Security Information

Motivation

Security in present home networks:
- Antivirus software on PC based computers
- No security features on other devices
- No network traffic analysis
  - Malicious traffic cannot be detected
  - Packet filter and NAT are the only network security mechanisms
- Better mechanisms for network traffic analysis are necessary!

Security in future home networks
- More devices connect to the local area network
- More services available in the home network
- Malware can attack a home network at several places
- Future home networks need a mechanism for protecting devices and services
- Security mechanisms need to protected various device types
- Network traffic analysis can be performed independently from device type

Malware Analysis

- Behavior based analysis of collected malware
- Observe network traffic
- Analyze observed traffic
- Receive network traffic fingerprint
- Approach: Install malware on a real operating systems in a controlled environment
  - Use operating system virtualization
  - Build a cluster for analyzing malware to analyze multiple malware samples
  - Allow network connections to the Command & Control (C&C) channel
  - Block malicious traffic to the Internet
  - Extract as many information as possible
  - Generate security information for AuthHoNe networks

Service Simulation

- Do not connect to the Internet
- Emulate services instead
- Emulated Services:
  - C&C channel
  - Vulnerable services
- Goals:
  - Observe C&C traffic
  - Observe malicious traffic
  - Expose no threat to the Internet

Collecting Malware

- Vendors need to collect malware
- Already done today
- Low Interaction Honeypots
  - Collect worms which use known attack vectors
- High Interaction Honeypots
  - Collect worms which use new attack vectors
- Client Honeypots
  - Collect malware from websites or emails

Knowledge Transfer

- Contract between vendor and AuthHoNe landlord possible
- Use Knowledge Plane to insert security information into AuthHoNe networks

Malware Identification

- Observe network traffic within the AuthHoNe network
- Use security information to detect C&C channels
- Block botnet communication
- Use information on malicious C&C channels
- Block unwanted traffic