Encryption, VPN
Secure sockets layer (SSL)

- transport layer security to any TCP-based app using SSL services.
- used between Web browsers, servers for e-commerce (shttp).
- security services:
  - server authentication
  - data encryption
  - client authentication (optional)
- server authentication:
  - SSL-enabled browser includes public keys for trusted CAs.
  - Browser requests server certificate, issued by trusted CA.
  - Browser uses CA’s public key to extract server’s public key from certificate.
- check your browser’s security menu to see its trusted CAs.
SSL (continued)

Encrypted SSL session:
• Browser generates *symmetric session key*, encrypts it with server’s public key, sends encrypted key to server.
• Using private key, server decrypts session key.
• Browser, server know session key
  – All data sent into TCP socket (by client or server) encrypted with session key.

• SSL: basis of IETF Transport Layer Security (TLS).
• SSL can be used for non-Web applications, e.g., IMAP.
• Client authentication can be done with client certificates.
IPsec: Network Layer Security

- **Network-layer secrecy:**
  - sending host encrypts the data in IP datagram
  - TCP and UDP segments; ICMP and SNMP messages
- **Network-layer authentication**
  - destination host can authenticate source IP address
- **Two principle protocols:**
  - authentication header (AH) protocol
  - encapsulation security payload (ESP) protocol
- For both AH and ESP, source, destination handshake:
  - create network-layer logical channel called a security association (SA)
- Each SA unidirectional.
- Uniquely determined by:
  - security protocol (AH or ESP)
  - source IP address
  - 32-bit connection ID
Authentication Header (AH) Protocol

- provides source authentication, data integrity, no confidentiality
- AH header inserted between IP header, data field
- protocol field: 51
- intermediate routers process datagrams as usual

AH header includes:
- connection identifier
- authentication data: source-signed message digest calculated over original IP datagram
- next header field: specifies type of data (e.g., TCP, UDP, ICMP)
ESP Protocol

• provides secrecy, host authentication, data integrity.
• data, ESP trailer encrypted.
• next header field is in ESP trailer.

• ESP authentication field is similar to AH authentication field.
• Protocol = 50.
Transport vs. Tunneling

• Two IPSec modes of operation:
  1. Transport: encrypt/authenticate payload only
  2. Tunneling: wrap entire IP packet in new IPsec packet

• Tunneling allows for NAT
• Tunneling allows for VPNs
What is a VPN?

• Making a shared network work like a private network

• Why do this?
  – Private networks have all kinds of advantages
  – But building a private network is expensive
    • (cheaper to have shared resources rather than dedicated)
Virtual Private Networks

• Setting up a private network over a public connection
  – i.e. over the internet
• Secure communication with IPSec or SSL
  – Authentication
  – Confidentiality
• Can be implemented in or behind a firewall
IP VPN benefits

- IP not really global (private addresses)
  - VPN makes separated IP sites look like one private IP network
- Security
- Bandwidth guarantees across ISP
  - QoS, SLAs
- Simplified network operation
  - ISP can do the routing for you
End-to-end VPNs

• Solves problem of how to connect remote hosts to a firewalled network
Customer-based Network VPNs

Customer buys own equipment, configures IPsec tunnels over the global internet, manages addressing and routing. ISP plays no role.
Provider-based Network VPNs

Provider manages all the complexity of the VPN. Customer simply connects to the provider equipment.
IEEE 802.11 security

• War-driving: drive around Bay area, see what 802.11 networks available?
  – More than 9000 accessible from public roadways
  – 85% use no encryption/authentication
  – packet-sniffing and various attacks easy!

• Securing 802.11
  – encryption, authentication
  – first attempt at 802.11 security: Wired Equivalent Privacy (WEP): a failure
  – current attempt: 802.11i
Wired Equivalent Privacy (WEP):

• authentication as in protocol ap4.0
  – host requests authentication from access point
  – access point sends 128 bit nonce
  – host encrypts nonce using shared symmetric key
  – access point decrypts nonce, authenticates host

• no key distribution mechanism

• authentication: knowing the shared key is enough
WEP data encryption

• Host/AP share 40 bit symmetric key (semi-permanent)
• Host appends 24-bit initialization vector (IV) to create 64-bit key
• 64 bit key used to generate stream of keys, $k_{iIV}$
• $k_{iIV}$ used to encrypt $i$th byte, $d_i$, in frame:
  • $c_i = d_i \ XOR \ k_{iIV}$
• IV and encrypted bytes, $c_i$ sent in frame
Breaking 802.11 WEP encryption

• Security hole:
• 24-bit IV, one IV per frame, -> IV’s eventually reused
• IV transmitted in plaintext -> IV reuse detected
• Attack:
  – Trudy causes Alice to encrypt known plaintext \textit{d1 d2 d3 d4} ...
  – Trudy sees: \textit{ci} = \textit{di} XOR \textit{kiIV}
  – Trudy knows \textit{ci di}, so can compute \textit{kiIV}
  – Trudy knows encrypting key sequence \textit{k1IV k2IV k3IV ...}
  – Next time IV is used, Trudy can decrypt!
Firewalls
Firewalls

Firewalls isolate an organization's internal network from the larger Internet, allowing some packets to pass while blocking others.
Typical Setup

- **Internal DMZ network**
  - Web server(s)
  - Email server
  - DNS server

- **Internal protected network**
  - Application and database servers
  - Workstations

- **External firewall**
- **Boundary router**
- **LAN switch**

- **Internet**
Firewalls: Why

• prevent denial of service attacks:
  – SYN flooding: attacker establishes many bogus TCP connections, no resources left for “real” connections.

• prevent illegal modification/access of internal data
  – e.g., attacker replaces CIA’s homepage with something else

• allow only authorized access to inside network (set of authenticated users/hosts)

• two types of firewalls:
  1. application-level
  2. packet-filtering
Firewalls not just protection from outside attackers

• Bandwidth control
  – Block high bandwidth applications
  – Netflix, BitTorrent
• Employee network usage control
  – Block games, pornography, non-business uses
• Privacy
  – Don’t let outside see what you have, how big you are, etc.
  – Similar to making corporate phone directory proprietary
Packet Filtering

- internal network connected to Internet via router firewall
- router filters packet-by-packet, decision to forward/drop packet based on:
  - source IP address, destination IP address
  - TCP/UDP source and destination port numbers
  - ICMP message type
  - TCP SYN and ACK bits

Should arriving packet be allowed in? Departing packet let out?
## Simple firewall policy configuration

<table>
<thead>
<tr>
<th>Source</th>
<th>Dest</th>
<th>App</th>
<th>Action</th>
</tr>
</thead>
<tbody>
<tr>
<td>any-inside</td>
<td>dmz-mail</td>
<td>SMTP</td>
<td>allow</td>
</tr>
<tr>
<td>any-inside</td>
<td>any-outside</td>
<td>SMTP</td>
<td>drop</td>
</tr>
<tr>
<td>any-inside</td>
<td>any-outside</td>
<td>HTTP</td>
<td>allow</td>
</tr>
<tr>
<td>any-inside</td>
<td>any-outside</td>
<td>FTP</td>
<td>allow</td>
</tr>
<tr>
<td>any-inside</td>
<td>any-outside</td>
<td>any</td>
<td>drop</td>
</tr>
<tr>
<td>any-outside</td>
<td>any-inside</td>
<td>any</td>
<td>drop</td>
</tr>
</tbody>
</table>
Conversations

• FTP consists of two flows, control flow and data flow
• Firewall must be smart enough to read control flow, identify subsequent data flow
• True for SIP as well
Stateful and stateless firewalls

• Original firewalls were stateless
  – Maintain static filter list, but no per flow state
  – For TCP, only look at SYN
    • Means that non-SYN TCP packets are allowed even if should be blocked
  – No concept of conversation

• Modern firewalls are typically stateful
  – Maintains dynamic list of all allowed flows
  – Better capability, harder to scale
Application gateways

• Filters packets on application data as well as on IP/TCP/UDP fields.
• **Example:** allow select internal users to telnet outside.

1. Require all telnet users to telnet through gateway.
2. For authorized users, gateway sets up telnet connection to dest host. Gateway relays data between 2 connections.
3. Router filter blocks all telnet connections not originating from gateway.
Limitations of firewalls and gateways

- **IP spoofing**: router can’t know if data “really” comes from claimed source
- if multiple app’s. need special treatment, each has own app. gateway.
- client software must know how to contact gateway.
  - e.g., must set IP address of proxy in Web browser

- filters often use all or nothing policy for UDP.
- tradeoff: degree of communication with outside world, level of security
- many highly protected sites still suffer from attacks.
IDS
Intrusion detection

• “Building burglar alarms for the net”
• Idea: make systems sensitive to threatening actions, and make them capable of alerting authorities when they notice anomalies
• Necessarily post-hoc
• Broad types
  – Statistical analyzers (anomaly based)
  – Rules-based systems, Attack-signature detectors (misuse)
  – Others
Intruder Behavior

1. Target acquisition and information gathering
   – Map network, identify vulnerable services, social engineering

2. Initial access
   – Brute force user’s web based password, exploit remote vulnerability, spear-phish browser exploit

3. Privilege escalation
   – Exploit local application with elevated privileges, capture admin password
Intruder Behavior

4. Gather information or exploit system
   – Scan for other targets or capture sensitive data

5. Maintaining access
   – Install rootkit backdoor, disable anti-virus/IDS

6. Covering tracks
   – Modify logs and remove any trace of intrusion, use rootkit to hide files installed on the system
Know Your Attacker

• Most attackers run scripts to probe for vulnerabilities, then return later to exploit them
• Probes tend to come in waves as new holes are discovered
• Probes look very different than typical network use
• Actual attack may come long after probe
Paradigms in Intrusion Detection

• **Misuse Detection Intrusion Detection Systems (MD)**
  – define “what is abnormal” using attack signatures
  – traffic that matches an attack signature as attack traffic

• **Anomaly Detection Intrusion Detection Systems (AD)**
  – define “what is normal” using profiles
  – traffic that does not match the profile as abnormal
Bad detection

• False positives
  – Report activity as an intrusion, but it isn’t
  – Reduce by loosening intrusion detection rules

• False negative
  – Miss reporting bad behavior as an intrusion
  – Reduced by tightening intrusion detection rules
The world’s simplest ID system

v=listen(frequently-exploited-unused-port);
while(1) {
    s=accept(v, who, howbig);
    notify_the_authorities(s, who, howbig);
    close(s);
}

• This won’t catch stealth scanners
• Doesn’t have a global view
• Can’t detect attacks on systems in use
• Surprisingly effective at catching scans nonetheless
Statistical analysis

• Constantly capture packets, watch logs, note typical flows
  – I.E. “95% of traffic flows from inside the firewall to outside web services”
  – Set off alarm bells when traffic not matching typical flows is seen
  – Can be a first alert against configuration problems

• Gains a global picture of the system
Rule-based systems

- Monitor logs and network for behavior violating or matching static rules
- Require some knowledge of attack behaviors
- Less prone to false alarms
- Often combined with anomaly detectors
Example: Snort

From: Rafeeq Ur Rehman, *Intrusion Detection Systems with Snort: Advanced IDS Techniques with Snort, Apache, MySQL, PHP, and ACID.*
Snort components

• Packet Decoder
  – input from Ethernet, SLIP, PPP...

• Preprocessor:
  – detect anomalies in packet headers
  – packet defragmentation
  – decode HTTP URI
  – reassemble TCP streams

• Detection Engine: applies rules to packets

• Logging and Alerting System

• Output Modules: alerts, log, other output
Snort detection rules

Alert will be generated if criteria met

<table>
<thead>
<tr>
<th>Action</th>
<th>Protocol</th>
<th>Address</th>
<th>Port</th>
<th>Direction</th>
<th>Address</th>
<th>Port</th>
</tr>
</thead>
</table>

Apply to all ip packets

Source ip address

Source port #

Destination ip address

Destination port

Rule options

alert ip any any -> any any (msg: "IP Packet detected";)

Alert will be generated if criteria met
Additional examples

alert tcp any any -> 192.168.1.0/24 111
(content:"|00 01 86 a5|"; msg: "mountd access");

alert tcp !192.168.1.0/24 any -> 192.168.1.0/24 111
(content: "|00 01 86 a5|"; msg: "external mountd access");

!= negation operator in address
content - match content in packet
192.168.1.0/24 - addr from 192.168.1.1 to 192.168.1.255

https://www.snort.org/documents/snort-users-manual
Using an IDS

- Plan your incident response process well before you install the system
- Know what you’re looking for
- Make the system comprehensive
- Don’t overreact to alarms
- If using a rules-based system, keep up with vulnerability reports
Future
S-BGP Design Overview

- IPsec: secure point-to-point router communication
- Public Key Infrastructure: authorization for all S-BGP entities
- Attestations: digitally-signed authorizations
  - Address: authorization to advertise specified address blocks
  - Route: Validation of UPDATEs based on a new path attribute, using PKI certificates and attestations
- Repositories for distribution of certificates, CRLs, and address attestations
- Tools for ISPs to manage address attestations, process certificates & CRLs, etc.
DNSSEC

• Basically no change to packet format
  – Goal is security of DNS data, not channel security
• New Resource Records (RRs)
  – RRSIG : signature of RR by private zone key
  – DNSKEY : public zone key
  – DS : crypto digest of child zone key
  – NSEC / NSEC3 authenticated denial of existence
• Lookup referral chain (unsigned)
• Origin attestation chain (PKI) (signed)
  – Start at pre-configured trust anchors
    • DS/DNSKEY of zone (should include root)
  – DS → DNSKEY → DS forms a link
Other

• IPv6 – new IP protocol with improved security features (IPSec is integrated, discourages fragmentation)

• SDN – software defined network (allows greater monitoring and control)