Taller de Administración de Servidores Linux

CC5308

Clase 6: 23 de marzo de 2011

Primitivas Criptográficas

Luis León Cárdenas Graide
lcardena [at] dcc . uchile . cl

Integridad - Errores

- Detectar adulteraciones (¡Eficiente!)
  - Errores de transmisión/almacenamiento
  - Probabilidad de detección
  - Adulteración malintencionada
  - ¿Corrección de errores?
- "Dígito verificador": MSJE-crc(msje)
  - "Distribución" imagen
- CRC: Cyclic Redundancy Check
  - Patrones de error
  - Linealidad vs Robustez Criptográfica
  - Adulteración malintencionada: Wi-Fi WEP (RC4)

Integridad - Criptografía

- Hashing: Funciones de resumen
  - hash(mensaje): String → Digest (string largo fijo)
- Robustez criptográfica
  - Resistencia preimagen (one-way function)
    - Dado h, difícil encontrar msje tq h = hash(msje)
  - Resistencia segunda preimagen
    - Dado msje1, difícil encontrar msje2 != msje1 tq hash(msje1) = hash(msje2)
  - Resistencia colisiones (fuerte)
    - Difícil encontrar msje1 != msje2 tq hash(msje1) = hash(msje2)
- "Difícil" = NP (Tiempo/Espacio: ~O(exp))

Integridad - Familias

- SHA-1: Rango ("fortaleza") 160 bits
  - <=2^160 entradas antes de colisión
  - >2^160: colisión segura
- Límites al tamaño del mensaje
- Rango efectivo < Rango teórico: Siempre empeora
  - Análisis matemático
  - Poder computacional (paralelo)
- **MD5 deprecado**
- SHA-1 si no hay otro, SHA-2 toda vez que se pueda
- SHA-3: Competencia NIST en curso

Privacidad - Cifrado

- Texto claro ↔ Algoritmo ↔ Texto cifrado
- Algoritmo: público, simple, analizable, estándar, intercambiable, demostrablemente seguro
- Principios Kerckhoffs vs Seguridad por oscuridad
  - Imposibilidad teórica vs efectividad práctica
  - Seguridad no dependa de diseño secreto ...
- Claude Shannon: "El adversario conoce el sistema"
- Texto claro ↔ Algoritmo(clave) ↔ Texto cifrado
- Seguridad: Cambio de clave, Bits Fuerza Bruta
- Propiedades: Difusión (mensaje), Confusión (clave)

Criptografía Simétrica

- Clave privada-compartida emisor-receptor
- Robustez: Fuerza bruta como peor caso (teórico)
  - Largo clave y malas claves, Análisis matemático
  - Robustez Efectiva < Robustez Teórica
- Algoritmos
  - Bloque: AES, DES, 3DES, IDEA, Blowfish...
    - Modos de operación: ECB(!), CBC, OFB, CFB
  - Flujo: RC*, ...
- Eficiencia
  - Rápidos + poco espacio extra: padding O(1)

Criptografía Simétrica

- Error en Clave → Descifrar basura
  - No se puede distinguir descifrado con clave incorrecta
  - Integridad: Hashing
- Petición de principio: ¿Cómo pre-compartir clave en forma segura?
  - Bootstrapping: Criptografía Asimétrica
- Análisis de Riesgo
  - **Usualmente**, algoritmos criptográficos no se quiebran...
  - Se **bypassean** por mal diseño/implementación del sistema que los usa

Eslabón más débil

Criptografía Asimétrica

- Generación Par de Llaves: Privada/Pública
- Privada: Se guarda en forma "segura"
  - "Jamás" se transmite (salvo protocolos avanzados)
- Pública: Se publica a todo el mundo
  - Asociadas matemáticamente
  - "Difícil" obtener privada a partir de pública
- Uso: Cifrado con Pública, Descifrado con Privada
- Robustez: Fuerza bruta como peor caso (teórico)
  - Largo llave y malas llaves, Análisis matemático
  - Robustez Efectiva < Robustez Teórica
- Algoritmos: RSA, DSA, Curva Elíptica

Criptografía Asimétrica

- Eficiencia
  - Generación par público/privado puede ser costoso
  - Cifrado más intensivo CPU que simétrico
  - Suele agrandar (mucho) los mensajes
- Protocolo Diffie-Hellman: Canal Seguro
  - Bootstrapping: Intercambio claves simétricas
- Ataques Texto escogido: Claves largas
- Logística: ¿Dónde/Cómo almacenar Llave Privada?
  - Smart-cards: Estándar FIPS 1, 2, 3...
  - Filesystem cifrado: Petición de Principio
  - Cluster P2P: Generación distribuida

Locura por bits ¿128, 4096, 10240?

- General: Hashing, Simétrica, Asimétrica
  - ¿Más bits? → Producción más "costosa"
    - + lenta (CPU), + energía, (asimétrica: + espacio)
  - Bits → "Compra" **plazo** presente de resistencia contra ataques futuros
    - Proyección capacidad computacional individual promedio (Ley de Moore: x2 c/18 meses)
    - Disponibilidad global de unidades (¿botnets?)
    - Disponibilidad energética (Sol: ~128 bits simétrica)
    - Análisis de riesgo: Costo/Beneficio Atacante por Años
- Hoy: 128 simétrica, 2048 asimétrica, 160 hashing
  - 40 años si resisten ataques **matemáticos**
  - **Más largas no necesariamente resisten mejor**

(Pseudo)Aleatoriedad

- Aleatoriedad: Impredecible
  - Fuentes de Entropía usualmente físicas: satélites, temperatura, ruido cuántico láser desfasado, radiación cósmica, etc.
- Pseudoaleatoriedad: Computable
  - Semilla PRNG (Pseudo-Random Number Generator)
  - Fuentes de Entropía: ¿Fecha/Hora, PID, carga, interacción usuario, **patrones** del sistema?
- Eficiencia: Ancho de Banda (Mbps/Gbps) vs CPU
- Calidad: Predicción de secuencias
- Generación: Software (CPU, kernel, red), Hardware (HSM: placas, dongles)

Autenticidad - Firma Digital

- (Integridad)
- Hash cifrado: protege Man-in-the-Middle (MITM)
- Simétrico: HMAC
  - Repudiable: tanto emisor como receptor pueden falsificar
  - Auto-mensajes con storage inseguro
    - Cookies web: seteadas y leídas por servidor
    - Almacenamiento: auto-comunicación futura
- Asimétrico
  - No repudiable
  - Hash Cifrado con Llave Privada y verificado con Pública

Identidad - Certificados Digitales

- Identificar Usuario y/o Servidor
  - ¿Con quién estoy hablando?
- Certificado Digital
  - Datos Personales / Sitio Web
  - Llave Pública [+ Llave Privada (passphrase)]
  - Firma de Autoridad Certificadora
    - Ligazón Usuario/Llave Pública
  - Usos autorizados, Algoritmos, etc.
- Cadena de Confianza y CRL
  - Trust Anchor: Certificado autofirmado preinstalado
  - SSL: Validación automática jerarquía

Actividad Personal

- Navegador Web: Conectarse vía HTTPS
  - Examinar certificado digital: campos
- Examinar BD con certificados preinstalados
- Ingresar a sitios con certificados autofirmados
  - ¿Aceptar una vez o permanentemente?
  - ¿Dónde se almacena?
- ¿Servicios que pidan certificado a cliente?
  - www.sii.cl
- Almacén seguro del navegador: contraseña maestra
  - ¿para qué?