Security Implications to Smart Addressable Objects

Nancy Cam-Winget and Monique J. Morrow, Cisco Systems

Introduction

IP Smart Object networks also referred to as LLN (Low power and Lossy Networks) have unique characteristics and requirements. Indeed, by contrast with “typical” IP networks where powerful routers are interconnected by highly stable links, LLNs are usually interconnected by low power low bandwidth links (offering between a few Kbits/s and a few hundreds of Kbits/s). In addition to providing limited bandwidth, such links (especially wireless) are usually extremely unstable with high BER (Bit Error Rate).

It is not unusual to see the PDR (Packet Delivery Rate) oscillating between 60% and 90% with large bursts of unpredictable errors and even loss of connectivity for some period of time. Note that such behavior can be observed both for RF links (such as IEEE 802.15.4) and PLC links that exhibit similar behaviors. Another characteristic of IP smart objects is that node failures (for example due to energy depletion) are significantly more frequent than in traditional IP networks where nodes are main-powered, highly redundant (multi processors, supporting non stop forwarding)

Another key characteristic is that LLNs do need to scale. Some LLNs can be made of dozens and even hundreds of thousands of nodes. This explains why specifying protocols for very large scale constrained and unstable environments bring its own sets of challenges. For the sake of illustration (other topics are discussed later), one of the golden rules was to under-react to failure by contrast with routing protocols such as OSPF or ISIS where the network needs to re-converge within a few dozens of milliseconds. This required a real paradigm shift since over-reaction would lead to network collapse very rapidly. Furthermore, control plane overhead had to be minimized, while supporting dynamic link/node metrics, MTR, and so forth.

With these physical constraints and requirements, this paper provides a rough first draft at describing the challenges in securing both LLNs and IP smart objects.

Security Implications

While the security considerations addressed in “typical” IP networks apply to LLNs, some special considerations must also be accounted for :

- Identification of the devices must be strong and rely on secure provisioning and management mechanisms. As an “IP Smart Object” there is the requirement to allow for these devices to hold a globally secure unique identifier that should be imprinted with zero human interaction; more importantly, these identities must also be managed and updated with automated techniques unlike “typical deployments” relying on human interaction for credential updates.
- Authorization and the policies defined to enforce such authorizations must now also differentiate the “object” type. Contextually aware networks must now also account and extend their authorization, policy decision and policy enforcement techniques to account for these “Smart Objects”.
- Resilience to external and internal attacks must now strongly consider tamper resistance as there must be strong assurances that these “smart objects” have not been stolen or tampered.
- Privacy and integrity of the data plane in an LLN must account for “lightweight” devices that may be restricted to low-power and limited cpu cycles
- Secure mobility becomes an interesting dimension to IP smart objects. As these are typically unmanned devices, appropriate policies to ensure stationary unmanned devices are prevented “being mobile” and conversely, addressing secure handoffs both inter- and intra-LLNs must be considered.

Within an LLN, it becomes imperative that there be a secure device management ecosystem as most of the Smart Objects are deployed in scenarios where human intervention and/or configuration is impossible.

Proposed Techniques

Many techniques used in “typical” IP networks may be leveraged today to address the security of LLNs and the Smart Objects. To begin, the framework used for mobile device management has strong applicability to Smart Objects as well. The extensions and considerations required to address Smart Objects include:

- Use of strong credentials employing lightweight cryptographic constructs. While the use of x.509 certificates remains relevant, the cryptographic constructs (e.g. RSA, DHE) must be updated with equally strong but computationally lighter (and lower key size footprint): ECC becomes such a candidate.

- Device management systems must coordinate with the credential/identity management systems to monitor and account for the need to update such credentials beyond the initial provisioning.
- Device management systems must also ensure that appropriate configurations are installed or updated both during provisioning and dynamically as policies are updated or as threats are escalated and mitigation through re-configuration is required.
- Configurations of Smart Objects should account for the “role” in which the Smart Objects are allowed access into the LLN.
- Beyond conventional network threats, Smart Objects must have and be configured to allow itself to be resilient against tampering. Use of technologies such as TPM can be viable to some Smart Objects but may still be cost prohibitive to the very low-end, inexpensive ones.
- Access Control Systems in an LLN must account for such “role” in the policy definition, decision and enforcement mechanisms.
- Security products must be adapted to be “Smart Object aware” and react to mis-behaviors, threats and attacks based on the “Smart Object” profiles.

Beyond these extensions, the use of lightweight “unmanned” devices raise interesting challenges in the research space to address:

- Finding lighter weight public key cryptographic techniques for strong authentication and key management that provide equal or better strength to that offered by ECC. While we can assert that ECC may be “good enough”, for very, very small devices such as temperature sensors (or any single function atomic sensor), both the computational and power demands to drive PKI algorithms may be prohibitive.
- Finding lighter weight, cost effective deployable techniques for addressing multi-point communications.
- Monitoring, sensing and addressing “Smart Object” behaviors to address their threat risks.
- Finding cost effective anti-tampering and anti-theft techniques for the Smart Objects.
- With “unmanned” devices connecting to an LLN and specifically needed to connect to other “unmanned” IP smart objects, secure discovery mechanisms will be required.

To ensure that the appropriate framework, protocols, tools and mechanisms are adopted, it is imperative to define the LLN and IP smart object deployment scenarios, requirements and map them to a risk and threat model assessment.

Summary

While there are new areas of research and work to be addressed in securing LLNs and the Smart Objects; there is a wealth of technology used in securing “traditional” IP networks today that can be leveraged and extended to LLNs and Smart Objects. Once the LLN deployment criteria and threat models are established and well understood, a framework for securing LLN and IP smart objects can be defined from which better determinations of how best to leverage current security technologies and define the extensions and new work remaining.

Acknowledgments

The authors would like to acknowledge David Lake, Cisco for his valuable input.

References

http://tools.ietf.org/html/draft-iab-smart-object-workshop-09

http://www.amazon.com/Interconnecting-Smart-Objects-IP-Internet/dp/0123751659