A New Approach to Securing the Smart Grid with Identity Networking

John Hayes, Founder and CTO
The Secure DGM LDRD Project at NREL

Distribution Grid Management, Laboratory Directed R&D

• The Secure DGM LDRD project testbed addressed the cybersecurity and resilience requirements of distribution grid management

• The function of the testbed is to emulate and demonstrate—as realistically as possible, real world environment

• Penetration testing performed by a 3rd party
BlackRidge Participation

- BlackRidge Transport Access Control (TAC) devices provide in-line blocking to protect the Enterprise Information System and the two Advanced Substation Platforms

- BlackRidge TAC inserts authenticated tokens into the first packet of a TCP session to ensure that only legitimate users access these nodes
Pen testers reported:

“all of the external vulnerabilities identified in the initial test were completely mitigated. The network hardening and installation of new hardware and software all contributed to an impenetrable outer layer of defense. The new architecture included an industry-recognized layered defense that would require multiple exploits to penetrate successive layers to reach the critical assets of the SCADA systems.”
Logical Architecture of the Test Bed

Utility Substation(s)
- Auto Sectionalizing and Restoration (ASR)
- Distributed Energy Control System (DECS)
- VAR/Volt Control (VVC)

Substation Management
- HMI
- Energy Field Technician

Utility Operations Center
- Distribution Management System (DMS)
- Enterprise Information System (EIS)
- HMI

Utility WAN (trusted)
- Transactions, Status Data
- Encrypted and Non-Encrypted Network Connection

Utility Enterprise Network (IT)
- Intrusion Detection, Test/Evaluation
- Identity Management, Authentication
- IT Services: Logging, File Storage, NTP, DNS, Mail
- Corporate Personnel (Accounting, Customer Support, IT ...)

Remote Devices
- Electric Vehicle Charging
- Electric Storage

www or Other (untrusted)
- Encrypted Network Connection

3rd Party Service Provider (3P)
- Vendor access
- Cloud Services

BlackRidge TECHNOLOGY
Test Bed Configuration

Diagram showing network components including:
- Enterprise Network
- Substation A
  - N-Dimension
  - Codenomicon
  - NexDefense Sophia
  - IT Services
- Substation B
  - N-Dimension
  - Codenomicon
  - NexDefense Sophia
  - IT Services
- Substation Switch
- Albeado Sniffer
- SecLab Denelis
- Power Grid
- Smart Power Inverter
- Smart EV Charger
- ASP
- Enterprise Switch
- Utility ISP Switch
- Tap
- Firewall
- DMS
- BlackRidge TAC
- EIS
More BlackRidge Use Cases
Securing Legacy Resources: No Application Changes

• Transport Access Control (TAC) uses existing identity infrastructure to protect network and key internal resources
• High throughput, low latency, turn-key physical or virtual operates transparently to networks and users
• Compatible with existing infrastructure, topology independent, and incrementally deployable

1) TAC Learns Identity
2) TAC inserts identity token into network sessions
3) TAC authenticates identity and enforces policy

Blue Group

Green Group

Active Directory

Network

Unprotected

Green Server

Blue Server
Financial Deployment: Partner and 3rd Party Access

- Company A (red) can access all servers
- Partner B (green) can only access green and grey servers
- Partner C (blue) can access green, blue, and grey servers
Live Test Results: Blocking 100% of Unauthorized Traffic

Firewall IPS Protection

<table>
<thead>
<tr>
<th>Time Frame</th>
<th>erhp Educational Site, Protected by a Juniper SRX 3600</th>
<th>erhp2 Educational Site, Protected by a Juniper SRX 3600</th>
</tr>
</thead>
<tbody>
<tr>
<td></td>
<td>Number of Days</td>
<td>Total SSH attempts</td>
</tr>
<tr>
<td>erhp So Far Today</td>
<td>1</td>
<td>12</td>
</tr>
<tr>
<td>erhp This Month</td>
<td>24</td>
<td>605</td>
</tr>
<tr>
<td>erhp Last Month</td>
<td>31</td>
<td>13,828</td>
</tr>
<tr>
<td>erhp This Year</td>
<td>115</td>
<td>15,001</td>
</tr>
<tr>
<td>erhp Since Logging Started</td>
<td>437</td>
<td>46,275</td>
</tr>
<tr>
<td>erhp Normalized Since Logging Started</td>
<td>1,784</td>
<td>30,777,390</td>
</tr>
</tbody>
</table>

Adding BlackRidge Protection

<table>
<thead>
<tr>
<th>Time Frame</th>
<th>Number of Days</th>
<th>Total SSH attempts</th>
<th>Average Per Day</th>
<th>Std. Dev.</th>
</tr>
</thead>
<tbody>
<tr>
<td>ALL Hosts So Far Today</td>
<td>1</td>
<td>68,246</td>
<td>N/A</td>
<td>N/A</td>
</tr>
<tr>
<td>ALL Hosts This Month</td>
<td>24</td>
<td>2,593,017</td>
<td>108,042.38</td>
<td>27,977.56</td>
</tr>
<tr>
<td>ALL Hosts Last Month</td>
<td>31</td>
<td>3,233,914</td>
<td>104,320.45</td>
<td>36,333.54</td>
</tr>
<tr>
<td>ALL Hosts This Year</td>
<td>115</td>
<td>10,404,982</td>
<td>90,473.76</td>
<td>37,445.92</td>
</tr>
<tr>
<td>ALL Hosts Since Logging Started</td>
<td>480</td>
<td>62,832,633</td>
<td>130,903.40</td>
<td>78,322.18</td>
</tr>
<tr>
<td>ALL Hosts Normalized Since Logging Started</td>
<td>1,784</td>
<td>30,777,390</td>
<td>17,027.68</td>
<td>25,442.11</td>
</tr>
</tbody>
</table>

Firewall with IPS allows large number of TCP connection attempts through and information to leak to scans.

BlackRidge does not allow any unauthorized connection attempts or scans (information leakage) to occur.

http://longtail.it.marist.edu/honey/statistics_all.shtml
BlackRidge Provides A New Network Security Element:

Identity
Identity

Who or What is responsible for an action or event

Provides Trust and Accountability

Identity is widely used by applications today…

… but not by the network
Identity Networking Benefits

Session authentication before allowing access and response
- Policy based on requestor’s Identity, requested resource
- Separates Identified and Authenticated traffic from unidentified traffic

Blocks Network Scanning and Reconnaissance
- Protected services are cloaked from unauthorized access
- No response to unidentified or unauthenticated traffic

Separates Security Policy from Network Design
- Supports dynamic addresses and NAT
- Network can change without requiring changes in security policy
What is Transport Access Control?

Transport Access Control (TAC) inserts and authenticates Identity on each and every TCP/IP session.

Every TCP session is individually authenticated using First Packet Authentication.

Works with legacy network, security, identity and application infrastructure.
Transport Access Control

Transport Access Control (TAC) Authenticates every TCP session request before responding and establishing the session.

TAC is **Simple**, Efficient, End-to-End, NAT tolerant, Highly Scalable & Topology Independent.

TAC First Packet Authentication performed here, prior to session establishment.

Traditional session authentication is performed here, after the session has already been established.
Analytics and Feedback

• Provides session attribution information to analytics systems at earliest possible time
  • Enables better, more efficient analytics

• Analytics detect behavioral changes undetectable by Identity based systems

• Analytics provide feedback to Network Identity based security systems
  • Policy feedback via Trust level – efficient, deterministic
  • Independent of network topology
Identity Networking - Summary

- Identity – A new network security element
- Blocks scanning, reconnaissance, DDoS and unauthorized access with non-interactive authentication protocol
- Horizontal applicability - protects SCADA, Enterprise and Cloud Resources
- Works with legacy network, security, identity and application infrastructure
- Network topology and address independent – Supports dynamic addresses and NAT
- Provides attribution information to analytics systems at earliest possible time
Company Facts

- Founded in Q3 2013
- ~$14 million in total funding
- Team strength: 38
  - DNA: MobileIron, Citrix, Juniper Networks, Riverbed, Avaya, Radware
- Company launch: H2-2015
- Patents: 7 Filed
Soha: Enterprise Secure Access; Delivered As A Service

- Unified Solution for Enterprise Access
- Improved Security Posture
- Easy To Deploy
- Superior Access Control & Visibility
Companies Say Building A Secure Access Stack Is Hard!

Lots of Moving Parts
75%
agree they have to touch 5 to 14 network and application components when adding new external user groups

Expect More Breaches
62%
while 62% of respondents didn’t believe their organization was vulnerable to an attack from their parties, 79% expect their competitors have or will suffer a serious data breach in the future

Third Parties are Prime Suspects
63%
of all data breaches are linked to third parties, and will likely get worse as enterprises grow their use of outside resources
Traditional Secure Access Stack

1. Install software clients on endpoints

2. Maintain complex infrastructure in DMZ; open firewall ports; network segmentation …
Traditional Secure Access Stack

1. Install software clients on endpoints

2. Maintain complex infrastructure in DMZ; open firewall ports; network segmentation …

… But Enterprises Networks Continue To Get Breached…
Building Out App Security Infrastructure Is Complex

Operational Challenges

• Deploy/manage complex appliances (physical or virtual) in DMZ
  • High (CapEx + OpEx) undertaking

• Manage network segments spanning DMZ, internal network, etc.
  • Time to deploy new app measured in weeks, not hours/minutes

Security Challenges

• Inbound firewall ports opened up per app
  • Attack surface grows with each new app deployed in network

• Users granted access to the network, not just to needed apps
  • Network access is an easy path for malware proliferation
  • Risk even greater with 3rd parties
Soha Cloud: Enterprise Secure Access As A Service

DC Network

DMZ

Soha Cloud

Ent. Apps

Ent. Apps

Employee

Third Party

SAP

SharePoint

Oracle Applications

Atlassian

infor
Soha Cloud Is Different

- Inline solution that enterprises consume as a service
- Radically new security approach: Shut down inbound firewall ports
- Works in any (private or cloud) network env
- No software on endpoints
### Soha Cloud vs. Traditional L4-7 Solutions

<table>
<thead>
<tr>
<th>Faster Deployment</th>
<th>Delivered as a service - no more appliances to deploy in the DMZ</th>
</tr>
</thead>
<tbody>
<tr>
<td></td>
<td>No need for network segmentation in the data center</td>
</tr>
<tr>
<td></td>
<td>Up and running with strong app security in &lt;30mins</td>
</tr>
<tr>
<td>Lower OpEx</td>
<td>Enable secure access in minutes and save 100s of man hours per app</td>
</tr>
<tr>
<td></td>
<td>One-time deployment works for any number of apps - eliminate projects for additional apps</td>
</tr>
<tr>
<td></td>
<td>Do all this at a fraction of the cost of competitive, appliance-based solutions</td>
</tr>
<tr>
<td>Better Security</td>
<td>Zero open ports on your edge firewall</td>
</tr>
<tr>
<td></td>
<td>Attack surface moved to Soha Cloud</td>
</tr>
<tr>
<td></td>
<td>Application infrastructure &quot;hidden&quot; from bad guys</td>
</tr>
</tbody>
</table>
Soha Cloud Is Most Suitable For …

✓ Companies providing 3rd parties with enterprise application access
✓ Companies deploying apps in new environments, e.g. AWS or Azure
✓ Companies suffering from IT slowdowns due to access related complexity

Learn more at http://soha.io
Thank you
Backup
Connectivity 101

The Traditional Way

Application (Layer 7) Connection

Transport (Layer 4) Connection
Connectivity 101

The Traditional Way

Transport (Layer 4) Connection
Connectivity 101

The Traditional Way

Application (Layer 7) Connection

Transport (Layer 4) Connection

DMZ
A Whole New Way Of Thinking About Connectivity

A New Way

Soha Cloud (Cloud-based Broker)

Multi-step Transport (Layer 4) Connections

Application (Layer 7) Connection

Soha Cloudlet (Co-located Broker)