About PaaS Security

Donghoon Kim
Henry E. Schaffer
Mladen A. Vouk

North Carolina State University, USA
May 21, 2015 @ ICACON 2015
Outline

- Introduction
  - Background
  - Contribution

- PaaS Vulnerabilities and Countermeasures
  - Software Platform
  - Virtualization
  - Data Security & Integrity

- Some Security Trends
  - Isolation for multi-tenant environments
  - Protection of sensitive data
Introduction: Background

- Three Service delivery model for cloud computing
  - Defined by NIST
    - SaaS (Software)
    - PaaS (Platform)
    - IaaS (Infrastructure)

- PaaS (Platform as a Service)
  - Provide middleware resources to cloud customers (E.g., developers and providers of SaaS)
  - Hide complexity of maintaining the infrastructure
  - Enable low costs and higher computing efficiency

- Surveyed over the last five years (i.e., since 2010)
  - Research papers, industrial technical reports, etc.
Introduction: Contribution

- Three categories of PaaS security issues
  - Vulnerabilities and corresponding countermeasures
- PaaS security trends
  - Isolation for multi-tenants against side-channel attacks
  - Protection of sensitive data

Cloud Software Environments (PaaS)

- Features:
  - Runtime environments
  - Database
  - Web server
  - Development tools
  - Programming environments
  - Etc.

Vulnerabilities

- SW Platform
- Virtualization
- Data

Side-channel attacks

Protecing sensitive data
Software Platform (1/2)

- OS to Hypervisors and Virtual Platform (VP) (e.g., Java and .NET platform)
- The limitation of achieving proper isolation for multi-tenants
  - OS limitation as a hosting environment (i.e., PaaS Platform)
    - PaaS providers may prefer simplified abstractions
    - OS may not support a set of applications;
    - Need tuning depending on each application
  - Proper isolation mechanisms with three options
    - Isolation at OS level
    - Isolation at Standard Java Security
    - Isolation at VM level
Main open security issues at different layers
  - OS, Java VM, Container

Container for controlled environments
  - Dockers released in March 2013
    • Resource isolation features of the Linux kernel
    • Provide lightweight containers to run processes in isolation.

The user needs to “own” the whole stack for complete isolation.
  - Bare machine or sole-use may be the only safe solution
Virtualization (1/2)

• Major components of cloud computing
• Drive the growth of clouding computing
• Enabling sharing of resources for multi-tenancy
• Multi-tenancy vulnerabilities
  – The adversary may identify internal cloud structure which can launch a comprised VM
  – Cross-VM side channel attacks due to the sharing of physical resources (e.g., a single core CPU, cache)
• Countermeasures
  – Cloud providers may obfuscate both internal structure of their services and the placement policy
  – Avoid co-residence
  – Expose the risk and placement policy directly to users
Virtualization (2/2)

- **Vulnerabilities**
  - Components sharing between VMs, but lack of isolation
- **Countermeasures**
  - Strong isolation, nevertheless a large overhead
    - Performance between isolation and consolidation
    - Major cause: contention on memory channels or processor caches on the physical machine
  - Physical and functional hierarchical
    - Functional: divide a platform into available zone
Data Security & Integrity

• Protecting data and maintaining data integrity are important for all cloud service delivery model
• Additional security checks should be applied to sensitive data
• Countermeasures
  – Storing meta-data information in different locations; making information invaluable if a malicious user tries to recover
  – Secure block storage for encrypted data chunks
  – Authentication scheme by Merkle tree-based structure
    • Practical and scalable by reducing the storage overhead
  – Data Geolocation technique
Some Trends

• A side-channel attach is still popular due to multi-tenant virtualization
  – Require proper isolation mechanism
  – But, existing countermeasures may not applicable
    • Too specific (i.e., application-specific)
• Protecting sensitive data
  – Minimize the exposure of sensitive data as a plaintext
  – To protect personal data, the EU issued EU Data protection Directive
    • Limited storage in organization or governmental agencies while a tremendous increase in the scale of data
  – Need more robust methods of data geolocation