# Virtualizing Alice and Bob

Dr. Edward G. Amoroso
Chief Executive Officer, TAG Cyber LLC
Mobile: (201) 454 – 1854
eamoroso@tag-cyber.com

## Abstract

As enterprise data centers and networks shift to cloud virtualization, the corresponding cyber protections must be adjusted accordingly. Specifically, security focus must shift from physical hardware systems communicating over networks to virtual software processes communicating across APIs. *(Analyst Note: This note was inspired by a technical discussion on application virtualization with Prevoty Systems and AlienVault in March 2016.)*

## Traditional Hardware Model

The traditional underlying model for cyber security protection involves client *Alice* and server *Bob* sharing information over some communications medium. The cyber security threat derives from the medium being accessible by some malicious actor *Eve* trying to tap or block the shared information flows. Here is how this familiar model is typically drawn in every cyber security textbook:

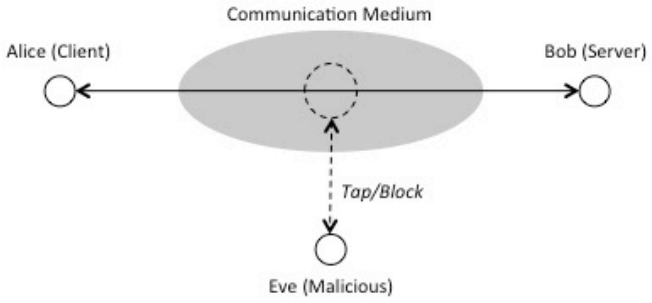


**Figure 1**. Traditional Alice and Bob Model

Implementation of this traditional model has involved physical hardware endpoints such as PCs and mobiles communicating over Internet protocol (IP)-based networks such as the public Internet. In this model, Eve corresponds to a malicious hacker using physical access to network packet flows to either sniff data or deny services. To provide risk reduction, security engineers have traditionally deployed physical hardware-based protections onto the physical endpoints and the IP network. Typical protections include firewalls, intrusion prevention systems (IPS), and encryption.

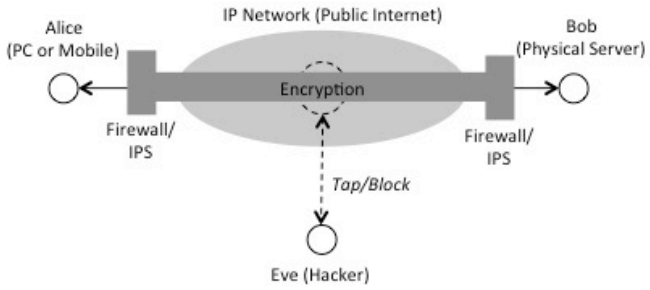


**Figure 2.** Traditional Alice and Bob Model with Security

The traditional model has been useful to security engineers for three decades and has been the basis for enormous growth in the current cyber security technology marketplace. Many security vendors have created more software-based protections to improve flexibility and extensibility. But this minor shift does not change the overall security architecture in a substantive manner; replacing custom integrated hardware appliances with less customized software running on more generalized platforms is still basically the same Alice and Bob architecture.

## Virtual Software Model

Modern data centers and networks are currently being virtualized at an astounding rate. This virtualization is being done in private data centers to reduce the maintenance burden associated with hardware appliances. It is being done in public clouds to streamline the introduction of new services and to enable the use of mobiles for enterprise application computing. In both cases, the computing and networking changes are significant, and introduce a fundamentally different set of cyber security issues.

The *conceptual* model for virtual communication between Alice and Bob in the presence of Eve does not change from the traditional view. It still looks like the familiar depiction of Alice, Bob, and Eve connected across some information-sharing medium. What changes substantially, however, is the implementation of this model on a virtualized, cloud-based operating system. The new primitives in such a model are virtual process executables – vAlice and vBob, and the communication is no

longer done over a network, but is instead done by software function calls across an application-programming interface (API). Eve, of course, is no longer sniffing or blocking a network, but is instead a piece of malware inserted at compile time as a Trojan horse, or executing as malware alongside Alice and Bob in the local cloud-based run-time operating system.

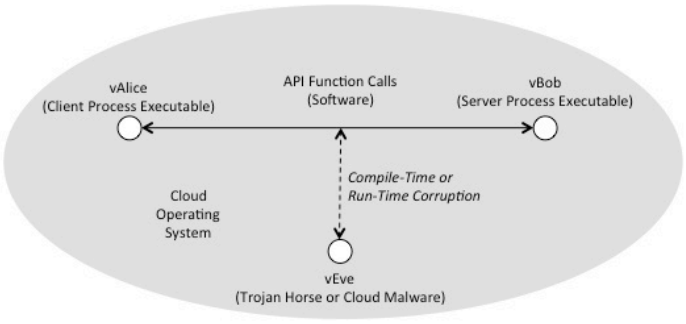


**Figure 3**. New vAlice and vBob Model on Virtual Operating System

The consequences of this change in the underlying model for cyber security are considerable. For example, where a firewall and intrusion prevention system would normally collect packets on a *tangible*, *physical* network between communicating systems, a new type of mediation must be performed between software processes. Similarly, where encryption would normally be done by physical or software encryptors on endpoints or at network gateways, software encryption would be implemented as software library functions compiled into the virtual endpoints. Programmers know that software controls can be created in two possible manners:

- *Static Compile-Time Software Controls* – The source code can be designed to include embedded, integrated protections. That is, software can include special regions of code that provide firewall, intrusion prevention, or similar functions. These functions are compiled into the executable, probably from special security software libraries, and would be controlled exclusively by the programmer.
- *Dynamic Run-Time Software Controls* – The operating system can be designed to include run-time mediations that control how the software operates. In a cloud operating system such as OpenStack, for example, the run time environment can ensure that a given piece of software does not attempt to execute outside a boundary-defined region, sometimes referred to as a container. The cloud operating system lifecycle maintenance team would control these run-time security functions.

The implementation of these controls is obviously quite different from the tangible, physical controls in any traditional cyber security architecture. The specific categories of security controls, however, such as encryption, firewalls, intrusion prevention systems, data leakage prevention, two-factor authentication, log

management, security information event management (SIEM), and user behavioral analytics, would remain the same.

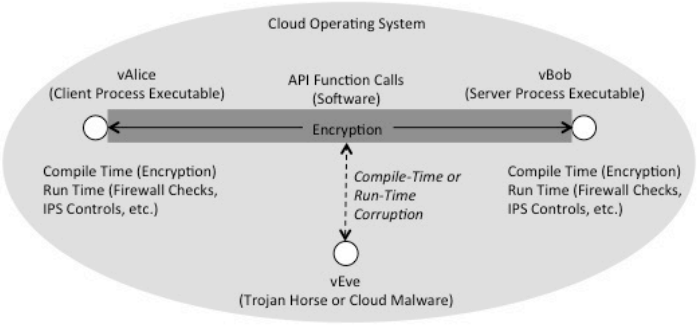


**Figure 4**. New Virtual Cyber Security Architecture Across Cloud APIs

Interestingly, in the new model, Eve shifts from a traditional, wiretapping, man-in-the-middle hacker to a piece of malware embedded in the code or run-time environment. Preventing this malware from being inserted into the virtual endpoint executables becomes the new obligation for endpoint security solution. Preventing this malware from being inserted into the cloud operating environment becomes the new obligation for the data center virtualization or cloud system administration teams.

## Implications

Data center and network designers, enterprise security teams, and interested observers such as compliance managers and regulatory authorities must immediately begin to adjust their understanding from traditional to virtual cyber security protection models. Furthermore, as cyber security vendors make this shift to a virtual software model, the investment community will have to adjust its thinking as well, perhaps assigning much higher valuation to companies that focus on virtual software and APIs versus ones that sit in-line with physical systems over networks.

Perhaps the biggest shift in thinking, however, will have to come from the offensive attack community, because virtual, software-based architectures will prove to be much more difficult to attack. Tapping into virtual communications between virtual processes requires a fundamentally different set of attack procedures, so enterprise security teams are advised to virtualize as quickly as possible. Granted, if the virtualization is not performed with the requisite corresponding security protections, then unauthorized access through provisioning, user access, and administrative controls will be easily obtained.

An early observation is that this shift to virtualization and cloud will create a much greater obligation to improve all phases of the software development and maintenance process lifecycle, since malware insertion into code becomes the new

baseline attack vector for virtualized computing. Security for the now-popular Agile and Dev/Ops processes thus becomes a key factor in providing virtual security for cloud applications.

---

**About TAG Cyber LLC**

Founded in 2016 by former AT&T Chief Security Officer, Dr. Edward G. Amoroso, TAG Cyber LLC is focused on bringing world-class, military-grade cyber security analysis, training, consulting, and media services to enterprise CISO teams around the world. The *TAG Cyber Security Annual* is its flagship annual publication, offered to enterprise security teams as an eBook or free PDF download from select cyber security vendors.