Secure Out-of-band Remote Management in Infrastructure as a Service

Tomohisa Egawa
Kyushu Institute of Technology
egawan@ksl.ci.kyutech.ac.jp

Naoki Nishimura
Kyushu Institute of Technology
naonishi@ksl.ci.kyutech.ac.jp

Kenichi Kourai
Kyushu Institute of Technology
kourai@ci.kyutech.ac.jp

Infrastructure as a Service (IaaS) provides virtual machines (VMs) hosted in data centers. Its users can set up the systems in the provided VMs called *user VMs* and use them as necessary. They usually manage their systems through remote management software such as VNC. To allow the users to access their systems even on failures inside their VMs, IaaS often provides *out-of-band remote management* via a special VM called the *management VM*. Unlike traditional remote management, VNC servers are run in the management VM, not in user VMs, and directly interact with virtual devices for user VMs, such as virtual keyboards and video cards. Even if the networks of user VMs are disconnected due to configuration errors or if the systems crash in user VMs, the users can continue to manage their VMs.

However, this out-of-band remote management increases security risks because the management VM is not always trustworthy in IaaS. The management VM may be compromised by outside attackers if it is not maintained securely. If some of the administrators are malicious, they may mount insider attacks. Such attackers can easily eavesdrop on the inputs and outputs in remote management by replacing the VNC servers with malicious ones. For example, they can extract passwords from keystrokes sent from VNC clients, and take screenshots of user VMs to steal sensitive or private information. In addition, they may execute arbitrary commands inside user VMs by sending keyboard events to them.

To solve this security issue, we propose *FBCrypt*, which protects sensitive information in out-of-band remote management against the attackers in the management VM. FBCrypt encrypts the inputs and outputs in remote management between a VNC client and the virtual machine monitor (VMM), as illustrated in Figure 1. It can prevent information leakage via the management VM between them in a manner transparent to a user VM. For the inputs to a user VM, the keyboard and mouse events are encrypted by the VNC client, decrypted by the VMM, and passed to the user VM. For the outputs from a user VM, updated video data are encrypted by the VMM and decrypted by the VNC client. As such, only encrypted data are passed to the management VM. In addition to the confidentiality, the VMM checks the integrity of the inputs. It verifies the hash values generated from inputs and detects the modification before passing the inputs to a user VM.

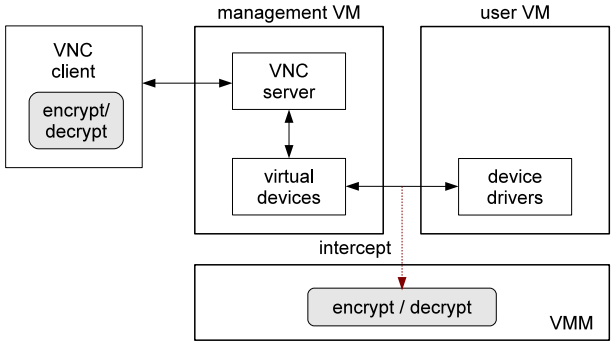

Figure 1. The architecture of FBCrypt.

To guarantee the integrity of the VMM in IaaS, FBCrypt performs remote attestation of the VMM with a trusted server outside IaaS. Remote attestation certifies the authenticity of the VMM by tamper-resistant hardware such as the trusted platform module (TPM). It measures the VMM by calculating its hash value, sends the signed measurement to a trusted server, and verifies its integrity. Although the management VM often has high privileges, the code and data of the VMM are still protected against the management VM. Thanks to the memory protection, the attackers in the management VM cannot steal secret keys for encryption in the VMM or modify the code in the VMM to invalidate the proposed security.

We have implemented FBCrypt in TightVNC and the Xen VMM for para-virtualized and fully-virtualized Linux. For the keyboard and mouse inputs in para-virtualization, the VMM identifies the input queue in a user VM and writes decrypted inputs into it. In full virtualization, it returns decrypted inputs to a user VM via its CPU register. For the video outputs, the VMM replicates a virtual framebuffer (VFB) for a user VM and provides the original and encrypted VFBs to the user VM and the VNC server, respectively. It synchronizes two VFBs when the user VM updates its VFB. Our experimental results show that keystrokes and screenshots are not stolen by the attackers in the management VM and that the overheads of the encryption and decryption are not so large.