CSCI 1800 Cybersecurity and International Relations

Network Based Cyber Attacks

John E. Savage

Brown University
Outline

• Firewalls, inward and outward facing.
• Network address translators (NATs)
• Tunneling
  – SSH, IPsec
• Intrusion detection
  – Types of alarm, IDS system, event, data collection
  – Port scanning, honeypots
• Data Loss Prevention
• Wireless networking
Two Approaches to Attacks

• Keep the bad guys out.
  – Use **firewalls** and **intrusion detection** to stop them

• Cope with them once they get in.
  – **Detect, disrupt, prevent data loss** – deny attackers access to their **command & control centers**

“There are two types of corporations, those that know they have been compromised and those that don’t.”

*Dmitri Alperovitch, Crowdstrike*
Firewalls

• Usually placed at the periphery of a network
  – May be in a special processor (a proxy) or software

  – But may be placed at interior boundaries as well

• They examine only packet headers!

• Policies limit traffic going out and coming in.
  – Packets are allowed through, dropped, or rejected.
  – May use whitelists (blacklists) of sites (not) allowed to communicate with the network or machine.
Sample Firewall Policies

Packets arrive at an IP address with a port number

1. Allow HTTP (HTTPS) traffic only on port 80 (443)
2. Only internal users may initiate HTTP sessions.
3. Reject VoIP traffic—may hide malicious traffic
4. Don’t allow traffic to/from blacklisted sites
5. Only allow traffic to whitelisted sites.
Stateless Firewalls

• No info kept on packets previously seen.
  – If a server handles only web request, it need not initiate connect – don’t accept SYN packets from it on port 80.
Network Address Translator (NAT)

• When a network has more computers than addresses, it puts the computers on a private network and connects to the Internet via a NAT.

• A computer on an private network with address IA may initiate an external connection via a NAT.
Network Address Translator (NAT)

- It is given external address EA, drawn from a pool of external addresses, and port number EP.
- A table mapping IA to (EA, EP) created. The NAT can now direct returning traffic to computer IA.
- Outside addresses don’t know this mapping!
Stateful Firewalls

• Stateful firewalls examine contents of packets.
• Like NATs, they keep data on previously seen packets, such as IP addresses, port number, sequence number, and protocol type.
• They have many uses.

• **Application layer firewalls** manage accesses based on content at the application layer.
  – Could filter SQL queries to avoid injection, deny access to malicious web sites, drop malware, etc.
Tunneling

- **Tunneling** is the embedding of packets from one protocol as payload of another protocol, often for security.

  - Security requires robust identity and authorization.
  - Encryption/decryption increases overhead.
Types of Tunneling

• Secure shell (SSH), provides a secure terminal connection.

• IPsec, provides authenticity & privacy at the lowest level, the network layer

• Virtual Private Network (VPN) allows trusted sharing of remote network resources. It simulates being on site at the remote computer.
Public-Key Cryptography

• Each party has **public** & **private** keys
  – Alice: \( \text{Priv}_{\text{Alice}}, \, \text{Pub}_{\text{Alice}} \); Bob: \( \text{Priv}_{\text{Bob}}, \, \text{Pub}_{\text{Bob}} \).

• Alice encrypts message \( M \) for Bob with
  \[ X = E_K(M) \text{ where } K = \text{Pub}_{\text{Bob}}. \]

• Bob decrypts Alice’s encrypted message with
  \[ M = D_{K^*}(X) \text{ where } K^* = \text{Priv}_{\text{Bob}}. \]

• Idea proposed by Diffie and Hellman

• Rivest, Shamir and Adleman (RSA) gave first practical method (1977).
Symmetric vs Public Key Crypto

• Symmetric key encryption is much faster than public key encryption.
  – PKC often used to create/exchange secret key

• **Symmetric key system** has one key per user pair
  – Thus, there are n(n-1)/2 keys for n users.
  – If n = 10^4, that’s about 50x10^6 keys!

• In public-key system, 2n keys suffice, e.g. 2x10^4
  – Each party publishes one key, keeps the other secret
RSA Public-Key System

• Brief definition of modular arithmetic
  – Here addition and multiplication of integers is modulo n
  – That is, the result is the remainder after division by n.
  – E.g. \((3+4) \mod 5 = 2, (4*3) \mod 3 = 0\)

• Bob’s public key is pair of integers \((e,n)\). His secret key is \(d\).
  – Message is integer \(M\) in \(\{0,1,2,\ldots n-1\}\), \(n\) is product of two primes.
  – \(e,d\) and \(n\) are such that \(M^{de} \mod n = M\).
  – Finding \(d\) from \(e\) and \(n\) is as hard as factoring \(n\) – very hard!

• A message is represented by an integer \(M\).

• Alice encrypts message \(M\) for Bob as \(C = M^e \mod n\)
• Bob decrypts by computing \(C^d \mod n = M\). Note that
  \[ C^d \mod n = (M^e)^d \mod n = M^{de} \mod n = M \]
Secure Shell (SSH)

- Uses public key cryptography (PKC) to create and exchange a private key for efficient, secure communication.
  - TCP used to connect client and server
  - Both agree on SSH version, encryption method.
  - Exchange secret session key using PKC.
  - Client authentication occurs

- SSH provides secure access to resources, such as file transfer and command prompt.
• Alice and Bob need a common secret.
• Start with common color
• Each chooses secret color
• They mix their two colors
• Send mixtures to other
• Add in their secrets
• Create a common secret!
• Can do this with numbers!
Diffie-Helman Key Exchange

• B & A choose prime $p$ & primitive root $g \mod p$.
  
  – $g$ is primitive if for each integer in $\{0,1,2,..., p-1\}$ is equal to $g^k \mod p$ for some integer $k$.

• Alice’s secret is $a$ and Bob’s secret is $b$.

• A sends $r = g^a \mod p$ to B. B sends $s = g^b \mod p$.

• A computes $s^a \mod p$. B computes $r^b \mod p$.

• Let $Q = s^a \mod p = (g^b \mod p)^a = g^{ba} \mod p = g^{ab} \mod p = r^b \mod p$. The common secret is $Q$!
Security of Diffie-Hellman

- The values of $a$ and $b$ are secret.
- Alice sends $r = g^a \mod p$ to B in the clear.
- Bob sends $s = g^b \mod p$ to Alice in the clear.
- These transmissions will reveal $a$ and $b$ if it is possible to deduce $a$ from $r = g^a \mod p$ or $b$ from $s = g^b \mod p$.
- But no polynomial time algorithm is known for this *discrete logarithm problem*. 
IPsec

• IPsec offers secure communication at network layer
  – It is completely transparent to applications.
  – Provides confidentiality, authentication & data integrity.

• Initializing Ipsec:
  – Parties set up initial generic encrypted channel.
  – They decide on subsequent encryption method, hash algorithm, and authentication method.
  – Now ready for secure communication.
IPsec

- Two modes: transport and tunnel
- Tunnel Mode:
  - Entire old packet encrypted, placed in new packet
  - Used for VPN
- Transport Mode:
  - Only payload is encrypted or authenticated
  - IPsec header information inserted before payload.
Intrusion Detection

• Intrusion detection systems (IDSs) are more complex than simple firewalls.

• They monitor activity. Rules based on activity determine whether alarms are sounded.
  – Can you invent some interesting rules?

• Many IDSs do deep packet inspection (DPI).
  – DPI: packet content analyzed, not just the headers

• US Department of Homeland Security (DHS) has designed three IDSs, Einstein 1, 2 and 3.

Types of IDS Alarms

- Malware attack
- ARP (address resolution protocol) spoofing
- Denial of service attack
- Port scans – one site testing many ports
- Attempt at DNS cache poisoning
Types of Attacker

• Masquerader – attacker impersonates another.
• Misfeasant – insider exceeds granted authority
• Clandestine – user tries to cover his tracks
Types of IDS

• Host IDS
  – Monitors activity on one machine.
  – Tries to catch criminal & clandestine user.
  – Looks for abnormal or unauthorized activity.

• Network IDS
  – Traditional IDS, placed at periphery of network.
  – Does DPI looking for static or statistical signatures.
  – May look for protocol violations, e.g. on web server.
IDS Events

• Alarm sounded
  – False positive – benign event found, annoying
  – True positive – malicious event found – good

• Alarm not sounded
  – True negative – benign event – good
  – False negative – malicious event, serious oversight
Data Loss Prevention (DLP)

• Monitor outgoing Internet traffic
  – **Endpoint DLP (@host)** or **network DLP (@ border)**
  – Works on unencrypted files only!
  – Look for structured content or “indices” on unstructured data

• Structured content
  – Keywords, SSNs, credit card #s

• Unstructured content
  – Software, text pictures
A hash function is any function that maps data of arbitrary size to data of fixed size.

– The result is called the hash of the data.
– If two pieces of data have the same hash, they are likely to be duplicates of one another.

A cryptographic hash function $h$ is a function that is easy to compute but for which given a hash value $H$, it is very difficult to find data $D$ such that $h(D) = H$. 

Hash Functions
Data Loss Prevention (DLP)

• **Unstructured data chopped** into standard pieces and hash of each piece is computed

• Hashes are stored in database.

• As data exits network,
  – Compare **structured data** to template or database
  – Compute hash of **unstructured data** and compare to hashes in database

• DLP is a supplement to other technologies.
Port Scanning

• Internet-based computers communicate using IP addresses and port numbers.

• Some port numbers:
  
  - 22 – SSH
  - 80 – HTTP
  - 143 – IMAP
  - 179 – BGP
  - 443 – HTTPS
  - 28910 – Nintendo WiFi

• For security, firewalls block access to most ports
  
  - A port is open (responding) or blocked (non-responding).

• What is a port scan?
  
  - It’s a scan of ports at an IP address to see which ports respond. Code running at a port might have a flaw, such as a buffer overflow vulnerability, allowing penetration.
Types of Scan

- **TCP Scans** – attempt to connect via TCP
- **SYN Scans** – try TCP SYN packet on all ports. If response received, send RST – port is open.
- **Fingerprinting** – the identification of the OS running on a computer along with the services running at ports and the browser in use.
Blind Port Scan

- **Blind port scan** is a method to do a port scan on a victim without revealing your identity (aka idle scan).

1. **Attacker A** sends a TCP packet to innocent zombie **Z** to get its sequence number **X**. **Z** increments **X**.

2. **Attacker A** sends a TCP packet to victim **V** with **Z** as source. If **V** responds to **Z**, **Z** will increase its sequence number **X+1** to **X+2**.

3. **A** sends the 3rd TCP packet to **Z** to learn if **Z**’s sequence number is **X+2**, a sign that **V** has responded.
Honeypots

• A **honeypot** is a collection of machines, data and applications that looks real but serves no other purpose than to attract an attacker.
  – Any traffic to a honeypot is deemed suspicious.

• Can be used for following reasons:
  – Intrusion detection – allows defenders to study intrusion methods.
  – Evidence – incriminating evidence may be left.
  – Diversion – can distract attackers from real thing.
Wireless Networking

• All traffic sent via radio – can be heard by all!
• Wireless protocols support encryption methods
  – WEP (wired equivalent privacy) not very secure
  – WAP (Wi-Fi protected access) is considered secure
Review

• Firewalls, inward and outward facing.
• Network address translators (NATs)
• Tunneling
  – SSH, IPsec
• Intrusion detection
  – Types of alarm, IDS system, event, data collection
  – Port scanning, honeypots
• Data Loss Prevention
• Wireless networking