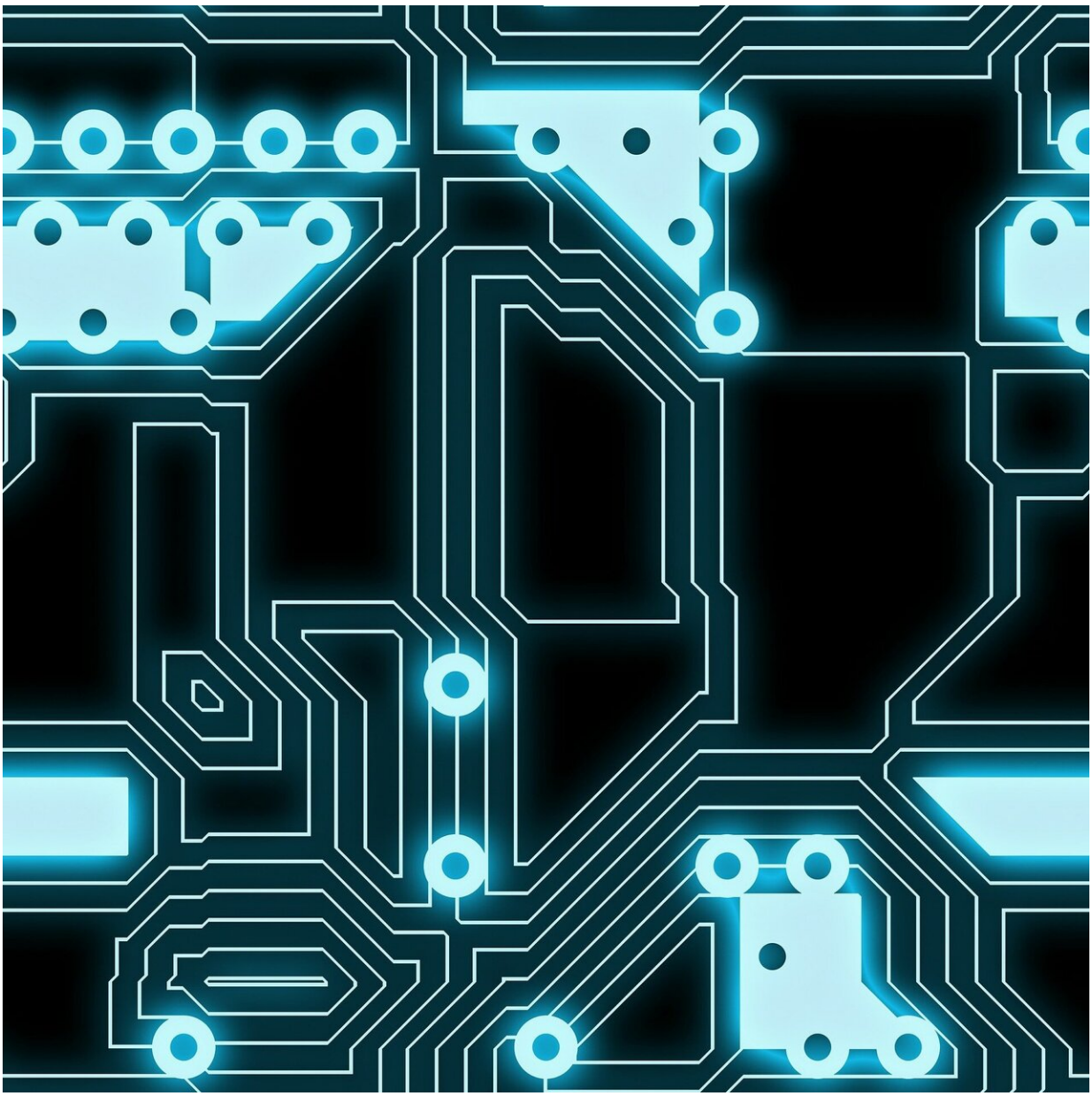
A methodology for enabling forensic analysis using hypervisor vulnerabilities data

June 7 2019



Credit: CC0 Public Domain

Hardware/Server Virtualization is a foundational technology in a cloud computing environment and the hypervisor is the key software in that virtualized infrastructure. However, hypervisors are large pieces of software with several thousand lines of code and are therefore known to have vulnerabilities. Hence, a capability to perform forensic analysis to detect, reconstruct and prevent attacks based on vulnerabilities on an ongoing basis is a critical requirement in cloud environments.

To gain a better understanding of recent hypervisor vulnerabilities and attack trends, identify forensic information needed to reveal the presence of such attacks, and develop guidance on taking proactive steps to detect and prevent those attacks, NIST has published NIST Internal Report (NISTIR) 8221, A Methodology for Enabling Forensic Analysis Using Hypervisor Vulnerabilities Data, which outlines a methodology to enable this forensic analysis.

Two open-source hypervisors—Xen and Kernel-based Virtual Machine (KVM)—were chosen as platforms to illustrate the methodology; the source for vulnerability data is NIST's National Vulnerability Database (NVD). The methodology is broken into three steps:

1. Classify the vulnerabilities based on three categories: hypervisor functionality where the vulnerability exists, attack type, and attack source. The outcome of this step is to obtain the relative distribution of recent hypervisor vulnerabilities for the two products in the three categories.
2. Identify the hypervisor functionality that is most impacted, then build and run sample attacks, along with logging system calls.
3. Perform an iterative process that identifies gaps in the evidence

data required for fully detecting and reconstructing those attacks and to identify techniques required to gather the needed evidence during subsequent attack runs.

More information: A Methodology for Enabling Forensic Analysis Using Hypervisor Vulnerabilities Data: csrc.nist.gov/publications/det … il/nistir/8221/final

This story is republished courtesy of NIST. Read the original story here.

Provided by National Institute of Standards and Technology