SusTech 2013

Introduction to the Security Fabric

Security Fabric Alliance Founder
Charles Speicher

August 2nd, 2013
Vision

To create a mass movement that will transform how security is designed in and how the management of intelligent devices operate within a common operating environment.

Mission

To build a community of practicing professionals who are committed to achieving end to end security within the ecosystem of all critical infrastructure by shaping the security fabric reference architecture as an interoperable system of systems.
• McAfee Security Fabric Product
The embedded security system solution is composed of an interlocking arrangement of framework options

• Security Fabric Architecture
The framework of embedded system components that provide the basis for end-to-end security and remote device management

• Security Fabric Alliance
The Security Fabric Alliance is an informal collection of companies, organizations, and individuals that have through discussions designed conceptual reference architecture called the “Security Fabric”.

You need a balanced plan!

The enterprise zones are currently well considered… what we are emphasizing is extending security to the control elements.
Our strategy is to provide certified interoperability to the key devices controlling the grid.

All points must connect to each other in an end-to-end system.

The embedded systems include:

- Secure Communication Flows
- Electrical Flows
- Domain

Our solution would be embedded at each critical point in the energy infrastructure.
What is being asked for is a secure system of systems that blankets the complexity and delivers it autonomically.

This is the embedded side of the operation in addition to the companion enterprise side.  

Intel and McAfee Confidential
These are the seven tenets of security as described in the NIST-IR 7628 Guidelines.

1. **Identity Management**
   - Ensures the device identity is established genuinely

2. **Mutual Authentication**
   - Allows both the Device Node and the Controller to verify the trustworthiness of their identity to each other.

3. **Authorization**
   - Manages permission to proceed with specific operations.

4. **Audit**
   - Records noteworthy events for later analysis

5. **Confidentiality**
   - Encrypts sensitive data for matters of privacy.

6. **Integrity**
   - Ensures that messages have not been altered.

7. **Availability**
   - Prevents denial of service attacks

To establish the secure communications from the Controller to the Device Node using the Security Fabric elements, you need to do all seven... not just some.
The sequence of projects drives the viral expansion.

This is the current roadmap for expansion.

- **Alstom**: embedding the Security Fabric in 20 of the top utilities as a feature upgrade to the existing EMS.
- **Electric Power Group**: embedding the Security Fabric in the heart of their phasor gateways.
- **ERCOT**: embedding the Security Fabric into the heart of their Texas transmission system.
- **Digi**: embedding the Security Fabric as the heart of their new hybrid cloud services system.
- **NASPInet**: embedding the Security Fabric into the heart of America’s entire electric grid.
- **N-Dimension**: embedding the Security Fabric into their managed service.

Intel and McAfee Confidential
How does the Security Fabric work?
Essentially, the Security Fabric is an end-to-end approach to things.

The Security Fabric is a semi-autonomous embedded device management agent and communications protocol set along with a central system and network management subsystem that bring security and other controls to the embedded world.

Let’s build this as if we were building a house.
There are obviously going to need to be several different devices involved. Our agent will be hidden right beside the application.

We want to add our security agent to each of them to do what we will do.
The devices need to be able to talk to each other securely, and trust each other on a limited basis.

This means that the solution will need to be a system as opposed to a piece part.
And all systems need to be administered relative to the configuration and policies that control them.

*These three ingredients are the soul of the Security Fabric.*
The Security Fabric follows the guidelines required by the NIST 7628 for the Department of Energy.

The industry as a whole is applauding this solution.
We always start by separating the management control agent from the payload application.
Managed Device Applications
Secure Communications Secure Storage Policy Management Personal Data Vault

The management agent always uses defense in depth.
Sometimes a device is an intermediate control point - there are additional management mechanisms that are important.

We add these areas of downstream control without interfering with any of the other substation functionality.
For the substation controller, we may have a couple of applications running.

Phasor Data Concentration & Sampling

Substation Communications

Local State Estimation and Decision Correlation
Routing Services is our inter-system + intra-device middleware; The DDS Subagent controls the private paths between processes.
The new Content Aware Firewall needs to be aware of what is flowing through the pipe(s).

The Content Aware Firewall deals with multiple layers and is state sensitive.
The Content Aware Firewall needs to be aware of:
the Layer 6 socket level interface,
as well as the intended sessions that will be flowing over it at Layer 5,
so that it can use UDP connections at Layer 4.

The detailed requirements will be determined during the requirements assessment phase.
What is really unfolding with the rise of the Internet of Things is the need for the Semi-Autonomous Policy Management Agent.

Each of the four compositions of rulesets is administered centrally and released to the remote device securely. The rulesets contain profiles, provisioned data, and Java-based rules. All distribution bundles are signed and are subject to local attestation and transition control.

Autonomous Policy Management Agent

IBM Autonomic Computing Model
The control of the smart grid is all about managing semi-autonomous devices.

The Security Fabric is all about safely deploying this concept.

The customer has to be able to delegate responsibility in small increments to the remote device to avoid the problem of unintended consequences.
The TM Forum security management model is oriented around operating states and formulating the state machine policy management system to transition between them.
Incident management has a process all unto itself.
But security of the critical infrastructure begins long before commissioning a control device.
Supply “Chain of Trust” is crucial for bringing under control pirated ICs.

25-35% of the ICs used in the grid today are pirated and come from unknown sources.
Certificates usually identify companies, and attributes are more easily revocable than certificates.