MSIN – 4210 – CRIPTOGRAFÍA MODERNA EN APLICACIONES

Universidad de los Andes

Facultad de Ingeniería

MESI - Maestría en Seguridad de la Información

18/05/2020

Las primitivas Criptográficas y su uso en Aplicaciones seguras por Diseño.

Las tecnologías criptográficas tienen el potencial de transformar radicalmente los procesos de negocio de las organizaciones en el mundo. Desde el registro de documentos públicos inviolable en una *blockchain*, la descarga de contenidos usando *torrents* y la *deep-web*, los mecanismos de doble factor de autenticación y el ciframiento *end-to-end*; estamos ad-portas de una revolución tecnológica, pendiente de capitalizar. Este curso se enfoca en el análisis de primitivas criptográficas: bloques LEGO cuya combinación en una aplicación permite concebir servicios tecnológicos realmente novedosos.

MSIN – 4210 –CRIPTOGRAFÍA MODERNA en APLICACIONES

LAS PRIMITIVAS CRIPTOGRÁFICAS Y SU USO EN APLICACIONES

JUSTIFICACIÓN

Después de años de evolución en el mundo académico, paulatinamente han surgido una serie de "primitivas criptográficas" de extraordinario interés. Estas primitivas son un conjunto de "bloques constructores", con un modelo formal bastante preciso de amenazas y fortalezas, las cuales combinándolas adecuadamente en su código, es posible derivar aplicaciones realmente novedosas.

Es decir, con la combinación precisa de bloques conocidos como árboles de Merkle, cadenas *blockchain*, criptografía de curva elíptica, firmas digitales en anillo o ciframiento maleable, es posible idear aplicaciones y servicios que resuelven elegantemente muchos de los problemas que tienen las organizaciones en sus procesos de negocio.

OBJETIVO

El objetivo fundamental de este curso es adquirir destrezas acerca de la criptografía como fuente de herramientas tecnológicas que pueden ser incorporadas en productos y aplicaciones novedosas. Cada primitiva criptográfica se estudiará desde el punto de vista de ingeniería, analizando su fortaleza matemática, su modelo preciso de amenazas, su ámbito correcto de uso y sus posibilidades de falla. Se espera que el estudiante al final del curso, haya adquirido una serie de destrezas acerca del uso de la criptografía moderna en aplicaciones.

METODOLOGÍA

El curso combina exposiciones magistrales con la realización de talleres prácticos. Se espera de parte del estudiante fluidez en un lenguaje de programación (al menos Python), conocimientos de álgebra moderna y teoría de números (o disposición para adquirirlos) y intuición general de los problemas de seguridad.

La inasistencia a clase con frecuencia causa dificultades en los parciales, toda vez que algunos de los contenidos del curso no se encuentran fácilmente en otras fuentes. Aún cuando la asistencia a cada sesión de clase no es obligatoria, es sin embargo fuertemente recomendada.

CONTENIDO

Los temas a tratar en el curso son:

- **Introducción**: criptografía, la ingeniería de bitcoin como una combinación inteligente de primitivas criptográficas,
- **Primitivas criptográficas:** random number generators, block and stream ciphers, Hash functions, hotp, totp, proof of work based on hash functions, Merkle's trees, Mask generation functions, encoding, base-64, base-58, zero knowledge proofs, key agreements, public-key cryptography, digital certificates, RSA, ECC, El Gamal, ECC Diffie-Hellman, Id-based cryptography, password-based encryption, HEKS, SCRYPT, malleable encryption, ring signatures, homomorphic encryption. Dependiendo del avance virtual broadcasts anónimos, big-key cryptography, oblivious transfer, private information retrieval y distributed point functions, homomorphic encryption.
- **App: criptomonedas**: *blockchains*, construcción de *blockchains*, *mining* de *bitcoin*, pseudo-anonimato.
- ***App: privacidad en las comunicaciones, El protocol Axolotl (Double Ratchet Algorithm)***: el protocolo criptográfico de Signal®, Telegram® y Whatsapp®. Uso como primitiva criptográfica.
- ***App***: Navegación privada.

MECANISMO DE EVALUACIÓN

El mecanismo de evaluación propuesto consiste en la elaboración de diferentes talleres del mismo valor, con dos evaluaciones escritas cada una con un valor del 30% de la nota final del curso. Los talleres deben remitirse de acuerdo con las instrucciones, en cada caso evitando usar archivos comprimidos Zip, rar, 7-Zip a menos que sean específicamente autorizados.

BIBLIOGRAFÍA

Bellare 2016. Big-Key Symmetric Encryption: Resisting Key Exfiltration. CRYPTO 2016. https://eprint.iacr.org/2016/541.pdf

Boneh 2016. Riposte: An Anonymous Messaging System Handling Millions of Users. IEEE Symposium on Security and Privacy 2015 ("Oakland 2015"). https://arxiv.org/abs/1503.06115

Rogaway 2014. Security of Symmetric Encryption against Mass Surveillance. https://eprint.iacr.org/2014/438.pdf

Adrian 2015. Imperfect Forward Secrecy: How Diffie-Hellman Fails in Practice. *CCS'15*. https://weakdh.org/imperfect-forward-secrecy-ccs15.pdf

Rogaway 2015. The Moral Character of Cryptographic Work. Asiacrypt 2015. http://web.cs.ucdavis.edu/~rogaway/papers/moral.html

Goldberg 2004. Off-the-Record Communication, or, Why Not To Use PGP. *WPES'04*. https://otr.cypherpunks.ca/otr-wpes.pdf

Feigenbaum 2015. Seeking Anonymity in an Internet Panopticon. Communications of the ACM, Vol. 58 No. 10, Pages 58-69. http://cacm.acm.org/magazines/2015/10/192387-seeking-anonymity-in-an-internet-panopticon/fulltext

Lazar 2016. Alpenhorn: Bootstrapping Secure Communication without Leaking Metadata. Usenix Technical Report. https://vuvuzela.io/alpenhorn-extended.pdf

Boneh 2012. The Most Dangerous Code in the World: Validating SSL Certificates in Non-Browser Software. proceedings of ACM CCS '12. http://crypto.stanford.edu/~dabo/pubs/abstracts/ssl-client-bugs.html

Rogaway 2009. Practice-Oriented Provable Security and the Social Construction of Cryptography. http://web.cs.ucdavis.edu/~rogaway/papers/cc.pdf

Chaum 1984. Untraceable Electronic Mail, Return Address and Digital Pseudonyms. Technical Note - Programming Techniques and Data Structures. https://www.freehaven.net/anonbib/cache/chaum-mix.pdf

Gentry 2009. Fully Homomorphic Encryption Using Ideal Lattices. STOC'09. https://www.cs.cmu.edu/~odonnell/hits09/gentry-homomorphic-encryption.pdf

Dwork 2014. The Algorithmic Foundations of Differential Privacy. Foundations and Trends in Theoretical Computer Science Vol. 9, Nos. 3–4 (2014) 211–407. https://www.cis.upenn.edu/~aaroth/Papers/privacybook.pdf

Percival 2016. Stronger key derivation via sequential memory-hard functions. https://www.tarsnap.com/scrypt/scrypt.pdf

Shamir 1985. Identity-based cryptosystems and signature schemes. Advances in Cryptology - CRYPTO '84, LNCS 196,pp. 47-53. https://discovery.csc.ncsu.edu/Courses/csc774-S08/reading-assignments/shamir84.pdf