On Cryptographic Approaches to Internet-Of-Things Security

S. Zhou (ZTE Corporation) Z. Xie (ZTE Corporation)
zhou.sujing@zte.com.cn xie.zhenhua@zte.com.cn

Internet Of Things is an evolution and superset of current internet of networks of computers. We are already on the way of connecting every Thing to internet, mobile internet focusing on 3G phones is a good pioneer example. Our focuses are turning from devices with high capability of computing and storage to those with constrained resources (CPU, memory, energy), from reliable transportations to lossy networks, from comfortable indoor install environments to all kinds of outdoor environments, from rather static user behaviors to variant user behaviors[1].

Given complicated IP protocols (e.g. IPv6 with many extensions and numerous options[3] , IPSEC with so many RFCs[4]) and all kinds of specialized sensor networks, e.g. Zigbee, the work is to adapt and converge them together. So many mismatches, e.g. capability mismatch between different devices, mismatch between communications and processing bandwidth[2], need to patch. Another important mismatch is from difference between the malicious environment of IOT and the current experience derived from internet.

Most of the security issues in IOT [5,6,7] are familiar, because they also exist in current internet. For example, eavesdropping, false routing, message tampering, unauthorized usage, DOS attack. we are not unprepared in this field.

A difference is that the specific attacks leading to the issues may be quite different. For example, DOS attacks can be achieved by sending signals to keep nodes from slumber[7].
Some issues may be major concerns in IOT but not in current internet. For example, because devices are easy to access physically or wirelessly in IOT, then physical destruction, secret extraction. tampering of nodes are more serious[7].

Therefore, resolutions to deal with the issues are required to have some extra characteristics, e.g., resilience in case nodes are compromised[7], and lightweight cryptographic technologies are preferred[14].

It is easy to misunderstand “lightweight” as less secure. Although devices to be protected are constrained in resources, but attackers are not. So we need security techniques and mechanisms that are lightweight in resource consuming, but NOT in security weight.

As reported in [14], in lightweight cryptography, we have secure symmetric cryptography: AES,CLEFIA and PRESENT, stream ciphers: Grain v1, MICKEY v2, and Trivium. But we don’t have good candidate in Hash function[14,15], maybe. As for asymmetric cryptography, ECC[13], XTR[17], IBC[11,12] are available candidates.

We also need security architectures, e.g., key management scheme including key provisioning, key updating, key revocation etc. In category of asymmetric keys, PKI is a mature scheme, and WPKI (especially designed for wireless environment) has been proposed and widely applied in WAP applications[8,9]. Another way to distribute and validate asymmetric keys is identity based schemes[11,12] [Note: IBC can be used with or without certificates] and certificateless scheme[17].

In category of symmetric keys, efficient key transportation, key agreement are needed. For example, ASKE (alpha-secure key establishment) deployed in Zigbee use polynomials to calculate shared master keys[18].

So, there are still some gaps between available techniques and requirements. For example, currently cryptographers are working on schemes .e.g. NTRU[19] , against quantum computation attacks. The proposals are not practical enough even for ordinary computers, what can be used to prepare IOT for post-quantum days?

What is important is that deficiency in the cryptographic techniques should be complemented by corresponding non-cryptographic management measure to keep the whole security level, although there are maybe some trade-offs between adopted security technique and efficiency, especially in the scenarios where a security incident may lead to loss of life or disaster.

References:

[1]Slides and Positions papers on Interconnecting Smart Objects with the Internet Workshop 2011 http://www.iab.org/activities/workshops/smartobjects/agenda/

[2]Interoperability Challenges in the Internet of Things, Jari Arkko, 2011

[3]RFC 2460 Internet Protocol, Version 6 (IPv6) Specification

[4]RFC 6071 IP Security (IPsec) and Internet Key Exchange (IKE) Document Roadmap

[5]Security Considerations in the IP-based Internet of Things http://tools.ietf.org/html/draft-garcia-core-security-03

[6]Security Bootstrapping of Resource-Constrained Devices http://tools.ietf.org/html/draft-sarikaya-core-sbootstrapping-03

[7]IPv6 over Low Power WPAN Security Analysis http://tools.ietf.org/html/draft-daniel-6lowpan-security-analysis-05

[8]Wireless PKI http://www.mpf.org.in/pdf/Wireless%20PKI.ppt

[9]WAP-217-WPKI-20010424-a [S]. WAP Application Protocol: WPKI.

[10]Wap-261-WTLS-20010406-a [S]. WAP Application Protocol: WTLS.

[11]RFC 6508 Sakai-Kasahara Key Encryption (SAKKE)

[12]RFC 5091 Identity-Based Cryptography Standard (IBCS) #1:Supersingular Curve Implementations of the BF and BB1 Cryptosystems

[13]RFC 6090 Fundamental Elliptic Curve Cryptography Algorithms

[14]Lightweight Cryptography for the Internet of Things, Masanobu Katagi and Shiho Moriai,Sony Corporation

[15] cryptographic hash Algorithm Competition. http://csrc.nist.gov/groups/ST/hash/sha-3/Round3/index.html

[16] The XTR public key system. Lenstra and Verheul. Crypto 2000

[17] Certificateless Public Key Cryptography Sattam S. Al-Riyami and Kenneth G. Patersony

[18] ZigBee Security, Cragie.

[19] http://ntru.sourceforge.net/