SEC-2016-0175

Discussions on New Work Item of Distributed Authentication

Group Name: SEC (WG4)
Source: Guilin Wang (Huawei)
Meeting Date: SEC#25, 2016-10-17
Agenda Item: WI-xxxx-Distributed Authentication

Objectives

- Explain the concept of “Distributed Authentication”
- Refine the justification of this new work item
- Discuss the feasibility of IBS for IoT devices
- Refine the scope of this new work item, together with an example protocol which we could design

The Concept of "Distributed Authentication"

- Distributed Authentication **does not mean**:
  - The authentication operation is done collectively by a number of entities, which locate at different sites logically and/or physically.
- It means that
  - One authentication credential can be used to authenticate one entity itself to many other entities
  - Therefore, it supports many to many communication better, without the direct involvement of centralized management.
- In this sense, it may be better to call it as "**Decentralized Authentication**"

Refined Justification I

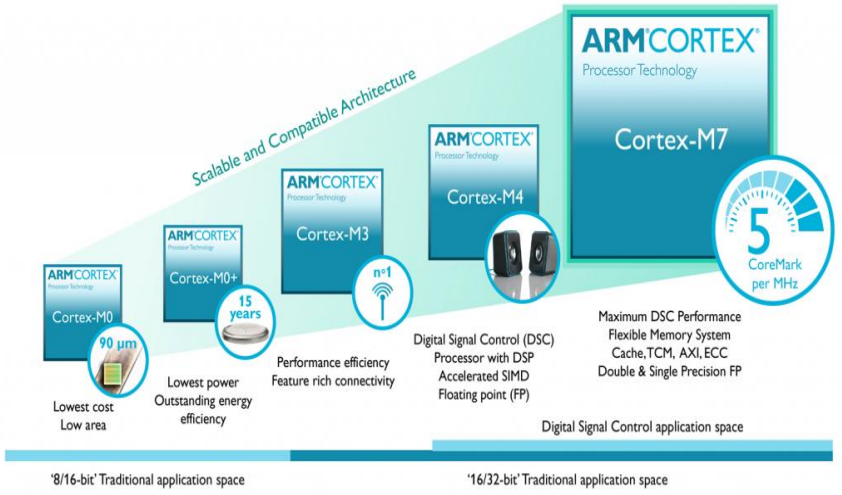
- To provide flexibility and reduce employment costs, various IoT application scenarios may require distributed authentication in which two entities (e.g. devices, applications and network components) can **authenticate each other directly and further establish secure channels** in a **lightweight** way without online centralized management.
- Namely, one authentication credential can be used to authenticate one enity itself to many other entities.
- The authentication mechanisms in TS003 require centralized node involved, such as M2M Gateway or M2M server, which cannot offer scalable distributed authentication.
- Moreover, as distributed authorization has been considered by SEC group in oneM2M, distributed authentication should be taken into account too.

Refined Justification II

- Finally, the distributed architecture is also considered in ARC group, in order to support this architecture, the corresponding security mechanism, such as distributed authentication, should be designed. Work Item WI-0047 is studying DDS to able multiple M2M Applications to interact with multiple M2M Devices/Gateways, i.e., many to many communication (OSR-009), in the framework of oneM2M. And the results from this Work Item can be used to support the security in the usasge of DDS in oneM2M.

Feasibility of IBS for IoT: IoT Chips

ARM Cortex-M series chips are for IoT devices.



	Board	CPU	RAM
Cortex-M0(+)	Freescale	48MHz	32KB
Contex-M3	NXP LPC1768	96MHz	32KB
Contex-M4	STM32	84MHz	96KB
SIM		5-20MHz CPU	0.1 – 6KB

	Board	CPU	RAM
NBIoT Zigbee	?	32 MHz	8 KB

1) **NBIoT Zigbee chips are weaker than Cortex M0(+).**
2) **So, IBS may be challenging for NBIoT now.**
3) **But, hardware progress is fast.**

Feasibility of IBS for IoT: Preliminary Testing Results of IBS Algorithms

- Algorithm (**IEEE-ECC-IBS, RFC 6507**), namely **signature generation and verification**, based on **OpenSSL Crypto Libratory**, running at single core with following models:
  - Model 1: Desktop with Intel(R) Xeon(R) CPU E5-2690 v2 @ 3.00GHz；
  - Model 2: computer rack with Intel(R) Xeon(R) CPU E3-1230 v3 @ 3.30GHz；
  - Model 3: Google Nexus 6 phone with Krait 450 @ 2.7 GHz.
- Network transmitting time not included.
- All algorithms are repeated 3000 times for each setting and the average running time is recorded.

Curve	Security Strength	Corresponding RSA bits	Average running time		
			Model 1	Model 2	Model 3
P-256	128bit	3072	2.16ms	1.57ms	9.84ms
P-521	256bit	15360	9.95ms	7.91ms	61.5ms

Expected Performance for P-256 @ ARM M3 (96M) Chip :

277 ms (signature generation+verification)

Feasibility of IBS for IoT: IBS Performance from Academic Research

Time for IBS Signature Generation (128 bit security) in ms:

	Contex-M0+ (48MHz)	Contex-M3 (96MHZ)	iPhone 4 (Cortex-A9,1.2GHz)	Signature Length (bit)
IETF-ECC-IBS@curve 25519	80	40	3.2	768
ISO-ECC-IBS@curve 25519	Offline:30 Online:15	Offline:15 Online:8	Offline:1.2 Online:0.6	768
ISO-Pairing-IBS@ BN pairing	669	335	26.8	508

Time for IBS Signature Verification (128 bit security) in ms:

	Contex-M0+ (48MHz)	Contex-M3 (96MHZ)	iPhone 4 (Cortex-A9,1.2GHz)	Signature Length (bit)
IETF-ECC-IBS@curve 25519	225	113	9.04	768
ISO-ECC-IBS@curve 25519	224	112	8.96	768
ISO-Pairing-IBS@ BN pairing	2324	1162	92.96	508

Source 1: High-speed Curve25519 on 8-bit, 16-bit, and 32-bit microcontrollers, Designs, Codes and Cryptography 2015 (Curve 25519).

Source 2: Efficient Pairings and ECC for Embedded Systems CHES 2014 (BN pairing).

Feasibility of IBS for IoT: Remarks

IBS Schemes:

- **IETF-ECC-IBS:** RFC 6507, 2012, used in 3GPP D2D (ProSe, 2014)
- **ISO-ECC-IBS**: SO/IEC 29192-4, 2013
- **ISO-Pairing-IBS:** ISO/IEC 14888-3, 2006

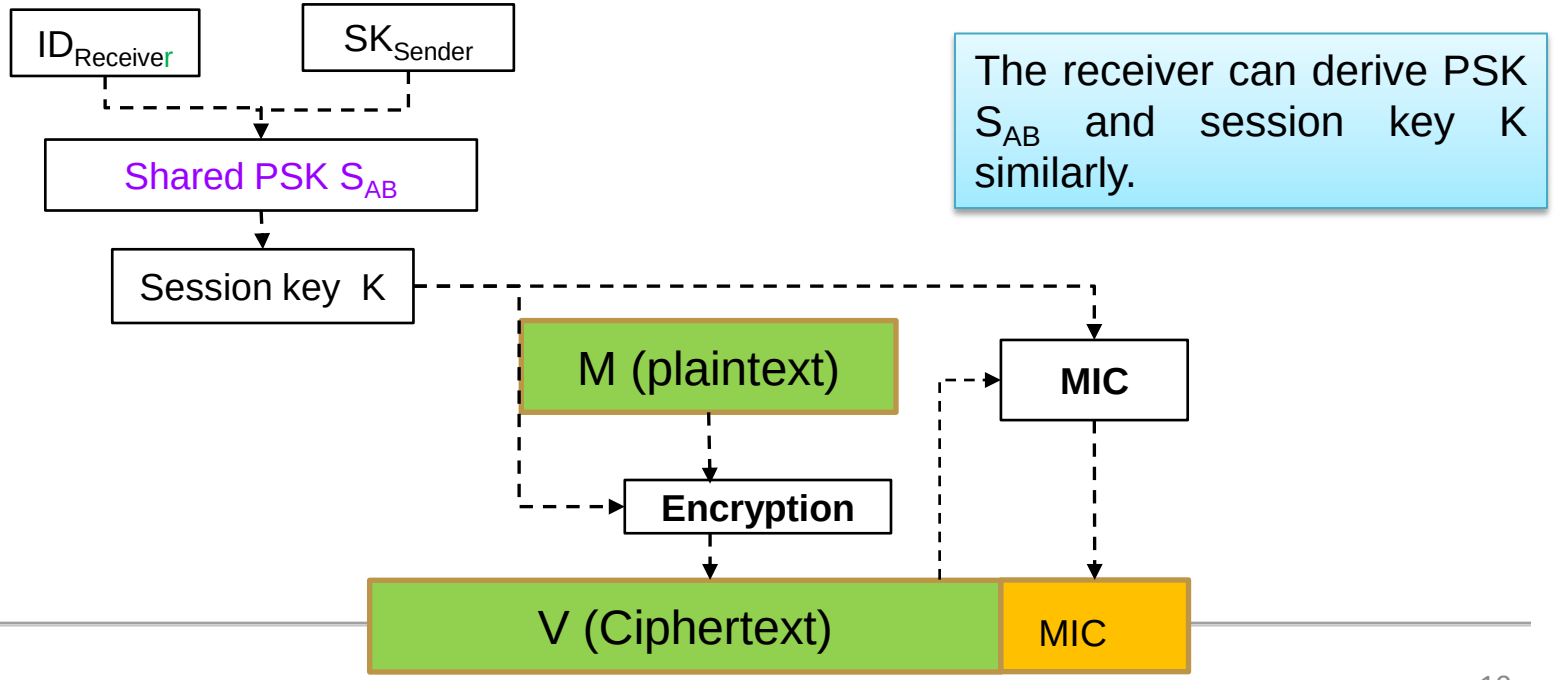
Remarks:

1) 126 bit security can be viewed very strong security for most of IoT devices (Recall that 1024 RSA only provides 80 bit security).
2) Performance relies on many factors: chip platform, ECC curves, crypto library, coding etc.
3) For the same security level, the running time for RSA signatures is about double.
4) **IETF-ECC-IBS Performance For Curve 25519 @ ARM M3 (96M) Chip : 153 ms (sign. gen. +ver.), which is bout 50% faster than the expected result. Reasons: different curves, coding quality.**
5) **So, IBS for IoT devices is feasible!**

Refined Scope and An Example Protocol

An Example Protocol using IBS: To derive PSK flexibly for supporting DDS

- Based on some IBS, a PSK can be generated from receiver's ID, sender's ID, and sender's private key.
- This can efficiently solve the problem of PSK distriution in many–to-many communication scenario.
- Using this PSK, encryption and integrity can be offered using traditional primitives



Refined Scope and An Example

- To investigate user cases and related security requirements.
- For considering the feasibility, to identify suitable primitives and mechanisms, which are expected to be a few asymmetric key based technologies but lightweight enough for IoT use (identity based cryptography, certificateless signatures, etc).
- To evaluate the value of distributed authentication.
- To design new distributed authentication mechanisms and protocols that are lightweight for oneM2M architecture. In particular, these protocols shall be considered to be implemented using TLS/DTLS.

Conclusions

- Should we change “**Distributed Authentication**” to “**Decentralized Authentication**”?
- After carefully selecting asymmetric algorithms (IBS etc), new lightweight protocols can be designed for IoT application under the oneM2M framework.
- So, the proposed work item is beneficial to oneM2M.