The Coming Identity Based Network Management Revolution; Interview with Blackridge Technology CTO John Hayes, Part III

Since the advent of the TCP/IP protocol, network administrators have had a major blind spot: the ability to reliably determine the identity of an individual device or user. BlackRidge's new Eclipse™ solution, built on BlackRidge's patented Transport Access Control (TAC), uses client drivers or gateway appliances to insert unique identity information to every TCP packet. In this third and final post in our blog interview series, BlackRidge Technology CTO John Hayes and I discuss where BlackRidge is heading and the challenge of managing infrastructures from the perspective of devices rather than networks.

Ben: *Let's discuss your recent identity aware networking solution release. What is different in this release?*

John: We've made a number of advances since our first release, which was targeted at government customers. The main advance is in scalability. We can now handle 10,000 Identities per physical or virtual gateway.

Next is manageability. We have a more comprehensive management interface, including a GUI. We have Active Directory and LDAP integration. In general, we have a better-defined integration with existing systems. We have also implemented log management so we can process the logs appropriately and feed into other systems.

Another interesting use case that we have found is in network

segmentation. One of the issues with VLANs is a technical limitation within the VLAN tag itself, you can only support 4,000, 4k VLANs. Eclipse allows you to implement the functionality of VLANs without having to deal with the limitations of VLANs.

I would consider VLANs to be another topological limitation of the networks. Think of it this way, VLANs were invented as a management control mechanism. It took one physical LAN and carved it up into a bunch of virtual LANs and it works well. But you are still tied to the policies of both the underlying physical and the virtual LAN. If you can completely free yourself from that, it makes policy implementation easier.

Ben: *How do you keep administrators from getting snowed under? This is a pretty revolutionary concept and when you are looking at managing individual devices it sounds complicated.*

John: You are right. At first glance this can viewed as a big hairball. We really are looking at this from the perspective of the Identity of an individual device or user.

But you probably do not want to manage everything – if I had 10,000 users, I do not want to manage every user individually. What we normally do is determine a couple of common groups. Then you drop users into those groups.

You are going to be in the engineering group. You are going be in the finance group. You are going be in the sales group. What that does is it allows you to say, here are the policy filters that for sales, and anybody in the sales group uses that policy.

That means I do not have to write individual policies for everybody in that group. And also I can modify those policies and modify the policies for sales, and it applies to everybody in the group. That is how we are looking at it.

If you need to, you can have a group of one or set specific

policies for a specific identity and it can be completely custom. Or I can say, you are going to follow the sales group policy, and then you are also going to have these other policies in addition.

But for most users, we would expect the administrator to say, "*OK, you are going to fall into this group of users and just follow those policies.*"

Ben: *You also announced a virtual appliance correct?*

John: Yes. The biggest challenge we have going into customers in many cases is they say, "*We love your product, but I do not have any rack space for you.*"

Having a virtual appliance gives us the ability to say, "*OK use your existing infrastructure. Just deploy us virtually and we can provide you the same features.*"

Again, this is in response to major customer feedback. Power, cooling, floor and rack space are some of the most precious commodities in the data center. Operating virtually gives our customers the ability to take advantage of the core reasons they deployed a virtual environment in the first place.

Ben: *This also helps organizations be more agile, is that the case?*

John: Yes. Actually, one of the areas that we are working on for future releases is enhancing both the agility, not only of the clients and the gateways, but also being able to track the resources that are being authenticated, or who the requests are being authenticated for. This is an exciting path for us.

Ben: *Speaking of the future, are you looking at any strategic partnerships?*

John: Yes we are. May has started off with a couple of very important announcements for us. The first announcement came

from Sypris Electronics. Sypris announced they are integrating our TAC technology into their key management system giving public and private sector customers a new level of network protection.

The second announcement came from McAfee. McAfee announced that we have joined their SIA program. McAfee's alliance program is enabling us to plug into an established framework for interoperable and compatible solutions within the security marketplace. We look forward to building tighter relationships with some of the other companies in this program.

Today, I would say our partner activity fall into three categories.

- On the client side, and I would also emphasize mobile here, it is very important for us to be able to get our clients out and accessible to the customer on as many platforms as possible. We are continuing to focus on that. Mobile initiatives based on BYOD or the 'Internet of Things' are going to continue to keep this top of mind for the foreseeable future.
- The second one is although we are just announcing Eclipse in both a physical and virtual appliance, there's other vendors doing integrated security devices that are also expressing interest in the Eclipse functionality. We are getting a fair bit of interest from OEM and channel partners right now.
- Third, when our products are in operation, we see a lot of things. We are able to learn things. By generating events I can tell that, "*Hey, we are getting a DOS attack from some place over there.*" Obviously, this is not saying that we are going to expose identities or things of that sort. But we can use those identities internally as an additional point of reference.

> *Using those additional points of reference you can basically gain operational knowledge of what's going on in the network. The ability to allow people to subscribe and to communicate to those events is another really interesting area that we are having some very interesting conversations with folks on. I think that's the area that you should probably keep an eye on for partnerships in the future.*

Ben: *John, thank you. I think this has been a very enlightening interview.*

John: Thank you Ben and the rest of the DCIG team! We look forward to keeping you updated as our product roadmap gets fulfilled.

In Part I of this executive interview series we examined the three practical use cases for network layer identification.

In Part II of thi
s executive interview series we discussed why most current authentication schemes fail in headless environments and described Eclipse's underlying technology, TAC.