SDP Hackathon #4 Analysis & Report

High Availability Public Cloud Research

March 28, 2016

Research Participants

The Software-Defined Perimeter (SDP) Research Workgroup of the Cloud Security Alliance (CSA) held its fourth Hackathon during the 2016 RSA security conference. The objective of the Hackathon was to research if a high availability public cloud could be created by using SDP and private IP services.

SDP Hackathon #4: High Availability Public Cloud

High availability application infrastructure is defined by three characteristics:

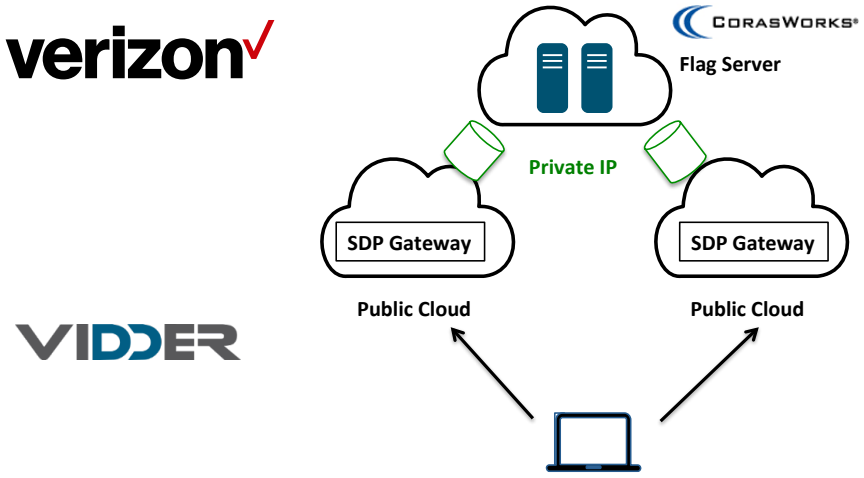
1. No single point of failure
2. Disruption tolerant operation
3. Failure detection

The current approach to building a high availability application infrastructure is to have a fully redundant network "front-end" meshed to a fully redundant compute "back-end" using specialized hardware. Additionally, the entire data center is geographically replicated to mitigate the risk of regional power and connectivity outages.

Hardware-based high availability infrastructures have been deployed for many decades by financial and government institutions and are viewed as a very safe and proven technology. Unfortunately they suffer from two substantial shortcomings:

- Extremely high cost (starting at $10s Millions) and
- Fairly long deployment times (years).

CSA, Verizon, and Vidder teamed up to research how a high availability infrastructure could be created using public clouds with the equivalent robustness of a dedicated data center. The key hypothesis was that while a dedicated data center is more "available" than a single public cloud, multiple public clouds should be more "available" than a single data center if all the compute resources could be connected.



To replicate the redundant "front-end" architecture found in data centers, software-defined perimeter (SDP) gateways were deployed on multiple public clouds. The SDP "front-end" ensured that users would have multiple paths to compute resources across the Internet. Next, to replicate the redundant "back-end", a private IP network was provisioned between the SDP gateways and compute resources. The private IP "back-end" ensured there were multiple paths from the SDP gateways to the compute resources (which were deployed in a redundant topology).

Hackathon Step Up

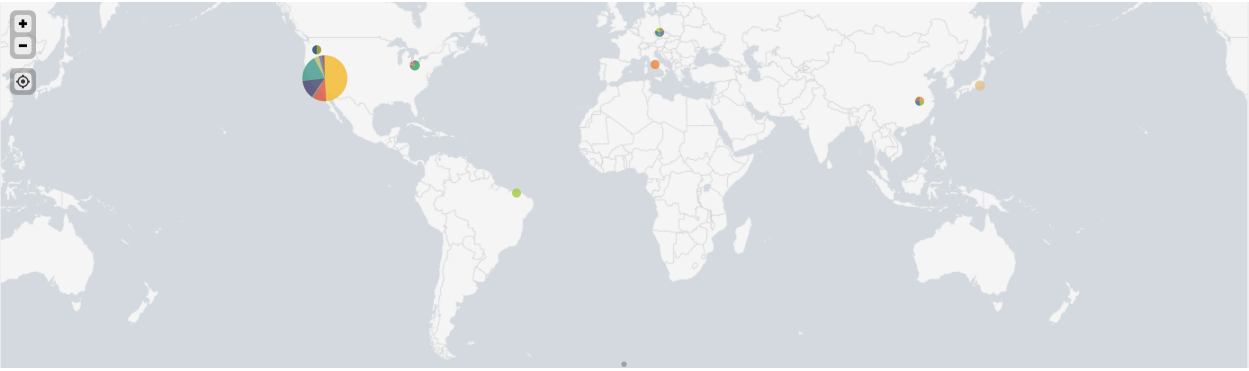
Participants in the SDP Hackathon were given the IP addresses of the SDP components and protected file server, a full packet capture of a user accessing the protected file server, as well as the credentials for the protected file server. A $10,000 prize was offered to the first person that could access the flag server.

To further showcase the SDP's strength to the US government sector, where the security requirements are more stringent, Verizon intentionally placed a private demo of a cloud-based UAV flight management system by CorasWorks on the same network as CSA's Hackathon. This network was under constant attacks, and the CorasWork application had no additional security protection but the SDP.

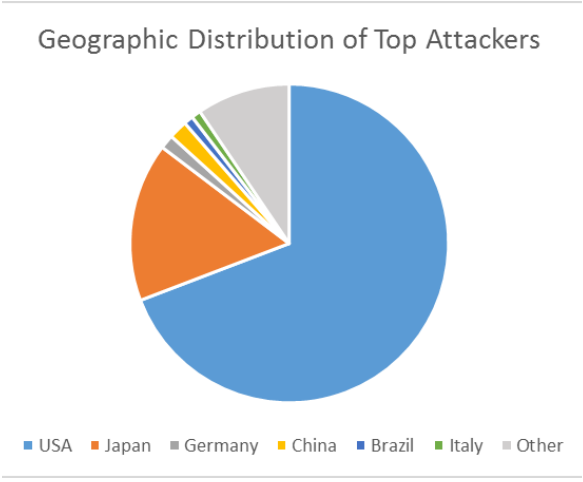
The provisioning and testing took one week and was led by Verizon and Vidder personnel. While the meshed public cloud architecture was novel, all of the components used were commercially available services.

Hackathon Results

Vidder PrecisionAccess Insight™ (Insight) monitoring platform was deployed to log attacks. Vidder's Insight identified 191 different attackers who generated millions of attacks.



Post-event forensic analysis revealed a number of highly sophisticated attacks in which the SDP protocols were reversed engineered to embed a MFA token inside the SSL/TLS Hello packet. While some attackers were able to create the correct SDP packet structure, none were able to generate the correct GMAC signature. The attackers who established a TCP connection to the SDP Gateway had their connections terminated once the GMAC error was detected. No activity was detected on the protected file server nor was there any disruption to CorasWorks UAV management demo throughout the entire event.



Conclusion

As a first attempt to create a high availability infrastructure by combing multiple public clouds, this Hackathon was extremely successful. The combined use of SDP to create a redundant "front-end" network and private IP to create a redundant "back-end" compute environment demonstrated the security and feasibility of creating a high availability infrastructure using a multiple public clouds strategy.

For organizations such as financial institutions and government agencies that are required to operate high availability networks, the results of this research project point to a more cost effective deployment strategy. **This Hackathon demonstrated that cloud-based services can replace hardware-based high availability infrastructure if the correct architecture is used.**

Appendix: History of SDP Hackathons

SDP Hackathon #1

Theme:	Insider Threat
Date:	RSA Conference 2014, Feb. 24 – 28, 2014
Goal:	Simulate inside attack by providing SDP client to participants
Result:	No attacker was able to establish a TCP connection
	Over a million port scans detected
	Greatest number of attack originated in Argentina

SDP Hackathon #2

Theme:	DDoS Attack
Date:	IAPP-CSA Congress, Sept. 17 – Oct. 17, 2014
Goal:	Provide IP addresses of SDP gateways to test DDoS mitigation
Result:	No attacker was able to impact application availability
	Attacks spread across 104 countries
	Greatest number of attacks originated in the USA

SDP Hackathon #3

Theme:	Credential Theft
Date:	RSA Conference 2015, April 20 – 24, 2015
Goal:	Provide credential of SDP client and application server to participants
Result:	Over 1 million server exploit attempts on SDP controller
	3,551 attacks with the correct ID but failed GMAC
	Greatest number of attacks originated in China

About Cloud Security Alliance

The Cloud Security Alliance (CSA) is the world's leading organization dedicated to defining and raising awareness of best practices to help ensure a secure cloud computing environment. CSA harnesses the subject matter expertise of industry practitioners, associations, governments, and its corporate and individual members to offer cloud security-specific research, education, certification, events and products. CSA's activities, knowledge and extensive network benefit the entire community impacted by cloud — from providers and customers, to governments, entrepreneurs and the assurance industry — and provide a forum through which diverse parties can work together to create and maintain a trusted cloud ecosystem. For further information, visit us at https://cloudsecurityalliance.org, and follow us on Twitter @cloudsa

About Verizon

Verizon Communications Inc. (NYSE, Nasdaq: VZ) employs a diverse workforce of 177,700 and generated nearly $132 billion in 2015 revenues. Verizon operates America's most reliable wireless network, with more than 112 million retail connections nationwide. Headquartered in New York, the company also provides communications and entertainment services over America's most advanced fiber-optic network, and delivers integrated business solutions to customers worldwide.

About Vidder

Vidder PrecisionAccess™ isolates the protected applications from all networked users and devices, connecting only authorized users and trusted devices to applications they are authorized to access. The resultant new paradigm enables enterprises to achieve agility with security, augmenting cloud migration and business ecosystem collaboration, while reducing risk for traditional IT. PrecisionAccess is the industry's first and most widely deployed solution based on the Software-Defined Perimeter (SDP) framework for advanced access control promoted by the Cloud Security Alliance (CSA). In 2015, Gartner named Vidder a Cool Vendor in Cloud Security Services. The company's headquarters are in Campbell, Calif. For more information, visit www.vidder.com