CRIPTOGRAFÍA POST-CUÁNTICA INTEGRADA EN SSL/TLS Y HTTPS

Diego Cordoba [1], Miguel Méndez-Garabetti[2]

[2] Univerisdad de Mendoza, Dirección de Posgrado, Facultad de Ingeniería
diego.cordoba@um.edu.ar, miguel.mendez@um.edu.ar

[1]Universidad de Mendoza, Facultad de Ingeniería, Subsede San Rafael

RESUMEN

La adopción del protocolo HTTPS para brindar seguridad a gran parte del tráfico web de Internet pone el foco en los algoritmos de cifrado que proveen las implementaciones de SSL/TLS.

La capacidad de cómputo de los ordenadores actuales permite concluir que algoritmos asimétricos como RSA son seguros. No obstante, estos mecanismos son vulnerables al criptoanálisis cuántico, por lo que disponer de una computadora cuántica pondría en peligro la seguridad de los datos cifrados con algoritmos asimétricos como RSA.

La computación cuántica es un hecho, y que es cuestión de tiempo para que se fabriquen computadoras cuánticas de cientos de qubits, por lo que es necesario encontrar alternativas a los algoritmos de cifrado y autenticación clásicos. La criptografía postcuántica cubre esta necesidad proveyendo una serie de algoritmos resistentes a ataques cuánticos. Existen proyectos que aportan librerías de desarrollo bajo licencias de código abierto. OQS provee una librería de algoritmos resistentes, y su integración en protocolos y aplicaciones como OpenSSL, una de las implementaciones de SSL/TLS de código abierto más utilizadas.

El presente trabajo de investigación analiza la integración de estas implementaciones de OpenSSL en el servidor web Apache2 para brindar un servicio HTTPS resistente a ataques cuánticos.

Palabras clave: criptografía; post cuántico; seguridad informática; criptografía asimétrica

CONTEXTO

El presente trabajo de I+D se desarrolla como proyecto se tesis de posgrado de la Maestría en Teleinformática, Dirección de Posgrado, perteneciente a la Facultad de Ingeniería de la Universidad de Mendoza, (Ciudad, Mendoza). El presente proyecto fue presentado como propuesta de tesis.

1. INTRODUCCIÓN

En la actualidad las comunicaciones en Internet, particularmente en el tráfico web, tienden a ser cifradas para mantener la confidencialidad de los datos del usuario, y la autenticación e integridad de los mismos entre los nodos que conforman el enlace. El incremento de adopción del protocolo HTTPS (HTTP over SSL/TLS) [1] marca tendencia, y algunos navegadores como Chrome o Firefox comienzan a advertir cuando los sitios accedidos no son seguros [2] [3] e incluso los buscadores en Internet comienzan a tener en cuenta el uso de HTTPS en el posicionamiento [4].

SSL/TLS le brindan a HTTP algoritmos de autenticación basados en certificados digitales X.509 y criptografía asimétrica. La criptografía asimétrica se basa en algoritmos matemáticos fundamentados en supuestos de complejidad computacional, es decir, problemas matemáticos muy simples de calcular, pero extremadamente difícil de revertir. De esta manera la generación de claves asimétricas, por ejemplo, pueden llevarse a cabo con operaciones denominadas "de una sola vía", tales como la multiplicación de dos números primos grandes. El producto de estos dos números primos es relativamente sencillo de computar para un procesador actual, pero encontrar estos dos números primos que dieron origen al producto resulta sumamente difícil aplicando algoritmos de fuerza bruta con las capacidades de cálculo actuales. Si a esto se agrega que las claves de cifrado y autenticación asimétrica suelen cambiar periódicamente dependiendo de la implementación de SSL/TLS que se utilice, y/o su configuración, podría decirse que romper un cifrado asimétrico de clave grande resulta, al día de hoy, prácticamente imposible para un atacante que necesita conseguir la clave de cifrado en un tiempo limitado.

Por otro lado, una computadora cuántica podría encontrar la clave de cifrado de manera relativamente rápida, y vulnerar, de esta forma, cualquier tráfico cifrado y autenticado con mecanismos basados en criptografía asimétrica.
El primer algoritmo cuántico no trivial que demostró un potencial de crecimiento exponencial de velocidad sobre los algoritmos clásicos fue el algoritmo de Shor [5]. Este algoritmo permite descifrar un mensaje encriptado mediante RSA [6] descomponiendo en factores la clave pública, que es producto de dos números primos grandes, en un tiempo $O((\log N)^3)$, siendo N el numero primo que representa la clave pública. Por su parte, los algoritmos clásicos no pueden realizar dicha factorización en un tiempo menor a $O((\log N)k)$ para ningún k, por lo que RSA sigue siendo considerado, en la actualidad, un algoritmo seguro [7] [8].
El algoritmo de Shor, al ser un algoritmo cuántico, permite obtener el resultado de manera probabilística y con un determinado grado de acierto de acuerdo a la cantidad de iteraciones a la que se lo someta. En la práctica Isaac Chuang en diciembre de 2001, liderando un grupo de trabajo de computación cuántica de IBM, logró factorizar el número 15 mediante una computadora cuántica de 7 qubits, y en marzo de 2016 un grupo de investigadores del MIT, entre los que se encontraba el mismo Chuang, también pudo factorizar el numero 15 con un 99% de certeza en una computadora cuántica de 5 qubits.

La aparición de las primeras computadoras cuánticas de cientos de qubits dejará obsoletos a la mayoría de los algoritmos asimétricos actuales, tales como RSA, DSA o ECDSA [7] [9] [10] [11].

Afortunadamente existen algoritmos asimétricos que hacen uso de mecanismos que son invulnerables al criptoanálisis cuántico. Estos algoritmos definen la criptografía post-cuántica, o criptografía resistente a ataques cuánticos, son considerados seguros y a ninguno de ellos se le ha podido aplicar el algoritmo de Shor.

Los algoritmos post-cuánticos pueden clasificarse en [7]:

1. *Criptografía basada en hash*, que incluye sistemas criptográficos como las firmas de Lamport y el esquema de firmas de Merkle.

2. *Criptografía basada en código*, que incluye el esquema de firmas de McEliece y códigos aleatorios Goppa [12].

3. *Criptografía basada en sistemas de ecuaciones multivariable*, que incluye el esquema Rainbow [13].

4. *Criptografía basada en enrejado*, que incluye algoritmos de intercambio de claves de aprendizaje con errores, NTRU [14] y BLISS [15].

5. *Criptografía simétrica basada en clave secreta de Rijndael*, más conocido como AES (Advanced Encryption Standard).

Para poder llevar a la práctica estos algoritmos es necesario que las implementaciones de protocolos SSL/TLS los soporte. Uno de los proyectos que se mantiene más activo en este aspecto es OQS – Open Quantum Safe [16].

El objetivo de OQS es dar soporte al desarrollo y *prototipado* de implementaciones de algoritmos resistentes a ataques cuánticos. Para ello desarrollaron liboqs, una biblioteca de algoritmos post-cuánticos en lenguaje C, y que sirve de API para utilizar dichos algoritmos, y está liberada bajo licencia de código abierto del MIT. OQS mantiene dos ramas de liboqs, la rama master, y la rama NIST. La rama master está enfocada en algoritmos seleccionados de encapsulamiento de claves y firma digital, y tiene determinados criterios de aceptación de las implementaciones. Por su parte, la rama NIST se centra en incorporar algoritmos remitidos al proyecto de estandarización de criptografía postcuántica del NIST [17]. Además, el proyecto OQS provee encapsulamientos / wrappers para lenguajes específicos como C#, C++ y Python.

Además de desarrollar y mantener liboqs, el proyecto OQS también realiza tareas de integración de su biblioteca en algunos protocolos e implementaciones de código abierto que pasan a beneficiarse con la incorporación de algoritmos postcuántico. Tal es el caso de OpenSSL, una de las implementaciones de SSL/TLS de código abierto más utilizadas actualmente, otorgándole al desarrollo los mecanismos resistentes a ataques cuánticos para la autenticación y el intercambio de claves.

Ademas, la biblioteca liboqs ha sido utilizada por proyectos de terceros, como ser la VPN postcuántica experimental de Microsoft, basada en OpenVPN [18], o el cliente beta de VPN de Mullvad [19], que utiliza intercambio de claves postcuántico.

2. LINEAS DE INVESTIGACIÓN Y DESARROLLO

Los algoritmos de cifrado, autenticación e intercambio de claves postcuánticos tienen una gran cantidad de aplicaciones en diferentes herramientas que hagan uso de criptografía asimétrica clásica.
Particularmente en este trabajo se lleva a cabo un análisis de la bibliografía existente, y las principales implementaciones de algoritmos resistentes a ataques cuánticos, y se centra el foco de atención el la librería liboqs del proyecto OQS, y las implementaciones de OpenSSL provistas por el proyecto que integran esta librería.
Los aspectos que se pretenden desarrollar con la presente investigación incluyen:

1. Analizar y documentar los algoritmos de cifrado, autenticación e intercambio de claves resistentes a ataques cuánticos disponibles en la actualidad.
2. Estudiar y realizar pruebas de concepto con las librerías de cifrado que soporten algoritmos postcuánticos, específicamente la librería liboqs del proyecto OQS, tanto en la rama master como en la rama NIST.
3. Compilar la suite OQS-OpenSSL tanto en la versión 1.1.1-stable como en la versión 1.0.2-stable (ambas liberadas en Noviembre de 2018) utilizando las bibliotecas liboqs de la rama master y nist, y realizar pruebas de concepto y conectividad cliente-servidor local.
4. Realizar pruebas de conectividad y negociación TLS de los algoritmos postcuánticos o híbridos para intercambio de claves provistos por la versión OQS-OpenSSL v1.1.1-stable (para TLS v1.3) y v1.0.2-stable (para TLS1.2).
5. Realizar la compilación de la última versión del servidor web Apache2 httpd (v2.4.38) junto con su módulo SSL/TLS, y realizar pruebas de concepto de conectividad, renegociación de *cipher suites* e intercambio de claves para ambas versiones de OQS-OpenSSL.
6. Realizar pruebas de carga tanto en las implementaciones de OQS-OpenSSL como en el servicio HTTPS de Apache2, respecto del establecimiento de conexiones cifradas y el intercambio de claves, y medir el rendimiento de los algoritmos postcuánticos comparado con el rendimiento de los algoritmos tradicionales provistos por OpenSSL.

3. RESULTADOS OBTENIDOS/ ESPERADOS

Al momento de publicar este artículo se han llevado a cabo satisfactoriamente las siguientes pruebas:

1. Compilación, configuración y puesta en marcha de OQS-OpenSSL-1.0.2-stable con liboqs rama nist.
2. Compilación, configuración y puesta en marcha de OQS-OpenSSL-1.1.1-stable con liboqs rama master.
3. Ejecución exitosa del comando de prueba de rendimiento *speed* de la suite OpenSSL, tanto para la v1.1.1-stable como para la v1.0.2-stable provistas por OQS.
4. Generación de claves asimétricas y certificados digitales X.509 haciendo uso de algoritmos asimétricos resistentes a ataques cuánticos.
5. Compilación, configuración y puesta en marcha del servidor web Apache2 con el módulo SSL/TLS compilado en base a la implementación OQS-OpenSSL v1.0.2-stable provista por el proyecto OQS.

Las pruebas realizadas sobre la versión v2.4.38 de Apache combinada con OQS-OpenSSL v1.0.2-stable generan inconsistencias en la detección de algoritmos postcuánticos de autenticación e intercambio de claves, negociación y renegociación de algoritmos durante el establecimiento del canal seguro de TLS v1.2. Esta inconsistencia queda pendiente de depuración, análisis y posible solución.

Por su parte, al finalizar el proyecto también se pretende obtener conclusiones acerca del rendimiento de los algoritmos postcuánticos de generación de claves comparados con los algoritmos clásicos partiendo de la información obtenida con el comando *speed* de OpenSSL y de herramientas de pruebas de stress específicas.

4. FORMACIÓN DE RECURSOS HUMANOS

La línea de I+D presentada está vinculada con el desarrollo de una tesis de posgrado por parte del Ing. Diego Córdoba, quien es estudiante de la Maestría en Teleinformática de la Universidad de Mendoza.

5. BIBLIOGRAFÍA

[1] EC Council, *Network Defense: Fundamentals and Protocols*. EC Council Press, 2010.

[2] C. Cimpanu, "Firefox Prepares to Mark All HTTP Sites 'Not Secure' After HTTPS Adoption Rises," 18-Dec-2017. [Online]. Available: https://www.bleepingcomputer.com/news/software/firefox-prepares-to-mark-all-http-sites-not-secure-after-https-adoption-rises/. [Accessed: 02-Aug-2019].

[3] Chromium Blog - Google, "A secure web is here to stay," 02-Aug-2018. [Online]. Available: https://blog.chromium.org/2018/02/a-secure-web-is-here-to-stay.html. [Accessed: 08-Feb-2019].

[4] Z. A. Bahajji and G. Illyes, "HTTPS as a ranking signal," 2014. [Online]. Available: https://webmasters.googleblog.com/2014/08/https-as-ranking-signal.html.

[5] P. W. Shor, "Polynomial-Time Algorithms for Prime Factorization and Discrete Logarithms on a Quantum Computer," *Journal SIAM Journal on Computing*, vol. 26, no. 5, pp. 1484–1509, 1997.

[6] R. L. Rivest, A. Shamir, and L. Adlemar, *A Method for Obtaining Digital Signatures and Public-Key Cryptosystems*. EEUU: Communications of the ACM, 1987.

[7] D. J. Bernstein, J. Buchmann, and E. Dahmen, *Post Quantum Cryptography*, 1ra ed. Berlin: Springer, 2009.

[8] E. W. Weisstein, "RSA-640 Factored," *MathWorld Headline News*, 05-Nov-2005.

[9] (European Telecommunications Standards Institute) ETSI, *Quantum Safe Cryptography and Security*, ETSI White Paper No. 8. France: ETSI, 2015.

[10] T. Takagi, Ed., *Post-Quantum Cryptography*, PQCrypto 2016. Fukuoka, Japón: Springer, 2016.

[11] R. A. Perlner and D. A. Cooper, *Quantum Resistant Public Key Cryptography: A Survey*. Maryland, EEUU: National Institute of Standards and Technology, 2009.

[12] D. J. Bernstein and T. Lange, "Attacking and Defending the McEliece cryptosystem.," presented at the PQCrypto 2008, 2008.

[13] P. Oechsli, *Making a faster cryptanalytical Time-Memory Trade-of. Advances in cryptology: Proceedings of CRYPT*. 2003.

[14] OnBoard Security, "NTRU Post Quantum Cryptography," *NTRU Post Quantum Cryptography*, 2018. [Online]. Available: https://www.onboardsecurity.com/products/ntru-crypto.

[15] L. Ducas, A. Durmus, T. Lepoint, and V. Lyubashevsky, "BLISS: Bimodal Lattice Signature Schemes," presented at the CRYPTO 2013, 2013.

[16] D. Stebila and M. Mosca, *Post-Quantum Key Exchange for the Internet and the Open Quantum Safe Project*. EEUU: Department of Computing and Software, Mc Master University, 2017.

[17] NIST (National Institute of Standards and Technology), "Post-Quantum Cryptography Project," 03-Jan-2017. [Online]. Available: https://csrc.nist.gov/Projects/Post-Quantum-Cryptography/Post-Quantum-Cryptography-Standardization. [Accessed: 13-Mar-2019].

[18] Microsoft, "Welcome to the PQCrypto-VPN project!," *Welcome to the PQCrypto-VPN project!*, Jul-2018. [Online]. Available: https://github.com/Microsoft/PQCrypto-VPN.

[19] Amagicom AB, "Introducing a post-quantum VPN, Mullvad's strategy for a future problem," 08-Dec-2017. [Online]. Available: https://www.mullvad.net/en/blog/2017/12/8/introducing-post-quantum-vpn-mullvads-strategy-future-problem/. [Accessed: 12-Mar-2019].