Communication Network Perspective on

Malware Lifecycle

(draft-fabini-smart-malware-lifecycle-00)

Joachim Fabini
TU Wien

Outline

- Institute and Research Group
- Background and Motivation
  - Systems and Protocols
- Research Questions
- A Generic Malware Lifecycle Model
- Future work
- Summary and Outlook

TU Wien, Institute of Telecommunications

- Institute: about 80 staff members
  - – Four full professors, six groups
- Research area: communications
  - – 5G, vehicular, antennas, IP-layer, security.
- **Communication Networks (CN) group**
  - – **Research focus: anomaly detection**
  - – Data analysis, (real-time) algorithms, measurement methodologies, hardware, ...
  - – Data methods
    - Measurement methodologies, flow export, feature selection, clustering, anomaly detection (machine learning),...

Background: Systems

- **The illusion of "secure systems"**
  - – Vulnerabilities **do** exist in any system. Discovering them is a matter of skills and time
- **System complexity: not reliably manageable**
  - – Hardware, firmware, software
  - – Modular structure, reuse, interfaces
- **System monocultures**
  - – Cost pressure, many incentives
  - – (Tens of) thousands of identical devices
    - IoT, smartphones, PC (BIOS, OS, CPU, …)

IETF Perspective on System Security

- **IETF security area's activity focus:**
  - – RFC 3552: "Protecting against an attack when one of the end-systems has been compromised is extraordinarily difficult"
  - – Rely on the "chain of trust"
- But systems **are** vulnerable
  - – Malware exploits these vulnerabilities
  - – Solutions needed for critical infrastructures
  - – Low-cost, physical access for adversaries
    - EV charging 350kW (equals 500+ households)

Background: Protocols

- **Security protocols deployed at large scale**
  - Defense against pervasive monitoring
  - Use cases (and references): RFC 8404

    "Effects of Pervasive Encryption on Operators"
  - Random numbers (signatures, encryption)

Security paradoxon

- Security protocols build an ecosystem that supports hidden communications
  - Covert (subliminal) channels
  - Example: signatures in blockchains [3]

Motivation: Malware Communications

- **Malware has strong incentives to communicate**
  - – Modular and distributed malware structure
  - – Various communication types: infect, propagate, update, coordinate, attack, …
  - – The more communications, the higher the malware threat for the overall (large) system
- **Challenges in detecting** communication
  - – Malware attempts to hide communications
  - – Chronology comm. -> activity is uncertain

Proposal: Improve Defense Against Malware

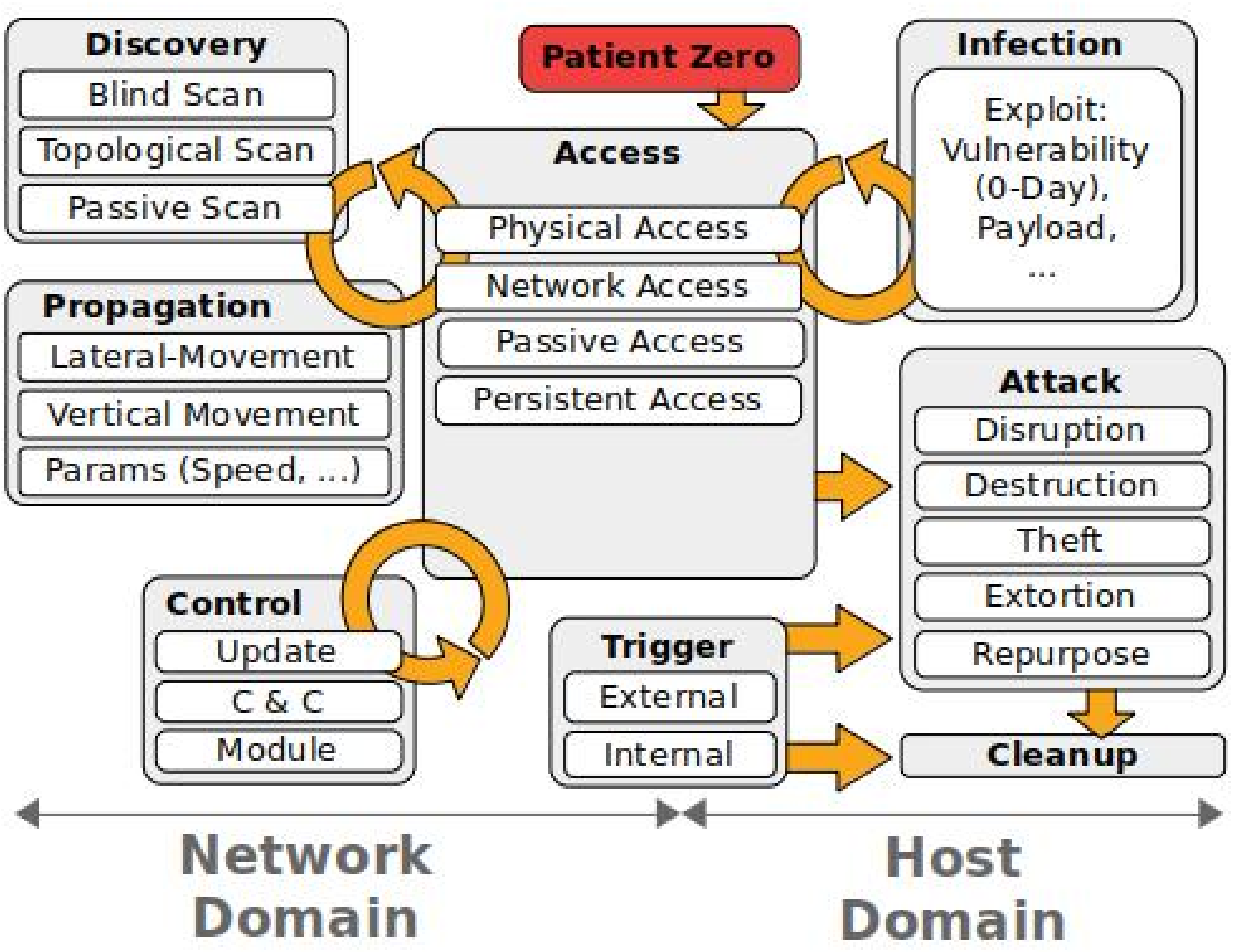
- Focus on malware communications
  - Complement existing security measures
- **Proactive measure(s):**
  Inhibit malware communication by design
  - Rate protocols, interfaces and architectures
    - Define metrics quantifying the ability of protocols to inhibit hidden communications
- **Reactive measure(s):**
  Detect hidden communications
  - Detect communication anomalies to detect infected subsystems in order to isolate them

The First Step: A Malware Lifecyle Model

- **Research question**
  - Can we capture malware behavior and communication needs through a model?

- **Method**
  - Analyze existing malware
  - Identify patterns in communications and state transitions of malware
  - Design a generic malware lifecycle model

A Generic Malware Lifecycle Model



Source: figure has been extended based on Fig. 1 of [2]

Future Research Question

- **(How) Can malware misuse existing security protocols (subliminal channels)?**
  - Prerequisites and countermeasures
  - Channel capacities, needs vs. offers
  - Traits that inhibit or support hidden communications
  - Develop metrics to quantify threat
  - Guidelines for robust protocol design

Summary and Outlook

- Generic malware lifecycle model enlarges the scope of current IETF security work
  - **Home: IRTF or IETF? Specific WGs?**
- Funded research project will start Jan. 2020
  - Seven partners (one AV/security, two utilities, one ministry, three research institutions); focus on utilities and e-vehicle charging infrastructure (including legals).
  - Results of relevance to IRTF/IETF work
    - Early feedback may reveal additional aspects

Bibliography

- **Bibliography**

[1]: Draft: https://datatracker.ietf.org/doc/draft-fabini-smart-malware-lifecycle/

[2]: Eder-Neuhauser, P., Zseby, T., Fabini, J., and G. Vormayr, "Cyber Attack Models for Smart Grid Environments“ Elsevier Sustainable Energy, Grids and Networks Volume 12, 2017, pp 10-29.
Pre-published version available for download at https://publik.tuwien.ac.at/files/publik_261089.pdf

[3]: D. Frkat, R. Annessi, T. Zseby: "ChainChannels: Private Botnet Communication Over Public Blockchains"; 2018 IEEE International Conference on Blockchain, ISBN: 978-1-5386-7975-3; pp 1244-1252.

Thank You!

Feedback and opinions welcome!

Email contact:
Joachim.Fabini@tuwien.ac.at