TCG Trusted Network Connect
IF-MAP Metadata for ICS Security

Document Draft Comments

Prepared by Joseph J. Januszewski, III, CISSP

Page vi:

Although the document is concerned solely with the Metadata for ICS Security, it would be helpful for the uninitiated to TNG to have a one line explanation, or at the very least, the acronyms in the components of the IWG TNC Document Roadmap.

Page 14:

"Any ICS device communications that flow between BHIs over the backhaul network are protected by encryption and integrity checks so that other users of the backhaul network are unable to view or modify the ICS data."

To: "Any ICS device communications that flow between BHIs over the backhaul network **shall be** protected by encryption and integrity checks so that other users of the backhaul network are unable to view or modify the ICS data."

Page 15:

"During that time, configuration of the underlying IP network may well change; indeed, in the case of wireless and/or mobile control system components, much of this coordination information regarding the backhaul network interfaces may vary from one minute to the next due to roaming-triggered address changes."

While the "specification anticipates that different implementations of the BHI functionality", how is this affected by an eventual migration to IP6 from IP4, either of the local facility, or (likely nearer-term) by the back-haul network provider?

Page 19:

"Implementations of IF-MAP Metadata for ICS Security must support the use of cryptographic identities in the form of x.509 certificates for authentication; other forms of authentication MAY be supported as well (e.g., username/password)."

It would be helpful to limit, e.g., *to highly discourage*, the use of a username and password as a sole form of authentication in this environment, as we have seen in various cases where control systems have experienced intrusions due to exploitation of a default vendor or cryptologically weak (3-character) password.

Page 22:

In Section 3.1.2, it would be worth noting the advantage of using a commercial CA-issued digital X.509 certificate, as opposed to a system self-signed certificate, which could potentially be forged with little notice.

Also, won't the BHIs have at most two identifiers, since use of the FCert and the CCert are mutually exclusive, per Section 3.1.2.3, *BHI Customer Certificate (CCert) Identifier*?

Page 23:

"The validity of the FCert SHOULD be at least two years from the date of manufacturer."

To: "The validity of the FCert SHOULD be at least two years from the date of **manufacture**."

"The manufacturer MAY provide a method whereby FCerts may be refreshed as part of a certificate lifecycle management process."

To: "The manufacturer SHALL provide a method whereby FCerts may be refreshed as part of a certificate lifecycle management process."

Having certificates which will expire with no mechanism for replacement in an environment where it has been noted that a technology refresh may be on the order of decades is reprehensible.

This certificate mechanism is cludgy at best. Drawing from the networking environment, a network interface is licensed by the manufacture's hardware code (MAC), currently assigned and maintained by the IEEE. However, the assignment of a certificate that will: 1.) need to be refreshed, and 2.) not be used in the event of a customer-defined PKI, is superfluous. In a security environment, the unfortunate reality is that if a process is difficult to implement or maintain, it will simply not be used.

Page 25:

Section 3.2.2, *Operational Communications Facilitation* should contain recommended minimal mechanisms of message privacy and integrity. Obviously, these will need to be updated as advances in brute-force methods, processing capabilities, etc., obviate necessary increases in key-lengths, advanced algorithms, and the like. However, a standard minimum starting point is advantageous.

Section 3.2.4, *MAP Server Auto-Discovery* proposes "DNS-based Service discovery using SRV resource records". The inherent danger with that approach is the potential for introduction of an attack vector by pointing to a compromised system or network. That SHOULD be prevented by proper access-control, however, if a back-haul provider (or providers) have not exhibited an appropriate level of due diligence, and the back-haul network has been compromised, devices can potentially be pointed to a compromised system, which has been used to infiltrate the ICS network or remote facility.

Page 25:

Section 3.5, *IF-MAP Metadata for ICS Security Types* discusses the "discovered-by link" as "an ip-address identifier representing the IP address of another system that the BHI has detected on the network". Allowing discovery of other neighboring devices makes for easier connectivity in home networks and office LANs, which are usually smaller in scope, and are not geographically separated. Permitting discovery of other network-connected devices and links by ICS is a security concern, which potentially opens new vectors to attackers.

Page 31:

The `administrative-domain` attribute of the `ip-address` and `mac-address` identifiers MUST match the name of the associated overlay network, in order to prevent confusion when the same IP addresses and MAC addresses are used in different overlay networks (see section 3.3.1).

A MAC address CANNOT be used on two separate addresses, unless the MAC address has been spoofed, or has been modified at the the specific interface, using interface-vendor-specific software.

Page 33:

In Section 3.5.6 *dn-hit,* an example is given where new private keys are distributed. Does this not mean public keys? In PKI, the private keys are generated as part of a key pair and are maintained in the keystore, not distributed.

Page 34:

In Section 3.5.8 *ip-mac*, this mapping creates a redundancy of the function already defined and performed by the Address Resolution Protocol (ARP).

Page 38:

In Section 4.1.1 *MAP Server Selection*, the act of selecting a MAP Server using unspecified discovery methods in MAP Server discovery opens the BHI to the potential to select a spoofed MAP Server.

Page 43:

In Section 4.1.9.2 *Overlay Policy Prioritization*, IP packets are indicated as "a specific type of layer-2 packet". IP functions at ISO Layer 3. MAC addresses reside at ISO Layer 2. Also, the mixed-use of terminology "layer-2", "L2", "layer 2", "L3" and "layer 3 (IP)" should be made uniform.

Page 49:

Section 5, *Security Considerations* makes a passing reference to countermeasures. Based upon multiple vulnerability reports from Mitre/NIST, DHS and private control system security groups, the depth of defense in these control systems is typically minimal, at best. Therefore countermeasures, as referenced in Section 5, do not exist in many (dare we say, most) examples.

Section 5.1.3, *MAP Clients* should also account for a denial of service attack by adding the following:

· *Avoid creating too many connections to the MAP Server.*

Page 50:

Section 5.1.7, *ICS Devices* assumes that an ICS can be trusted to not send device traffic in its overlay network, nor to impersonate another ICS device. To assume that an ICS device (or any intelligent agent or server, for that matter) *cannot* be compromised and be used to impersonate another device, or become a victim of a man-in-the-middle attack, or to not send data where it should not, is a potentially dangerous assumption to make. What are we to premise this implicit trust upon? Are the operating systems of the ICS devices hardened? Is it impossible for their configuration to be modified, such as using a write-once PROM? In our experience, nearly any device that can be reconfigured can be used for malfeasance.

Page 51:

In Section 5.1.10 *MAP Server*, as a design goal, the resistance to attack of a server is a worthy goal. However, the reality of the situation is such that a server is typically dependent on its components, such as operating system, or network interface and communications protocol subsystem, etc. Once resources are exhausted, e.g., in a denial of service attack, the system must fail gracefully, i.e., to restart in an attempt to clear the state of over-utilization without allowing access, or an elevation in privilege.

Also, a risk inherent to not requiring a MAP Server to validate data against schema can create a decrease, or a total lack in a multiple mode failure scenario, of situational awareness.

Page 52:

The scenario illustrated in Section 5.2.2 *MAP Clients* in that the assumption made that does not take into account an unauthorized MAP client with forged credentials, i.e., outside of the MITM scenario. In that event, ANY action could then be taken, as the unauthorized MAP client is viewed by the MAP server as authorized. Section 5.2.2 points to this scenario in light of a limiting factor, making an assumption which may not be valid. The Overlay Manager in Section 5.4.2 is also potentially exposed to the scenario.

Pages 55 and 56:

Section 5.3.2 *Securing MAP Clients* posits that the danger to MAP Clients "can be reduced tremendously by restricting the privileges of MAP Clients with MAP Server policies." As the "eyes and ears" of the overall control environment, denial-of-service with regard to any MAP Clients results in a reduction of situational awareness.

Sections 5.3.2 through 5.3.5 are too cursory in their recommendations and threat assessments. Furthermore, the tone of Section 5.3.6 gives the appearance of the recommendation of a utility operating their own private CA.

Page 57:

Section 6 *Privacy Considerations* indicates that privacy considerations may not a substantial factor in an Industrial Control Systems environment. However, the layout of a network and relevant operating data may very well be an issue of privacy, if the aforementioned Industrial Control Systems are implemented in a "controlled" environment, where manufacturing, utility, military or government privacy controls are statutorily-deemed.

Additional:

What accommodations are made for "last gasp" traffic, signaling the imminent failure of an ICS device?

Section 4.3 or 4.4 should contain verbiage relating to the vitality of maintaining the security of the Administrator role, simply due to its sheer level of authority.