Security Annual

2020 EDITION

OUTLOOK FOR 50 CYBER CONTROLS

PUBLISHED BY TAG CYBER

Interviews with Cyber Luminaries

Handbook & Reference Guide

AN INTERVIEW WITH JOHN HAYES
CTO, BLACKRIDGE TECHNOLOGY

IDENTITY-BASED SOLUTIONS FOR NETWORK SECURITY

A significant weakness in any IP-based enterprise is that easily spoofed source addresses complicate access decisions based on incoming packets. Instead, what generally happens is that best-effort approaches are taken to inspect source address ranges, to direct the inbound traffic to a hosted gateway that will provide application-level security decision-making. This has the obvious drawback of allowing potentially malicious packets into the enterprise and to also move laterally within it.

BlackRidge Technology offers a creative solution to this problem using an identity-based enhancement to the TCP/IP protocol suite. A special gateway called a Transport Access Control (TAC) gateway is used to interrogate incoming packets for evidence of proper source authentication before traffic is permitted to proceed. We spent some time with John Hayes, CTO of BlackRidge Technology, to learn more about the approach and its implication on zero trust security.

EA John, what specifically is the weakness in the Internet protocol that your team set out to address?

JH As you know, Ed – the original TCP/IP protocol suite does not include native support for strong authentication. Security gateways must therefore do the best they can to determine the source and intent of any packet that initiates a new session. The traditional five-tuple used in packet filters has been the most popular means for making such decisions, but this is not a sufficient level of assurance in networks that must protect truly valuable assets.

EA How does the BlackRidge solution to this problem work?

JH We've created and integrated an identity-based solution that works at the protocol level to identify incoming packets using a special gateway. The scheme we've invented is called Transport Access Control or TAC – and it allows a BlackRidge TAC Gateway to be positioned at the network entry point or in front of valuable assets, perhaps next to other access or edge security components. Incoming packets are then interrogated using an identity authentication scheme that is much stronger than inspection of easily spoofed source IP addresses. Using BlackRidge TAC, our customers can ensure that only approved traffic ever enters a trusted domain or enterprise.

EA You've suggested that the TAC scheme is consistent with the goal of zero trust in an enterprise. How does that work?

JH When packets are received from the Internet, it is 100% appropriate to view their associated source information with low confidence. It is this notion of confidence as a factor in determining trust that we find interesting. That is, we envision a confidence scale where assurance activities move the needle on the scale, depending on the strength of the action. When a packet arrives with a weak source address, we assign low confidence to its origin, but once the TAC gateway has interrogated the packet and authenticated its source identity, we can move the needle on the confidence scale.

EA Do you find that higher assurance environments demand the type of protection offered by the TAC?

JH Certainly, we see the higher assurance customers as the earliest adopters of our technology, if only because the urgency to protect infrastructure is so high. But we believe that any organization with security policy requirements for secure access, and certainly any organization that provides identity and access management services for third parties, will really benefit from our solution.

EA What future directions do you see in this area of identity-based network security?

JH Well, zero trust security is going to increase in importance as a design philosophy, and this is good because it is consistent with trends in cloud and IoT architectures. We also expect to see security policies for identity-based controls become more tightly enforced. The idea that network traffic can enter a network segment without authentication and access restrictions is just asking for trouble. We believe this will be rectified – and we're excited that BlackRidge will be an important part of that equation with our identity-based Transport Access Control.