Packet-Based Authentication and Security

An Interview With *John Hayes, CTO BlackRidge Technology*

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

FOR MANY years, enterprise security teams have had to react to adversaries' ability to conduct network scanning and reconnaissance, and attacks on an organization's IT environment. The implicit trust required by the Internet Protocol (IP) generally allows packets from any IP address to progress inbound and put an organization at risk. If access management policies could be better enforced on inbound IP addresses, greater security can be ensured.

A company at the forefront of ensuring better network packet-based authentication and security is BlackRidge. The company has developed technology that creatively enhances the TCP/IP suite to provide authentication of the packet sender's identity and enforcement of enterprise policy before connections are established. We recently caught up with John Hayes of BlackRidge Technology to understand better how such protocol security methods work.

EA: Can you explain the basic concept behind the BlackRidge Transport Access Control method?
***JH*:** We use authenticated identity to authenticate TCP sessions before allowing them to be established. Each TCP session is individually authenticated with a cryptographic token inserted into the first packet (TCP-SYN) of a TCP session. Our software approach enables deployment in enterprise, cloud, SDN and IIoT infrastructure.

EA: What threats specifically are addressed by your technology?
JH: With today's security threats, any information used in the security decision process must be authenticated before it is used. Using unauthenticated information in this decision process provides an attack surface for the adversary. Applying this concept to network traffic, most network security approaches use a combination of network addresses and content to make decisions. Addresses cannot be authenticated. Content, when available, is not always authenticatible. I say "when available" with respect to content because as more and more content is being encrypted, it is not available for decision making, unless the encryption keys are shared with the network security device. Not all customers are willing to do that. BlackRidge uses authenticated identity for its decision process that is available at the network

layer, independent from the content, whether encrypted or not. Getting back to relying on authenticated information when making security decisions, another thing to consider is how the authentication is performed. If the authentication requires interaction- a series of communications between the requesting party and the authenticating party- then the authentication mechanism itself can be used for mapping and discovery. This is how PKI certificates, TLS and IKEv2 operate. BlackRidge uses non-interactive authentication, blocking scanning and discovery from unauthorized sources in addition to managing access to BlackRidge protected resources.

EA: What aren't existing IP-based tools sufficient for authentication and security?
JH: Existing IP-based tools use a combination of rules, heuristics and statistical metrics for decision making. These tools use information which cannot be authenticated, and which often needs continuous updating. The limitation of these tools is that they suffer from both false positives and false negatives, limiting both their deployability and effectiveness. A false positive, by the way, is a false alarm, an indication of a security event when no event exists. A false negative is an undetected attack. It is the false positives that that preclude the automation of these tools for cyber defense. BlackRidge, with its cryptographically secured identity tokens have an extremely low false positive rate (<0.0001%) enabling deployable cyber defense automation.

EA: How do customers integrate your solution into their security architecture?
JH: BlackRidge products are designed to work as an overlay software solution to block unidentified and unauthorized access and protects resources from discovery from unauthorized network mapping and reconnaissance. By integrating with existing Identity Management systems (IDMS) enables existing identities to be used to authenticate network sessions and automate security policies. We have also integrated our event reporting with several SIEM and analytics systems, providing visibility to events within a customer's existing monitoring and response infrastructure. Operationally, we deploy our BlackRidge TAC software as inline layer 2 (transparent) or layer 3 (addressed) enforcement points. Being able to select layer 2 or layer 3 operation enables us to deploy in both LAN environments and cloud/SDN environments. In this way, we can extend a customer's identity-based security policies from the enterprise to the cloud, enabling an identity secured hybrid solution.

EA: What threat trends are you hearing from customers?
JH: The largest growth of threats we are seeing is coming from the Industrial IoT (IIoT) sector and Operational Technology (OT) converging onto enterprise IT networks. This includes industrial control systems, building management systems, medical equipment and factory automation. Legacy, non-networked devices that have been migrated to networks and new IoT devices have paid little attention to the security of the networks and devices, providing new surfaces for attack. Now we are being asked how to secure both legacy (brownfield) IIoT as well as new deployments. BlackRidge's identity-based technology can be applied "on the wire" to authenticate and secure both legacy (brownfield) IIoT as well as new deployments.