Network Security
Attack Overview

Dr. Dr. habil. Robert Koch
Prof. Dr. Peter Martini

Focus of Chapter 2

- Definition of attacks
- Attack taxonomies
- Attacker capabilities
- Examples of attack techniques with technical details

CIA Triad

- Model for security policy development
- Important: regularly, one can't improve all aims simultaneously
- Today, lot of additional and subcategories are available
Protection Targets

- Untraceability
- Unobservability
- Unlinkability
- Anonymity
- Pseudonymity
- Covertness/Obscurity
- Plausible Deniability
- Accountability
- Authenticity
- Non-Propagation
- Controllability
- Dependability/Reliability
- Flexibility/Transparency
- Finality/Immutability
- Integrity

An Attack...

- What is it? Legal vs. technical issues, ...
- Attack defined by Committee on National Security Systems (CNSS): "Any kind of malicious activity that attempts to collect, disrupt, deny, degrade, or destroy information system resources or the information itself"  
- Cyber attack defined by CNSS: "An attack, via cyberspace, targeting an enterprise's use of cyberspace for the purpose of disrupting, disabling, destroying, or maliciously controlling a computing environment/infrastructure; or destroying the integrity of the data or stealing controlled information"

Reports and Statistics

- There are numerous well-known reports on a regularly base, e.g., ISTR, DBIR, M-Trends, X-Force, MS SIR, ...
- That gives an idea, but enough for making hard decisions?
- Trivial, but important: what’s in?  
  - Pings, scans and respective statistics...  
  - Significant incidents, e.g., CSIS
- But... Where does the data come from? And what does it mean?
The Devil is in the Details

- Data used in reports can be heavily biased
- E.g., „Top 10 exploited vulnerabilities“ in DBIR 2015
- Evaluation of CVE-2002-1931, …, by Rory McCune and Jericho


- Read the links!

Even Worse

- Same applies for Vulnerability Statistics
- What can they really provide?

https://blog.osvdb.org/category/vulnerability-statistics/
Christey and Martin, „Buying into the bias: Why vulnerability statistics suck,” BlackHat 2013
- Read the link/presentation!

Attack Taxonomy

- What for?
  - General characteristics (Lindqvist and Jonsson, 1997)
    - The categories are mutually exclusive, no overlapping between categories
    - Clear and unambiguous classification criteria: a repeated classification should produce the same results
    - Comprehensible and useful
    - Comply with established terminology
Kill Chain

- A kill chain is a **phased-based model** to describe stages of an attack
- The identified information can help to prevent attacks

**Find** → **Fix** → **Track** → **Target** → **Engage** → **Assess**

- Adaptation: Cyber Kill Chain by Lockheed Martin
What is an „APT”?

- Advanced: operators have a full spectrum of intelligence-gathering techniques at their disposal. These may include computer intrusion technologies, but also extend to conventional intelligence-gathering techniques, such as telephone-interception technologies, satellite imaging and Human Intelligence (HUMINT) capabilities.
- Persistent: priority to a specific task, rather than seeking for financial or other gain.
- Threat: intent, opportunity, capability

Known Groups

- More than 130 Groups tracked worldwide
- First comprehensive analysis: Mandiant APT1 Report, 2004

„APT Detection“

- Talking about IDS/IPS in Chapter 7
- But remember „pizza box detection“
Most Important: WHO can do WHAT and HOW?

6-Tier Attack Model

- Tiers V–VI: Introducing new vulnerabilities
- Tiers III–IV: Finding new/unknown vulnerabilities
- Tiers I–II: Exploitation of known vulnerabilities

Existential vs. Trivial

Source: DSB TASK FORCE REPORT

Attack Overview: Service & Transmission

- Client
  - Phishing
  - Spoofing
  - XSS
  - Malicious Content

- DNS
  - Sniffing
  - MITM
  - Session Hijacking
  - DNS Relaying
  - Cache Poisoning
  - HTTP Request Smuggling

- Web Server
  - Buffer Overrun
  - Format String
  - Directory Traversal
  - Standard Accounts
  - ...
Refresher: Transmission Control Protocol

- Provides reliable, ordered and full-duplex byte streams
- Segment-based: data can be split up into segments
- Connection-oriented: special segments for session control
- Reliable: segments are acknowledged by the recipient
- Ordered: sequence numbers denote a segment’s offset in a stream

Refresher: TCP Header

Refresher: TCP State Diagram
**Attack Technique: (D)DoS**

- Denial of Service attacks the availability
- Broad definition of DoS → Ransomware, etc., too!
- Network-centric view: hampers the use of web services, ...
- Numerous variations
- Quite trivial, but still effective
  - Estonia 2007
  - Dyn 2017

**Example: SYN Flooding**

- TCP SYN flooding attack uses the TCP three-way handshake to attack the server
- Simple basic idea
- Attacker only requires moderate resources

\[
\begin{align*}
\text{CLIENT} & \quad \text{SYN} & \quad \text{SYN/ACK} & \quad \text{ACK} & \quad \text{CLOSED} \\
\text{SERVER} & \quad \text{LISTEN} & \quad \text{ESTABLISHED} & \quad \text{SYN_RECV} & \quad \text{ESTABLISHED} \\
\end{align*}
\]

- Retransmissions of an unacknowledged SYN/ACK segment occur after 3, 6, 12, 24, and 48 seconds (standard Linux)
- Last retransmission: timeout value 96s
- Socket remains in state SYN_RECV, which means it uses resources on the server system
- Resources are blocked until the session times out after 3 minutes and 9 seconds!
Example: SYN Flooding

- Server reserves resources for administrating the connection
- Client does not need resources for opening
- Huge amounts can be requested quickly
- Result: Server is blocked by half-open connections
- Note: Client can use forged sender addresses

Attack Technique: (D)DoS (cont’d)

- Variations like, e.g., Reflective DNS Response attack
- Reflector could be a legitimate, uncompromised server
- Therefore, difficult to mitigate!

Attack Technique: Spoofing

- Spoofing is the usage of a fake identity
- In human communication usage of fake identities is common as well, but common sense often helps to discover these attacks
- In network protocols information identifying the sender is usually unprotected, the recipient often simply trusts the sender entry
- Works, e.g., for ARP/DNS/IP/ICMP/Email/Web/... spoofing
- Very fast and simple: Email with forged sender address
Forged Email Sender Address

15.04.18
Attack Overview/Dr. Dr. habil. Robert Koch/Network Security

DNS Spoofing: Background

- IP addresses are generally hard to remember
- Names are easier to remember… → DNS
- When the browser tries to access a page, first the name has to be resolved to its IP address

DNS Spoofing: Request in Whireshark
DNS Spoofing: Answer in Whireshark

Query response after 0.0021s

Answer is 216.58.207.132

DNS Spoofing: The Attack

- The attacker...
  - has access to the network with your computer,
  - sees your DNS query,
  - and sends a prepared answer with another IP address
- If he is faster than the real answer,
  - the asking program receives the attacker's answer first
  - accepts it, if the Transaction ID fits,
  - and believes the answer. Even worse, it stores it in its cache
- Browser displays the URL http://www.google.com, but displays the content of the redirected website

DNS Spoofing: Defence

- RFC 3833 (called DNS Threat Analysis) analyzes potential attacks targeted to the Domain Name System
- Countermeasure: cryptographic protection
- DNSsec (DNS security extensions), published in 2005 (RFC 4033, 4034, 4035)
- Idea: sign (cryptographic signature, see chapter 4) answers of DNS servers
The Role of Certificates

15.04.18
Attack Overview/Dr. Dr. habil. Robert Koch/Network Security

Examples of Certificate Incidents

15.04.18
Attack Overview/Dr. Dr. habil. Robert Koch/Network Security

Homograph Attack

15.04.18
Attack Overview/Dr. Dr. habil. Robert Koch/Network Security
Based on the Principles of Routing: Layer 3/4

- Example: NSA’s QUANTUMINSERT
- Kind of racing condition
- Profound number of well-positioned systems required

Example: QUANTUMINSERT

Original request

Example: QUANTUMINSERT (cont’d)
Quantum-inserted packet containing HTTP 302 redirect to fox-it.com

Source: https://github.com/fox-it/quantuminsert/

Original server response, HTTP 301 redirect to https://www.linkedin.com

Source: https://github.com/fox-it/quantuminsert/

Requests http://fox-it.com

Browser goes to http://fox-it.com
Ok, Bad, but what's Missing?

Layer 1

- Phishing
- Spoofing
- XSS
- Malicious Content
-...

But what about Layer 1? TX Ethernet Stream

IEEE 802.3 Frame MAC

But what about Layer 1? TX Ethernet Stream

IEEE 802.3 Frame MAC

What about Layer 1? IEEE 802.3-2012

- RECONCILIATION
- MDI
- MDI
-....

Façt or Fiction? Look at protocol diagrams...
But what about **Layer 1? 100Base-TX PHY Encoding**

- **De**
- **tect**
- **i**
- **o**
- **n**

Fast Look @**Fibre**

- Splicing
- Splitter/Coupler, Curve-Method
- Non-touching optical tapping

Wireless

- **Passive**
  - History: van Eck Phreaking
  - Improved: NSA's Rangemaster
- **Active**
  - Jamming, e.g., Iran & US RQ-170 Sentinel
  - Spoofing, e.g., Iran & US RQ-170 Sentinel
  - Protocol Weaknesses
  - Implementation Weaknesses
  - Organizational Weaknesses, e.g., ISR Drohne
- Example: KRACK Attack
Example: Cellular Networks

Preliminary Design

Implementation Phases...

Attack Overview: Supply Chain

- Complexity!
- Huge number of opportunities...
- E.g., interdiction operations

Source: Becker et al., Stealthy Dopant-Level Hardware Trojans, Springer 2013

Hardware Manipulations

Fake Bake Lipo Bronze Self-Tan 135 ml, 1er Pack (1 x 133 ml)
Key Take-Aways Chapter 2

- Protection targets
- Cybersecurity reports
- Taxonomies
- (Cyber) Kill Chain
- 6-Tier Attack Model and application
- Attack techniques, e.g., DDoS, Spoofing, ...
- Attacks on Layer 1
- Supply Chain & Hardware-based attacks

Upcoming

- Testing Frameworks
- Detection of Vulnerabilities
- OWASP Catalogue