2018 TAG CYBER SECURITY ANNUAL

VOLUME 2

INTERVIEWS WITH CYBER LUMINARIES

Expert Advisory Research

Dr. Edward G. Amoroso
Chief Executive Officer, TAG Cyber

September 2018

Micro-Segmenting Data Centers and Networks Using Strong Separation and Abstraction

Using embedded trusted identity tokens to enhance enterprise security and policy enforcement at the network protocol layer.

John Hayes, Founder and CTO of BlackRidge Technology

Security policies are typically designed with the intent to check credentials associated with access requests before entry is permitted. The problem is that the network protocols such as TCP are bidirectional and must allow multi-step back-and-forth handshakes between clients and servers to establish identity credentials at the application layer. This violation of most enterprise policies can be solved through advanced separation methods that employ embedded credentials into the network protocol. John Hayes, CTO of BlackRidge, caught up with us recently and helped us understand how BlackRidge supports such separation to truly enforce enterprise policies.

EA: John, explain in a nutshell, how your technology works?
JH: Our technology inserts a cryptographically-secured identity token into the first packet of every TCP session. Across the network, this identity token is recognized and access to network resources is allowed or denied. This allows network and cloud resources to have the identity of the user or device connecting to them before establishing the TCP session. It's really a secure version of Caller-Id for the Internet.

EA: Do clients or servers have to modify their TCP stacks to use your solution?
JH: No, we do not modify the TCP stack. Our endpoint software operates as a shim below the TCP stack and above the device driver. The native TCP stack is unaware of our presence and we operate transparently to the stack and the applications. In this way, we can add identity and authentication to legacy networks and applications without a forklift upgrade of the infrastructure.

EA: Where does a security team position the BlackRidge gateway?
JH: There are several common use-cases and deployment models that position BlackRidge gateways, our identity recognition and policy enforcement points, in different locations. These are positioned at the perimeter of an enterprise to identify and authenticate all external traffic; within the enterprise to provide micro-segmentation; in front of cloud resources to protect those cloud resources from discovery and access, even when using public cloud infrastructure; and in front of the management plane to separate and isolate critical management infrastructure and authenticate access.

EA: Do you support virtualization and cloud environments?
JH: Yes, we support the leading virtual and cloud environments. Public cloud infrastructure does not provide the same discovery protection that traditional physical infrastructure provides, and segmentation within and across heterogeneous environments is difficult to achieve and prove. Cloud resources protected and segmented by BlackRidge do not respond to network scans and network reconnaissance, restoring the discovery privacy and compliance controls previously enjoyed only by physical data centers.

EA: What are the risks of not deploying strong separation solutions such as yours in the data center or enterprise?
JH: Traditional network management relies on using addresses and topology. Addresses can be spoofed and being topologically dependent requires constant synchronization with how the network is currently connected. This creates quite a few hassles today, trying to manage firewall rules and router ACLs. By introducing strong separation via cryptographically-secured identity to the network, BlackRidge provides both authenticated access control on a per TCP session basis and provides attribution information gleaned from our identity tokens to SIEM and analytics systems. This authenticated attribution information is unavailable in traditional data centers and enterprise deployments otherwise.

EA: What special advantages does BlackRidge have for micro-segmentation over other vendor's approaches?
JH: BlackRidge performs First Packet Authentication. This is the ability to determine the identity of the originator of a TCP session on the very first packet of the TCP session, before any response is made to the requestor. This blocks port scanning with no packet leakage problems common to other firewall and application firewall security solutions. By operating at the TCP layer on the first packet, BlackRidge enforces policy at the earliest possible time to provide strong separation with attribution, supports multi-vendor and heterogeneous data center and cloud environments, and provides automation and abstraction from the network.