CloudSkulk: Design of a Nested Virtual Machine-based RITM Attack

Authors: Joseph Connelly Boise State University, Haining Wang University of Delaware, Jidong Xiao Boise State University

Goal

- Introduce a novel software security attack against cloud platform guest-host victim pairs to help aid in advancing cloud system security.

Background

- SubVirt: VM can act like a rootkit = STEALTH!!! (proof of concept)
- CloudSkulk: Introduce a new type of Rootkit-in-the-Middle (RITM) attack
- BluePill: real world VMM attack implementation project
- Man-in-the-Middle (MITM) attack:
  - relay (passive), alter (active) communication between users

- Full Virtualization: complete sim + hardware, unmodified guest OS
- Live Migration: copy running VM image to another guest

Our Approach

- CloudSkulk: Introduce a new type of Rootkit-in-the-Middle (RITM) attack
  - VM can act like MITM + rootkit = CLOUD STEALTH!!!
  - Exploit IaaS cloud platform QEMU/KVM software infrastructure
  - Full-Virtualization, Live Migration, Host-Port Forwarding

Implementation

- Step #1: SET-UP
- Step #2: PRIVILEDGES
- Step #3: ROOTKIT
- Step #4: NESTING
- Step #5: MIGRATION

Targets

- IaaS Cloud Platform Vendors:
  - Google Compute Engine, IBM SmartCloud Enterprise,...
- Targeted guest applications or users:
  - Spotify, Coca-Cola, Motorola, or any normal individual cloud users

Conclusions

- Significantly easier to implement than SubVirt, BluePill
- STEALTH!!! Maintain control for extended periods of time