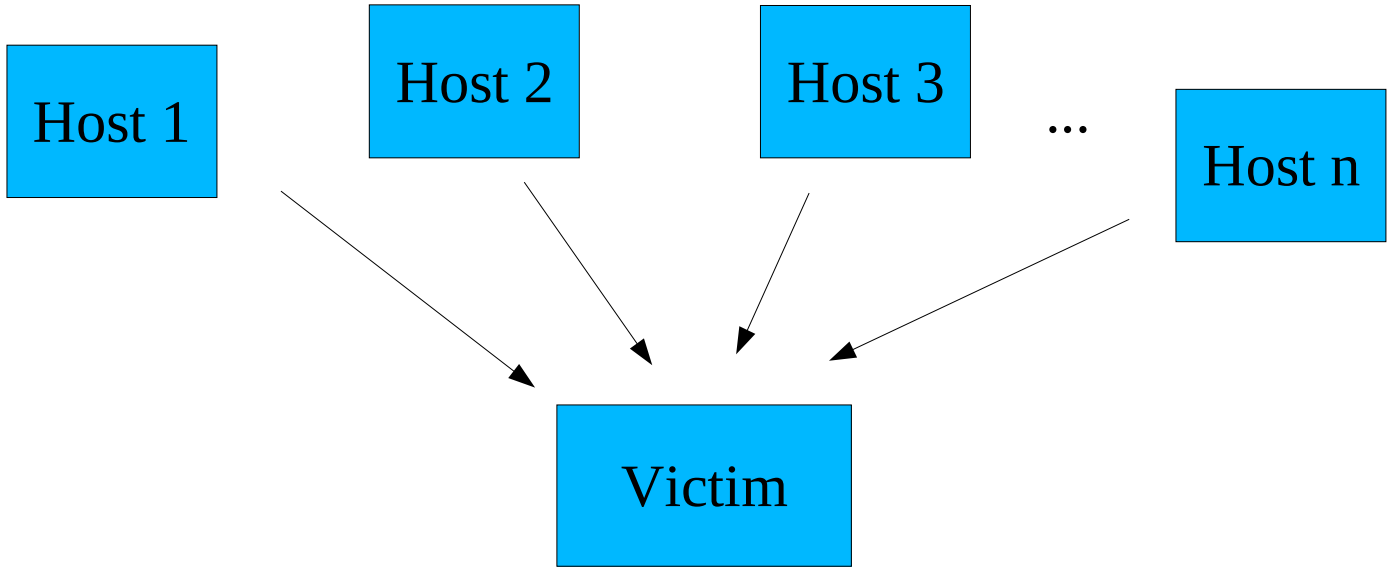
Distributed Denial of Service Attacks **(DDoS)**

Olli Salonen
olli.salonen@hut.fi

Introduction

- DoS attacks where attacker uses multiple hosts to perform the attack
- Targets are often big public webservers, also IRC servers draw a lot of attacks



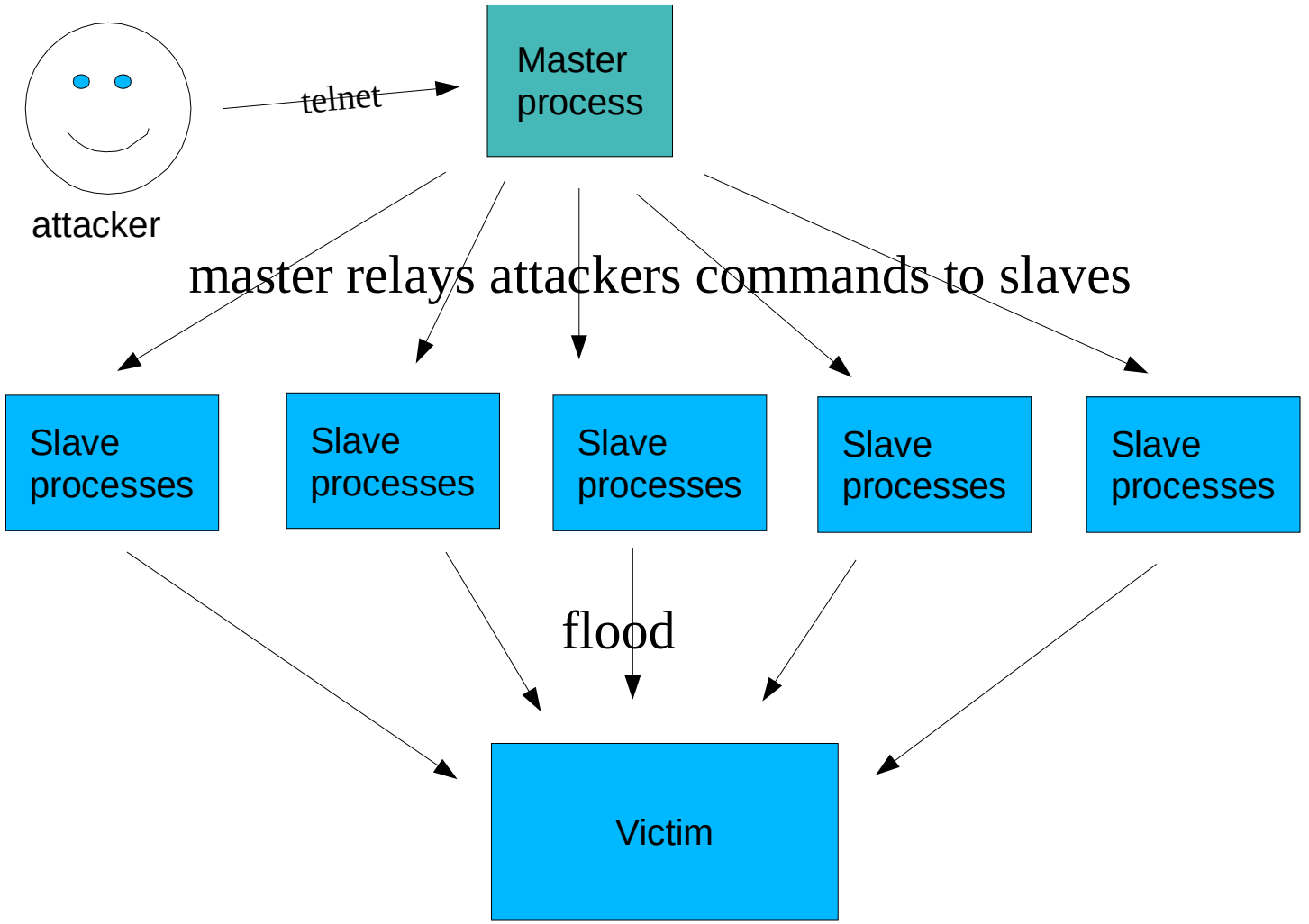
Introduction

- Attacks are relatively uncomplex to perform
- There is no easy way to protect from DDoS
- There are several DDoS tools for both Unix and Windows platforms
  - trin00
  - TFN and its successor TFN2k
  - Stacheldraht (barb wire in German)
- Growing threat to fluent Internet traffic and e-commerce

Master-Slave Configuration

- Typically there is one master process controlled by the attacker
- Slave systems are compromised systems, which run a slave process, that listens to master's commands and report their status to the master
- Slaves carry one or more DoS routines
- Slaves can be on any system regardless of the platform
- Master processes are typically carefully protected
- Attacker can access master process anywhere

Master-Slave Configuration



Impact

- Target host will notify a huge increase in network traffic
- Attack may come from valid addresses or random addresses spoofed by the slave hosts
- If target system vulnerable to the DoS attack used it may crash, if not, then it's network capacity will be exhausted
- Attack rates of several gigabits per second have been reported

Defending against DDoS

- When you're under a well-made DDoS attack there's not much to do
  - try to wait until the attack ceases -> no service
  - pull the plug -> no service
- Depending on the attack type, it may be possible to limit the attack with ACLs and applying CARs
- There are several software products, which provide some tools to detect, react and stop these attacks
- Cooperation with upstream providers
- Multiple server farms

Some incidents

- February 7-9, 2000
  - Amazon, CNN, eBay, ZDnet, Yahoo experienced several hours of DDoS attacks cripling their services
- October 21, 2002
  - DDoS attack against all 13 root DNS servers rendered 7 of them completely unusable for an hour

Why?

- Because they can do it
- To see if they can do it
- IRC channel takeover
- Disrupt business in the Internet

Future

- Millions of hosts added into Internet monthly
  -> nof badly administrated systems increases
- Home PCs with fast Internet connections provide a suitable computers for attackers to use as slaves
- DDoS techniques are evolving - countermeasures often lag behind or impossible to implement
- Legislation