Network Security Protocols and Defensive Mechanisms

*Slides borrowed from John Mitchell*
Network security

What is the network for?

What properties might attackers destroy?

- Confidentiality: no information revealed to others
- Integrity: communication remains intact
- Availability: messages received in reasonable time
Network Attacker

Intercepts and controls network communication

• Confidentiality
• Integrity
• Availability
Plan for today

- Protecting network connections
  - Wireless access—802.11i/WPA2
  - IPSEC

- Perimeter network defenses
  - Firewall
    - Packet filter (stateless, stateful), Application layer proxies
  - Intrusion detection
    - Anomaly and misuse detection
Last lecture

Basic network protocols
- IP, TCP, UDP, BGP, DNS

Problems with them
- TCP/IP
  - No SRC authentication: can’t tell where packet is from
  - Packet sniffing
  - Connection spoofing, sequence numbers
- BGP: advertise bad routes or close good ones
- DNS: cache poisoning, rebinding
  - Web security mechanisms rely on DNS
Protocol and link-layer connectivity
802.11i Protocol

Supplicant
Auth/Assoc
802.1X UnBlocked
PTK/GTK

Authenticator
Auth/Assoc
802.1X UnBlocked
PTK/GTK

Authentication Server
(RADIUS)
No Key

Link Layer

EAP/802.1X/RADIUS Authentication

4-Way Handshake

Group Key Handshake

Data Communication

802.11 Association

MSK
Network Protocol Stack

- Application
- Transport
- Network
- Link

Application protocol
TCP protocol
IP protocol
Network Access
Data Link

Application
Transport
Network
Link
TCP/IP CONNECTIVITY

How can we isolate our conversation from attackers on the Internet?
Basic Layer 2-3 Security Problems

- Network packets pass by untrusted hosts
  - Eavesdropping, packet sniffing
  - Especially easy when attacker controls a machine close to victim

- TCP state can be easy to guess
  - Enables spoofing and session hijacking
Virtual Private Network (VPN)

- Three different modes of use:
  - Remote access client connections
  - LAN-to-LAN internetworking
  - Controlled access within an intranet

- Several different protocols
  - PPTP – Point-to-point tunneling protocol
  - L2TP – Layer-2 tunneling protocol
  - IPsec (Layer-3: network layer)
IPSEC

- Security extensions for IPv4 and IPv6
- IP Authentication Header (AH)
  - Authentication and integrity of payload and header
- IP Encapsulating Security Protocol (ESP)
  - Confidentiality of payload
- ESP with optional ICV (integrity check value)
  - Confidentiality, authentication and integrity of payload
Recall packet formats and layers
IPSec Transport Mode: IPSEC instead of IP header

[Diagram of network protocols and packet structures]

http://www.tcpipguide.com/free/t_IPSecModesTransportandTunnel.htm
IPSEC Tunnel Mode
IPSec Tunnel Mode: IPSEC header + IP header
Mobile IPv6 Architecture

Mobile Node (MN)

Direct connection via binding update

Corresponding Node (CN)

- Authentication is a requirement
- Early proposals weak
- RFC 6618 – use IPSec
Summary

Protecting network connections

- **Wireless access**– 802.11i/WPA2
  - Several subprotocols provide encrypted link between user device and wireless access point
  - Ideally – wireless attacker in range of access point has no better chance for attack than a remote attacker

- **IPSEC**
  - Give external Internet connections equivalent security to local area network connections

- **Mobility**
  - Preserve network connections when a device moves to different physical portions of the network
  - Ideally – no attacks other than against non-mobile user
Second topic of today’s lecture

- Perimeter defenses for local networks
  - Firewall
    - Packet filter (stateless, stateful)
    - Application layer proxies
  - Intrusion detection
    - Anomaly and misuse detection
LOCAL AREA NETWORK

How can we protect our local area network from attackers on the external Internet?
Basic Firewall Concept

- Separate local area network from internet

All packets between LAN and internet routed through firewall
Screened Subnet Using Two Routers
Alternate 1: Dual-Homed Host
Alternate 2: Screened Host
Basic Packet Filtering

- Uses transport-layer information only
  - IP Source Address, Destination Address
  - Protocol (TCP, UDP, ICMP, etc)
  - TCP or UDP source & destination ports
  - TCP Flags (SYN, ACK, FIN, RST, PSH, etc)
  - ICMP message type

- Examples
  - DNS uses port 53
    - Block incoming port 53 packets except known trusted servers

- Issues
  - Stateful filtering
  - Encapsulation: address translation, other complications
  - Fragmentation
Source-Address Forgery
More about networking: port numbering

**TCP connection**
- Server port uses number less than 1024
- Client port uses number between 1024 and 16383

**Permanent assignment**
- Ports <1024 assigned permanently
  - 20, 21 for FTP
  - 23 for Telnet
  - 25 for server SMTP
  - 80 for HTTP

**Variable use**
- Ports >1024 must be available for client to make connection
- Limitation for stateless packet filtering
  - If client wants port 2048, firewall must allow incoming traffic
- Better: stateful filtering knows outgoing requests
  - Only allow incoming traffic on high port to a machine that has initiated an outgoing request on low port
Filtering Example: Inbound SMTP

Assume we want to block internal server from external attack

Can block external request to internal server based on port number
Filtering Example: Outbound SMTP

Assume we want to allow internal access to external server

Known low port out, arbitrary high port in
If firewall blocks incoming port 1357 traffic then connection fails
Stateful or Dynamic Packet Filtering

Assume we want to allow external UDP only if requested.
Telnet

How can stateful filtering identify legitimate session?

1. Client opens channel to server; tells server its port number. The ACK bit is not set while establishing the connection but will be set on the remaining packets.

2. Server acknowledges

Stateful filtering can use this pattern to identify legitimate sessions.
FTPL

How can stateful filtering identify legitimate session?

1. Client opens command channel to server; tells server second port number.

2. Server acknowledges.

3. Server opens data channel to client’s second port.

4. Client acknowledges.

FTP Server

FTP Client

20 Data

21 Command

“PORT 5151”

“OK”

DATA CHANNEL

TCP ACK

34
Normal IP Fragmentation

Complication for firewalls

Flags and offset inside IP header indicate packet fragmentation
Abnormal Fragmentation

Low offset allows second packet to overwrite TCP header at receiving host
Packet Fragmentation Attack

- Firewall configuration
  - TCP port 23 is blocked but SMTP port 25 is allowed

- First packet
  - Fragmentation Offset = 0.
  - DF bit = 0 : "May Fragment"
  - MF bit = 1 : "More Fragments"
  - Destination Port = 25. TCP port 25 is allowed, so firewall allows packet

- Second packet
  - Fragmentation Offset = 1: second packet overwrites all but first 8 bits of the first packet
  - DF bit = 0 : "May Fragment"
  - MF bit = 0 : "Last Fragment."
  - Destination Port = 23. Normally be blocked, but sneaks by!

- What happens
  - Firewall ignores second packet “TCP header” because it is fragment of first
  - At host, packet reassembled and received at port 23
TCP Protocol Stack

Application protocol

TCP protocol

IP protocol

Data Link

Network Access

Application

Transport

Network

Link

Application

Transport

Network

Link
Proxying Firewall

- Application-level proxies
  - Tailored to http, ftp, smtp, etc.
  - Some protocols easier to proxy than others
- Policy embedded in proxy programs
  - Proxies filter incoming, outgoing packets
  - Reconstruct application-layer messages
  - Can filter specific application-layer commands, etc.
    - Example: only allow specific ftp commands
    - Other examples: ?
- Several network locations – see next slides
Firewall with application proxies

Daemon spawns proxy when communication detected ...
Application-level proxies

- Enforce policy for specific protocols
  - E.g., Virus scanning for SMTP
    - Need to understand MIME, encoding, Zip archives
  - Flexible approach, but may introduce network delays
- “Batch” protocols are natural to proxy
  - SMTP (E-Mail)          NNTP (Net news)
  - DNS (Domain Name System)  NTP (Network Time Protocol)
- Must protect host running protocol stack
  - Disable all non-required services; keep it simple
  - Install/modify services you want
  - Run security audit to establish baseline
  - Be prepared for the system to be compromised
Web traffic scanning

- Intercept and proxy web traffic
  - Can be host-based
  - Usually at enterprise gateway
- Block known bad sites
- Block pages with known attacks
- Scan attachments
  - Virus, worm, malware, ...
Firewall references

Elizabeth D. Zwicky
Simon Cooper
D. Brent Chapman

William R Cheswick
Steven M Bellovin
Aviel D Rubin
Intrusion detection

Many intrusion detection systems
- Network-based, host-based, or combination

Two basic models
- Misuse detection model
  - Maintain data on known attacks
  - Look for activity with corresponding signatures
- Anomaly detection model
  - Try to figure out what is "normal"
  - Report anomalous behavior

Fundamental problem: too many false alarms
Example: Snort

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

http://www.snort.org/
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

Apply to all ip packets

Source ip address

destination ip address

Source port #

Destination port

Rule options

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

- Misuse detection – avoid known intrusions
  - Database size continues to grow
  - Snort version 2.3.2 had 2,600 rules
  - Snort spends 80% of time doing string match

- Anomaly detection – identify new attacks
  - Probability of detection is low
Difficulties in anomaly detection

- Lack of training data
  - Lots of “normal” network, system call data
  - Little data containing realistic attacks, anomalies

- Data drift
  - Statistical methods detect changes in behavior
  - Attacker can attack gradually and incrementally

- Main characteristics not well understood
  - By many measures, attack may be within bounds of “normal” range of activities

- False identifications are very costly
  - Sys Admin spend many hours examining evidence
Summary

Protecting network connections
- Wireless security – 802.11i/WPA2
- IPSEC

Perimeter network perimeter defenses
- Firewall
  - Packet filter (stateless, stateful),
  - Application layer proxies
- Intrusion detection
  - Anomaly and misuse detection

Network infrastructure security
- BGP vulnerability and S-BGP
- DNSSEC, DNS rebinding