Software Abierto para la Evaluación de Sistemas Criptológicos Integrados

Cipriano, Marcelo[1]; Malvacio, Eduardo; Estevez[2], Carlos; Fernández, Darío García, Edith[1], López, Gabriel; Liporace, Julio[1]; Maiorano, Ariel[1] Vera Batista, Fernando[1]

[1]Laboratorio de Investigación en Técnicas Criptográficas y Seguridad Teleinformática. Escuela Superior Técnica, Facultad del Ejército. Universidad de la Defensa Nacional - UNDEF
[2] Instituto de Investigaciones Científicos y Técnicas para la Defensa – CITEDEF.-)

{marcelocipriano; dfernandez; verabatista}@est.iue.edu.ar
{edithxgarcia; jcliporace; maiorano; edumalvacio}@gmail.com

RESUMEN

Es permanente la evaluación de la seguridad que debe llevarse a cabo en los sistemas de información, en la actualidad. Facilitar esta tarea tiene un alto impacto, así sea en la calidad de la seguridad del sistema, como en el aspecto económico de la misma al aumentar las herramientas de gestión de la seguridad, como así también un aporte a la reducción del tiempo de evaluación.

Este proyecto persigue el diseño y desarrollo de una herramienta que permita llevar adelante la automatización de tales análisis y la realización de pruebas que permitan realizar el estudio de manera veloz y eficiente.

Los usos de esta herramienta tiene aplicaciones DUAL, es decir puede destinarse para usos en el ámbito militar como también en el civil para ser aplicado en sectores gubernamentales, empresariales, educativos o privados.

La modalidad de Código Abierto o FOSS (por siglas en inglés de Free Open Source Software) permite y facilita la amplia difusión de los usos y aplicaciones de esta herramienta.

La evaluación de la seguridad implementada en un determinado sistema informático se ve ayudada por esta herramienta al permitir análisis estadístico de secuencias binarias para aplicar en algoritmos de Cifrado de Flujo (Stream Ciphers) y Generadores Pseudaleatorios de Números (Pseudo Random Numbers Generators) y de la Complejidad Lineal. Tales secuencias pueden ser generadas por LFSRs (Linear Feedback Shift Registers), NLFSRs (Non-Linear Feedback Shift Registers), CCGs (Clock Controlled Generators), protocolos de seguridad de la información, programas o dispositivos para la Generación de Claves, Block Ciphers y demás algoritmos aplicados en entornos de Software como de Hardware.

Palabras Clave

Criptología, Criptoanálisis. Stream Ciphers.

CONTEXTO

En el marco de la carrera de grado de Ingeniería en Informática y el posgrado en Criptografía y Seguridad Teleinformática que se dictan en la *Escuela Superior Técnica "Gral. Div. Manuel N. Savio" (EST)*, dependiente de la *Facultad del Ejército, Universidad de la Defensa Nacional (UNDEF)* se llevan adelante tareas de I+D+i por parte del *Grupo de Investigación en Criptología y Seguridad Informática (GICSI).*

GICSI depende del *Laboratorio de Investigación en Técnicas Criptográficas y Seguridad Teleinformática (CriptoLab)* perteneciente al *Laboratorio Informática (InforLab).* Y está conformado por docentes investigadores, profesionales técnicos y alumnos de dicha área.

Esta línea de investigación aquí presentada corresponde a un proyecto que fue presentado, evaluado, aprobado y financiado en su integridad por la Universidad de la Defensa Nacional a través de su Programa UNDEFI, cuyos objetivos son:

- Fomentar estrategias colaborativas que incentiven la cooperación e integración transversal de las Facultades en investigación.
- Reconocer y potenciar capacidades de investigación existentes favoreciendo la interrelación entre grupos.
- Profundizar los esfuerzos institucionales dirigidos a la formación y perfeccionamiento de los recursos humanos para la investigación

1. INTRODUCCIÓN

Las comunicaciones del siglo XXI precisan de más y mejores algoritmos de cifrado, de autenticación y de integridad de la información que posibiliten la confidencialidad e integridad de las comunicaciones.

El aumento en los últimos tiempos en el empleo de Internet en general y el advenimiento en particular de las tecnologías de VoIP (voz sobre IP), Teleconferencias, VideoStreaming, VideoOnDemand y los Sistemas Móviles han incrementado la necesidad de asegurar estos servicios.

Los mecanismos de seguridad deben satisfacer las necesidades particulares de cada una de estas tecnologías, como por ejemplo las demandas de altas Tasas de Transmisión de Información, entornos de trabajo con recursos limitados de cálculo, memoria, energía y espacio, entre otros.

Las modernas técnicas criptológicas se han ido adaptando a estas necesidades que dieron nacimiento a llamada Criptografía Ligera o Liviana[1] . Es por ello que desde hace varios años muchos han sido los algoritmos que investigadores, universidades y empresas han dado a conocer a la comunidad científica y al público en general.

El estudio y análisis de las propiedades matemáticas de los Generadores de Secuencias Pseudorandom generadas por:

- Substitution Boxes (S-BOXs) creadas para los modernos Block Ciphers[2].
- Stream Ciphers -en particular a aquellos algoritmos que involucran LFSRs (Linear Feedback Shift Registers).[3]
- NLFSRs (Non Linear Feedback Shift Registers)[4-6].
- CCG (Clock Controlled Generators)
- Autómatas Celulares
- Generadores de Números Pseudoaleatorios permite evaluar sus propiedades criptológicas a fin de poder identificar el nivel de robustez y seguridad de dichos algoritmos.

Muchas de las propiedades matemáticas y específicamente criptológicas se encuentran ocultas detrás del algoritmo. Esto quiere decir que al observar un algoritmo los autores describen con detalle el funcionamiento del mismo por medio de gráficos y demás especificaciones para “seguir la danza de los bits” y muchas veces las explicaciones técnicas más profundas no son abordadas tan en detalle y son parcialmente expuestas. Los investigadores deben profundizar en cada algoritmo y mediante su estudio, deducir sus propiedades.

A su vez en el ciclo de vida del algoritmo se encuentra una etapa que corresponde a los ataques a los que ha sido sometido. Muchas veces esos ataques son exitosos y van apareciendo vulnerabilidades. Otras veces es el estudio analítico y en detalle el que permite detectarlas. Muchas de ellas son resueltas con el advenimiento de versiones mejoradas de los mismos [7].

Es por ello que la permanente evolución de los algoritmos debe ir acompañada de la actualización de las pruebas y de-

más procesos que permitan evaluar la seguridad de los mismos.
Muchos algoritmos criptográficos fueron reconocidos por una norma internacional, como ser ISO (International Organization for Standardization y IEC (International Electrotechnical Commission), conocidas como normas ISO/IEC:

- ISO/IEC18033-3:2005 llamada "Information Technology. Security Techniques. Encryption Algorithms. Part 3: Block Ciphers" Algoritmos de Cifrado en Bloques (Block Ciphers) de 64 bits: TDEA, MISTY1, CAST-128, HIGHT. De 128 bits: AES, Camellia, SEED. [8]
- ISO/IEC 29192-3:2012 "Information Technology. Security Techniques. Lightweight Cryptography. Part 3: Stream ciphers". Algoritmos de Cifrado en Cadena (Stream Ciphers) Enocoro y Trivium.[9]
- ISO/IEC 18033-4:2011 "Information Technology. Security Techniques.Encryption Algorithms. Part 4: Stream Ciphers" presenta 5 algoritmos de Cifrado de Flujo: Decim-v2., KCipher-2 (K2), MUGI, Rabbit, SNOW 2.0. [10]

Aunque bienvenido, este renacimiento mundial por la búsqueda de nuevos algoritmos por sí sólo resulta insuficiente a la hora de establecer parámetros criptográficos seguros.
En la actualidad no existe una única modalidad general de criptoanálisis. Cada algoritmo, cada primitiva, cada protocolo debe ser atacado mediante una técnica adecuada a su estructura, si es que sus diseñadores atendieron a la necesidad de resistir los ataques conocidos.
El criptoanálisis tiene un impacto significativo en el mundo real, puesto que los algoritmos criptológicos, los protocolos y también los tamaños de las claves entre otros, son seleccionados basándose en el estado del arte del criptoanálisis.

2. LÍNEAS DE INVESTIGACIÓN y DESARROLLO

Se ha dado en planificar este proyecto de investigación siguiendo 5 etapas:

a) Investigación bibliográfica acerca de las técnicas de ataque criptoanalíticas conocidas y más difundidas.
b) Estudio de factibilidad acerca del grado de automatización que requieren.
c) Determinación de la metodología a automatizar.
d) Elaboración de los módulos del programa y sus pruebas.
e) Integración de los módulos en un marco general.

Los indicadores de avance previstos para el proyecto son:

a) Identificación y selección de las herramientas matemáticas para la elaboración del software.
b) Desarrollo de los módulos respectivos.
c) Pruebas de los módulos.
d) Integración en la aplicación final.

3. RESULTADOS OBTENIDOS / ESPERADOS

Se espera diseñar y desarrollar un software abierto que permita la evaluación de las propiedades criptográficas y de seguridad de secuencias pseudoaleatorias binarias procedentes de algoritmos criptográficos del tipo Stream Ciphers, Block Ciphers o Generadores de Números Seudoaleatorios.
El enfoque propuesto para el desarrollo se centra en el estudio e implementación de las diferentes técnicas criptoanalíticas aplicables de acuerdo a la bibliografía, su conjunción y el desarrollo de un conjunto de herramientas que permitan analizar las propiedades criptológicas.
Más allá del conocimiento que el equipo investigador obtenga de la realiza-

ción de este proyecto, se espera que el software que se desarrolle pueda ser empleado por:

- Administradores de Red que deseen probar la afectividad y seguridad de algoritmos criptográficos para su posterior uso.
- Investigadores que trabajen sobre vulnerabilidades en criptosistemas
- Organismos de Seguridad Informática.
- Docentes del área de Seguridad Informática y Criptografía para que puedan anexar esta herramienta al dictado de sus respectivas cátedras.

4. FORMACIÓN DE RECURSOS HUMANOS

Los docentes investigadores participantes del proyecto dictan las asignaturas *Criptografía y Seguridad Teleinformática, Matemática Discreta y Paradigmas de Programación I, II.* Desde esas cátedras se invita a los alumnos a participar en los proyectos de investigación. Es por ello que los alumnos *Cabrera Ezequiel* y *Dorado Mariano* forman parte del proyecto y próximamente se sumarán 2 alumnos, cuando UNDEF apruebe su incorporación. En particular los tres últimos serán postulantes para la beca "Estímulo a las Vocaciones Científicas" (EVC) otorgadas por el Consejo Interuniversitario Nacional (CIN) por encuadrarse en las condiciones pedidas.

Asimismo este proyecto tiene una importante impronta para la formación de recursos humanos pues a los 6 investigadores con experiencia se les suman 2 investigadores que recién inician su experiencia.

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] https://www.nist.gov/programs-projects/ lightweight-cryptography consultada el 10-3-18.

[2] Daemen, J.; Rijmen, V.*; The Design of Rijndael: AES - The Advanced Encryption Standard*. Springer. New York. 2002.

[3] Muller F., Peyrin T. *Linear Cryptanalysis of the TSC Family of Stream Ciphers.* Roy B. (eds.) Advances in Cryptology - ASIACRYPT 2007. Lecture Notes in Computer Science, vol. 3788. Springer, Berlin, Heidelberg. 2005.

[4] Wu H., Preneel B. *Differential Cryptanalysis of the Stream Ciphers Py, Py6 and Pypy*. Naor M. (eds.) Advances in Cryptology. EUROCRYPT 2007. Lecture Notes in Computer Science, vol. 4515. Springer Berlin, Heidelberg. 2007.

[5] Pasalic, E.; *On Guess and Determine Cryptanalysis of LFSR-Based Stream Ciphers*; IEEE Transactions on Information Theory. Vol.55 Ed.7º, 2009.

[6] Ding C.; *The differential cryptanalysis and design of natural stream ciphers*. In: Anderson R. (eds.) Fast Software Encryption. FSE 1993. Lecture Notes in Computer Science, vol. 809. Springer Berlin, Heidelberg.

[7] Dinur I., Shamir A. *Cube Attacks on Tweakable Black Box Polynomials*. Advances in Cryptology - EUROCRYPT 2009. Lecture Notes in Computer Science, vol 5479. Springer, Berlin, Heidelberg. 2009.

[8]https://www.iso.org/standard/37972 .html consultada el 12-3-18.

[9] https://www.iso.org/standard/59948 .html cunsultada el 12-3-18.

[10] https://www.iso.org/standard/ 54532.html consultada el 12-3-18.