Seguridad de Sistemas Informáticos
Programa de contenidos

Resumen

Este curso de 60 horas reales tiene como objetivo introducir a los alumnos a los conceptos modernos de seguridad aplicados a los sistemas informáticos. Se centra fundamentalmente en las técnicas aplicadas al aumento de seguridad, y en menor medida a los aspectos legales y sociales que rodean a esta disciplina extremadamente joven y en constante evolución. Está orientado a estudiantes, investigadores y profesionales de la disciplina informática.

1. Conceptos básicos de Seguridad

Definición de seguridad. Principios de seguridad: integridad, confidencialidad, disponibilidad, irrefutabilidad. Seguridad por oscuridad y exposición. Seguridad Paranóica. Falsa Seguridad. Definición de conceptos empleados en seguridad: vulnerabiliad, riesgo, ataque, impacto. Seguridad precavida, reactiva y proactiva. Ingeniería Social. Técnicas para incrementar la seguridad: criptología, criptografía, criptoanálisis, esteganografía.

2. Criptología

Definición de criptología, criptografía, criptoanálisis y esteganografía. Conceptos utilizados en criptología: criptosistema, criptograma, mensaje en claro, clave, codificación y decodificación, cifrado y descifrado.

2.1. Criptografía antigua

Historia de la criptografía: utilización en la Edad Media, Segunda Guerra Mundial, Guerra Fría, Actualidad. Cifrados clásicos: sustitución y transposición. El cifrado de César, sustitución monoalfabética y polialfabética. Sustitución homofónica. Cifrado de Vigenère. La máquina Enigma.

2.2. Criptografía moderna

Criptografía simétrica de una y dos vías. Base matemática de la criptografía simétrica. Algoritmos criptográficos de una vía: *Secure Hash Algorythm* (SHA), *Message Digest Algorithm 5* (MD5). Algoritmos criptográficos de dos vías: *Data Encryption Standard* (DES), *Triple DES* (TDES), *Advanced Encryption Standard* (AES). Criptografía asimétrica. Fundamentos. Utilización para autenticar,

cifrar, firmar y garantizar irrefutabilidad. Base matemática de la criptografía asimétrica. Algoritmos: RSA, *Digital Signature Algorithm* (DSA), Criptografía de Curva Elíptica (ECC), Algoritmos Cuánticos BB84 y E91.

2.3. Criptoanálisis

Técnicas de criptoanálisis. Análisis de la frecuencia. Indice de coincidencia. Criptoanálisis lineal, diferencial, integral, de módulo n, estadístico, XSL. Ataques criptoanalíticos: deslizamiento, *birthday*, *man-in-the-middle*, *meet-in-the-middle*, fuerza bruta, clave relacionada.

3. Software Criptográfico

PGP/GPG. Historia. Modelo de redes de confianza. Utilización práctica. Estándar X-509. Autoridades Certificantes. Infraestructura de Claves Públicas (PKI). OpenSSL. Generación de Certificados. Protección de Contraseñas. Estándar SASL. Implementaciones de SASL.

4. Ataque y defensa de Sistemas Informáticos

Análisis y descripción de las amenazas actuales. Definición de términos: *Malware*, *Spyware, Virus*, *Gusano*, *Troyano*, *SPAM*. Vulnerabilidades: saturación de memoria, ejecución de código arbitrario, escalamiento de privilegios, *cross-site scripting*, inyección de código SQL, liberación de información (*disclosure*). Herramientas de defensa y ataque: capturadores de paquetes, escaneadores de puertos, *rootkits*, escaneadores de vulnerabilidades. Ataques contra sistemas y redes o usuarios de los mismos: *SCAM*, *BlueJack*, *Phishing*, ataques de negación de servicio (DoS), DoS distribuídos (DDoS), espionaje de redes inalámbricas. Ataques dirigidos. Fraudes. Vandalismo Informático. Terrorismo Informático. Términos con que se definen actores de la Seguridad Informática: *Hacker* y sus acepciones, *Cracker*, *Script Kiddie.*

5. Normas y Organismos de Seguridad Informática

Introducción a las políticas de Seguridad. Función de las políticas de seguridad en una organización. Creación de políticas de seguridad. Norma ISO / IEC 27002 (ex 17799). Ley Orgánica de Protección de Datos de Caracter Personal (España). Organismos Oficiales de Seguridad CERT / AR-CERT.

Referencias

[1] **Cooper D.**; **Santesson S.**; **Farrel S.**; **S.Boeyen**; **Housley R.**; **Polk W.** «RFC 5280: Internet X.509 public key infrastructure certificate and certificate revocation list (CRL) profile». Informe técnico, Internet Engineering Task Force (IETF) (**2008**).

[2] **Callas J.**; **Donnerhacke L.**; **Finney H.**; **Shaw D.**; **Thayer R.** «RFC 4880: OpenPGP message format». Informe técnico, Internet Engineering Task Force (IETF) (**2007**).

[3] «ISO/IEC 27002: Information technology - security techniques - code of practice for information security management». International Organization for Standardization and International Electrotechnical Commission (**2006**).

[4] **Schneier B.** *Beyond Fear: Thinking Sensibly about Security in an Uncertain World* (Springer-Verlag New York, Inc., **2003**). ISBN 0-387-02620-7.

[5] **Schneier B.** *Secrets & Lies: Digital Security in a Networked World* (John Wiley & Sons, Inc., **2000**). ISBN 0-471-25311-1.

[6] **Schneier B.** «Self-study course in block cipher cryptanalysis». En *Cryptologia*, tomo 24(1):págs. 18–34 (**Jan 2000**). Http://www.schneier.com/paper-self-study.pdf.

[7] **Adams C.**; **Farrell S.** «RFC 2510: Internet X.509 public key infrastructure certificate management protocols». Informe técnico, Internet Engineering Task Force (IETF) (**1999**).

[8] «Ley orgánica 15/1999, de protección de datos de carácter personal». Boletín Oficial del Estado Español Nro. 298 pp.43088-43099 (**Dic 1999**).

[9] **Zimmermann P.R.** *The Official PGP User's Guide* (The MIT Press, **1995**). ISBN 0-262-74017-6, 978-0-262-74017-3.

[10] **Biham E.**; **Shamir A.** «Differential cryptanalysis of DES-like cryptosystems». En *Journal of Cryptology*, tomo 4(1):págs. 3–72 (**1991**).

[11] **Rivest R.**; **Shamir A.**; **Adleman L.** «A method for obtaining digital signatures and public-key cryptosystems». En *Communications of the ACM*, tomo 21(2):págs. 120–126 (**1978**). Http://theory.lcs.mit.edu/ rivest/rsapaper.pdf.

[12] **Shannon C.**; **Weaver W.** *The Mathematical Theory of Communication* (University of Illinois Press, **1963**). ISBN 0-252-72548-4.