Saudi Aramco and RasGas

In 2012, threat actors wiped data from approximately thirty-five thousand computers belonging to Saudi Aramco, one of the
Common types of enterprise attacks

• Data breach & Theft
• Denial of Service: [D]DoS
• Destruction & Defacement
• Ransomware: extort enterprise for money by hijacking enterprise data and/or machines (e.g., encrypt enterprise data w/ attacker key)
Common types of enterprise attacks

• Data breach & Theft
• Denial of Service: [D]DoS
• Destruction & Defacement
• Ransomware

• Functionality & physical-world attacks: hijack & use enterprise machines with useful functionality (e.g., control speed of nuclear centrifuges)
What actually happens in a “cyberattack”?

Simple data breach: Command injection attack
• e.g., Buffer overflow in server software or SQL injection attack

“…/bin/sh...x24\xf6\xff\xbfAAA…”
What about more complicated attacks?

More complex attacks: “the cyber killchain” or “APT lifecycle”

- Sequence of common attack stages seen in real attacks
The Conti Ransomware Attack on Ireland’s HSE (Healthcare System)

Ireland’s HSE: Health Services Executive
- National healthcare system w/ 54 hospitals

2021: major ransomware attack + data breach (700 GB exfiltrated)
- 4 months to remediate & recover
- Damage estimates over $50 million
The Conti Ransomware Attack on Ireland’s HSE (Healthcare System)

Several exact details are redacted, so some speculative analysis.
Spearphishing attack to Employee #0 (“Bob”)

- **Email Attachment**: Microsoft Excel file with malicious macro
  (Code plug-in that runs if enabled; e.g., can launch & command other apps: shell / cmd.exe)
- Successfully installs malware on Bob’s machine
Conti Attack on HSE: Establish Foothold

March 23-31, 2021

Establish Foothold: Persistent access and communication

- **Persistence**: ensure malware runs / attacker has access even if system reboots
  - e.g., modify startup program list, add attacker key to SSH authorized keys, etc.
- **Command & Control (C2)**: maintain (stealthy) line of communication w/ attacker
Why do attackers need C2 protocols / mechanisms?

- Firewall blocks the outside attacker from initiating comm with infected machine
- Need the infected machine to initiate communication to external entity
Why do attackers need C2 protocols / mechanisms?

- Firewall blocks the outside attacker from initiating comm with infected machine
- Attacks can take days -> months to fully execute
  - Very suspicious & impractical to keep one network session open for that long
Understanding Command & Control (C2)

Why do attackers need C2 protocols / mechanisms?

- Firewall blocks the outside attacker from initiating comm with infected machine
- Very suspicious & impractical to keep one network session open for days -> months
- C2 protocols solve these problems for the attacker (e.g., “beaconing”)
  - Infected machine periodically contacts attackers’ server(s) for new instructions
Conti Attack on HSE: Privilege Escalation

Privilege Escalation: Gain administrative privileges/credentials
(This stage often blends with internal reconnaissance: next slide)

- Credential cracking / attacks (e.g., keylogging, password cracking, Mimikatz)
- Exploiting vulnerabilities in the OS / applications of infected machine
Conti Attack on HSE: Internal Reconn

Early May? 2021

Public Internet

Directory & Auth Servers (e.g., Active Directory)

Internal Reconnaissance (“Discovery”)

Identify other machines in the enterprise: what they have & how to access

- **Local reconn**: look through infected machine (e.g., browser/shell/VPN/app history)
- **Active Directory reconn**: query central authentication & directory databases
- **Network scanning**: probe IP addresses to find machines & vulnerable services
Conti Attack on HSE: Lateral Movement

Early May 2021

Lateral Movement: Expand to more machines & Repeat

- Use stolen credentials to access more machines (from: Victim #0 machine + Internal Reconn + Brute-forcing)
- Exploit vulnerable software/services on other machines
- Repeat process (persistence/C2/privilege escalation/etc.) on newly compromised machine

Public Internet

Directory & Auth Servers (e.g., Active Directory)

pwd = “password”
Conti Attack on HSE: Complete Mission

**May 10, 2021**

Data Exfiltration + Launch Ransomware

- May 10-12: HSE security teams began noticing & responding to detection alerts
Conti Attack on HSE: Complete Mission

May 14, 2021

Data Exfiltration + Launch Ransomware

- May 10-12: HSE security teams began noticing & responding to detection alerts
- May 14: Ransomware activated to encrypt & disable systems/data
  - Same time or potentially earlier: attackers exfiltrate patient data from systems they have accessed
Conti Attack on HSE: Aftermath

• May 14, 2021: Ransomware launched with $20 million demand, and threat to sell/exfiltrate data.
  - HSE refused to pay.

• May 20, 2021: Attackers released a decryption key and software (very lucky for HSE).

• Sep 21, 2021: HSE decrypted 100% of servers and restored 99% of apps/services in the enterprise.
1. **Initial Reconnaissance [Step 1]:** find unpatched vulnerabilities, email addresses of employees to phish, etc.
2. **Initial Access & Foothold [Steps 2-3]:** get access to an enterprise machine/account
3. **Expand Internal Access [Steps 4-7]:** more machines/accounts/privileges
4. **Complete Mission [Step 8]:** steal data / launch ransomware / cause destruction / etc.
Outline

• What is enterprise security?

• Structure of enterprise networks & basic defenses

• Attacks on enterprises

• Common enterprise defenses
General Security Hygiene

**Data Backups:** Mitigates damage of ransomware & destructive attacks
• Issues: Storage Costs, Potentially increased risk of data breach

**Policies:** Employee Training, Managed software & devices, Use policies
• Issues: Unclear (potentially harmful) efficacy, Human costs

**Regular patching and Vulnerability scanning**
• Issues: Compatibility & downtime, Misaligned responsibilities & ownership
Defenses: Stronger Authentication & Isolation

**Basic authentication:** if username + password correct, allow access

**Stronger authentication:** Multi-factor authentication (MFA / 2FA)
- Require correct password AND additional hardware/physical verification

**Least privilege:** Dedicated admin / highly-privileged accounts
- “grantho” vs. “grantho-admin”: different passwords & permissions
Defenses: Stronger Authentication & Isolation

Basic network separation: Border firewalls keep external entities out
• Limitation: Once an attacker has an initial foothold: no more security!
Defenses: Stronger Authentication & Isolation

Basic network separation: Border firewalls keep external entities out
• Limitation: Once an attacker has an initial foothold: no more security!

Stronger Isolation: Network segmentation & bastion hosts
• Add *internal firewalling* that
  1. Creates specific machine groups and
  2. Restricts access to/from a group via their “bastion” machine or specific conditions
Defenses: Zero Trust Model

Require *all* accesses to machines & data to be strongly authenticated, and only grant minimum permissions needed.

Authenticating requests typically involves at least user password & 2FA, but can also involve other checks such as:

- Time-of-request
- Network properties of requesting device
- Specific device requirements (e.g., “managed” enterprise device, system and applications up-to-date, recently run anti-virus scan, etc.)
Network Intrusion Detection (NIDS)

NIDS: Typically combination of software + hardware
- Detect & terminate malicious or disallowed network traffic
- Lots of systems in real-world: Zeek, Suricata, Snort, etc.
Host-Based Intrusion Detection (HIDS / EDR)

Software program on a machine that detects & remediates malicious activity (e.g., detect, stop, remove malware on employee’s laptop)

Traditionally known as anti-virus (AV)

• Modern rebranding: EDR (Endpoint Detection & Response)
  (Provides more centralized control and functionality than older AV software)
Several NIDS vs. HIDS Trade-offs

**NIDS**
- Cheaper deployment & maintenance
- Robust against tampering

**Challenges**
- Traffic Visibility: Internal and/or encrypted
- Ambiguity & evasion
- Performance & scalability

**HIDS**
- Deeper visibility
- Protects against non-network attacks on hosts

**Challenges**
- Expensive deployment costs
- Still faces evasion & higher tampering risk
Implementing Detection & Response

Most enterprises deploy a combination of NIDS & HIDS for detection

• Additionally: Aggregate their logs + additional logs from systems & applications into a centralized SIEM

• **SIEM**: Security information and event management system
  Perform detection & analysis on aggregated data
General Detection Strategies

**Exact Detection (Rule Based)**

**Signature-based Detection:** write exact rules about what is an attack

**Specification-based Detection:** write exact rules about legitimate behavior; everything else is an attack

---

**ML-Based Detection**

**Supervised Detection:** learn characteristics of attacks
- Train model w/ prior attacks

**Anomaly Detection:** learn what benign behavior looks like; everything else is an attack
Detection Metrics

Data consists of attack events and benign events.

For all the attack events:
• True Positives: labeled as an attack
• False Negatives: labeled as benign

For all the benign events:
• False Positives: labeled as attack
• True Negatives: labeled as benign
Some Key Challenges for Detection

Fundamental challenge: balancing false positives & false negatives

• **Base rate fallacy**: attacks are very rare but there are many, many benign events
  • A detector has a 100% TP Rate & 0.1% FP Rate... Good or Bad?
  • If network traffic: 50 attack packets & 10 million benign / day = 10,000 false alarms / day

Evasion: Attackers constantly adapting methods to evade detection

• Simple C2 strategy: infected machine contacts same malicious server on random IP address
• Stealthy C2 strategy: infected machine & malicious server communicate via a OneDrive folder

Compute & Data storage

• One machine can generate millions of events per day... 1,000s of machines at many org’s
• Attacks happen over multiple machines and potentially multiple months
Broader Enterprise Security Challenges

- No unified and universal guidelines of security best practices
Broader Enterprise Security Challenges

• No unified and universal guidelines of security best practices
• Way too much advice out there & discrepancies / ambiguities
Broader Enterprise Security Challenges

• No unified and universal guidelines of security best practices
• Way too much advice out there & discrepancies / ambiguities
• No good advice on what to prioritize

Elissa M. Redmiles, Noel Warford, Amritha Jayanti, and Aravind Koneru, University of Maryland; Sean Kross, University of California, San Diego; Miraida Morales, Rutgers University; Rock Stevens and Michelle L. Mazurek, University of Maryland

https://www.usenix.org/conference/usenixsecurity20/presentation/redmiles

(To prioritize this advice. For example, experts perceive 89% of the hundreds of studied behaviors as being effective, and identify 118 of them as being among the “top 5” things users should do, leaving end-users on their own to prioritize and implement them.)
Several Components for Good Enterprise Security

• Strong authentication for systems and services
• Limit administrative & sensitive privileges (least privilege)
• Deploy comprehensive detection and audit logging
• Frequent patching for applications & OS across machines
• Periodic and secured back-up for critical data