TOWARDS A RUN TIME POLICY ENFORCEMENT FRAMEWORK FOR MULTI-PLATFORM SYSTEMS

Phu H. Phung, Ph.D.
Intelligent Systems Security Lab
Department of Computer Science
University of Dayton

Safe and Secure Systems and Software Symposium (SS)

Motivation

- Many hybrid programming models have been proposed and adopted in practice
  - Allows external software components developed by third parties to be integrated to create a eco-system
- This execution model might cause the security risks since the third-party code can be potential malicious.
  - How to monitor the execution of the third-party code to ensure the business and security?

Goal

Provide a platform-independent policy specification and enforcement framework
- Can be used to enforce a wide range execution and security policies for different systems

Approach and Case Studies

- We develop a platform-independent policy specification
  - Can express fine-grained security, execution policies and business contracts
- We develop a set of policy utilities
  - Ensure the transparency of high level policies crossing multiple platforms
- We provide enforcement tools
  - Can support the policy enforcement for different underlying platforms

Challenges

- Third-party code is given permissions to execute and access the base systems
  - May contain bugs/vulnerabilities
  - May be under the control of attackers or may be malicious by intention
  - Does not comply with business contracts

- Software Infrastructures/Architectures nowadays are heterogeneous
  - Multiple platforms/programming languages
  - How to specify generic policies crossing multiple platforms: to ensure both business contracts and security that go beyond the traditional access control mechanisms

Attacker model

- Software-Defined Machine Architecture in IoT Infrastructures
- Hybrid Mobile Application Architecture

Remarks

- We introduced a generic runtime policy enforcement framework
  - A generic execution policy specification for stateful policies and contracts
  - A set of tools to enable the instrumentation and enforcement of policies
- We implemented and evaluated the proposed framework
  - IoT service infrastructures (Java)
  - Hybrid mobile applications (JavaScript)

Future work

- Development of a comprehensive and complete framework with realistic policies for various complex infrastructures
- Provide corresponding tools/utilities to support run time enforcement on different platforms

Phu H. Phung, Ph.D.
Intelligent Systems Security Lab
Department of Computer Science
University of Dayton, Dayton, OH 45469

http://academic.udayton.edu/PhuPhung