Fingerprinting Multi-Tenant Computing Systems

Adam J. Sypniewski, Jose Nazario, Dylan Schmorrow
Soar Technology, Inc., Ann Arbor, MI 48105
adam.sypniewski@soartech.com

White paper submitted to the Office of Advanced Scientific Computing Research for the ASCR Cybersecurity for Scientific Computing Integrity Workshop: *Trust within Open, High-End Networking and Data Centers.*

Abstract The advent of widespread, easily accessible cloud compute environments has spawned a new generation of cyber attacks. We describe a new technique that "fingerprints" servers to augment the attack surface of an application deployed in a virtualized, distributed architecture. We also briefly discuss SoarTech's prior work in cybersecurity systems.

1 Introduction

The need for on-demand, scalable, and distributed allocation of computing resources has driven the advancement of resource-sharing architectures and businesses. Spurred by the advent of cheap hardware and efficient virtualization, batch processing and time-sharing have given way to cloud computing architectures. Systems such as Amazon's Elastic Compute Cloud (EC2) allow even relatively inexperienced users to quickly deploy large, distributed application servers in a multi-tenant, virtualized environment.

With this, of course, comes a new suite of security and privacy challenges. Ristenpart et al. [2] showed that cloud cartography (i.e., mapping the network architecture) is not well disguised, and that co-resident VMs can communicate over covert channels. Moreover, they went on to demonstrate a technique for instantiating a VM co-resident with a given target server, as well as a method for detecting co-residency. In both cases, the target is preselected, and co-residency is achieved by exploiting the behavior of the cloud's placement algorithm.

Here, we briefly describe a hypothetical side-channel attack that extends the work done in [2]. We suggest that by measuring any time-dependent dynamics of several systems, we can extract information about the resident tenants, even without preselected targets. In turn, this provides a means for parallelizing hypervisor or side-channel attacks against an application distributed across multiple physical servers.

2 Multi-tenant Information Leakage

Time-varying system dynamics can reveal incredible amounts of information about the underlying system. In fact, Takens' Theorem [3] specifies the conditions under which the steady-state behavior of a chaotic system can be reconstructed from time-dependent observables. In our case, the time-dependence of a server's observables (e.g,. CPU usage, HDD performance, or network latency) characterizes the services running on that machine, and for multi-tenant servers, this includes applications running on co-resident VMs. For example, given a time series $t \in \{t_0, t_1, \ldots, t_n\}$ of HDD latency data, time delay plots (t_i, t_{i+1}) are effectively "fingerprints" of the system, since their geometry is uniquely determined by the dynamics of each other application and tenant accessing the same HDD.

To exploit this phenomenon, an attacker would launch many VM instances on a distributed computing system, indicated by X in Figure 1. X will likely be co-resident with other tenants, labeled A, B, C, and D. The probe software X begins measuring time-dependent performance data, producing fingerprints of the physical system. By cross-correlating many such fingerprints from many instances of X, the attacker could determine each tenant's contribution to the server's fingerprint, allowing the attacker to enumerate the software being run on each

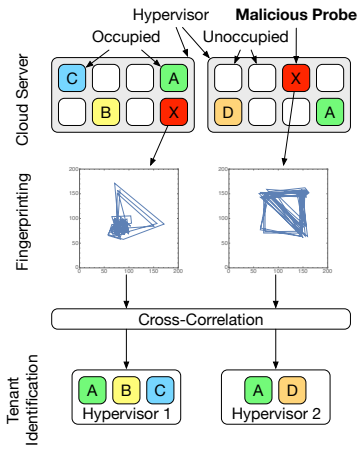

Figure 1: A hypothetical attack in which cross-correlating time-varying properties of servers effectively identifies VMs.

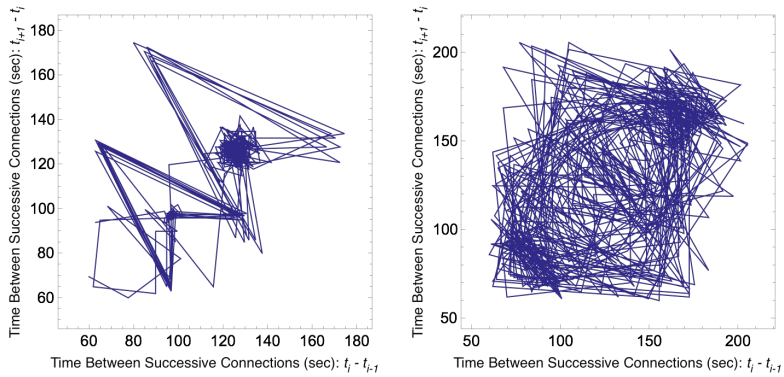

Figure 2: Experimental results demonstrating the uniqueness of time-varying dynamics. On the left are time delay plots of DNS connections to Twitter. On the right are similar measurements for an internal wiki.

physical server. Once a distributed application (one that is simultaneously virtualized on several physical systems, such as A) is discovered, our attacker has effectively increased the size of the attack surface, and can now coordinate and parallelize his attacks against that system. For example, he could attempt a side-channel attack to steal cryptographic keys, and now has access to multiple equivalent systems simultaneously.

3 Related Work

Soar Technology, Inc. (SoarTech) has ongoing research efforts that have identified key scientific research opportunities relevant to the DOE Office of Science. Recently, SoarTech participated in the Computational Cybersecurity in Compromised Environments (C3E) workshop sponsored by Special Cyber-operations Research and Engineering (SCORE). SoarTech showed that it is possible to detect some advanced persistent threats (APTs) in DNS data using similar time-domain analysis techniques as mentioned here [1]. Time delay plots from this work are shown in Figure 2, where it becomes immediately evident that fingerprinting dynamic processes is quite feasible.

In summary, as cloud computing environments become increasingly popular, they will also be subjected to a host of cyber attacks. SoarTech continues to pioneer research in novel cybersecurity techniques in order to better prepare today's cyber-operators for the next generation of attack vectors.

About the Author Dr. Sypniewski is a research scientist at Soar Technology, Inc. (SoarTech) in Ann Arbor, MI. He earned his Ph.D. from the University of Michigan studying experimental astrophysics, where he used machine learning, network theory, and data mining techniques to derive galactic properties from terabytes of data. He continues to apply this knowledge in the design of novel, cognitive agents, particularly for cybersecurity and autonomous systems applications.

References

[1] Parunak, H.V.D., Nickels, A., & Frederiksen, R. (2014). An Agent-Based Framework for Dynamical Understanding of DNS Events (DUDE). In *First International Workshop on Agents and CyberSecurity*, Paris, France.

[2] Ristenpart, T., Tromer, E., Shacham, H., & Savage, S. (2009). Hey, You, Get Off of My Cloud: Exploring Information Leakage in Third-Party Compute Clouds. In *Proceedings of the 16th ACM Conference on Computer and Communications Security*, Chicago, IL (pp. 199-212), New York, NY: ACM.

[3] Takens, F. (1981). Detecting strange attractors in turbulence. In D. Rand & L.-S. Young (Eds.), *Dynamical Systems and Turbulence* (pp. 366-381). New York: Springer.