Criptografía liviana para objetos conectados

Universidad Argentina de la Empresa

Ricardo Wehbe – rwehbe@uade.edu.ar
Adrián de Armas – adearmas@uade.edu.ar
Elizabeth Barrera – elbarrera@uade.edu.ar

1 Plan de investigación

1.1 Contexto

En los próximos años se acentuará una tendencia que ya ha comenzado, la interconexión de diversos objetos "inteligentes", denominada IoT (Internet of Things) [1]. Esto trae aparejado un problema de seguridad: los métodos habituales de criptografía simétrica y asimétrica (AES, DES, block ciphers entre los primeros; RSA, Diffie-Hellman, ElGamal, curvas elípticas entre los segundos) [2] [3] requieren un esfuerzo computacional del que estos dispositivos son incapaces.

La criptografía liviana (lightweight cryptography) [4] [5] tiene por objetivo lograr un aceptable nivel de seguridad para dispositivos de capacidades modestas.

Este proyecto se propone evaluar comparativamente los métodos de criptografía liviana propuestos actualmente desde el punto de vista de su consumo energético y los recursos computacionales requeridos.

1.2 Estado actual de conocimiento sobre el tema

Existen diversos algoritmos de criptografía liviana actualmente. Se los puede dividir en:

1. *Stream ciphers* (algoritmos que encriptan un flujo continuo de datos) como SNOW 3G, Trivium, Espresso, LIZARD, etc.

2. Funciones de *hashing* criptográficas (si bien no se utilizan directamente para encriptar, son un componente esencial de muchos esquemas de seguridad). Algunos ejemplos son Armadillo, QUARK, Photon, GLUON, etc.

3. *Block ciphers* (algoritmos que encriptan un flujo de datos por bloque) como TEA, RC5, Hight, PRESENT, KATAN, etc.

4. Algoritmos de criptografía asimétrica, (sistemas de clave pública), como RSA y curvas elípticas (ECC).

Dos buenos *surveys* son los de Bhardwaj et alii y Biryukov et alii [6] y [7], aunque el primero es excesivamente lacónico y el segundo sólo considera criptografía simétrica.

En este proyecto se pretende incluir a los principales algoritmos de criptografía liviana asimétrica, como RSA o ECC [8] [9]. No se ha encontrado antecedentes de estudios comparativos como el que querríamos realizar en esta área. En una etapa ulterior, queremos trabajar sobre funciones de *hashing* livianas y stream ciphers.

2 Objetivos

2.1 Objetivos generales

El objetivo del proyecto es efectuar un relevamiento de los algoritmos actuales de criptografía liviana, implementar estos algoritmos y compararlos desde el punto de su consumo energético y costo computacional.

2.2 Objetivos específicos

La idea es tener un panorama general de las ventajas y desventajas de los diferentes abordajes y de adquirir un *know-how* en la implementación y análisis de estos algoritmos.

Las diferentes familias de algoritmos se considerarán por separado (algoritmos simétricos, asimétricos y funciones de *hashing* [10].) Se implementarán estos algoritmos y se comparará la eficiencia relativa de cada uno de ellos para las diferentes familias consideradas. En una primera etapa nos conformaremos con implementaciones en software, aunque el objetivo final es llegar a las implementaciones en hardware.

3 Especificaciones metodológicas y técnicas

En una primera etapa se hará una selección de algoritmos en tres categorías (criptografía liviana simétrica, criptografía liviana asimétrica y funciones de hashing livianas).

Para cada una de las categorías se efectuará una implementación lo más eficiente posible, utilizando las técnicas que se ven en las materias

de programación avanzadas [11] [12]. Existen además de las técnicas generales, algunas técnicas específicas para este género de problemas (por ejemplo, la utilización de primitivas de las versiones livianas de AES para producir funciones de *hashing* livianas [13].)

El análisis procederá por dos caminos paralelos. Por una parte, estimar el orden de complejidad temporal a través del análisis del código con algunas de las notaciones asintóticas estándar (la notación O o θ [14][15].) Esto dará una estimación general de la eficiencia de un algoritmo. Pero, como se sabe, estas notaciones dejan de lado constantes que pueden ser importantes.

Por eso, se establecerá una medida de la duración real de ejecución sobre un conjunto de datos establecido para determinar la posible influencia de las constantes que las notaciones asintóticas dejan de lado. Se busca crear un ambiente de prueba en el que todos los algoritmos estén trabajando en igualdad de condiciones para que los resultados no estén sesgados.

Para la segunda etapa, la confidencialidad se conseguirá a través de un esquema de criptografía simétrica. Para la autenticación de datos de origen se utilizará, como es habitual, un esquema de clave privada. Se buscará establecer un esquema de confianza en la red para que los objetos estén en condiciones de aceptar o rechazar pedidos de conexión (un esquema similar al que se utiliza en [27]para redes de sensores.) Para ello se asume un contexto de ataques bizantinos [25], en el que se trata de mantener la coherencia de la información en un contexto en el que algunos nodos de la red pueden estar transmitiendo información poco confiable [26].

Un importante objetivo es la posibilidad de crear un grupo de interés que pueda eventualmente expandirse en otras direcciones y estar en el mediano plazo en condiciones de efectuar transferencia tecnológica.

Cabe destacar que algunos de los objetivos ya están cumplidos. Se ha realizado una comparación de diversos algoritmos de clave pública, clave simétrica y funciones de *hashing* livianas en tres diferentes trabajos finales de ingeniería. En todos los casos, se trató de implementaciones en software.

4 Formación de recursos humanos

Los participantes de esta investigación (alumnos de grado y maestría) serán capacitados para entender los fundamentos matemáticos de las principales herramientas criptográficas (funciones de *hashing* criptográficas, algoritmos de criptografía simétrica y asimétrica, MAC, firma digital, métodos de autenticación. Se implementarán algoritmos seleccionados en distintos lenguajes de programación y se realizará la verificación de los algoritmos implementados y la comparación entre las distintas implementaciones para determinar puntos de referencia respecto del mejor algoritmo para cada escenario.

En una etapa ulterior se prevé trabajar sobre hardware (posiblemente Raspberry.) Para ello, se planea un trabajo conjunto con la Facultad de Ingeniería.

5 Bibliografía

[1] Li, Shancang; Xu, Li Da; Zhao, Shanshan: The Internet of Things: a Survey, Inf. Syst. Front. 17, pp. 243–259, 2015.

[2] Delfs, Hans; Knebel, Helmut: *Introduction to Cryptography*, Springer, 2007.

[3] Cohen, Henri; Frey, Gerhard (eds.), *Handbook of Elliptic and Hyperelliptic Cryptography*, Chapman & Hall, 2007.

[4] Buchanan, William; Li, Shancang; Asiz, Rameez: *Lightweight Cryptography Methods*, Journal of Cyber Security Technology, 1(3-4), pp. 187–201, 2017.

[5] Dutta, Indira; Bayoumi, Magdy; Ghosh, Baskar: *Lightweight Cryptography for Internet of Insecure Things: a Survey*, Proc. of the 9th Annual IEEE Computing and Communication Workshop and Conf. (CCWC), 2019.

[6] Bhardwaj, Isha; Kumar, Ajay; Bansal, Manu: *A Review on Lightweight Cryptography Algorithms for Data Security and Authentication in IoT*, Proc. of the 4th IEEE Int. Conf. On Signal Processing, Computing and Control (ICSPCC), 2017.

[7] Biryukov, Alex; Perrin, Léo-Paul: *State of the Art in Lightweight Symmetric Cryptography*, IACR Cryptology ePrint Archive 2017: 511, 2017.

[8] Abd Zaid, Mustafa ; Hassan, Soukacna : *A Lightweight RSA Algorithm Using Three Prime Numbers*, Int. J. of Engineering & Technology, 7(4.36), pp. 293–295, 2018.

[9] Lara-Nino, Carlos; Díaz-Pérez, Arturo; Morales-Sandoval, Miguel: *Elliptic Curve Lightweight Cryptography: a Survey*, IEEE Access, 6, pp. 72514–72550, 2018.

[10] Hammad, Baraa Tareq; Jamil, Norziana; Rusli, Mohd Ezanee; Z'aba, Muhammad Reza: *A survey of Lightweight Cryptographic Hash Functions*, Int. J. of Scientific & Engineering Research 8(7), pp. 806–814, 2017.

[11] Cormen, Thomas; Leiserson, Charles; Rivest, Ronald; Stein, Clifford: *Introduction to Algorithms*, MIT Press, 2002.

[12] Dasgupta, Sanjoy; Papadimitriou, Christos; Varizani, Umesh: *Algorithms*, McGraw-Hill Education, 2006.

[13] Bos, Joppe; Özen, Onun; Stam, Martijn: *Efficient Hashing Using the AES Instruction Set*, Proc. of the Conf. on Cryptographic Hardware and Embedded Systems (CHES) 2011, pp. 507–522, 2011.

[14] Lewis, Harry; Papadimitriou, Christos: *Elements of the Theory of Computation*, Prentice-Hall, 1998.

[15] Sipser, Michael: *Introduction to the Theory of Computation*, Thomson Course Technology, 2006.

[16] Cheruvu, Sunil; Kumar, Anil; Smith, Neil; Wheeler, David: *Demystifying Internet of Things Security*, Apress Open, Springer, 2020.

[17] Hou, Jianwei; Qu, Leilei; Shi, Wenchang: *A survey on internet of things security from data perspectives*, Compter Networks 148(15), pp. 295–306, 2019.

[18] Veltri, Giuseppe: *Digital Social Research*, Polity Press, 2020.

[19] Stephens-Davidowicz,Seth: Everybody Lies. *Big Data, New Data, and What the Internet Can Tell Us about Who We Really Are*, Bloomsbury Publishing, 2017.

[20] Ohlhorst, Frank: *Big Data Analytics. Turning Big Data Into Big Money*, John Wiley & Sons, 2013.

[21] Alexandre, Laurent: *La guérre des intélligences : intélligence artificielle versus intélligence humaine*, JC Lattès, 2017.

[22] Liu, Donggang; Ning, Peng: *Security for Wireless Sensor Networks*, Springer, 2007.

[23] Jurdak, Raja: *Wireless Ad Hoc and Sensor Networks. A Cross-Layer Design Perspective*, Springer, 2007.

[24] Sohraby, Kazem; Minoli, Daniel; Znati, Taieb: *Wireless Sensor Networks. Technology, Protocols and Applications*, John Wiley & Sons, 2007.

[25] Lamport, Leslie: *The Byzantine Generals Problem*, ACM Trans. on Programming Languages and Systems 4(3), pp 387-389, 1982.

[26] Abdelhakim, Mai; Lightfoot, Leonard; Li, Tontong: *Reliable Data Fusion in Wireless Sensor Networks under Byzantine Attacks*, Proc. of the 2011 IEEE Military Comm. Conf. (MILCOM 2011), pp. 810-815.

[27] Chen, Haiguang;Wu, Huafeng; Zhou, Xi; Gao, Chuanshan: *Agent-Based Trust Model in a Wireless Sensor Network*, Proc. of the 8th IEEE Conf. on Software Engineering, Artificial Intelligence, Networking, and Parallel/Distributed Computing (ACIS), pp. 119-124, 2007.