

Criptografía Maliciosa y Ciberdefensa.

Cipriano, Marcelo^{1,2}; García, Edith¹, Maiorano, Ariel¹
Malvacio, Eduardo¹, Pazo Robles, María Eugenia¹

¹Laboratorio de Investigación en Técnicas Criptográficas y Seguridad Teleinformática.
Facultad de Ingeniería del Ejército (FIE), Universidad de la Defensa Nacional - UNDEF
²Departamento de Ciencia y Tecnología, Universidad Nacional de Quilmes UNQ.

{marcelocipriano; egarcia; maiorano; emalvacio; mepazorobles}@fie.undef.edu.ar

RESUMEN

El proyecto tiene por finalidad estudiar y analizar la aplicación de paradigmas y herramientas criptológicas modernas para la creación de software malicioso y puertas traseras, como así también indagar técnicas de prevención, detección y protección para ser consideradas en el ámbito de la Ciberdefensa Nacional.

Aunque comúnmente se entiende a la criptografía y a sus aplicaciones como herramientas de carácter defensivo, también pueden emplearse para usos ofensivos y maliciosos; a saber, el secuestro, extorsión y pérdida de información producidos mediante software malicioso denominado *ransomware*, en sus distintas variantes.

Por otra parte, la literatura también da cuenta de ataques en las etapas de diseño e implementación de algoritmos criptográficos, comúnmente llamados *backdoors* o puertas traseras, que pueden vulnerar la confidencialidad, integridad y disponibilidad. Es fácil observar las consecuencias directas sobre la ciberseguridad de usuarios particulares, empresas y organismos no gubernamentales de tales ataques.

Pero un aspecto de este tipo de ataques pasa desapercibido y sin embargo tiene un impacto mayor pues amenaza directamente a la población de una ciudad, provincia o llanamente, un país completo pues es capaz de afectar a sus organismos públicos, fuerzas de seguridad, estructura militar, política y

diplomática, como así también sus activos de información. Puede contribuir a la realización exitosa de ataques a las Infraestructuras Críticas, es decir, aquellas organizaciones relacionadas con la generación y distribución de energía, sistema financiero y bancario, organismos de salud como hospitales, servicio de potabilización y distribución de agua, saneamiento de desechos, entre otras.

Es decir, los ataques basados en puertas traseras o *backdoors* podrían menoscabar la ciberdefensa de una nación.

Palabras Clave

Criptología, Criptovirología, Kleptografía, Puertas Traseras Criptográficas. Ciberdefensa.

CONTEXTO

“MAC: Criptografía Maliciosa para la Ciberdefensa” es un proyecto perteneciente a la Facultad de Ingeniería del Ejército (FIE) “Gral. Div. Manuel N. Savio”, perteneciente a la Universidad de la Defensa Nacional (UNDEF).

Se encuentra enmarcado en el contexto de la carrera de grado de Ingeniería en Informática, la Especialización en Criptografía y Seguridad Teleinformática y, la Maestría en Ciberdefensa, que se dictan en la citada unidad académica.

Allí los investigadores conforman el Grupo de Investigación en Criptología y Seguridad Informática (GICSI) que

depende del Laboratorio de Investigación en Técnicas Criptográficas y Seguridad Teleinformática y lleva adelante tareas de I+D+i. El equipo está conformado por docentes investigadores categorizados en distintos regímenes científicos, profesionales técnicos, becarios y alumnos de la carrera de grado de Ingeniería en Informática, Especialización en Criptografía y Seguridad Teleinformática y de la Maestría en Ciberdefensa.

1. INTRODUCCIÓN

Comúnmente se aprecia a la criptografía y a sus aplicaciones como instrumentos de carácter defensivo que proporcionan confidencialidad en sistemas de comunicaciones, redes y bases de datos, entre otros.

En el año 1996 en un trabajo fundacional, *Adam Young* y *Moti Yung* [1] presentan lo que han dado en llamar *Criptovirología*. Los autores previeron y mostraron la posibilidad de llevar adelante ataques mediante virus informáticos, que cifran la información de sus víctimas a través de criptografía de clave pública, pidiendo luego rescate para su recuperación. En la actualidad este tipo de malware se conoce como *ransomware*.

Al año siguiente, los mismos autores presentan la llamada "*Kleptografía*": esto es el diseño e implementación de backdoors o puertas traseras en algoritmos criptográficos [2-4]. En particular los autores presentan el mecanismo criptográfico "*Secretly Embedded Trapdoor with Universal Protection*", conocido por sus siglas en inglés por el acrónimo de *SETUP*. Este *kleptograma* es una modificación a nivel matemático del algoritmo de intercambio de llaves *Diffie-Hellman*.

Con las modificaciones pertinentes, estas técnicas *kleptográficas* se podrían implementar en el corazón de otros algoritmos, podrían ser embebidos en

otros mecanismos criptográficos como son los esquemas de cifrado y de firma digital *ElGamal*, *DSA*, el algoritmo de firma de *Schnorr*, y el *PKCS* de *Menezes-Vanstone* y finalmente el reconocido algoritmo *RSA* [5-6, 8,13]. Es importante destacar que estos diseños no se limitan a criptografía de llave pública. Se cuenta en la literatura con publicaciones que describen ejemplos aplicados a funciones de hash, en donde se presentan colisiones para una versión de *SHA-1* modificando sus correspondientes parámetros [7], como también se presentan alternativas para protegerse de funciones de hash comprometidas en algoritmos de nivel superior, como *HMAC* y *HKDF* [14].

Por otro lado, tampoco los generadores de números de pseudo-aleatorios conocidos en la bibliografía como *Pseudo Random Numbers Generators* o *PRNG* por sus siglas en inglés. Estos algoritmos no serían inmunes a este tipo de ataques [10-13]. Básicamente la vulnerabilidad insertada afecta las propiedades estadísticas de un generador haciéndolo muy sensible a la entropía de la entrada. Por ejemplo, cuando los inputs tienen una distribución correcta, este mecanismo no tiene efecto, pero cuando están afectados por algún sesgo, el generador malicioso empeora considerablemente. En síntesis, la seguridad de los esquemas criptográficos se mide tradicionalmente como la incapacidad de un adversario, que cuenta con recursos limitados, de violar un objetivo de seguridad deseado [14]. Sin embargo, este argumento de seguridad generalmente se basa en un diseño sólido de los componentes subyacentes. Podría decirse que uno de los fracasos más devastadores de este enfoque se puede observar al considerar adversarios con la capacidad de influir en el diseño, implementación y estandarización de primitivas criptográficas.

Es entonces que considerando el impacto y la relevancia actual [16,17] de las técnicas y mecanismos mencionados se justificaría esta línea de investigación.

2. LÍNEAS DE INVESTIGACIÓN y DESARROLLO

El proyecto está conformado por distintas líneas de acción:

- Estudio de material actualizado, asistencia a Cursos, Congresos y Workshops específicos, profundización en el estado del arte tanto de la criptovirología como de la kleptografía, aunque el esfuerzo principal estará dirigido a esta última.
- Estudio y análisis de las diferentes variantes de criptovirología.
- Estudio y análisis de ataques kleptografía en la literatura aplicados a diferentes algoritmos o primitivas criptográficas.
- Profundización en el estudio y análisis de técnicas kleptográficas para el algoritmo RSA y algoritmos de generación de números pseudo-aleatorios específicamente.
- Implementación experimental, conceptual y de referencia de alguna o algunas de las técnicas analizadas.
- Análisis y conclusiones de los resultados obtenidos.

3. RESULTADOS OBTENIDOS / ESPERADOS

El proyecto propone estudiar y analizar la aplicación de los paradigmas y herramientas en la creación de software malicioso y puertas traseras criptográficas. En procura de desarrollar técnicas de prevención, detección y protección para ser considerados en el ámbito de la Ciberdefensa Nacional.

Por ejemplo someter a análisis a un algoritmo criptográfico o una parte de él, en procura de hallar indicios o técnicas de manipulación Kleptográficas, la inclusión de Backdoors Cryptography. Como así también el análisis del malware de tipo ransomware para el desarrollo de mecanismos de detección y prevención. De esta forma, procurar el desarrollo de herramientas de detección de vulnerabilidades criptográficas susceptibles de ser explotadas, afectando la ciberdefensa.

4. FORMACIÓN DE RECURSOS HUMANOS

Los investigadores que llevan adelante el proyecto dictan las asignaturas Criptografía y Seguridad Teleinformática, Matemática Discreta y Paradigmas de Programación. Desde esas cátedras se invita de forma permanente a los alumnos para participar como colaboradores.

Asimismo y por primera vez, varios alumnos de la especialización en Criptografía y Seguridad Teleinformática que están llevando adelante su Trabajo Final Integrador, como así también maestrands pertenecientes a la Maestría en Ciberdefensa, que se encuentran trabajando en el desarrollo de sus respectivas tesis; y que además abordan temáticas relacionadas a la de este proyecto, han sido invitados a participar del mismo. Se espera que la contribución mutua entre el equipo de investigadores, especializandos y maestrands permita alcanzar niveles sinérgicos de avance en la investigación, la formación de recursos humanos.

La Formación de Recursos Humanos permite incrementar el Know-How que tendrá el grupo de investigadores a lo largo de la vida del proyecto. Será un importante beneficio de sus integrantes

y de la institución en la cual desarrollan sus actividades científico-docentes. Por último y atendiendo a la responsabilidad ética y social que compete a la actividad científica y tecnológica, el Grupo Integrante de este Proyecto de Investigación, ya sea durante su ejecución o por la aplicación de los resultados obtenidos, desea expresar su compromiso a no realizar cualquier actividad personal o colectiva que pudiera afectar los derechos humanos, o ser causa de un eventual daño al medio ambiente, a los animales y/o a las generaciones futuras.

5. BIBLIOGRAFÍA

- [1] Young, Adam L. and Moti Yung. "Cryptovirology: extortion-based security threats and countermeasures." Proceedings 1996 IEEE Symposium on Security and Privacy (1996): 129-140.
- [2] Young, Adam L. and Moti Yung. "The Prevalence of Kleptographic Attacks on Discrete-Log Based Cryptosystems." CRYPTO (1997).
- [3] Young, Adam L. and Moti Yung. "Kleptography: Using Cryptography Against Cryptography." EUROCRYPT (1997).
- [4] Young, Adam L. and Moti Yung. "Malicious cryptography - exposing cryptovirology." (2004).
- [5] Young, Adam L. and Moti Yung. "A Space Efficient Backdoor in RSA and Its Applications." Selected Areas in Cryptography (2005).
- [6] Young, Adam L. and Moti Yung. "An Elliptic Curve Backdoor Algorithm for RSASSA." Information Hiding (2006).
- [7] Albertini, Ange, Jean-Philippe Aumasson, Maria Eichlseder, Florian Mendel and Martin Schl affer. "Malicious Hashing: Eve's Variant of SHA-1." Selected Areas in Cryptography (2014).
- [8] Young, Adam L. and Moti Yung. "Cryptography as an Attack Technology: Proving the RSA/Factoring Kleptographic Attack." The New Codebreakers (2015).
- [9] Russell, Alexander, Qiang Tang, Moti Yung and Hong-Sheng Zhou. "Ciphertext Clipping: The Power of Kleptographic Attacks." ASIACRYPT (2015).
- [10] Indarjani, Santi. Sugeng, Kiki. Widjaja, Belawati. "Modification Attack Effects on PRNGs: Empirical Studies and Theoretical Proofs." (2015).
- [11] Young, Adam L. and Moti Yung. "Cryptovirology: the birth, neglect, and explosion of ransomware" Commun. ACM 60 (2017): 24-26.
- [12] Teseleanu, George. "Random Number Generators Can Be Fooled to Behave Badly." IACR Cryptology ePrint Archive (2018).
- [13] Markelova, A. V. "Vulnerability of RSA Algorithm." (2018).
- [14] Fischlin, Marc. Janson, Christian. Mazaheri, Sogol. "Backdoored Hash Functions: Immunizing HMAC and HKDF." (2018): 105-118.
- [15] Xiao, Dianyan and Yang Yu. "Klepto for Ring-LWE Encryption." Comput. J. 61 (2018): 1228-1239.
- [16] Yogi, Manas. Aparna, S.. "Novel insights into Cryptovirology A Comprehensive Study." International Journal of Computer Sciences and Engineering. 6. (2018): 1252-1255.
- [17] Zimba, Aaron. Chishimba, Mumbi. "On the Economic Impact of Crypto-ransomware Attacks: The State of the Art on Enterprise Systems." European Journal for Security Research. (2019).