Networks and Security:
Denial-of-Service Attacks

Lehrvortrag zu Netzwerke und Sicherheit

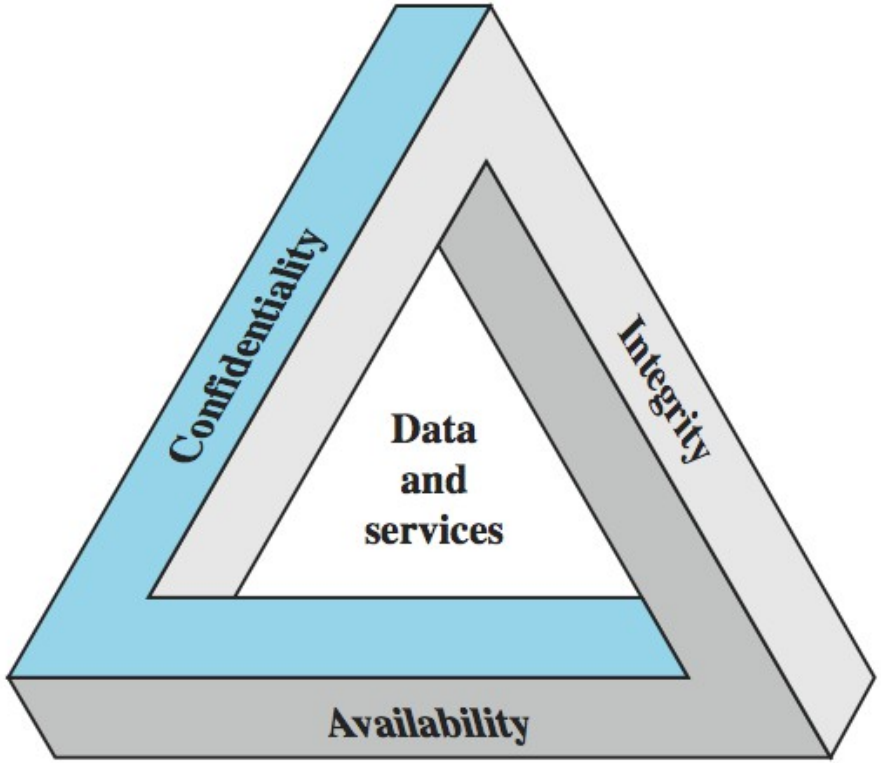
6. Februar 2013 15:00 – 16:00
JKU Linz, SCP1 MT 127

Priv.-Doz. DI Dr. René Mayrhofer

Reminder: basic security requirements

CIA Triad

- **Confidentiality** / secrecy: only authorized users are allowed to gain access to the protected data, message, service, resource, etc.
- **Integrity**: undetected modification is only allowed by authorized users
- **Availability**: authorized users should have access to resources, and unauthorized users should not be able to deny this access



Denial-of-service is an attack on availability

Figure from "Cryptography and Network Security" (5th edition) by William Stallings

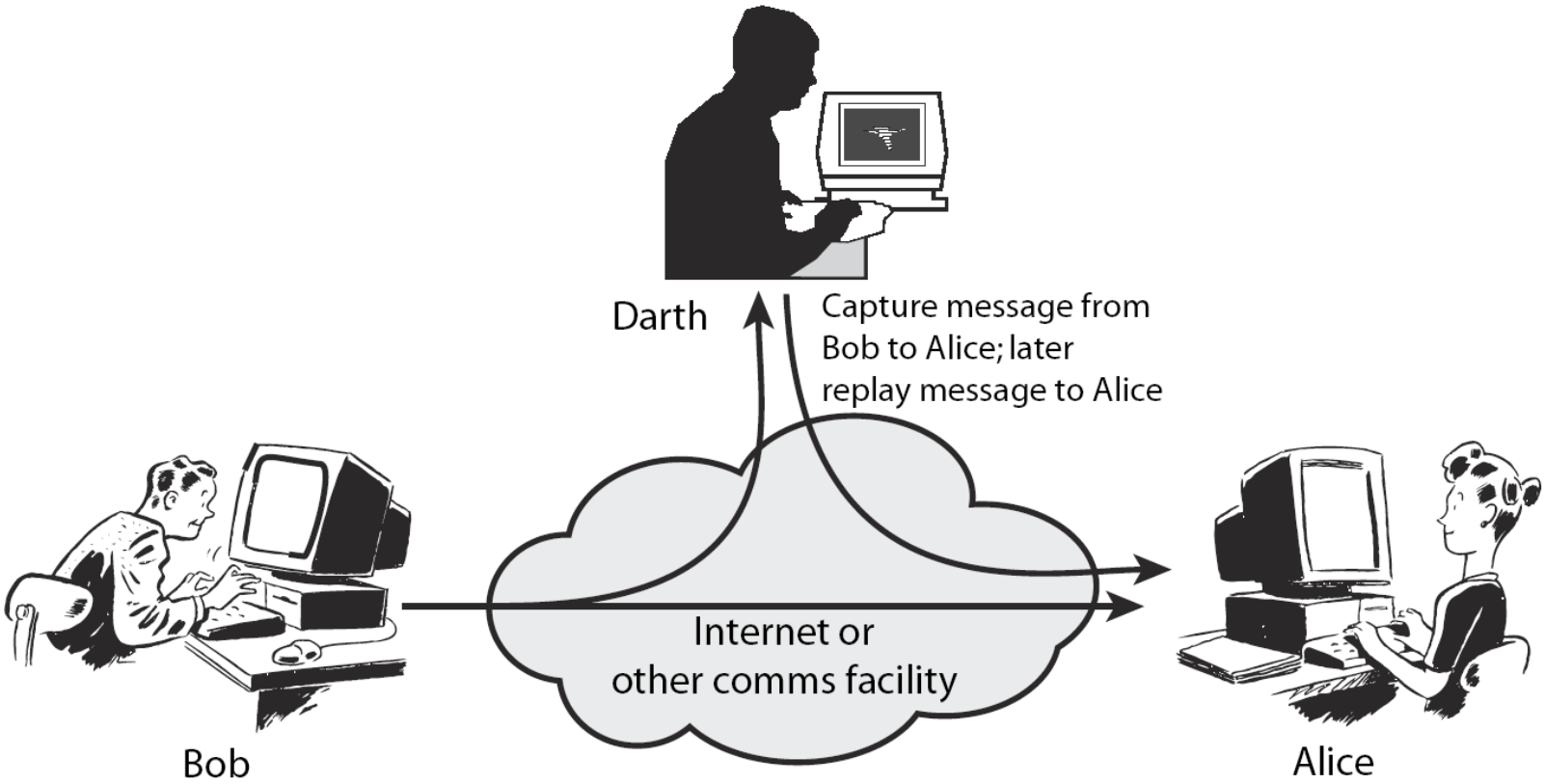
Classes of denial-of-service attacks

Denial-of-service attacks are possible at different layers

- Hardware: destruction, theft, exchange, ...
- OS: overload (e.g. with too many processes or memory usage) or crashing bugs
  - standard overload example: Fork bomb
  - e.g. current Samsung Android phones with USSD code "*2767*3855#" to initiate factory data reset
  - historical example: Ping of Death
- Network: either use up all server resources (TCP sessions, etc.) or network bandwidth
  - DoS attacks on e.g. router/gateway software would fall under the OS category
  - special category for wireless links: DoS for local attackers often trivial!
- Applications: e.g. by failed authentication attempts, potentially resulting in permanent blocks for smart cards (see Secure Element discussion)
- User: too many fake – or real – security warnings and errors will simply be ignored

In this lecture, will focus on network DoS

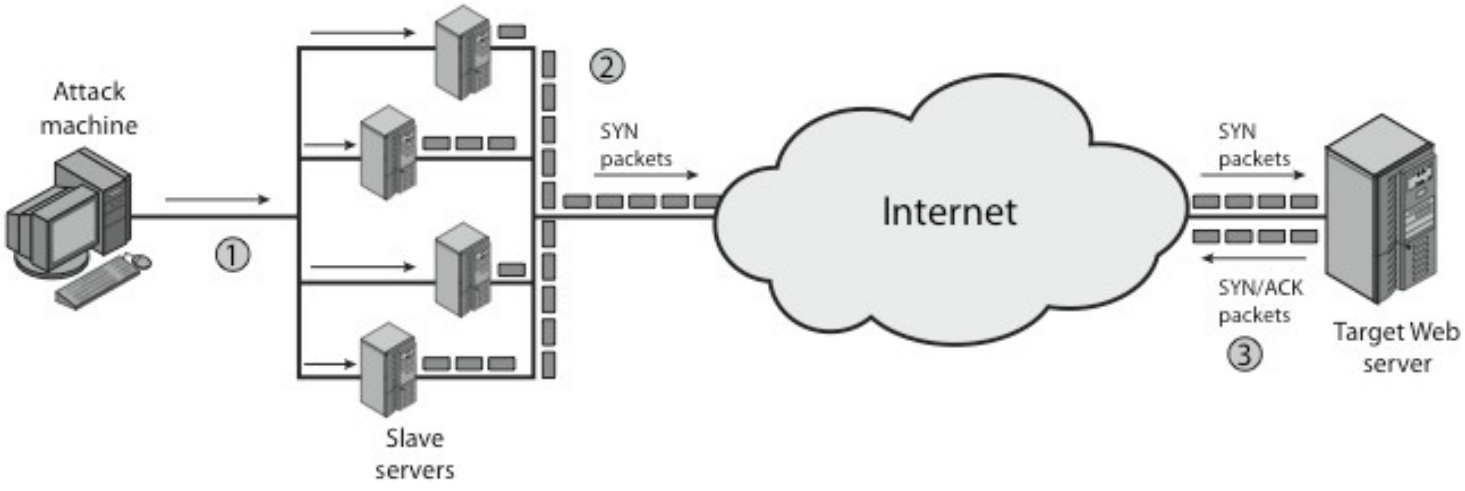
Trivial DoS on network connections by MITM



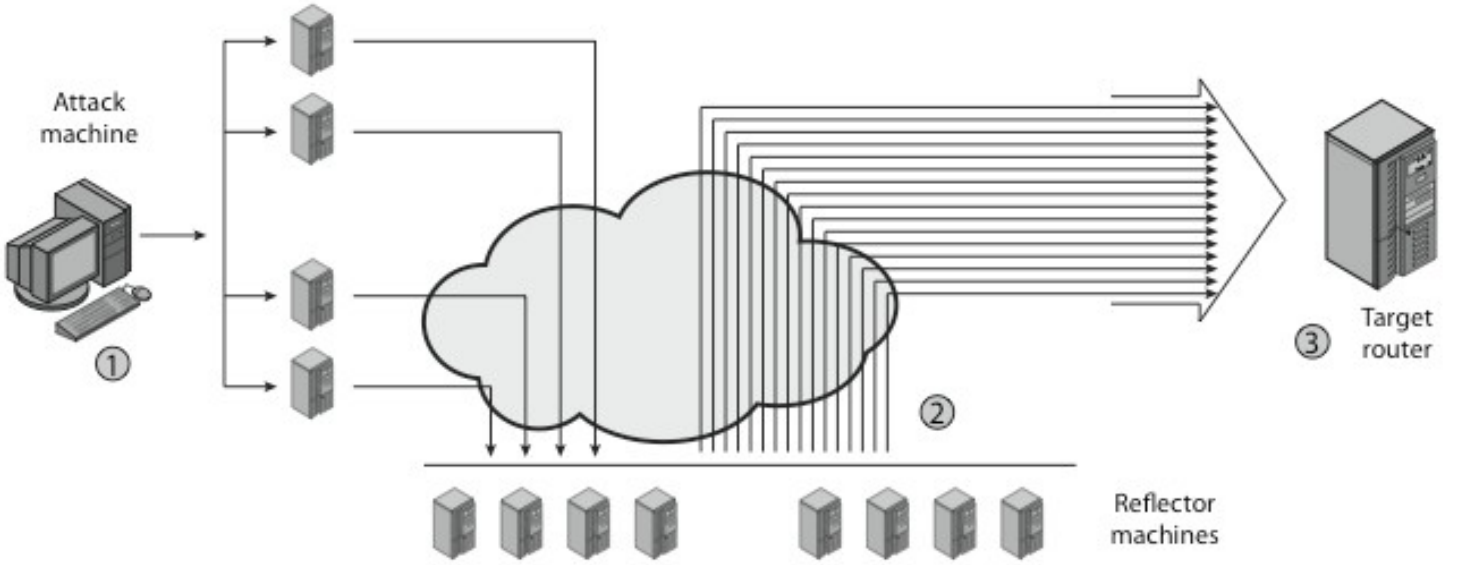
A man-in-the-middle can trivially disrupt all communication (remember: MITM is assumed to have full control over the network traffic)

Figure from "Cryptography and Network Security" (5th edition) by William Stallings

Distributed Denial-of-Service (DDos)



(a) Distributed SYN flood attack



(a) Distributed ICMP attack

Figure from "Cryptography and Network Security" (5th edition) by William Stallings

DDoS in detail

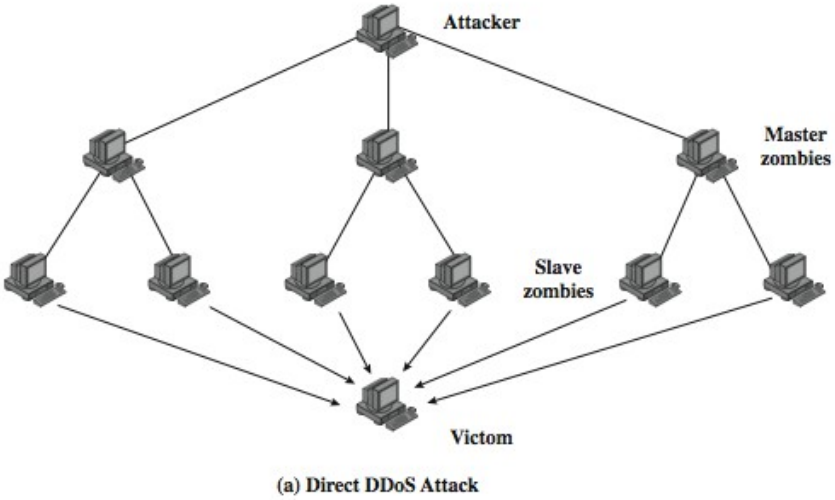
Attacker uses so-called "**zombie**" hosts

- infected, but no obvious issues
- instead, execute background tasks sent from command-and-control (C&C) server (e.g. IRC)
- typically desktop machines
- simple examples: ICMP or SYN flood

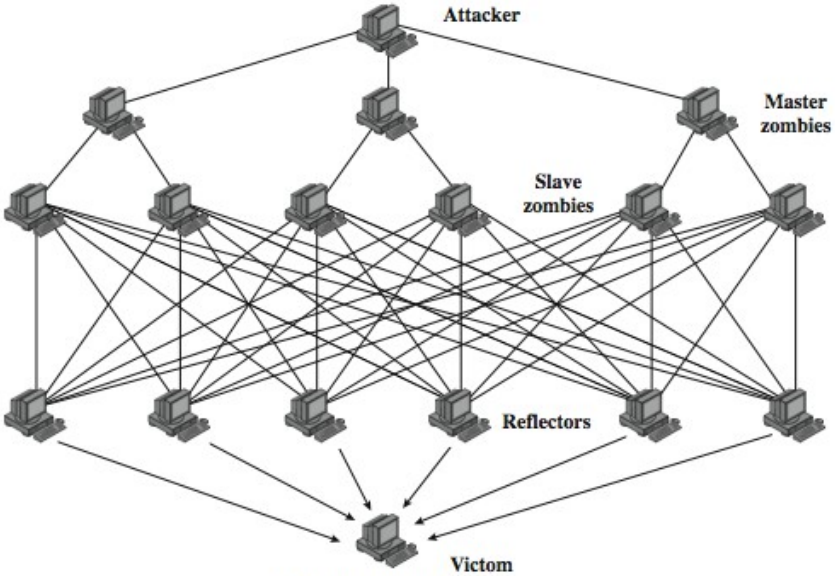
Target is simply overloaded by sheer number of zombies (cf. Slashdot...)

Enhanced DDoS: zombies+reflectors

- reflectors are well-connected (e.g. web servers, DNS servers, routers, etc.)
- service requests with fake source address yield response messages to the target
- historical example: Smurf attack



(a) Direct DDoS Attack



(b) Reflector DDoS Attack

Figure from "Cryptography and Network Security" (5th edition) by William Stallings

Advanced DoS attacks on the network stack

Try to exhaust any resource in the network stack of the target system

- any layer will do, e.g. wireless MAC buffers, TCP sessions, etc.
- recent DoS attack of this type: Slowloris
  - attack on HTTP servers by holding sessions open
  - TCP session is fully and correctly established
  - open partial request, and keep open by sending subsequent HTTP headers, but never complete request
  - fills maximum concurrent connection pool of HTTP server
  - many servers vulnerable, e.g. Apache until v2.2.15 (ships mod_reqtimeout since then to mitigate the problem)
  - Demo: http://localhost/server-status, pyloris v3.2

Or alternatively abuse network security mechanisms with fake requests

- e.g. send known-to-be-invalid IP packets with fake source address to IPS ⇒ will block this address
- e.g. cause authentication failure counters to reach a limit and force a timeout
  - may be permanent for network devices with embedded smart cards

Preventing DoS attacks

Often hard or impossible with only technical methods

- need organizational support, e.g. for tracing network resource abuse back to its root and executive forces

Some technical methods for mitigation of network-based DoS:

- L1: rapid channel hopping for wireless channels (see Bluetooth) or spread spectrum techniques (see UWB)
- L2/L3: switches with rate limiting and traffic shaping, provider support for DDoS on upstream connectivity
- L3/L4: stateful firewalls to validate TCP handshake, apply QoS (traffic shaping) rules, and validate source/destination addresses
- L5-L7: Intrusion Prevention Systems (IPS), Web Application Firewalls (WAF)
- L8: don't bother the end-user with warnings they will ignore anyway or ask them for security critical decisions they cannot make ⇒ proper user interaction design and implicit instead of explicit security!

Thank you for your attention!

Slides: http://www.mayrhofer.eu.org/presentations
Later questions: rene@mayrhofer.eu.org

OpenPGP keys: 0x249BC034 and 0xC3C24BDE
717A 033B BB45 A2B3 28CF B84B A1E5 2A7E 249B C034
7FE4 0DB5 61EC C645 B2F1 C847 ABB4 8F0D C3C2 4BDE