Chair of Network Architectures and Services
Department of Informatics
Technical University of Munich

Internet Security Evaluation using Active and Passive Network Measurements

Oliver Gasser
gasser@net.in.tum.de

Internet Security

- More and more devices are connected to the Internet
  - Internet of Things
  - IPv6
- Devices mostly not designed with security in mind
- Challenges
  - Long product lifecycle
  - Patching of security flaws
  - Security through obscurity

Use network measurements to assess Internet security

Active Network Measurements

- Send probe packets to the network
- Response packets yield important information on device's security
- Target selection
  - IPv4: complete 0/0 approach is possible
  - **IPv6: smart address selection needed**
- "Ethical scanning"
  - Reduce scanning rate
  - Provide information on scanning machine
  - Blacklist annoyed admins

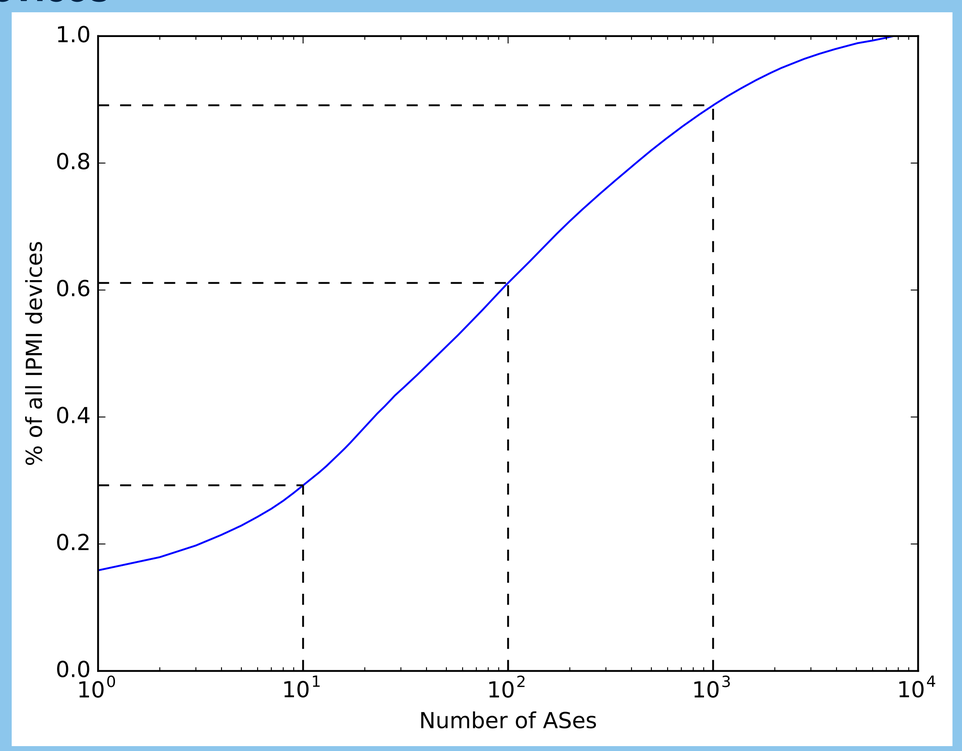
Presentation at TMA'16

Passive Network Measurements

- Passive approach, i.e. no probe packets
- Measurement sources
  - Real-world traffic
  - Flow data (IPFIX, NetFlow)
  - SNMP
  - ...
- Usage scenarios
  - Directly assess security based on traffic
  - Further investigation with active measurements

IPMI Scanning

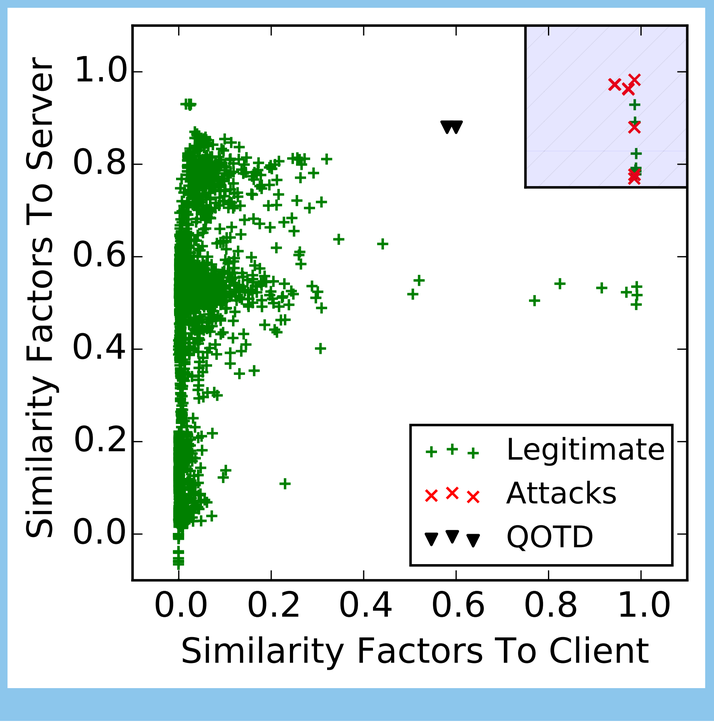
- IPMI is e.g. used to restart servers remotely
- Should not be accessible from the public Internet
- Scans show that this assumption does not hold
- Different scanning technique yields **previously undiscovered devices**



Presentation at TMA'16

Amplification Attack Detection

- Detect amplification attacks inside amplifier network
- Use inherent traffic characteristics to distinguish between benign and malicious traffic
  - Packets in/out
  - Bytes in/out
  - Payload similarity
  - Length similarity



Traffic Measurement and Analysis Workshop (TMA), Belgium, April 2016