Operational Practices

Internet Security [1] VU

Engin Kirda engin@infosys.tuwien.ac.at
Christopher Kruegel chris@auto.tuwien.ac.at

Admin Issues and News

- Reminder: Exam on the 28th, registration required
  - You will *only* be allowed to take the exam if your account has not been suspended (login and find out) and any open issues have been resolved. Further exam next semester, in urgent cases, contact us (oral exam possible any time)
- TUWIS Bewertungsform (do give us feedback)
- CTF last Friday (no, we did not take part as claimed ;-))
  - http://www.heise.de/newsticker/meldung/60443
  - http://futurezone.orf.at/futurezone.orf?read=detail&id=268141
  - We will take part next semester

Outline

- Basic Steps
- *Wrappers*
- *Firewalls*
  - General Overview
  - Packet Filter, Stateful-Inspection
    - `iptables`
  - Circuit-Level Gateway, Application Gateway
- Intrusion Detection (ID) and ID Systems
- Basic Wireless Security

Basic Steps in Protecting Yourself

- Update your computer(s):
  - Windows: *Windows Update*
  - Linux: apt-get (Debian), yum (Fedora), urpmi (Mandrake)
- Updating will “protect” you against buffer overflows, viruses, worms, etc.
- Use anti-spyware programs
  - e.g., AdAware, Spybot, Hijackthis

TCP Wrappers

allow host based access control on connections

- tcpd replaces daemons from inetd
- listens at ports, accepts connections
- checks `hosts.allow` and `hosts.deny`
- allows
  - log connection
  - perform double reverse lookups (prevent DNS/spoofing attacks)

Firewall

- Local network is trusted
- “Outside” is potentially malicious
- Unprotected network
  - security is implemented on each host
  - single vulnerable host would violate whole network security
  - administrative nightmare
- Protected network
  - place barrier at the borders of trusted, inside network
  - barrier provides access control
  - helps with system monitoring and simplifies management

  → such a barrier is called firewall

Firewall

- Not the ultimate solution
  - cannot deal satisfactorily with content
  - vulnerable to inside attacks and covert channels
  - potential performance bottlenecks
  - when compromised, network is unprotected
- Security Strategies
  - least privilege
    - only permissions that are necessary should be granted
  - defense in depth
    - additional security installations should be present
  - controlled access
  - fail-safe
    - a failing firewall may not reduce security

Filtering Routers

- Filtering Routers route packets between internal and external hosts
  - do it selectively – perform filtering
    - allow or block certain types of packets
- Screening procedure is based on
  - Protocol (whether the packet is a TCP, UDP, or ICMP packet)
  - IP source/destination address
  - TCP or UDP source/destination port
  - TCP flags
  - ICMP message type
  - interfaces where packets are arriving and leaving

Filtering Rules

- specify the filtering that is used

- Each rules specifies
  - action (allow, deny)
  - source address/port pattern
  - destination address/port pattern
  - presence or absence of flags

- When a packet is received the rules are applied in an ordered sequence
  - if a rule matches the corresponding action is taken
  - if no rule matches, a default action is taken

Packet Filter

- Old ones might be vulnerable to spoofing
- Fragmented Datagrams
  - discarded when not enough information to apply filter
  - when first fragment contains enough information, remaining ones are passed unchecked
  - potential vulnerability
    - first fragment with innocent values
    - other fragments with non-zero offset rewrite these values with malicious ones
    - reassembled fragment is delivered to protected service

Filtering UDP Datagrams

- Not possible without keeping state
- impossible to associate a UDP reply to a UDP request, e.g.
  - internal host sends UDP datagram to remote host (localhost,localport,remotehost,remoteport)
  - remote host sends back a udp reply (remotehost,remoteport,localhost,localport)
- so usually UDP traffic is blocked in stateless firewalls

- Solution: Dynamic Filtering
  - filtering router remembers outgoing UDP packets
  - creates a temporary rule that lets reply packets pass

Packet Filter

- Advantages
  - easy to implement (relies on existing hardware)
  - good performance
- Limits
  - limited auditing
  - difficult to configure
  - not very flexible, extensible
- Linux and Windows
  - `iptables`, `ipchains`, `Windows XP SP2`

iptables

- `iptables` is used to set up, maintain, and inspect the IP firewall rules in the Linux kernel

- Rules are organized in “chains” (i.e, ordered lists)
  - chains can be associated with different phases in the datagram handling process
    - input, output and forward chain
  - `iptables` supports user-specified chains
    - allow to “jump” to a chain of rules in case of a match

Stateful Inspection

- acts as a packet filter
- but accesses higher-level protocol information
  - check also content of packet / deny on match (e.g. virus)
  - allows to track sessions (e.g. ftp, http)
  - virtual sessions for connection-less protocols (e.g. UDP)
    - firewall stores ports used in a particular UDP transaction
    - temporarily creates an exception to let the answer pass through
- `Checkpoint` firewall

Gateway

- A gateway is a host with two (or more) network interfaces
  - (usually) operating system is configured so that IP forwarding is disabled
  - Traffic can pass across the gateway only if there is an application that explicitly operates the transfer (proxy)
- Proxy Service
  - application that acts as an intermediary between client within the protected network and server in the outside world and vice versa
  - when a client requests a connection to the outside, it actually connects to the proxy
  - proxy examines the connection request with respect to security policy
  - and possibly opens the actual connection to the server on behalf of the client

Circuit-Level Gateway

- Not only checks packets, but sessions / connections
  - based on user / password (e.g. first telnet to gateway, then telnet to the outside)
  - time of day
- all traffic is disallowed, only validated sessions may transfer data
- do not need to be aware of the protocol
- cannot perform application-level filtering

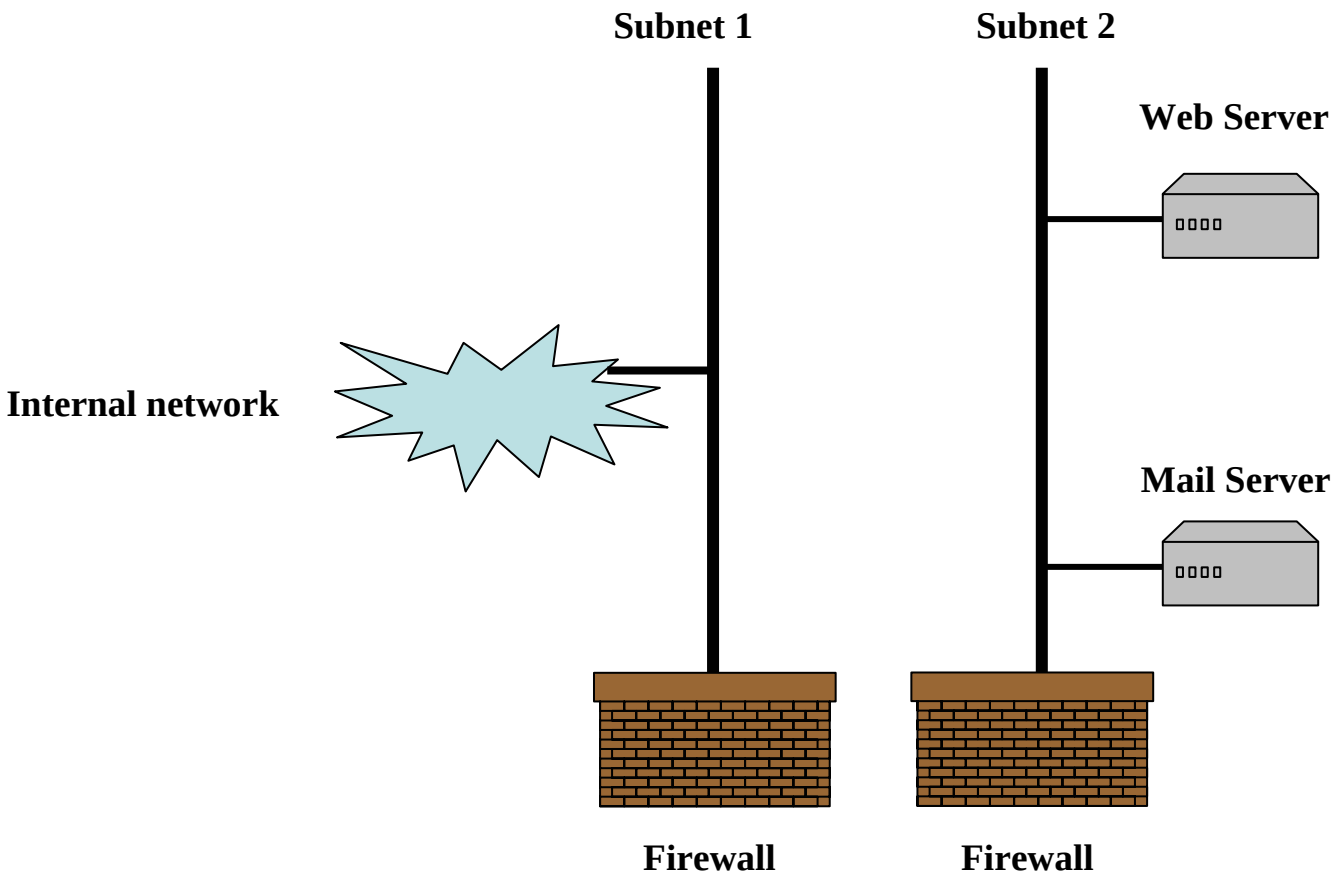
Application Gateway

- Application-level gateways interpret the particular application protocol being “proxied”
  - e.g. HTTP / FTP
  - need to know the application protocol details
  - need a different proxy for each protocol
  - can perform advanced filtering
- Advantages
  - cheap
  - extensive logging possible
  - secure – internal network invisible
  - might cache requests and replies
- Limits
  - scalability, performance bottleneck

De-Militarized Zone

- DMZ – de-militarized zone
  - network area between two packet filters
    - external filter only allows traffic from outside
    - internal filter only allows traffic from inside
  - separates external and internal network
  - contains hosts that provide
    - external services (e.g. web server, DNS) and
    - application gateways for internal clients
  - when hosts are compromised
    - internal traffic cannot be sniffed
    - protection from internal packet filter

De-Militarized Zone 2



Intrusion Detection

- Process of identifying and responding to malicious activities targeted against networks and its resources

- System that performs intrusion detection is called *Intrusion Detection System* (IDS)
  - complements prevention techniques (e.g. firewalls)
    - defense mechanism behind outer barrier
    - works against insiders
  - important market for security companies (ISS, Cisco)

Intrusion Detection Techniques

- Misuse-based
  - observed behavior is compared against description of known, undesirable behavior (signatures)
  - intrusion assumed when signature spotted in input data
  - comparable to virus scanner
  - all commercial systems follow this approach

  - Advantages
    - accurate reports (low false positive rate)

  - Disadvantages
    - needs continous update of signatures (like virus scanner)
    - unable of detecting novel intrusions

Intrusion Detection Techniques

- Anomaly-based
  - behavior is compared against description of anticipated, legal behavior (profile)
  - intrusion assumed when deviation between input and profile significant
  - statistical methods, AI techniques (neural networks)

  - Advantages
    - capable of detecting novel attacks

  - Disadvantages
    - difficult to configure / train
    - high number of false alarms (incorrect detects)

Intrusion Detection Domains

- Network-based
  - input data is gathered from the network
  - packet sniffer, protocol analysis
  - Advantages
    - access to events related to multiple hosts from a single sampling point
  - Disadvantages
    - performance issues (de-fragmenting, reassembling)
    - encryption

Network-Based Detection

- Commercial systems
  - RealSecure (ISS)
- Academic systems
  - NetSTAT (UCSB): describes attacks using state transitions
  - Emerald (SRI), expert systems, correlation
- Snort (`http://www.snort.org`)
  - designed to be lightweight and fast
  - based on libpcap (reads/writes tcpdump files)
  - simple rule-based analysis engine
  - simple pattern-matching functionalities

Intrusion Detection Domains

- Host-based
  - produce data related to host activity
  - two main sources
    - operating system
      - Syslog Daemon, `klogd`
      - Solaris Auditing – Basic Security Model (BSM)
      - Windows NT Events
    - application level
      - `Apache` logs
      - `ftpd` logs

Intrusion Detection Domains

- Syslog
  - Logging facility available in all UNIX system
  - accessible through `syslog()` that sends a log message to `syslogd/klogd`
- Syslog message
  - Identity - usually the program name
  - Facility – specifies the source of the message (kernel, user, mail, lpr, authpriv, daemon)
  - Level - determines the importance of the message (emerg, alert, crit, err, warning, notice, info, debug)
  - Text message

Intrusion Detection Domains

- Syslog Configuration
  - syslog behavior is customized using `syslog.conf`
  - lines `<facility>.<level spec> <destination>`
- Destination
  - file (e.g., /var/log/messages)
  - remote host (e.g., @logger.infosys.tuwien.ac.at) UDP (514)
  - user
  - named pipe (e.g. |/tmp/my-log)

```
kern.* /var/adm/kernel
kern.crit @logger
kern.info;kern.!err /var/adm/messages
```

Intrusion Detection Domains

- Linux Intrusion Detection System (http://www.lids.org)
  - LIDS implements a reference monitor and mandatory access control in the Linux kernel
  - allows one to specify access control for files, processes, and device that cannot be bypassed even by root
  - configurable through lidsadm, command line tool with syntax similar to ipchains
  - to access the LIDS system it is necessary to provide a password which has to be set during a LIDS-free session
  - LIDS can be configured to log through klogd any attempt to violate the rules

Intrusion Detection Domains

- On-line
  - Swatch
    - Simple WATCHdog – checks for patterns in syslog files
  - USTAT
    - UC Santa Barbara – State Transition Analysis Technique
  - Emerald

- Off-line
  - Tripwire (http://www.tripwire.org)
    - cryptographical checksums of important files (MD5 hash)

Intrusion Detection Framework

- Common Intrusion Detection Framework (CIDF)
  - is an effort to develop protocols and application programming interfaces
  - intrusion detection research projects can
    - share information and resources (intrusion reports)
      - IDMEF (ID messase exchange format)
    - and reuse components
- CIDF defines the IDS architecture in terms of
  - E-boxes - Event generators
  - A-boxes - Event analyzers
  - D-boxes - Event databases
  - R-boxes - Response units

Intrusion Detection Challenges

- Recognize malicious actions in the huge stream of events provided by network monitors and host auditing facilities
- Detect intrusions in real-time
- Correlate detection results within and across security domains
- Integrate different systems so that all techniques (anomaly, misuse) and domains (host, network) are covered
- Deploy ID systems in very different environments and take into account the characteristics of the protected computer networks

IDS and firewalls

- Firewalls and IDS will eventually be combined into a single capability
  - Many firewalls can trigger alerts when traffic to “bad destination” is seen
  - This capability can be used to build “burglar alarms”
- A burglar alarm is a misuse detection system that is carefully targeted
  - You may not care about people port-scanning your firewall from the outside, but this information is important if it is happening from the *inside*.
  - Trivial burglar alarms can be built using tcpdump and perl

Honey Pots

- A honey pot is a system that is deliberately named and configured so as to *invite* attack
- Goals:
  - Make it look inviting (e.g., Bigbank.com)
  - Make it look weak and easy to crack
  - Instrument every piece of the system
  - Monitor all traffic going in or going out
  - Alert administrator whenever someone accesses the system
- Trivial honey pots can be built using tools like
  - Tcpwrapper
  - Restricted/logging shells (sudo, adminshell)

Honey Pots 2

- Advantages:
  - Easy to implement
  - Easy to understand
  - Reliable
  - No performance cost
- Disadvantages:
  - Assumes hackers are not “intelligent”
    - Most hackers know about the presence of honey pots and “sophisticated” hackers may be careful

Wireless LAN (IEEE 802.1)

- Terminology
  - Station (STA): Most of the time, STAs are regarded as computing devices taking part in the wireless network and used by the end user
  - Access Point (AP): Any entity that has station functionality and provides access to the distribution services, via the wireless medium (WM) for associated stations
  - The Basic Service Set (BSS) is the basic building block of a wireless network, Communications take place in the so called Basic Service Area (BSA)
  - Service Set Identifier (SSID), network name

Overview of WLANs

- Wireless networks are increasingly getting popular
  - You find them around you (at home ;-)), hotels, conferences, airports etc.
  - Wardriving (looking for “open” networks)
  - IEEE 802.11 (Wireless LAN) offers basic network protection at best. New standards have emerged, but are currently “not” widely used. Insecure 802.11b very common
- Wireless access points are popular destinations of attack because…
  - Attackers are looking for “free” or anonymous access
  - The current encryption algorithm is weak and can be cracked
  - Extra antennas can be mounted to improve reception and hence are easily reachable (wired access needs physical presence!)

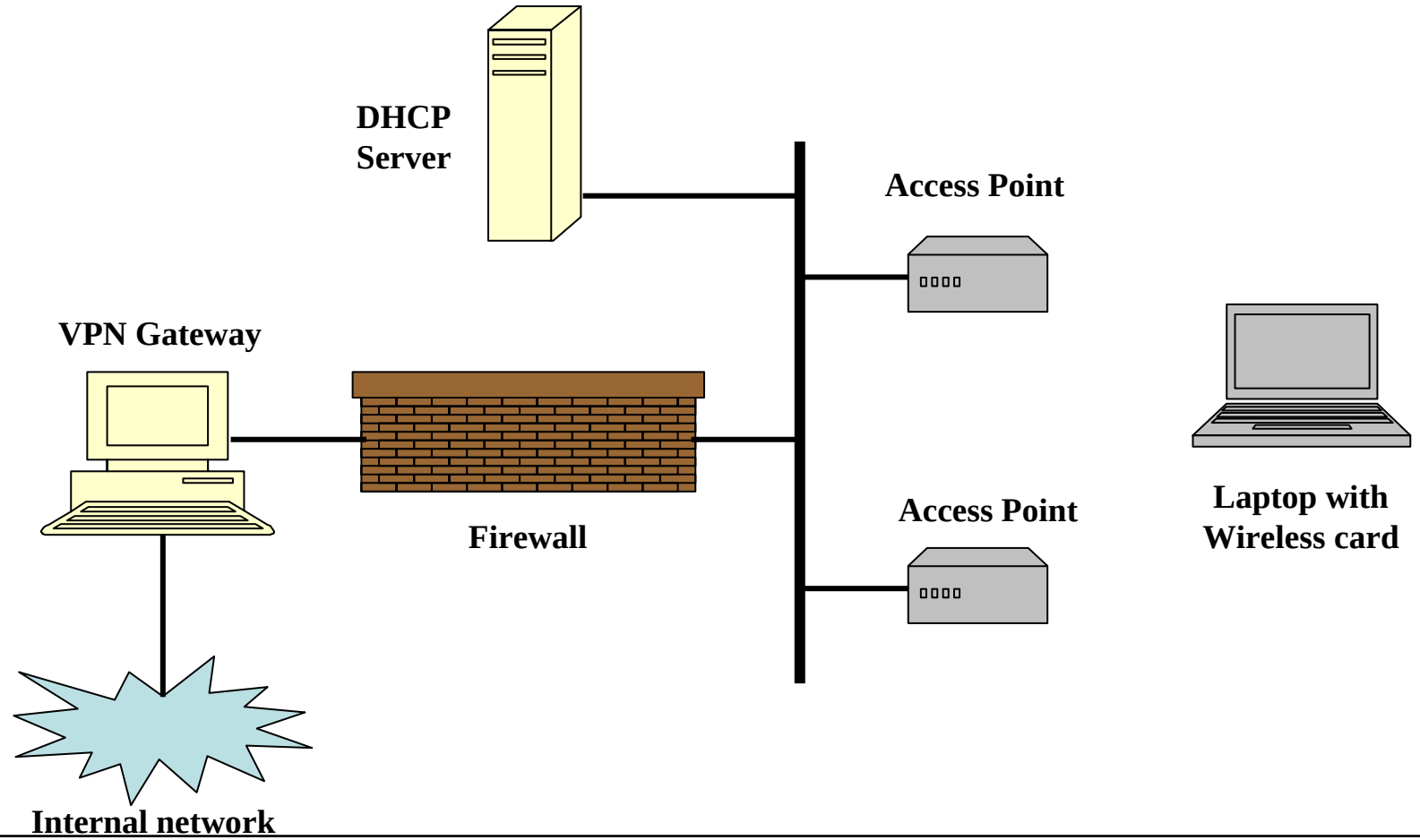
Wireless Security

- WEP encryption used in wireless networks is weak
  - The cracking process typically involves two programs: One program is used to sniff packets and a program such as *WEPCrack, Airsnort* can be used to recover the key by analyzing the packets
  - May take anywhere from a couple of hours to a couple of days to gather packets and a couple of hours to crack the key (new attack techniques: minutes)
- WEP and MAC access controls at best security through obscurity
  - The attacker can passively sniff network traffic – there is no way to stop this

Wireless Security 2

- Limiting the signal leakage outside the building
  - Difficult, but would provide protection against passive sniffing
- Wireless networks may only allow access to certain MAC addresses
  - Some WLAN cards may allow you to change the MAC address of your card! Many tools exist such as xNix or Windows itself ;-) Some default Windows drivers provide the ability to change MAC address
  - SSIDs (network identifier) in WLAN is not a security mechanism – it is better not to broadcast it (attacker has to sniff)

A “good” wireless network architecture



Conclusion

- In this lecture, we looked at:
  - Operational practices and defense techniques
  - Firewalls, Intrusion Detection Systems
  - Honeypots
  - Basic wireless network security
- Next time, Joe Pichlmayr will talk about viruses and the anti-virus business
  - Get insight about real-life virus / worm issues
  - Basic virus concepts (part of exam topics)