Ciberdefensa y Criptología Maliciosa

Cipriano, Marcelo[1,2] ; García, Edith[1], Maiorano, Ariel[1]
Malvacio, Eduardo[1],

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

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

RESUMEN

Generalmente se considera a la *Criptografía* y a sus aplicaciones como herramientas de carácter defensivo. Sin embargo y desde hace ya varios años, se observa una amplia difusión de sus aplicaciones maliciosas: el secuestro, extorsión y pérdida de información producidos mediante software malicioso denominado *ransomware*, en sus distintas variantes.

Sin embargo, en la literatura científica también se pueden hallar registros de ataques, comúnmente llamados *backdoors* o *puertas traseras.* Lo que los distingue de otros ataques, es que estas "*puertas traseras*" fueron incorporadas en las etapas de diseño e implementación de algoritmos criptográficos. Y lo que es peor aún, posiblemente fueron diseñadas con ese fin, por sus propios autores u organismos que los han creado o patrocinado.

No es difícil imaginar el elevado orden de magnitud del impacto de tal ataque. Pueden vulnerar la *Confidencialidad*, *Integridad* y *Disponibilidad* sin mayores dificultades. Y posiblemente, puedan pasar desapercibidos por mucho tiempo.

Esta amenaza puede afectar directamente a la población, en cualquiera de sus niveles: local, provincial o nacional. Podría incluso afectar a sus organismos públicos, fuerzas de seguridad, estructura militar, política y diplomática, como así también sus activos de información en *Infraestructuras Críticas.* Estas con 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.

Este proyecto tiene como objetivo profundizar el estudio, análisis de paradigmas criptológicos modernos usados en la creación de software malicioso y puertas traseras para así poder indagar acerca de la creación de técnicas de prevención, detección y protección para ser consideradas en el ámbito de la Ciberdefensa Nacional.

Palabras Clave

Criptología, Criptografía Maliciosa, Puertas Traseras Criptográficas, Ciberdefensa.

CONTEXTO

"Criptología Maliciosa para la Ciberdefensa" (CRIPTO-MC) es un *Proyecto de Desarrollo Tecnológico y Social* (PDTS) aprobado por la Disposición Decanal Nro 667/2022, 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 pertenece al *Laboratorio de Informática, |Software Seguro y Criptografía* (*LISSyC*), que 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*, de la *Especialización en Criptografía y Seguridad Teleinformática* y de la *Maestría en Ciberdefensa.*

1. INTRODUCCIÓN

En 1996, *Adam Young* y *Moti Yung* [1] publican un trabajo seminal, en el que dieron a conocer a la comunidad científica, lo que han dado en llamar *Criptovirología*. Los autores expusieron las técnicas posibles que permiten ejecutar ataques mediante virus informáticos. Hasta allí nada novedoso, pues los virus eran la mayor amenaza informática, en aquellos días. La novedad radicaba en que tales programas maliciosos cifraban la información de sus víctimas a través de criptografía de clave pública, pidiendo luego rescate para su recuperación.
Este tipo de malware, en el presente, se lo conoce como *ransomware*. Y contraria| mente a lo que muchos puedan creer, no son una amenaza actual. Tal como se ha mostrado, al menos conceptualmente, existe desde hace décadas.
Los mismos autores, al año sigiente, presentan una nueva amenaza, la llamada *Kleptografía.* Esto es el diseño e implementación de *backdoors* o puertas traseras en algoritmos criptográficos [2-4]. En esa oportunidad, 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.* El objetivo era que las víctimas puedan establecer sus claves criptográficas, a traves del mencionado procedimiento. Pero el atacante que ha diseñado *SETUP*, tendría acceso exclusivo a la clave así generada. Así, las comunicaciones entre sus víctimas le resultarían completamente transpa-rentes. Y además, con la seguridad que el ataque pase completamente desapercibido y sin ningún tipo de mitigación.
Con las debidas adecuaciones, estas técnicas kleptográficas se podrían imple-mentar en otros algoritmos criptográficos: 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].
Además, este ataque con se limita a los esquemas de clave pública. Puede extenderse a los esquemas simétricos o de clave privada. La literatura científica da cuenta de ataques a algoritmos de hash. Se puede hallar una versión modificada de SHA-1[7], como también funciones como *HMAC* y *HKDF* [14].
También pueden afectarse los generadores de números de pseudo-aleatorios (*Pseudo Random Numbers Generators* o *PRNG* por sus siglas en inglés)[10-13].
Si se considera que la seguridad de los esquemas criptográficos se mide usualmente como la incapacidad de un adversario de violar un objetivo de seguridad deseado [7,14]. Pero este tipo de ataques le entrega al adversario o atacante, la capacidad de influir en el diseño, implementación y estandarización de primitivas criptográficas[15-17].

2. LÍNEAS DE INVESTIGACIÓN y DESARROLLO

El proyecto contempla las siguientes líneas de acción:

- Seguimiento de bibliografía y publicaciones científicas acerca de las aplicaciones de la tecnología kleptográficas y criptología maliciosa.
- Asistencia y/o seguimiento de cursos, jornadas, congresos y workshops de relevancia, tanto nacionales como internacionales.
- Análisis de primitivas matemáticas, el estudio de las puertas traseras keptográficas y ataques conocidos.
- Estudio de las propiedades criptológicas específicas de la Keptografía aplicadas a los diferentes algoritmos criptográaficos asimétricos y generación de números pseudo aleatorios (PRNG) entre otros.

3. RESULTADOS OBTENIDOS / ESPERADOS

Se persiguen los siguientes objetivos y resultados:

- Estudiar y analizar los paradigmas y herramientas criptológicas modernas en la creación de software malicioso, como así también las técnicas de prevención, detección y protección para ser considerados en el ámbito de la Ciberdefensa Nacional.
- Estudiar y analizar las diferentes variantes de *Criptovirología* y ataques kleptográficos existentes en la literatura, que son aplicados a diferentes algoritmos o primitivas criptográficas, con el objetivo de su detección y/o prevención.
- Elaborar criterios y herramientas que posibiliten la detección de algoritmos criptográficos backdoreados, procurando su mitigación o su eliminación.

4. FORMACIÓN DE RECURSOS HUMANOS

Se espera que los resultados del proyoecto puedan contribuir con el incremento del capital de conocimiento y recursos humanos del espacio académico civil y militar de la *Facultad de Ingeniería del Ejército*, de la *Universidad de la Defensa Nacional* y de las *Fuerzas Armadas* en general.

A través de la difusión y publicación de los resultados, como así también la realización de talleres, jornadas de capacitación. Además, se procura la difusión de estas temáticas en el ámbito de la *Ciberdefensa Nacional*, permitiendo visibilizar y promover la especialización y la maestría.

Los investigadores que llevan adelante el proyecto dictan las asignaturas tanto en la carrera de grado como en la especialización antes mencionadas. Por ejemplo las asignaturas *Matemática Discreta*, *Criptografía y Seguridad Teleinformática, Criptografía* y *Criptografía Avanzada.* Desde esas cátedras se invita de forma permanente a los alumnos, de grado y posgrado, a para participar en los proyectos y programas que se llevan adelante desde *LISSyC*. En particular cabe destacar que del proyecto participan maestrandos que llevan adelante tareas de investigación y la redacción de su tesis de maestría.

Se espera que la contribución mutua entre el equipo de investigadores, futuros especialistas y maestrandos 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 DiscreteLog 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 Schläffer. "*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. "*Cliptography: 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)