Seminar Computer Security

DoS/DDoS attacks and botnets

Hannes Korte

Overview

- Introduction
  - What is a Denial of Service attack?
  - The distributed version
  - The attacker's motivation
- Basics
- Bots and botnets
- Example attacks
- Defending a system

The Denial of Service attack

- Attempt to prevent legitimate users from accessing information or services of a targeted host

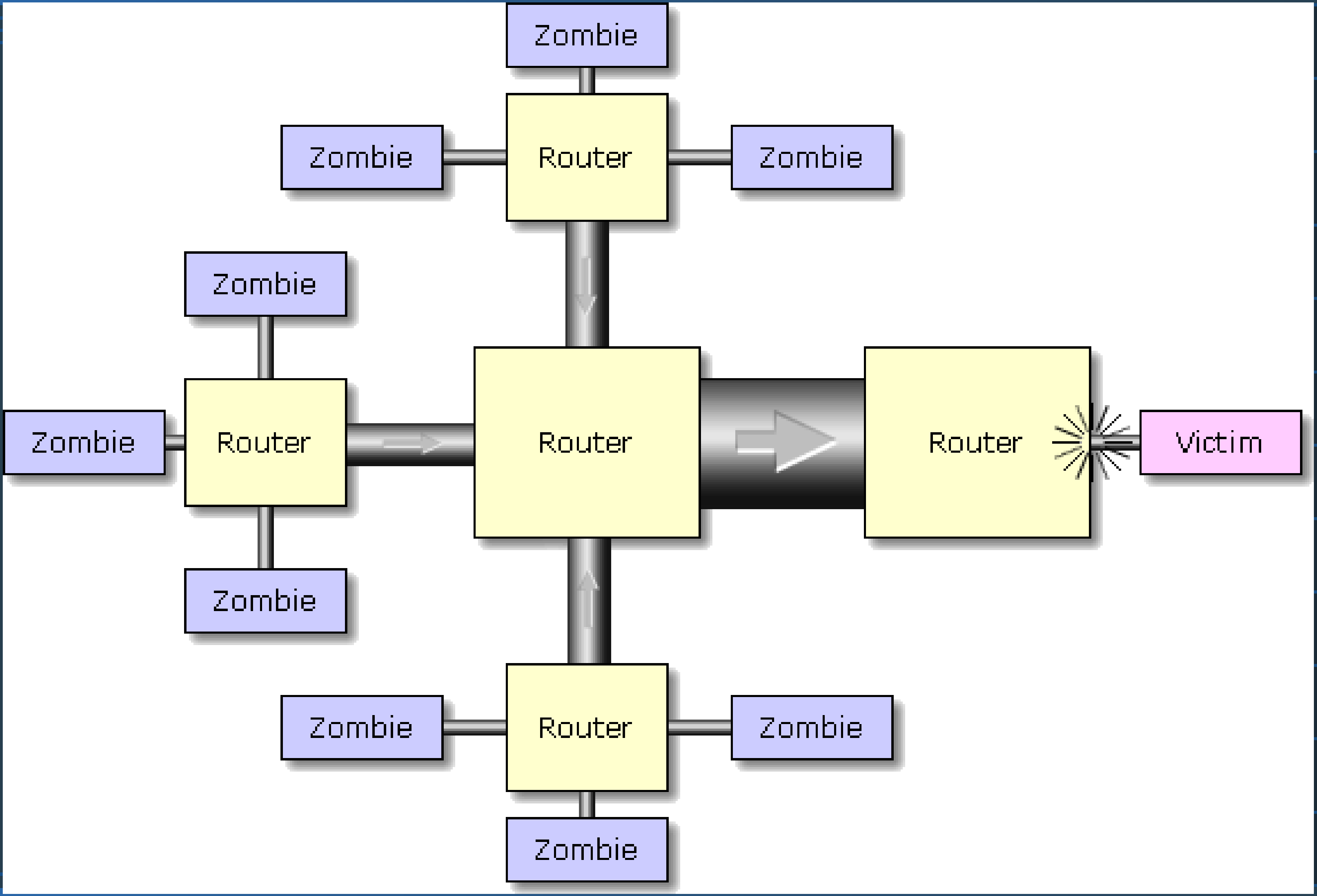
- Consume all available resources
  - bandwidth consumption
  - disk space consumption

- Usually not done directly, but from a bot running on a captured machine

The Distributed Denial of Service attack

- Many hosts attacking the same victim at the same time
- The power of bundled bandwidth
  - possibility of bandwith consumption attack

Bandwidth consumption with DDoS attack



Motivation for DoS attacks

- No direct benefit for attacker
- Maybe just like sports or to see what is possible
- But mostly there are commercial interests
- Bind the network administrators at one server
- ...and break into the system at another point without beeing seen

Overview

- Introduction
- Basics
  - Exploits
  - Internet Relay Chat
- Bots and botnets
- Example attacks
- Defending a system

Exploits

- Software that takes advantage of bugs or other vulnerabilities of systems
- Two types of classification:
  - what is attacked?
    - buffer overflow
    - code injection
  - what is done on attacked system?
    - unauthorised data access
    - code execution
    - denial of service
- fixed through a patch -> obsolete exploit

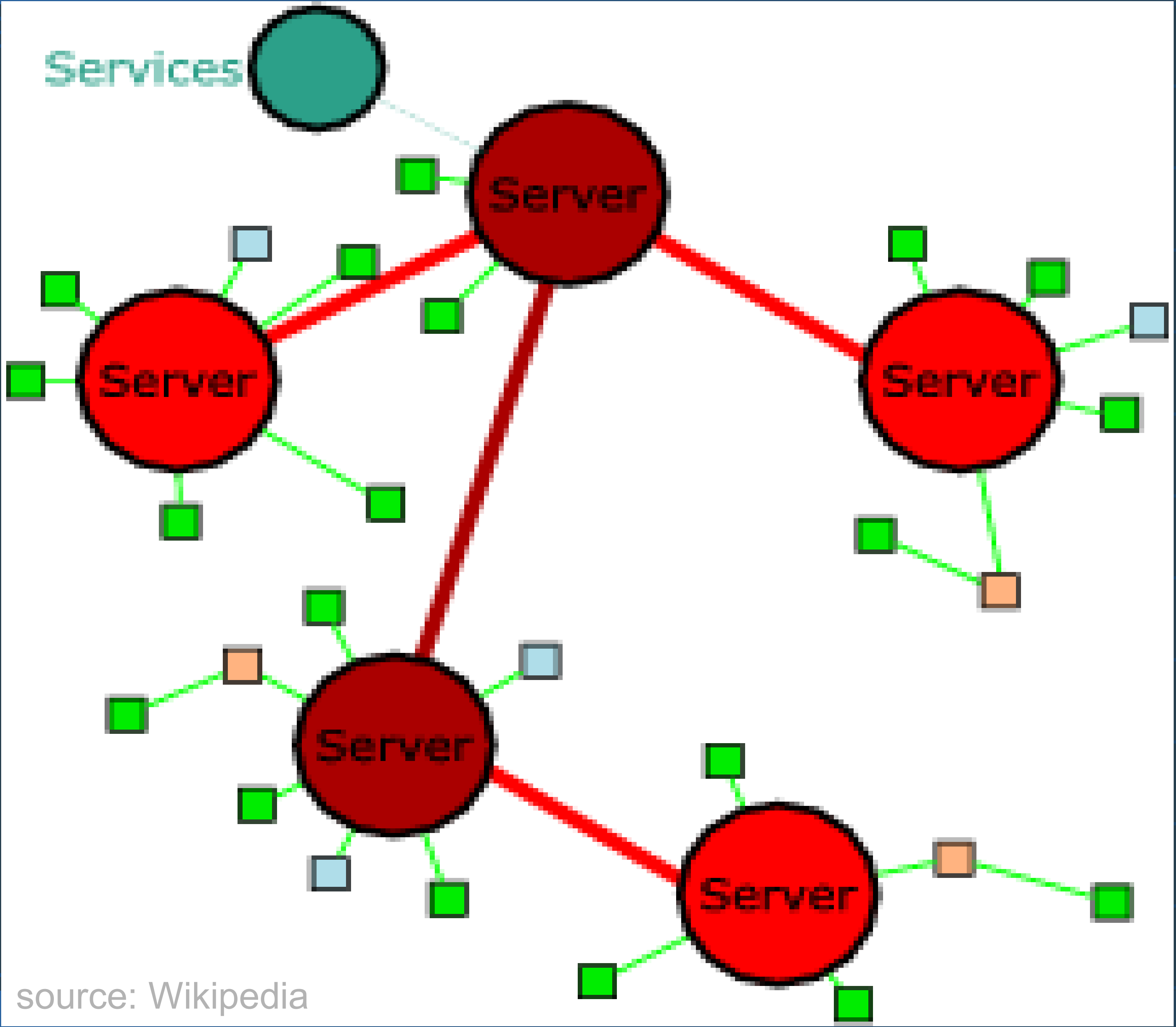
Internet Relay Chat (IRC)

- Text based chat system
- Network of IRC servers
- Support for private messages between only two users or communication in channels
- public, password-protected and secret channels
- optionally encrypted with SSL

Internet Relay Chat (IRC) (2)

- Bots act as virtual users to do specific tasks
  - e.g. registration and management of nicknames and channels
- Many independent IRC networks all around the world
- „The Big Four“ networks
  - EFnet
  - IRCnet
  - QuakeNet
  - Undernet

Internet Relay Chat (IRC) (3)



source: Wikipedia

Overview

- Introduction
- Basics
- Bots and botnets
  - What is a so called “bot”?
  - Distribution
  - Command & Control
- Example attacks
- Defending a system

Bots

- Name is derived from the word „robot“
- Mostly used for computer applications that can work without human interaction
- First bots were used in the IRC
- Are also used for malicious tasks
- Many bots are open source and implemented with a modular structure
  - Can be configured easily
  - New exploits can be added easily

Bots (2)

- Often bots try simulate human users
- ALICE bot: virtual female conversation partner
- eBay: Bots can bid automatically
- IM bots like „SmarterChild“ can be added to the personal contact list
- GoogleBot spiders websites and memorizes found pages

Malicious bots

- Infect systems and open a backdoor to receive commands
- Infected systems are then also called zombies or drones
- Usually full rights on the captured machine
- A group of bots is called botnet

Distribution of bots

- Bots can be in form of a trojan
- Email attachments are not the most popular or effective way to spread bots
- Websites with infectious downloads or even infectious HTML using the Active-X exploit for Microsoft Internet Explorer
- Bots scan the network for possible entry points on other machines
  - old software with known exploits
  - other malware

Distribution of bots (2)

- Self installing on other machines like viruses or worms
- Teamwork
  - Phatbot followed Sasser on the route of infected machines
  - Scan for other trojans like Subseven
    - Maybe the user does not care about securing his system
- Hard to detect new variants with virus scanners

Command & Control mechanism

- Usually Client / Server based communication
- Central IRC server
  - Bots connect to a password-protected and secret (hidden) channel
  - A master posts commands to that channel
- Use of a dynamic DNS address
  - If the used IRC server changes, only the destination IP of that DNS entry has to be changed

Command & Control mechanism (2)

- Unavailability of the IRC server leads to a lost botnet, because the commands do not reach the bot anymore
- New variant spotted: Peer-to-peer botnets
  - Bots have a list of IPs they try to connect to
  - Seed nodes send out a list of other peers
  - It is hard to eliminate these botnets
  - Not yet widely used

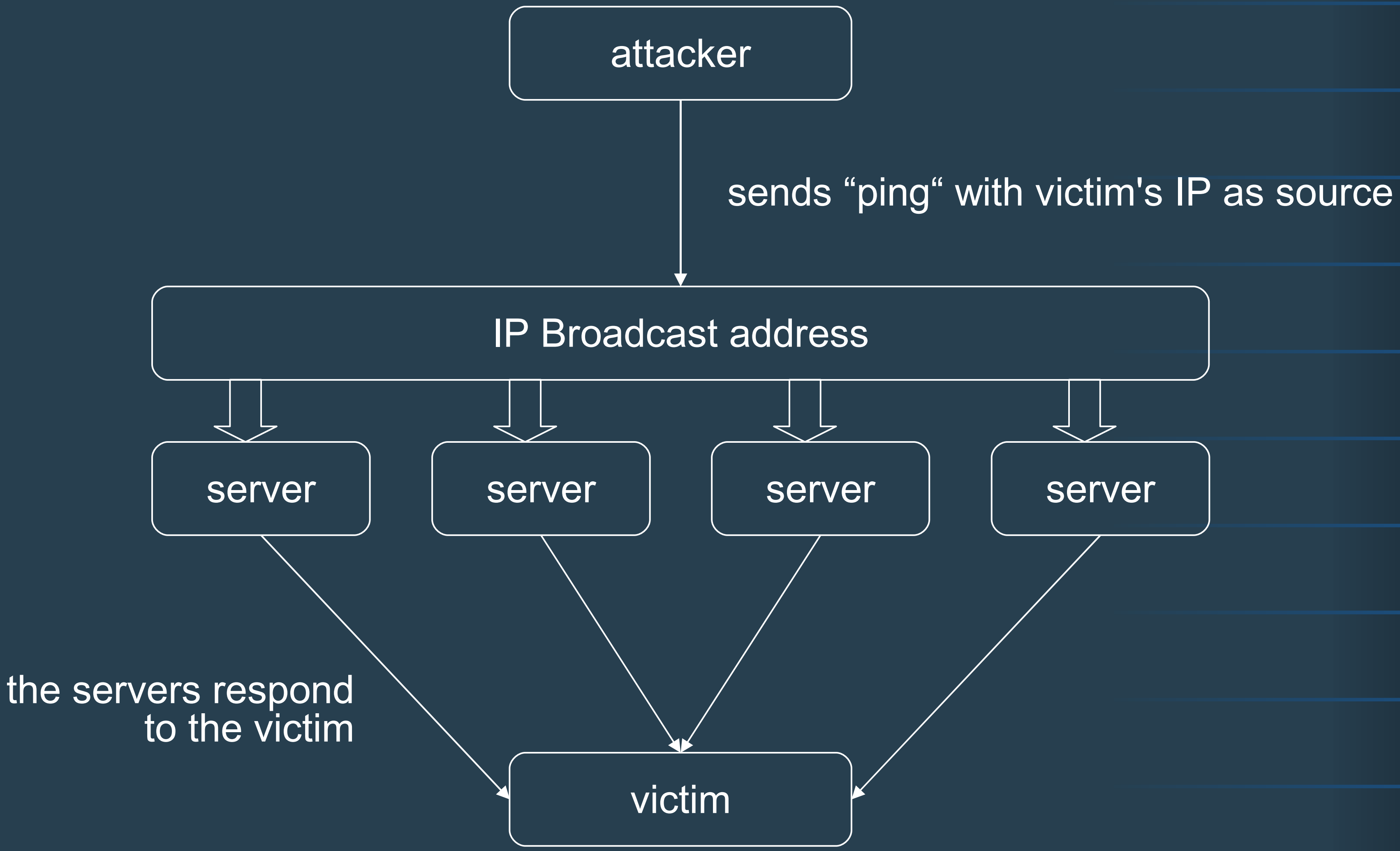
Overview

- Introduction
- Basics
- Bots and botnets
- Example attacks
  - Smurf attack
  - SYN flood
  - DRDoS
- Defending a system

Smurf attack

- ICMP echo request "ping"
- Forged source IP address
- Sent to an IP broadcast address
- Ping receiving servers response
- Effective attack
  - low bandwidth needs for attacker
  - high produced traffic for victim host

Smurf attack (2)



attacker

sends “ping“ with victim's IP as source

IP Broadcast address

server

server

server

server

the servers respond
to the victim

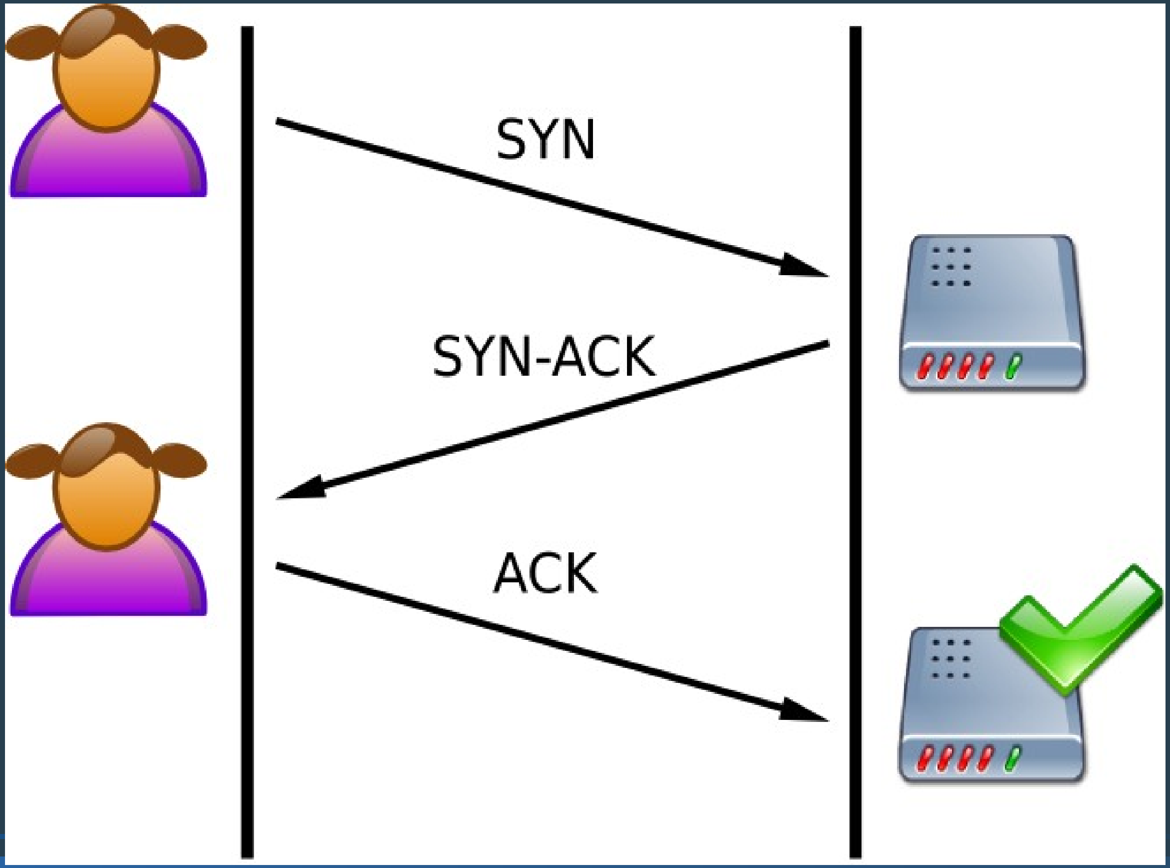
victim

Smurf attack (3)

- A variation called Fraggle attack
  - causes UDP floods instead of ICMP floods
- Many years ago, most networks were "smurfable"
- Do simply not reply to broadcast pings

SYN flood

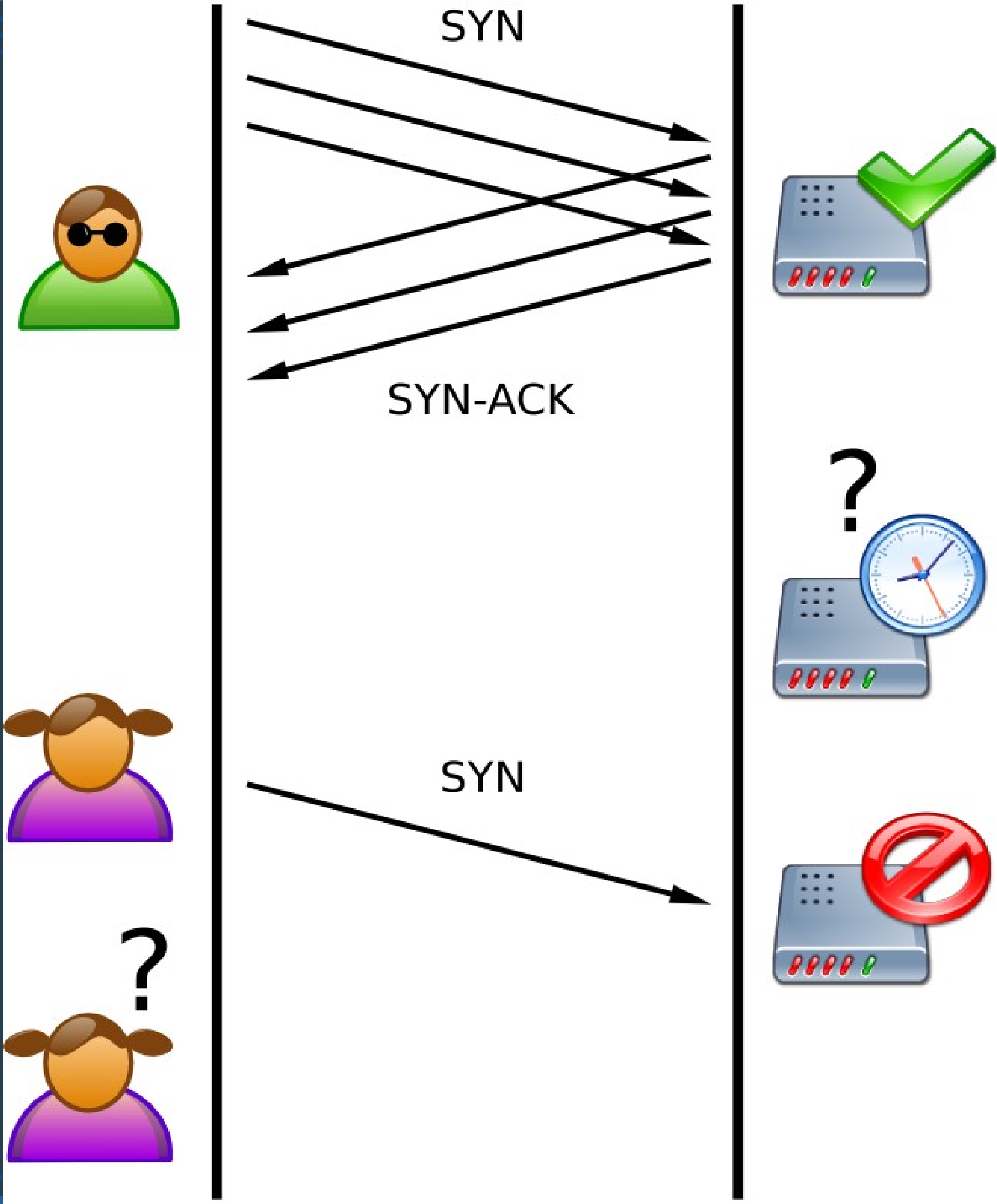
- TCP connection setup is initiated
- The Three-way-handshake:



SYN flood (2)

- Many SYN packets are sent (optionally with forged source IP) to the attacked server
- The SYN+ACK is ignored
- A lot of half-open connections
- No bandwidth consumption
- Resources are bound on the server

SYN flood (3)



SYN Cookies

- The solution is not to store any information before the last ACK arrives
- Therefore encode all needed information in the initial sequence number
  - Some time related counter
  - The Maximum segment size value that the server would have stored in the SYN queue entry
  - The result of a cryptographic secret function computed over the server IP address and port number, the client IP address and port number, and the value of the counter

SYN Cookies (2)

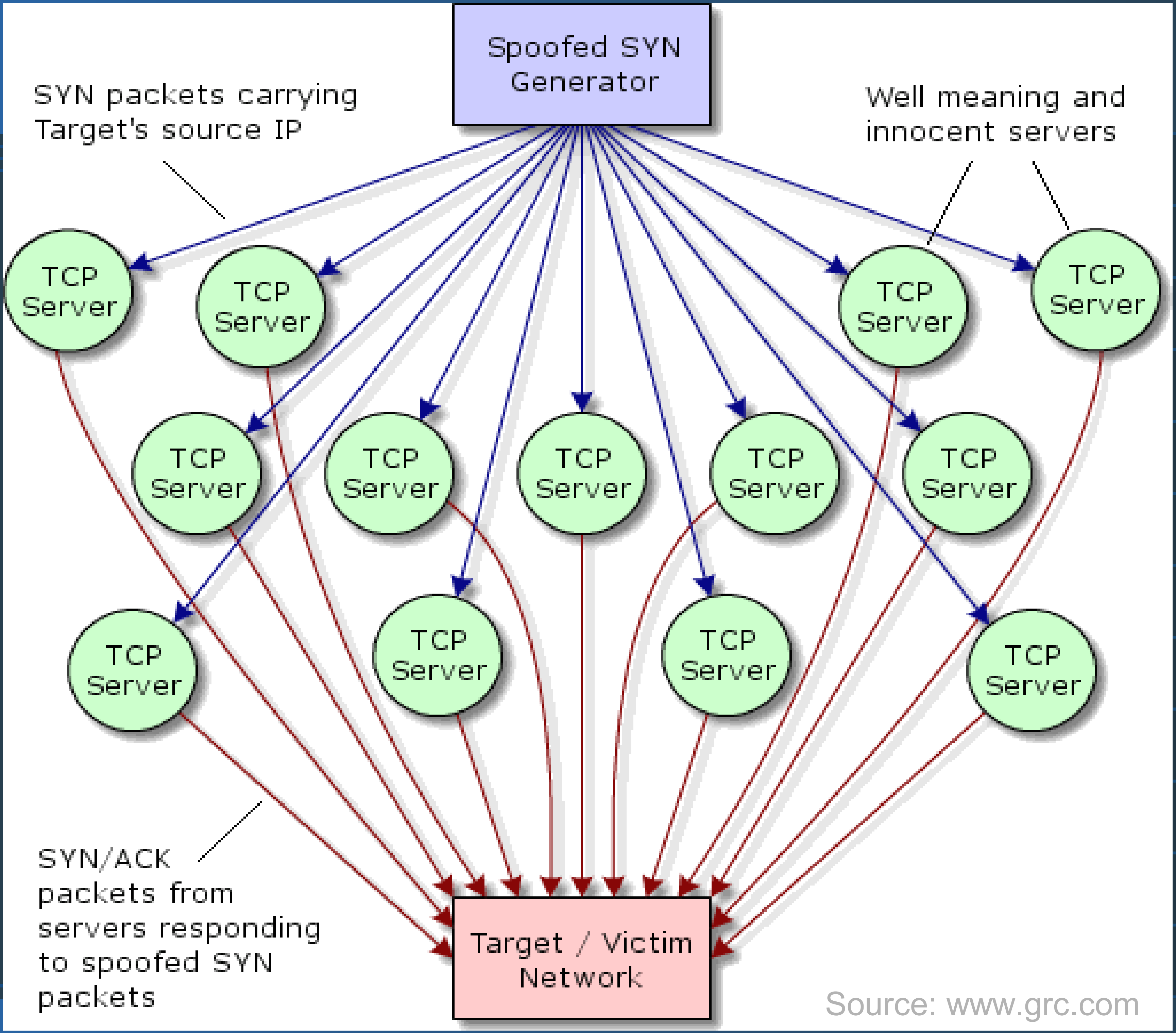
- No storage of SYN packet information is needed
- TCP is not violated
- Actually today not needed anymore due to large resources of modern hardware

Distributed Reflection DoS attack

- Victim is not attacked directly
- Bandwidth attack
- IP packets with the victim's IP address as the source are sent to servers in expectation of a server response
- Use of high-bandwidth servers
- Victim gets attacked by innocent servers

Many tiny SYN floods

- The bots get a list of servers to use for an attack and the victims IP
- SYN floods are evenly distributed on the list of servers
- The server's administrators maybe don't even notice the SYN flooding
- Very hard to block



SYN packets carrying Target's source IP

Well meaning and innocent servers

SYN/ACK packets from servers responding to spoofed SYN packets

Source: www.grc.com

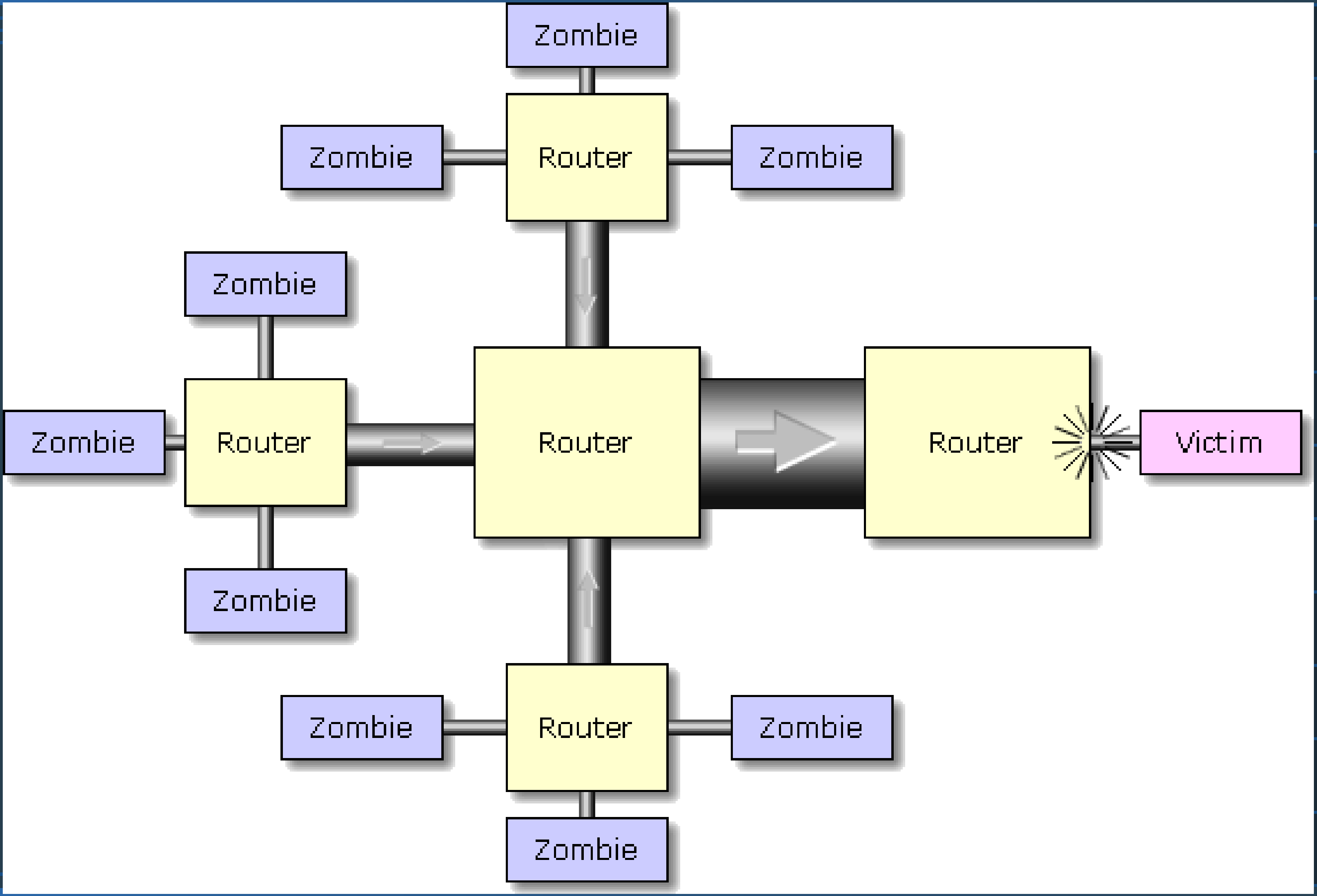
Overview

- Introduction
- Basics
- Bots and botnets
- Example attacks
- Defending a system
  - Firewalls

Firewalls

- Firewall filters have to be set up at the ISP's side to prevent the bandwidth attacks' effects
- It's like snorkeling: When the snorkel is filled with water you can close your mouth, but you still can't breathe

Again the diagram



Reactions

- Analyze the packets used in the attack
  - Try to find characteristics of the packets to set the firewall rules accordingly
  - Possibly a specific port is used that can simply be blocked
- Maybe temporarily stop one service to let others remain available
- DRDoS attacks are hard to block if the destination port of the attack is also used by the offered services of the attacked system

How to prevent DRDoS attacks

- The most effective way of preventing DRDoS attacks could be done by ISPs
- Drop IP packets from the internal net to the internet with an obviously forged source IP address (an IP, that does not exist inside the network)

What else should be done?

- Apply patches to existing exploits regularly
- Observe your log files

Thank you!