Wireless Security in an Internet of Things Era

Joe Chen
joe.chen@rice.edu

Zilong Liao
zl15@rice.edu

Heng-Yi Lin
henry.hy.lin@rice.edu

1. INTRODUCTION

Network security faces several new challenges in an Internet of Things (IoT) scenario. First, IoT devices are typically wireless sensors or low-powered appliances, meaning they are resource-constrained. This makes the traditional cryptographic defense that support confidentiality, integrity, and authencity difficult to implement [30]. Second, IoT devices are often devices such as health sensors and home network appliances. These devices by nature carry personal and dynamic information about the user that can be leaked if proper security measures are not implemented [19]. Third, Radio Frequency Identification (RFID) technology uses passive tags to help a user identify an object or location. However, this technology is vulnerable to both non-malicious collisions and adversarial denial-of-service attacks [21].

For the remainder of this paper, we propose three potential semester projects and discuss existing works in each of these fields. In Section 2, we aim to cross-compare multiple existing lightweight cryptographic algorithms on the same platform. In Section 3, we propose using gesture recognition on multiple devices for pairing authentication. Finally, in Section 4, we implement and evaluate a reputation system for IoT networks under multiple environments.

2. LIGHTWEIGHT CRYPTOGRAPHY

While the conventional cryptography may have provided sufficient protection for the sensitive data and built robust foundation for various aspects of information security, modern cryptosystems based on them are not applicable to most cases in the IoT Era. Most IoT devices are resource-constrained that they typically have limited computing power, memory, and battery capacity. They may also be low-cost and small-sized. All these possible constraints make conventional strong cryptographic schemes, which require relatively high performance computing platform, practically or commercially infeasible [8].

To overcome aforementioned limitations, research work and applications focus on lightweight cryptography, specified in ISO/IEC 29192-1 [14], which is suitable for environments where may encounter any of the following limitations:

- chip area,
- energy consumption,
- program code size and RAM size,
- communication bandwidth,
- and execution time.

Lightweight cryptography is always coped with tradeoff among security, cost, and performance in varied implementations ("Lightweight Ciphers," 2016)[1]. According to a survey by Eisenbarth et. al. [11], these implementation can be classified in two ways: software-oriented against hardware-oriented or symmetric against asymmetric. First, software-oriented implementations are used in areas where memory requirements and power consumption are main concerns, while hardware-oriented ones are implemented in scenarios where the chip size and number of clock cycles are primary consideration. Second, asymmetric cryptography are secure with more functionality but more demanding in memory, computing power, and power consumption compared with symmetric cryptography [27].

Among various proposed lightweight cryptographic schemes, we enumerate existing standardized schemes under ISO/IEC 29192 standardization. Our objective for this project is to evaluate those schemes based on their performance, security level, and practical feasibility on the same platform.

In the following subsections, we briefly depict some differences between lightweight and conventional primitives, and introduce primitives which we intend to analyze.

2.1 Lightweight Symmetric Cryptography

2.1.1 Block Ciphers

Unlike conventional block ciphers such as AES and Twofish, lightweight ciphers commonly have smaller key size and block size. As Bogdanov et. al. [5] has specified, they also tend to extremely simplify key schedule but have more required number of rounds due to the deeper dependence on elementary operations.

Among proposed lightweight block cryptography, PRESENT [1], an ultra-lightweight block cipher based

[1]In CryptoWiki. Accessed: 2016-02-18, from http://cryptowiki.net/index.php?title=Lightweight_ciphers

ACM ISBN XXXX.
DOI: XXXX

on S-P networks, and CLEFIA [26], a generalized Feistel-structured block cipher with Diffusion Switching Mechanism, has been adopted as the new international standards for lightweight cryptographic implementations under ISO/IEC 29192-2 [15].

2.1.2 Stream Ciphers

Because of the nature of stream ciphers, stream ciphers are of great use in processing unknown-length or varied-length data. Furthermore, they are generally more efficient than block ciphers that software-oriented ones take fewer CPU cycles and hardware-oriented ones require smaller chip area. These characteristics make them suitable for IoT settings.

Among current lightweight stream ciphers, ISO/IEC 29192-3 [16] has specified the following two stream ciphers as international standards for lightweight stream ciphers: Trivium, a hardware-oriented stream cipher proposed by De Cannière and Preneel [3] in eSTREAM project, which leverages an idea from the design principles of block ciphers to reduce linear correlations and provides flexibility between number of gates and speed of encryption; and Enocoro, a hardware-oriented stream cipher proposed by Watanabe et. al. [28], which is efficient in both software and hardware implementation compared to eSTREAM hardware-oriented stream ciphers.

2.1.3 Hash Functions

In the IoT era, low-cost RFID tags are used extensively and they often rely on hash functions for encryption. According to Juels and Weis [20], RFID tags have only 2000 gates for security purpose. However, the conventional hash functions generally have more than 10000 gates that they are costly and exceed the security gate count budget. Therefore, lightweight hash functions are designed to mitigate gate counts that they can then fit into this scenario. Even though ISO/IEC 29192-5 is still under development, presented strong candidates of lightweight hardware-optimized hash functions including PHOTON (738GE[2]) and SPONGENT (865GE) both have significantly low gate count[3].

2.2 Lightweight Asymmetric Cryptography

Asymmetric cryptography is widely known by its strength in securing the channel with an insecure medium and is used in various applications, but it comes with a price that it typically requires more in computational platform resources. In the context of the IoT, its demanding characteristic may make it seem less practical. Nonetheless, recent research has proposed several lightweight mechanisms based on asymmetric techniques and some of them have been adopted as ISO/IEC 29192-4 [17] standards. These adopted lightweight mechanisms include: cryptoGPS [13], an identification scheme based on discrete logarithm; ALIKE (previously called SPAKE) [9], an authenticated key exchange protocol based on RSA (Rivest-Shamir-Adleman) encryption; and an identity-based signature scheme proposed by Liu et. al. [25].

3. MOTION AUTHENTICATION

[2]Gate Equivalence.

[3]Statistics from Lightweight Hash Functions. In CryptoLUX. Accessed: 2016-02-21, from https://www.cryptolux.org/index.php/Lightweight_Hash_Functions

Biometrics is becoming increasingly easy to observe in commercial products. Biometric recognition is based on human physiological and/or behavioral characteristics [18]. Fingerprint authentication, a typical example of physiological biometrics, is being applied to more and more smartphones since Apple embedded a fingerprint recognition module in iPhone. Behavioral biometrics utilizes human dynamic characteristics and has become a trend in biometrics. Some human dynamic characteristics can be used to recognize the genuineness of user correctly, such as prehension biometrics[10]. Similarly, motion recognition is suitable for IoT systems which feature small sensors and low powered devices because motion recognition can achieve high accuracy with just an accelerometer [29].

3.1 A Possible Application

Based on above analysis, therefore, one possible application of motion recognition is for pairing smartphone with IoT devices embedded with accelerometers. Pairing authentication is necessary because smartphone is one of the most popularly used device to control IoT networks in today's market. We propose the following solution: the smartphone shows a specific personalized moving pattern that was defined by user previously and then the user needs to move the IoT device in this pattern and the accelerometer data from the IoT device is sent to the smartphone. The smartphone then compares the motion data with the existing database to check if the pattern is correct and is done by the same user with behavioral biometrics analysis. If so, the pairing succeeds. In this case, even though the smartphone is controlled by an attacker, the pairing cannot succeed. Conversely, in the opposite case, the IoT device can ask the smartphone to perform a predefined motion and IoT device with stronger processor or connection to a server can determine if the motion data from the smartphone matches. Also, if the IoT is small enough, the user can hold both the IoT device and the smartphone to perform a specific motion at the same time. Then both devices can just compare the motion data from the other device with its own. In this case, no database is needed.

3.2 Feasibility

As mentioned above, motion recognition with only accelerometer gives high accuracy, thus how to set up a biometric database to check if the motion is performed by correct user become the main concern of this solution. A feasible solution provided by Guerra et al. [4] is as the following. They let the user to invent their personal gesture and offer 7 samples to the database. Users give really different gestures, such as writing a word and drawing some symbol in the air. All these gestures are collect while holding a device with an accelerometers embedded. The result from Guerra et al. [4] shows that the impostors has a very low chance of imitating successfully. This method can be applied to the pairing between smartphone and IoT devices. Smartphone can just show a hint of the gesture or even nothing to have a higher security level.

3.3 Equipment and Algorithm

Obviously, a smartphone and an additional device embedded with accelerometers that can connect with the smartphone in bluetooth or some other ways are needed for this solution. Other than these, an efficient recognition algorithm:

uWave can be used in this solution, because this algorithm requires only one accelerometer and is proved by Jiayang et al. [23, 24] from Rice University that it well recognized personalized gestures.

4. AUTHENTICATION MODELS

In traditional networks over the internet, the certificate authority hosts validates sites as authentic. This system protects a user from thinking they are visiting one site (e.g. Amazon, Google, etc.) when they are actually visiting another site. However, this paradigm is not achievable in an IoT environment because there is no certificate authority for every device in the environment. As a result, an IoT network must rely on its own alternative methods to support peer-to-peer authentication.

In this project, we propose implementation and a security analysis of one of the existing security paradigms for peer-to-peer authentication listed in the following sections. In particular, we aim to simulate a reputation system and evaluate it under different environments and attackers. Our evaluation would be geared towards minimizing both false positives and false negatives when a node has to decide whether or not to trust a new node trying to authenticate itself.

In the remainder of this section, we discuss existing IoT authentication methods in greater detail.

4.1 Gateway Authentication

One simple method of peer-to-peer authentication is the use of a gateway. In this method, the gateway (e.g. a smartphone) serves as a central authority and all IoT devices (e.g. sensors, controllers, etc.) authenticate themselves to the gateway. The gateway then validates authentication individually. One form of gateway authentication was proposed in [2] where one party is inside the local IoT network, and one device is outside the network. The gateway communicates with the external device using traditional security protocols (e.g. IPSec) and will rencrypt communication with the local device. In the Secure Gateway Application (SGA), the authors propose offloading heavy cryptographic primitives needed for authentication schemes to a central SGA server, allowing for a lightweight implementation on non-gateway devices [7]. A centralized gateway for authentication is also used as the cornerstone of the IoT framework proposed in [12].

Gateway authentication produces a heavy traffic burden on the gateway itself and may bottleneck in systems with a dense deployment of IoT devices. These gateways also become a critical point for security because a compromised gateway undermines the security of the entire network [30].

4.2 Reputation System

An alternative to gateway authentication is to instead offload the trust system into the peer-to-peer network itself. Leister et. al. propose a trust indicator model for IoT devices. Based on observers already trusted in the network, a device calculates a priori trust to determine if it should trust the new party [22]. Similarly, Chen et. al. use a fuzzy trust model as their reputation system. This model uses the observations of neighbors to calculate the reputation of a node using the following metrics: end-to-end packet forwarding ratio, energy consumption when delivering/receiving messages, and packet delivery ratio [6].

Although distributing this decision reduces the strain on the gateway, this reputation system weakens if a malicious device slips into the network [30].

5. REFERENCES

[1] A. Bogdanov, L. R. Knudsen, G. Leander, C. Paar, A. Poschmann, M. J. Robshaw, Y. Seurin, and C. Vikkelsoe. PRESENT: An Ultra-lightweight Block Cipher. In *Proceedings of the Conference on Cryptographic Hardware and Embedded Systems (CHES '07)*, Vienna, Austria, Jun 2007.

[2] R. Bonetto, N. Bui, V. Lakkundi, A. Olivereau, A. Serbanati, and M. Rossi. Secure Communication for Smart IoT Objects: Protocol Stacks, Use Cases and Practical Examples. In *Proceedings of the Conference on World of Wireless, Mobile and Multimedia Networks (WoWMoM '12)*, San Francisco, CA, Jun 2012.

[3] C. De Cannière and B. Preneel. Trivium: A Stream Cipher Construction Inspired by Block Cipher Design Principles. In *Proceedings of the International Conference on Information Security (ISC '06)*, Samos Island, Greece, Aug 2006.

[4] J. G. Casanova, C. S. Avila, A. de Santos Sierra, G. B. del' Pozo, and V. J. Vera. A Real-Time In-Air Signature Biometric Technique Using a Mobile Device Embedding an Accelerometer. In *Proceedings of the Conference on Networked Digital Technologies*, Communications in Computer and Information Science, Prague, Czech Republic, Jul 2010.

[5] M. Cazorla, K. Marquet, and M. Minier. Survey and Benchmark of Lightweight Block Ciphers for Wireless Sensor Networks. In *Proceedings of the International Conference on Security and Cryptography*, Reykjavik, Iceland, Jul 2013.

[6] D. Chen, G. Chang, D. Sun, J. Li, J. Jia, and X. Wang. TRM-IoT: A Trust Management Model Based on Fuzzy Reputation for Internet of Things. *Journal on Computer Science and Information Systems (ComSIS)*, Oct. 2011.

[7] H.-C. Chen, I. You, C.-E. Weng, C.-H. Cheng, and Y.-F. Huang. A Security Gateway Application for End-to-End M2M Communications. *Computer Standards & Interfaces*, 2016.

[8] Cisco Systems, Inc. Securing the Internet of Things: A Proposed Framework. http://www.cisco.com/c/en/us/about/security-center/secure-iot-proposed-framework.html. (Accessed: 2016-02-16).

[9] J.-S. Coron, A. Gouget, P. Paillier, and K. Villegas. SPAKE: A Single-Party Public-Key Authenticated Key Exchange Protocol for Contact-Less Applications. In *Proceedings of the International Conference on Financial Cryptograpy and Data Security*, Canary Islands, Spain, Jan 2010.

[10] A. Drosou, D. Ioannidis, D. Tzovaras, K. Moustakas, and M. Petrou. Activity Related Authentication Using Prehension Biometrics. *Pattern Recognition*, 48(5):1743–1759, May 2015.

[11] T. Eisenbarth, S. Kumar, C. Paar, A. Poschmann, and L. Uhsadel. A Survey of Lightweight Cryptography Implementations. *IEEE Design and Test of Computers*

- *Special Issue on Secure ICs for Secure Embedded Computing*, Nov 2007.

[12] D. Gessner, A. Olivereau, A. Segura, and A. Serbanati. Trustworthy Infrastructure Services for a Secure and Privacy-Respecting Internet of Things. In *Proceedings of the Conference on Trust, Security and Privacy in Computing and Communications (TrustCom '12)*, Liverpool, UK, June 2012.

[13] M. Girault, G. Poupard, and J. Stern. On the Fly Authentication and Signature Schemes Based on Groups of Unknown Order. *Journal of Cryptology*, Oct 2006.

[14] ISO/IEC 29192-1. Information Technology – Security Techniques – Lightweight Cryptography – Part 1: General. Technical report, International Organization for Standardization, Geneva, Switzerland, May 2012.

[15] ISO/IEC 29192-2. Information Technology – Security Techniques – Lightweight Cryptography – Part 2: Block Ciphers. Technical report, International Organization for Standardization, Geneva, Switzerland, Jan 2012.

[16] ISO/IEC 29192-3. Information Technology – Security Techniques – Lightweight Cryptography – Part 3: Stream Ciphers. Technical report, International Organization for Standardization, Geneva, Switzerland, Sep 2012.

[17] ISO/IEC 29192-4. Information Technology – Security Techniques – Lightweight Cryptography – Part 4: Mechanisms Using Asymmetric Techniques. Technical report, International Organization for Standardization, Geneva, Switzerland, May 2013.

[18] A. K. Jain, A. Ross, and S. Prabhakar. An Introduction to Biometric Recognition. *IEEE Transactions on Circuits and Systems for Video Technology*, 14(1):4–20, Jan 2004.

[19] Q. Jing, A. V. Vasilakos, J. Wan, J. Lu, and D. Qiu. Security of the Internet of Things: Perspectives and Challenges. *Wireless Networks*, 20(8):2481–2501, Nov 2014.

[20] A. Juels and S. A. Weis. Authenticating Pervasive Devices with Human Protocols. In *Proceedings of the International Cryptology Conference (CRYPTO '05)*, Santa Barbara, California, August 2005.

[21] B. Khoo. RFID as an Enabler of the Internet of Things: Issues of Security and Privacy. In *Proceedings of the International Conference on Cyber, Physical and Social Computing Internet of Things (iThings/CPSCom '11)*, Oct 2011.

[22] W. Leister and T. Schulz. Ideas for a Trust Indicator in the Internet of Things. In *Proceedings of the International Conference on Smart Systems, Devices and Technologies (SMART '12)*, Stuttgart, Germany, 2012.

[23] J. Liu, L. Zhong, J. Wickramasuriya, and V. Vasudevan. User Evaluation of Lightweight User Authentication with a Single Tri-axis Accelerometer. In *Proceedings of the International Conference on Human-Computer Interaction with Mobile Devices and Services (MobileHCI '09)*, Bonn, Germany, Sept. 2009.

[24] J. Liu, L. Zhong, J. Wickramasuriya, and V. Vasudevan. uWave: Accelerometer-based Personalized Gesture Recognition and Its Applications. *Pervasive and Mobile Computing*, 5(6):657–675, Dec 2009.

[25] J. K. Liu, J. Baek, J. Zhou, Y. Yang, and J. W. Wong. Efficient Online/Offline Identity-based Signature for Wireless Sensor Network. *International Journal of Information Security*, Aug 2010.

[26] T. Shirai, K. Shibutani, T. Akishita, S. Moriai, and T. Iwata. The 128-bit Blockcipher CLEFIA. In *Proceedings of the International Conference on Fast Software Encryption*, Luxembourg, Luxembourg, Mar 2007.

[27] R. Tripathi and S. Agrawal. Comparative Study of Symmetric and Asymmetric Cryptography Techniques. *International Journal of Advance Foundation and Research in Computer*, Jun 2014.

[28] D. Watanabe, K. Ideguchi, J. Kitahara, K. Muto, and H. Furuichi. Enocoro-80: A Hardware Oriented Stream Cipher. In *Proceedings of the International Conference on Availability Reliability and Security*, Barcelona , Spain, Mar 2008.

[29] R. Xu, S. Zhou, and W. J. Li. MEMS Accelerometer Based Nonspecific-User Hand Gesture Recognition. *IEEE Sensors Journal*, 12(5):1166 – 1173, Sep 2011.

[30] Z.-K. Zhang, M. C. Y. Cho, and S. Shieh. Emerging Security Threats and Countermeasures in IoT. In *Proceedings of the Symposium on Information, Computer and Communications Security (ASIA CCS '15)*, Singapore, Apr. 2015. ACM.