

# Criptología Maliciosa y Ciberdefensa

Marcelo Cipriano<sup>1,2</sup>, Edith García<sup>1</sup>, Ariel Maiorano<sup>1</sup>, Eduardo Malvacio<sup>1</sup>

<sup>1</sup> Laboratorio de Investigación en Técnicas Criptográficas y Seguridad Teleinformática. Facultad de Ingeniería del Ejército (FIE), Universidad de la Defensa Nacional – UNDEF.

<sup>2</sup> Departamento de Ciencia y Tecnología, Universidad Nacional de Quilmes UNQ.  
{marcelocipriano, egarcia, maiorano, emalvacio}@fie.undef.edu.ar

**Abstract.** Desde antaño, la *Criptografía* ha ofrecido mecanismos defensivos ofreciendo *Confidencialidad* a los mensajes. Incorporándose luego la *Autenticación e Integridad* a sus prestaciones. Pero esta disciplina ha comenzado a utilizarse maliciosamente. Aunque la mayoría de estas aplicaciones se enmarcan en el delito informático, una sustancial porción de ellas ha sido diseñada para atacar infraestructuras críticas de una nación y/o su instrumento de defensa: plantas de energía, oleoductos y sistemas militares afectan su *ciberdefensa*. Es relevante el desarrollo de esquemas anti-kleptográficos de generación de números aleatorios, funciones hash, algoritmos simétricos y asimétricos, libres de *puertas traseras criptográficas*. Es por ello que el proyecto "*Criptología Maliciosa para la Ciberdefensa*" (*CRIPTO-MC*) que se lleva adelante en el *Laboratorio de Informática, Software Seguro y Criptografía*, estudia las técnicas de *Criptografía Maliciosa* e indaga la creación de mecanismos de prevención y detección de los mismos, como contribución a la *Ciberdefensa Nacional*.

**Keywords:** Ciberdefensa, Criptografía Maliciosa, Criptovirología.

## 1 Introducción

Adam Young y Moti Yung [1] publican en 1996, 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. Lo que sí fue novedad es 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 la actualidad recibe el nombre de *ransomware*, aunque no fue creado recientemente. Tal como se ha mostrado, al menos conceptualmente, existe desde hace décadas.

Al año siguiente, los mismos autores presentan una nueva amenaza, que dieron en llamar *Kleptografía*. Esto es el diseño e implementación de *backdoors* o *puertas traseras* en algoritmos criptográficos [2-4]. En esa oportunidad, los autores presentan en particular, 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 pudieran

establecer sus claves criptográficas, a través 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 transparentes. 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 implementar 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].

Este ataque se limita a los esquemas de clave pública. Pero podría extenderse a los esquemas *simétricos* o de *clave privada*. La literatura científica da cuenta de ataques a algoritmos de *hash* también. 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 Resultados obtenidos / esperados

El proyecto de investigación persigue 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.

## Referencias

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 Schl  ffer. "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).