CERIAS

The Center for Education and Research in Information Assurance and Security

Malware Defense with Access Control Policy and Integrity Levels

Nicole Hands[1] & Harish V. Kumaravel[1] With Dr. Chris Jenkins, Sandia National Labs

[1]Purdue University

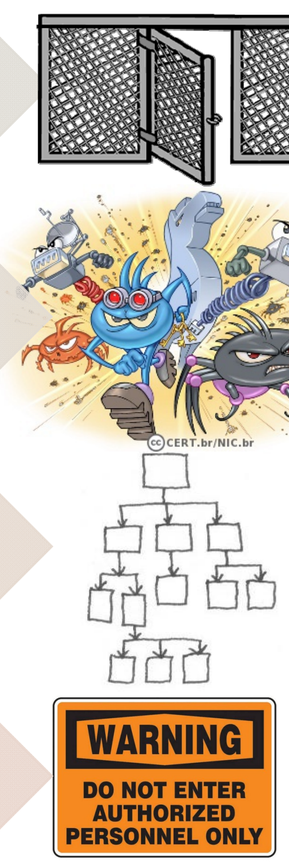
Research Question

Working under the assumption that system compromise is inevitable, what FTP server states exist such that they:

- can serve as a model of the system at large
- serve as indicators of malware infection
- can be used as inputs to define access control policy rules that allow or disallow execution of defined computational units

Integrating Multiple Fields of Study

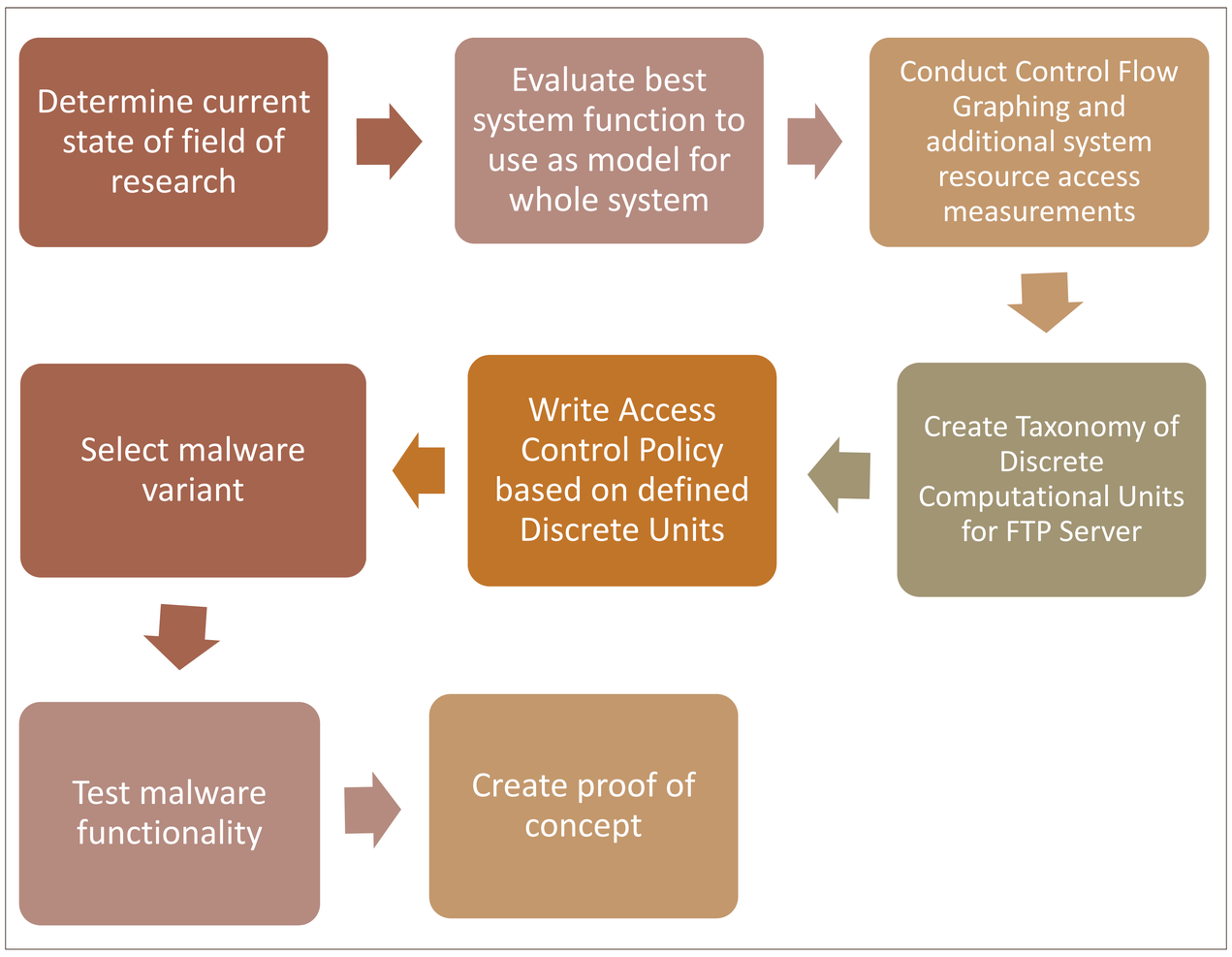
- Intrusion Detection
- Malware Mitigation
- Discrete Computational Units
- Access Control Methods



Motivation and Broader Impact

- Recognized the increasing impact of malware infection socially and economically
- Attempt to create a resilient system assuming inevitable compromise(s)
- Consider system design with analogies to the human immune system and the fight against parasites
- Represent an attempt to "step out of the box" and define a new way of addressing the malware arms race – rootkits, polymorphic malware, and as of yet undefined and unknown threats

Methods



Current Progress

- Conducted extensive literature review
- Analyzed system processes
- Selected model system
- Obtained computational resources
- Designed test environment

Next Steps

- Conduct control Flow Tracing/Graphing of FileZilla source code
- Define Taxonomy of "Discrete Computational Units"
- Validate taxonomy

Sources

Bruschi, D., Martignoni, L., & Monga, M. (2006). Detecting self-mutating malware using control-flow graph matching. In *Detection of Intrusions and Malware & Vulnerability Assessment* (pp. 129-143). Springer Berlin Heidelberg.

Eisenbarth, T., Koschke, R., & Simon, D. (2003). Locating features in source code. *Software Engineering, IEEE Transactions on*, *29*(3), 210-224.

Jenkins, C. 2014. Integrity Levels: A new paradigm for protecting computing systems. [Video File]. Retrieved from http://www.cerias.purdue.edu/news_and_events/events/security_seminar/archive/searchyear/2014.

Petroni, N., Fraser, T., Walters, A., and Arbaugh, W. (2006). An Architecture for Specification-Based Detection of Semantic Integrity Violations in Kernel Dynamic Data. *Proc. of the 15th USENIX Security Symposium*.

Rhee, J., Lin, Z., & Xu, D. (2011, March). Characterizing kernel malware behavior with kernel data access patterns. In *Proceedings of the 6th ACM Symposium on Information, Computer and Communications Security* (pp. 207-216). ACM.

Malware. (2012). Image. CERT.br.

Rootkit. (2012). Image. CERT.br.

(1) "INSuRE (http://insurehub.org) is training students in information security research with problems provided by the National Security Agency, Sandia National Labs, Pacific Northwest National Labs, and the Indiana Office of Technology. Any opinions, findings, and conclusions or recommendations expressed in this material are those of the author(s) and do not necessarily reflect the views of the aforementioned."

PURDUE UNIVERSITY