

PA197 Secure Network Design

7. Network Defense Mechanisms

Eva Hladká, Luděk Matyska

Faculty of Informatics

April 12, 2016

Content

- 1 Firewalls and application gateways
 - Firewalls
 - Packet Filters
 - Stateful Firewalls
 - Application gateways
 - Personal firewalls
- 2 Intrusion Detection Systems
 - IDS for Mobile Networks
- 3 Honeypots

Firewalls

- Concept of **inside** and **outside** of a network
 - different trust levels
 - different security levels
 - access control is on the **boundary** (**perimeter**)
- **Firewall** as the boundary keep
 - makes decisions to allow or deny passage of packets according to a specified policy
 - **demilitarized zone (DMZ)**
 - reference monitor
 - unbypassable, tamperproof, analyzable (logs)
 - defines security perimeter
 - access control/security imposed
 - exposure limit
 - partitions the network (security domains)

Firewall Policy

- Firewall enforces a policy
 - administrative boundaries
 - what kind of data to block/pass?
- Philosophies
 - default: allow or deny?
 - inbound or outbound traffic
 - symmetric or asymmetric (same/different rules for in/out bound traffic)
- Rules
 - generation: manual versus automatic (learning)
 - simple or complex rules?

Characteristics

- Design goals
 - all traffic between “inside” (network behind the firewall) and “outside” network must go through the firewall
 - only authorized traffic is allowed to pass
 - security/access policy
 - firewall itself is tamperproof
 - use of trusted system
 - secure operating system

Characteristics II

- General techniques
 - **service** control
 - what can be accessed
 - **user** control
 - who can use a particular service
 - **behaviour** control
 - how the service is used
 - **direction** control
 - inbound and outbound traffic treated differently

Types of Firewalls

- **Packet filters**
 - first generation
 - operate at the IP layer
- **Stateful inspection**
 - second generation
 - also called **circuit-level** firewalls
 - operate at the transport layer
- **Application layer**
 - third generation
 - also called **application gateway**
 - higher layers, it can “understand” the traffic
- **NAT**
 - only partially belongs here
 - hides internal network
 - protects against network reconnaissance

Packet Filters

- Basic properties
 - list of rules to apply
 - IP addresses, ports, protocols, flags, interfaces, ...
 - usually using data from IP (or TCP) header
 - not strictly layer 3 only
- **Stateless**
 - applies **set of rules** to each incoming packet
 - forwards or discards it
- **Uni-directional**
 - each direction is treated independently
- **High throughput**

Stateful Firewalls

- Tracks state information of connections
 - maintains table of active connections
 - passively monitors them
- **Context sensitive**
 - context established by preceding packets
 - dynamic change of filtering rules
- Expensive setup, cheap processing
 - inclusion of a session (TCP, UDP) into the table
 - cheap processing of packets within a session
- UDP and ICMP problems
 - not truly stateful protocols
 - end of session only through timeout

iptables and nftables

- Linux application to configure Linux kernel firewall
- Different modules:
 - iptables for IPv4
 - ip6tables for IPv6
 - arptables for ARP
 - ebtables for Ethernet frames

Gradually replaced by nftables

- Features:
 - packet filtering
 - connection tracking (stateful)
 - NAT
 - rate limiting
 - logging

nftables—examples

- Project to provide packet filtering and classification for Linux
 - Linux kernel engine: a virtual machine optimized for network packet inspection controlled through a bytecode; also atomic rule replacement API
 - user space utility: translates rules into bytecode
- Command line tool: **nft**
- Examples of simple rules
- Drop TCP traffic for port 22
 - `nft add rule filter forward tcp dport 22 drop`
 - `nft add rule filter2 input tcp dport { telnet, http, https } accept`

Simple firewall

```
table firewall {
    chain incoming {
        type filter hook input priority 0;
        # accept established and related connections
        ct state established,related accept
        # accept loopback interface traffic
        iifname lo accept
        # accept icmp
        icmp type echo-request accept
        # open sshd (22) and httpd (80) tcp ports
        tcp dport {ssh, http} accept
        # reject everything else
        drop
    }
}
```

Application Layer Firewalls

- Proxy (application gateway)
 - the firewalls serves/looks as a **proxy**
 - all traffic goes through it (relay at the application layer)
 - decisions customized to the application
 - application context
 - examples: e-mail or web filter
- **Deep packet inspection**
 - beyond stateful inspection
 - deep knowledge of **application payload**
- Challenges
 - performance (induced latency)
 - complexity
 - breaks end-to-end principle—secure connections

Personal firewalls

- The original idea of **secure perimeter** is becoming obsolete
 - too many intentional holes in firewalls
 - VPNs, VLAN extensions
 - encrypted traffic
- Insiders' threats
 - 60–80 % attacks go from inside the network
- The “demilitarized zone” pushed to a single machine
 - each machine protected independently
 - highly adaptive (to full programs)
 - excellent context
 - performance impact

Demilitarized zone

- An environment with machines/systems **deliberately** exposed to the external network
- Allows to provide service to external subjects
- Also behind the firewall
 - all traffic between DMZ and internal network as well as between DMZ and external network goes through the firewall
- Single firewall solution
 - three lines from a firewall
 - to the external world
 - to the internal network
 - to the DMZ
- Two firewalls solution
 - the first firewall stands between the DMZ and the external world
 - the second firewall stands between the DMZ and internal network

Firewall shortcomings

- Bugs and errors
 - software bugs and misconfigurations occur
- Perimeter redefinition
 - WiFi and mobile devices
 - external partners with need to access internal network
 - BYOD policy
- Perimeter extension through VPN
 - weak control of the other side
- Insider threats
 - majority of attacks from inside
 - weakening the perimeter does not help
 - social engineering, phishing, allowed services exploits

Intrusion Detection Systems

- We should accept that no protection is perfect
 - the attacker will get in!
- Intrusion Detection Systems
 - monitor network activity
 - look for sign of intrusion/intrusion attempts
 - detect and then react
- Where to monitor
 - Network IDS
 - like an application gateway
 - Host IDS
 - like a personal firewall

Network IDS

- Monitors network for malicious or suspicious events
 - network tap
 - span port
 - software in promiscuous mode (tcpdump)
 - deployed across the (local area) network
- Advantages
 - low cost
 - transparent to users (and adversary)
 - isolation
 - visibility across network
 - recognizes gradual attack
- Problems
 - encryption
 - evasion techniques
 - not able to detect “normal” modes

Alerts

- IDS raises an alert if an anomaly is found
- Accuracy is of critical importance
- Correct modes:
 - True positive
 - a true attack is correctly recognized
 - True negative
 - an anomaly is correctly detected as “no attack”
- Incorrect modes
 - False positive
 - reports an attack that does not exist
 - False negative
 - attack goes unrecognized (no alert)

Detection

- Looking for **anomalies**
 - unexpected behaviour taken as evidence of intrusion
 - needs a model of “normal” behaviour
 - thresholds/statistical modeling/Markov-based (state)
 - **statistical anomaly-based**
- Used metrics
 - traffic extent, connection attempts, payload byte distribution, flows
 - selected features should characterize expected behaviour
- Advantages
 - broad coverage (**learning**; able to detect previously unknown attacks)
 - not easy to evade
- Disadvantages
 - need training, false positives (alerts), legitimate changes in behaviour

Misuse Detection

- Direct search for **known bad** behaviour
- **Signature-based**
 - rule-based detection
 - **signatures**; states, pattern-matching
 - activity patterns matching known attack or policy violation
- Database of signatures
- Advantages
 - lower false positive rate
 - could include specific alerts
- Disadvantages
 - narrow (only known attacks)
 - evasion prone
 - need constant updates (external source)

Snort

- Widely used open source NIDS
 - signature based
- Features
 - protocol analysis
 - content searching/matching
- Attack detection
 - buffer overflows
 - stealth port scans
 - CGI attacks
 - SMB probes
 - OS fingerprinting etc.
- Available at <http://www.snort.org>

IDS for Mobile Wireless Networks

- Use case will be provided based on the following articles:
 - Y. Zhang, W. Lee, Y-A. Huang (2003): Intrusion Detection techniques for Mobile Wireless Networks.
 - P.M. Mafra, J.S. Fraga, A.O. Santin (2014): Algorithms for a distributed IDS in MANETs. J. Comp. Syst. Sciences, VOI 80(1), pp. 554–570.

Honeypots

- Using **deception** as a defense
 - diverting attack to a secure site
 - consuming attacker's resources
 - forcing them to reveal their techniques/goal
- Pretends to be the attacker's target
- Allows to study vulnerabilities and what adversary does after gaining control
- Hig/Low interaction honeypots

High Interaction Honeypots

- Real (full) systems and services
- Allow full compromise of the target system
- Mostly virtual systems
 - easily to replace/manage
- Challenges
 - maintenance, scaling
 - risk of further attacks (originating from honeypot)
 - intrusion detection (e.g. dynamic taint analysis)
- Output
 - attack footprint (registers, memory, applications, ...)

Low Interaction Honeypots

- Just emulate aspects of real system
 - limited interaction
 - statistics collection
- Advantages
 - simplicity, maintenance
 - easy installation
 - low risk (no attack originating from honeypot)
- Outputs similar to high interaction honeypots

Summary

- Definition of a **perimeter** and internal and external network
- Putting **firewall** at the perimeter
 - able to detect and stop open attacks
 - weak against current perimeter diffusion
 - majority of attacks from inside
- Continuous monitoring through IDS
 - could reveal attacks regardless of origin
 - adaptable to new threats
 - improper setup could be dangers (e.g. too many false positives)
- Next lecture: More extensive traffic monitoring