Emerging Ways to Protect your Network

From Vulnerability Scanning to Real-time Monitoring and Detection of Cyber-attacks

Konstantinos Xinidis
Software Engineer
xinidis@vtripgroup.com

Research & Technological Development Dept.,
http://www.vtrip.net
Virtual Trip, Ltd.
Thessaloniki, Greece
Roadmap

- Motivation
- Approaches
  - Estia
    - What are vulnerability scanners?
    - Estia architecture
  - NoAH
    - What are honeypots?
    - NoAH architecture
- Conclusions
Motivation

- **Estia**
  - Too many *known* vulnerabilities
  - Most users do not know that they are vulnerable

- **NoAH**
  - *Exploits for unknown vulnerabilities are used for installing malicious software (malware)*
  - Viruses, worms, trojans, keyboard loggers continue to plague our computers
  - Malware spreads too fast while human intervention is too slow
  - Traditional approaches (e.g. IDS)
    - too slow
    - too inaccurate
    - looking for *known attacks*
Estia Goals

- Provide a service that
  - improves the security of computers/small networks
  - users can find and remove vulnerabilities
  - SMEs can easily remove vulnerabilities from their networks
  - requires no expertise
    - no installation of complex software packages
  - easy to use web-based interface

www.estiasecurity.gr
What is a Vulnerability Scanner?

- A tool that can be used to
  - analyse, define, identify, and classify the security holes (vulnerabilities) in a system
  - evaluate the effectiveness of countermeasures

- Vulnerability scanners
  - rely on an up-to-date database of vulnerabilities
  - try to exploit each vulnerability that is discovered
  - provide clear reports of the found vulnerabilities
  - provide recommendations for countermeasures to eliminate discovered vulnerabilities
- Estia uses **nessus** vulnerability scanner
- The examined system can be behind a firewall or NAT
Estia Limitations

- Estia pinpoints only **known** vulnerabilities
  - Unprotected against worms that exploit unknown vulnerabilities (zero-day worms)
- Estia requires human intervention
  - Malware spreads too fast for humans to react
- Network of Affined Honeypots (NoAH)
  - Protects against **unknown** vulnerabilities
  - **No humans** in the loop
**NoAH Goals**

**Goals**
- Detect zero-day attacks and worms
- Track down selective attacks
- Analyse unknown exploit code
- Generate signatures

**Reach the goals by**
- building a pilot infrastructure that allows for malware collection, identification and analysis
  - combination of low- and high-interaction honeypots
  - dark traffic redirectors

www.fp6-noah.org
What is a Honeypot?

- An “undercover” computer
  - Which has no ordinary users
  - Which provides no regular service
    - or a few selected services if needed
  - Just waits to be attacked...

- Its value lies on being compromised
  - or in being exploited, scanned, etc.

- Honeypots are an “easy” target
  - But heavily monitored ones
  - If attacked, they log as much information as possible
Low- and High-Interaction Honeypots

- **Low-interaction honeypots emulate services using scripts**
  - Lightweight processes, able to cover large network space
  - Emulation cannot provide a high level of interaction with attackers

- **High-interaction honeypots do not perform emulation, they run real services**
  - Heavyweight processes, able to cover small network space
  - Provide the highest level of interaction with attackers

- **NoAH uses the advantages of both types**
Low-Interaction Honeypots and Funnels

- **Low-interaction honeypot: honeyd**
  - Emulates thousands of IP addresses
  - Highly configurable and lightweight
  - Filters out efficiently unestablished and uninteresting connections
  - Proxy for connections to high-interaction honeypots

- **Funnel component**
  - Based on farpd (or router configuration)
  - Allows a wide dark address space to be handled by few honeypots
  - Aggregates and forwards traffic to the NoAH core
High-Interaction Honeypot: Argos

- An emulator, based on Qemu
  - Emulates entire PC systems
  - OS agnostic, runs on commodity hardware
- Key idea: data coming from the network should never be executed
- Tracks network data throughout execution
- Detects illegal uses of network data
- Detects all exploit attempts, including zero-days!

www.few.vu.nl/argos
- Honeypots listen to unused IP address space
  - This space is limited to provide results fast and accurately
  - NoAH tries to empower people to participate with honey@home

- Tool appropriate for home users
  - Monitors unused IP addresses
    - Usually provided by DHCP
  - Redirects possibly malicious traffic to NoAH core

- No configuration, install and run!
Conclusions

- **Estia** protects systems from **known vulnerabilities**
  - Uses *nessus* vulnerability scanner
  - Easy to use for non-expert

- **NoAH** protects systems from **unknown vulnerabilities**
  - Distributed architecture
  - Detects all exploits, including zero-days
  - No human intervention
  - Enables unfamiliar users to effortlessly participate to NoAH
Questions?
Thanks!

http://www.vtrip.net
http://www.fp6-noah.org
http://www.estiasecurity.gr