Security Challenges For the Internet Of Things

Tim Polk <tim.polk@nist.gov> & Sean Turner <turners@ieca.com>
IETF Security Area Directors
February 14, 2011

Abstract: The Internet of Things (IoT) will present new security challenges in cryptographic security, credentialing, and identity management. Currently available cryptographic techniques require further analysis to determine applicability in the Internet of Things. Credentialing presents significant challenges in the current Internet and these challenges will be exacerbated by the sheer number of devices and the expected limitations in user interfaces. Identity management is currently oriented towards either user or device identity; in the Internet of Things making an implicit or explicit mapping between IoT device identities and Internet user identities may be required. Network security devices, such as firewalls and network guards, will be essential to meet security requirements. Security will be in tension with usability, privacy, and devices' constrained resources.

Current Internet security protocols rely on a well-known and widely trusted suite of cryptographic algorithms: the Advanced Encryption Standard (AES) block cipher for confidentiality; the Rivest-Shamir-Adelman (RSA) asymmetric algorithm for digital signatures and key transport; the Diffie-Hellman (DH) asymmetric key agreement algorithm; and the SHA-1 and SHA-256 secure hash algorithms. This suite of algorithms is supplemented by a set of emerging asymmetric algorithms, known as Elliptic Curve Cryptography (ECC). Adoption of the ECC algorithms has been slowed by significant IPR concerns, but publication of RFC 6090 and recent IPR disclosures may encourage adoption.

These cryptographic suites were designed with the expectation that significant resources (e.g., processor speed and memory) would be available. The applicability of these cryptographic techniques to the Internet of Things is unclear, and requires further analysis to ensure that algorithms can be successfully implemented given the constrained memory and processor speed expected in the IoT. For initial IoT protocol development, developers are encouraged to look to AES-GCM, which is an combined mode supporting authentication and encryption, and the ECC asymmetric algorithms. As the resources available on common IoT devices becomes clearer, researchers may determine that these algorithm suites are not optimal, and research into more suitable cipher suites will advance. This will be a source of tension with implementers: any techniques that are easy to implement in the IoT could be easy to break by users with more traditional computing resources. Regardless of the device footprint, we would suggest requiring at least 112 bit "security level" for all cryptographic techniques, which is the current baseline for less constrained devices. Assuming that an attacker will have the same limitations in resources is clearly an incorrect assumption!

To ensure that early adopters have security features available when needed, it is essential that IoT protocol suites specify a mandatory to implement but optional to use security solution. This will ensure security is available in all implementations, but configurable to use when not necessary (e.g., in closed environment). We expect initial deployments to proceed with security configured "off", but exploits that leverage such vulnerabilities will surely emerge in short order. The experience with home and small business WEP wireless deployments is informative: weak cryptography was rapidly discovered and exploited. Deploying the IoT without security will surely have the same result.

The most difficult aspect of cryptographic security is always key management. While many Internet protocols have been deployed with manual key management (i.e., "pre-shared keys") manual configuration of the number of devices in the IoT is unlikely to scale. In addition to the large number of devices, limited user interfaces will make it difficult to deploy meaningful security in this manner. Even if the devices can be manually keyed on initial deployment, automated re-key after deployment is essential. Careful study of BCP 107/RFC 4107, "Guidelines for Cryptographic Key Management", and enforcement of those requirements is strongly recommended.

Credentialing users and devices presents significant challenges in the current Internet, and these challenges will be exacerbated by the sheer number of devices and the expected limitations in user interfaces. Security techniques that combine automatic and manual techniques for initial deployment will likely be need in the IoT. In particular, so-called "pairing protocols" such as those relied upon for blue tooth security may need to be incorporated as a deployment strategy. However, we envision that static keys will only support initial deployment, rather than be used as the traffic keys. Leap-of-Faith technologies, such as those employed in the "Better Than Nothing Security" (BTNS) IPsec profile, may also fill a key role in these protocols.

In the IoT, we expect that most devices will not be associated with a single person. A house only needs one toaster even if it serves a family of four! There may be a need to map device identities to groups of people (e.g., the adults in that family of four) in ways that are not commonly performed today.

Usability concerns will also provide a significant challenge. Regardless of whether the device is a toaster, washer, or dryer, it is essential that the device experience little or no increase in difficulty for deployment or use. This will be a significant challenge even for the networking aspects; providing usable security is going to be a research topic. Jonny still can't encrypt, yet we will soon be demanding that from our toaster!

Privacy issues are also expected to be significant. Our experiences with Smart Grid demonstrate the sensitivities of exposing electricity usage associated with a home or business. The IoT has the potential to expose the precise application of that

energy demand, further violating the privacy expectations of the population. In combination with these privacy issues, compromises in the IoT protocol suites are likely to require establishing a security perimeter that monitors and restricts IoT devices. Older technologies from the military and intelligence communities, such as "network guards", once used to prevent information leakage may be needed once again.

In summary, the security challenges for the IoT are daunting. It is essential that early IoT protocols include mandatory to implement security features, even if those features stretch the capabilities of such devices. Automated key management is always a challenge, but it is even more critical that IoT protocols do not rely on pre-shared keys. Credentialing/registration of devices will also be a challenge, but pairing protocols are well-understood and provide one possible solution set. Privacy concerns may provide incentives for adoption for technologies designed to prevent information leakage in military/intelligence environments.