Optimización de las fórmulas para la detección de Infraestructuras de Clave Pública anómalas.

Castro Lechtaler, Antonio[1, 2]; Cipriano, Marcelo[1]; Malvacio, Eduardo[1];
Dulio, Nicolás[1]; Pérez, Pablo[1]

[1]Laboratorio de Investigación en Técnicas Criptográficas y Seguridad Teleinformática.
Escuela Superior Técnica, Facultad de Ingeniería. Instituto Universitario del Ejército.
[2] CISTIC/FCE - Universidad de Buenos Aires.

acastro@est.iue.edu.ar , marcelocipriano@est.iue.edu.ar, edumalvacio@gmail.com
nico_n44@hotmail.com

1. Resumen.

Este proyecto de investigación persigue elaborar un software de auditoría que permite detectar comportamientos anómalos en una Infraestructura de Clave Pública (Public Key Infrastructure: PKI por sus siglas en inglés) en lo concerniente a la calidad de los números primos en los certificados emitidos por la entidad.

Dada la imposibilidad de abarcar todo el universo de certificados posibles que una PKI puede emitir, se llevará adelante un análisis estadístico de un conjunto de muestras formadas por certificados entregados, basado en las propiedades matemáticas de la densidad y distribución de números primos de determinado tamaño.

La existencia de sesgos o problemas en la generación y/o selección de los números primos que constituyen a cada certificado, puede devenir en vulnerabilidades susceptibles de ser explotadas. Afectando de esta manera el control de acceso al sistema, el intercambio de claves para sesiones seguras, problemas con la autenticación de usuarios, mensajes y equipos, etc.

El estudio y análisis de las propiedades matemáticas involucradas y la determinación de criterios adecuados a la detección del comportamiento anormal permitirán desarrollar un software auditor de PKI.

Al día de hoy no existen fórmulas que generen números primos ni se conoce con exactitud la forma en que dichos números se distribuyen. Asimismo la cantidad de dichos números y el tamaño de los mismos agregan un componente complejo al problema. Y ello sin mencionar la dificultad computacional para realizar cálculos precisos con ellos.[1]

Palabras Clave:

Seguridad en Redes, Infraestructura de Clave Pública, PKI, Detección de Anomalías, Open-SSL, RSA.

2. Contexto.

El CriptoLab (Laboratorio de Investigación en Técnicas Criptográficas y Seguridad Teleinformática) pertenece a la Escuela Superior Técnica "Gral. Div. Manuel N. Savio" (EST), Facultad del Ejército, Universidad Nacional de la Defensa (UNDEF) en el área de la carrera de grado de Ingeniería en Informática y el posgrado en Criptografía y Seguridad Informática que se dictan en esta institución.

[1]Calcular n! con n del orden de 2048 bits, por ejemplo.

Las Fuerzas Armadas en general como el Ejército en particular destinan recursos a la investigación y el desarrollo científico-tecnológico por ser considerados relevantes a nivel estratégico.

En particular, el Instituto de Investigaciones Científicas y Técnicas para la Defensa (CITEDEF) realizó aportes a través de Proyectos de Investigación Científico Tecnológicos Orientados (PICTO) para la realización durante 6 años del proyecto recientemente finalizado sobre "REDES PRIVADAS COMUNITARIAS".

En el marco de dicho proyecto se pudo realizar parte de esta investigación. Los resultados parciales o finales han sido presentados en varios CACIC (Congreso Argentino de Ciencias de la Computación) para su difusión y consideración de la comunidad científica.

Dentro de la EST esta línea de investigación se lleva adelante bajo el nombre de VULCLAP: Vulnerabilidades en Clave Pública.

CITEDEF y el Consejo Profesional de Ingeniería de Telecomunicaciones, Electrónica y Computación (COPITEC) dieron su aval por escrito para este proyecto, dado su interés en ser aplicado en sus propios sistemas y redes.

3. Introducción.

Los sitios de internet pueden autenticarse por medio de certificados digitales. De manera parecida los sistemas pueden componer una estructura que permita ese servicio y otros. Tal subsistema recibe el nombre de Infraestructura de Clave Pública (PKI).

Existen PKI de código abierto y libre e incluso algunas tienen licencia de uso gratuita.

¿Se puede comprobar si estos procesos y servicios contienen errores que pueden minar la seguridad? [1].

Una manera de hacerlo es acceder a su código fuente y revisar todas las líneas de programación y analizar su comportamiento. Está clara la complejidad de tal tarea y la dificultad (o imposibilidad, al menos hasta ahora) de automatizarlo.

Otra manera es el software que se lograría con el progreso de esta línea de investigación.

La filosofía del código abierto (open source) y la ley de Linux [2] por sí mismas no garantizan la ausencia de errores. Un ejemplo es el bug descubierto por Luciano Bello en OpenSSL2 de Debian. Pasaron 20 meses desde que la versión defectuosa fuera informada [3] hasta que se publicó un parche. Y este no es el único ejemplo. Recientemente han sido detectados problemas de seguridad en SSL/TSL en el iOS7 de Apple y GnuTSL de Linux, entre otros.[3]

Si una PKI generase un conjunto sesgado de números primos para emitir sus certificados, entonces un atacante podría vulnerar la seguridad de dicho sistema.

Lenstra y otros [4], han hallado repetición de los números primos en el 5% de una gran muestra de certificados digitales de 1024 bits. Si se repiten los primos, entonces tales certificados son vulnerables.

4. Líneas de Investigación, Desarrollo e Innovación.

Se pudo determinar una fórmula, con la que se elaboró una herramienta informática, que permite hallar los primos que

[2] Una mala inicialización de una variable provocó una predictibilidad en el generador de números, abriendo una vulnerabilidad inimaginable.

[3] http://www.securitynull.net/

componen un módulo RSA con la información que aportan su clave pública y privada [5].

Las posteriores pruebas de codificación e implementación demostraron que este procedimiento corría muy veloz [6].

Se comparó el rendimiento del mismo con el procedimiento existente en la bibliografía tradicional para la enseñanza de la criptografía [7].

Los análisis indicaron que la complejidad computacional del algoritmo era del orden O (log n) mientras que el de la bibliografía de referencia tenía un orden O (log3 n) [8].

Se elaboró la herramienta matemática que permitiría detectar anomalías [9].

Se realizó un abordaje probabilístico del problema [10] y por último el diseño final de la herramienta probabilística y estadística [11-13]

Simultáneamente al avance matemático se ensamblaron y codificaron todas las herramientas matemáticas antes mencionadas, en una plataforma de software programado en C++.

5. Resultados y Objetivos.

Se llevaron adelante pruebas por muestras o lotes, evaluándose 80.000.000 de módulos agrupados en 80000 lotes de 1000 cada uno.

Actualmente se está tratando de mejorar la fórmula matemática del modelo estadístico pues se necesita computar enormes factoriales y su resolución es, hasta ahora, muy costosa computacionalmente hablando.

Concluido este paso, se simularán diferentes PKI´s con vulnerabilidades y sin ellas. Cada una será testeada por la herramienta de auditoría en elaboración. El comportamiento esperado es que detecte las vulnerables e informe al respecto.

Se elaboró una plataforma de computación distribuida a los efectos de acelerar la investigación.

6. Formación de Recursos Humanos.

Desde el año 2012 algunos algoritmos que utilizamos en esta investigación fueron codificados y probados en el contexto de la Cátedra de Computación I a cargo del Ing. Mg. Alejandro Repetto, que posee nuestra facultad en la carrera de Ingeniería Informática.

Desde el año 2013 un equipo de docentes y alumnos del Centro de Investigación y Desarrollo de Software del Ejército Argentino (CIDESO) trabaja en el diseño y elaboración de una plataforma de computación distribuida para que se pueda emplear en problemas de criptología a los que se dedica el CriptoLab y se han publicado sus resultados [12, 14].

Durante el año 2015 se han sumado al proyecto dos alumnos de 4to año de la carrera de Ingeniería Informática. Uno de ellos es Pablo Pérez como alumno ayudante y Nicolás Dulio que ha recibido la beca Estímulo a las Vocaciones Científicas, perteneciente al Programa Estratégico de Investigación y Desarrollo, Plan de Fortalecimiento (Componente de Formación de Recursos Humanos) del Consejo Interuniversitario Nacional.

7. Referencias

[1] Young A and Yung M. *An Elliptic Curve Asymmetric Backdoor in Open-SSL RSA Key Generation.* Chapter 10. Cryptovirology. 2006.

http://www.cryptovirology.com.

[2] Glass, Robert *"Facts and Fallacies of Software Engineering*". Addison-Wesley Professional, 2003.

[3] Bello L, Bertacchini M. *"Generador de Números Pseudo-Aleatorios Predecible en Debian"*. III Encuentro Internacional de Seguridad Informática. Manizales, Colombia. Octubre 2009.

[4] Lenstra, A; Hughes, J; Augier, M y otros. Ron was wrong, Whit is right. e-print International Association for Cryptologic Research. 15 Feb 2012

http://eprint.iacr.org/2012/064,

[5] Cipriano, M. "Factorización de N: recuperación de factores primos a partir de las claves pública y privada." XIV Congreso Argentino de Ciencias de la Computación CACIC 2008. Chilecito, La Rioja, Octubre 2008.

[6] Castro Lechtaler, C; Cipriano, M; Benaben A; Quiroga, P. *"Study on the effectiveness and efficiency of an algorithm to factorize N given e and d*". IX Seminario Iberoamericano en Seguridad de las Tecnologías de la Información, La Habana, CUBA. 2009.

[7] Menezes, A; van Oorschot, P and Vanstone, S. *Handbook of Applied Cryptography*. CRC Press. 5th Edition, 2001.

[8] Benaben, A; Castro Lechtaler, A; Cipriano, M; Foti, A. *"Development, testing and performance evaluation of factoring algorithms whit additional information*" XXVIII Conferencia Internacional de la Sociedad Chilena de Computación. Santiago de Chile. 2009.

[9] Castro Lechtaler, A; Cipriano, M. "*Detección de anomalías en Oráculos tipo OpenSSL por medio del análisis de probabilidades*". XVII Congreso Argentino de Ciencias de la Computación CACIC 2011. La Plata, Buenos Aires, Octubre 2011.

[10] Castro Lechtaler, Antonio, Cipriano Marcelo; Malvacio Eduardo; Cañón, Sebastián; *Procedure for the Detection of Anomalies in Public Key Infrastruture (RSA Systems)*. XIII Simposio Argentino de Tecnología, 41 Jornadas Argentinas de Informática e Investigación Operativa JAIIO – SADIO. La Plata, Buenos Aires, Agosto 2012.

[11] Castro Lechtaler, Antonio; Cipriano, Marcelo; Malvacio, Eduardo. *Experimental detection of anomalies in public key infrastructure*. XVIII Congreso Argentino de Ciencias de la Computación CACIC 2012. Bahía Blanca, Buenos Aires, Octubre 2011.

[12] Castro Lechtaler, A; Repetto, A; Bianchi, O; Cipriano, M; Arroyo Arzubi, A; Cicerchia, C; Malvacio, E. *ULTRACOM: Computación de alto rendimiento para criptoanálisis*. XX Congreso Argentino de Ciencias de la Computación, La Matanza, Buenos Aires, 2014.

[13] Castro Lechtaler, Antonio; Cipriano, Marcelo; Malvacio, Eduardo. *Probabilidades de referencia para aplicar en la detección de Infraestructuras de Clave Pública anómalas* XXI Congreso Argentino de Ciencias de la Computación, Junín, Buenos Aires, 2015.

[14] Castro Lechtaler, A; Repetto, A; Bianchi, O; Cipriano, M; Arroyo Arzubi, A; Cicerchia, C; Malvacio, E. *Computa-ción en grilla de escritorio para evalua-ción de algoritmos criptográficos. XVII* Workshop de Investigadores en Ciencias de la Computación, Salta, 2015.