Ciberdefensa y los Usos Maliciosos de la Criptografía.

Cipriano, Marcelo[1,2] ; García, Edith[1], Maiorano, Ariel[1]
Malvacio, Eduardo[1], Pazo Robles, María Eugenia[1]

[1]Laboratorio de Informática, Software Seguro y Criptografía, 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; mepazorobles}@fie.undef.edu.ar

RESUMEN

Los objetivos principales del proyecto son el estudio, análisis, paradigmas y herramientas criptológicas modernas destinadas a la creación de software malicioso y puertas traseras criptográficas. Asimismo indagar mecanismos y metodologías que posibiliten la prevención, detección y protección para ser aplicadas en el ámbito de la Ciberdefensa Nacional.

La criptografía y todas sus aplicaciones (firma digital, autenticación, etc.) suele ser conocidas por ser de las más importantes herramientas de carácter defensivo. Los últimos años esa idea viene levemente cambiando hacia el sentido opuesto. Es decir que puede emplearse en aplicaciones ofensivas y maliciosas. Las más difundidas, al menos hasta ahora, son el secuestro, la pérdida de información y la extorsión. El responsable de llevar adelante tales actos, es una nueva clase de malware, conocida como *Ransomware.*

Otra aplicación, no tan conocida y de igual o mayor impacto aún, es el diseño e implementación de algoritmos criptográficos que incluyan las llamadas *Backdoors Cryptography* o puertas traseras criptográficas. Estas pueden vulnerar la confidencialidad, integridad y disponibilidad de la información que, en teoría, deberían proteger.

Son evidentes las graves consecuencias sobre la ciberseguridad de usuarios particulares, empresas y organismos no gubernamentales de tales ataques.

Mayor aún es el impacto que podrían tener sobre la protección de las Infraestructuras Críticas (IICC) de una sociedad, los sistemas de información y comunicación empleados en las fuerzas que defienden la nación, como así también la amenaza directa sobre la población.

Si las IICC están comprometidas, en forma directa o indirecta, entonces la vulnerabilidad trasciende a la ciberseguridad, sino que afecta directamente a la Ciberdefensa. Entendidas aquí a las IICC como 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.

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

CONTEXTO

El proyecto *"MAC: Criptografía Maliciosa para la Ciberdefensa"* perteneciente a la *Facultad de*

Ingeniería del Ejército (FIE) "Gral. Div. Manuel N. Savio", perteneciente a la *Universidad de la Defensa Nacional* (UNDEF).

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

Los investigadores conforman el *Grupo de Investigación en Criptología y Seguridad Informática (GICSI)* que pertenece al *Laboratorio de Informática, Software Seguro y Criptografía* y lleva adelante tareas de *I+D+i.*

El equipo está conformado por docentes investigadores categorizados en distintos regímenes científicos, profesionales técnicos y alumnos de las carreras antes mencionadas.

1. INTRODUCCIÓN

Suele reconocerse como instrumentos defensivos a la Criptografía cuando ofrece en sistemas de comunicaciones, redes y bases de datos -entre otros- confidencialidad, integridad y autenticación.

Pero esa visión demostró ser parcial, pues en 1996 *Adam Young* y *Moti Yung* [1] presentan lo que han dado en llamar *Criptovirología.*

Ellos demostraron la posibilidad convertir la criptografía en una herramienta de ataque. Asociada adecuadamente a un virus informático, se convierte en un poderoso vector de ataque. Primeramente se infecta el sistema mediante el virus informático. Una vez dentro del sistema, el virus activa su *payload* malicioso, cifrando la información de su víctima. Finalmente, muestra por pantalla un mensaje extorsivo, donde le pide al usuario que pague rescate si quiere recuperar la información así "secuestrada".

Lo que los autores estaban describiendo en aquel trabajo fundacional, era lo que hoy se conoce como *ransomware*[1] considerado un malware de alto impacto y profunda afectación de los sistemas que ataca.

En 1997, los mismos autores presentan la llamada *"Kleptografía*": esto es el diseño e implementación de *Backdoors Cryptography* o *Puertas Traseras* en A*lgoritmos Criptográficos* [2-4].

Para demostrar la viabilidad de la *Kleptografía* más allá de su concepción abstracta, los autores presentan a *"Secretly Embedded Trapdoor with Universal Protection", SETUP*.

Este *kleptograma* es una modificación a nivel matemático del algoritmo de intercambio de claves *Diffie-Hellman (DH),* considerada la mejor herramienta para resolver el problema de la *Distribución de Claves* que durante milenios estuvo sin solución.

¿Qué consecuencias acarrearían la aplicación de tales *técnicas kleptográficas* en otros algoritmos? Por mencionar algunos ejemplos: 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], entre otros.

Se podría asumir que la *Keptografía* se acota a la *Criptografía Asimétrica o de Clave Pública*. Sin embargo se encuentran publicadas funciones hash. Por ejemplo una versión de *SHA-1* modificado[7].

También se pueden hallar alternativas para protección de funciones hash comprometidas en algoritmos de nivel superior, como *HMAC* y *HKDF* [14].

[1] Ransom: rescate en inglés.

Tampoco quedan indemnes los generadores de números seudo-aleatorios, conocidos como *Pseudo Random Numbers Generators* o *PRNG* [10-13]. A rasgos generales, se inserta una vulnerabilidad en el núcleo de la primitiva criptográfica, que afecta las propiedades estadísticas de tales generadores.

La seguridad de los esquemas criptográficos se mide tradicionalmente, entre otras consideraciones, como la incapacidad de un adversario de violar un objetivo de seguridad deseado, al contar con ciertas limitaciones en sus recursos [14].

Se observa que este argumento de seguridad se basa en un diseño sólido de los componentes subyacentes a los que un adversario no tiene acceso para afectar o influir. Si estas consignas no se satisfacen, es decir que un adversario pueda influir en el diseño de un algoritmo aplicando *Kleptografía*, entonces las consecuencias devastadoras de tal acción, resultan evidentes[16,17].

Peor aún, el daño que podría ocasionar si tal algoritmo, además, fuera estandarizado mediante alguna norma y/o adoptado por algún protocolo o aplicación.

Nadie puede aseverar que este escenario aquí propuesto es sólo una presunción realizable a futuro, o una realidad presente.

2. LÍNEAS DE INVESTIGACIÓN y DESARROLLO

El proyecto sigue 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 seudo-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 persigue estudiar y analizar la aplicación de los paradigmas y herramientas en la creación de software malicioso y puertas traseras criptográficas, para así poder desarrollar técnicas de prevención, detección y protección para ser considerados en el ámbito de la Ciberdefensa Nacional.

4. FORMACIÓN DE RECURSOS HUMANOS

Los docentes del equipo de investigación dictan distintas asignaturas en las carreras de grado y posgrado en FIE. Y desde dichas cátedras se invita de forma permanente a los alumnos para participar como colaboradores.

Se han incorporado al equipo algunos alumnos de la especialización en *Criptografía y Seguridad*

Teleinformática (Ciberseguridad) que están llevando a cabo su *Trabajo Final Integrador (TFI)* como así también alumnos de la *Maestría en Ciberdefensa*, que se encuentran trabajando en el desarrollo de sus respectivas tesis. En ambos casos se abordan temáticas afines a la de este proyecto.

Se espera que la contribución mutua entre el equipo de investigadores, especializandos 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 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 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).