Seguridad en Sistemas de Información

Curso en Zacatenco y Tamaulipas [Q2 2013]

Luis J. Dominguez Perez

Cinvestav, Mayo 13 de 2013

Contenido, sección 1

La firma electrónica en México

- Es un paso hacia la transformación de la gestión pública.
- Coadyuva en la erradicación de la corrupción
- Provee una mayor productividad
- Reduce los costos de la ciudadanía al ejercer sus derechos y obligaciones.

Una fórmula para mejorar México

Ley que garantice la equivalencia entre:
firma autógrafa y de tipo digital

Esquema que fomente la productividad

Economía más competitiva
un México más fuerte
más próspero
con mejor futuro.

Inicios de la firma electrónica

- En un principio, el SAT instruyó el proyecto “Tu firma” (2004)
- Banxico intentó autorizar a terceros para validar las firmas
- SAT crea la CIEC - Clave de Identificación Electrónica Confidencial
- Nace la “FEA” - Firma Electrónica Avanzada (2005)
- Se instrumenta un esquema de PKI

Inicios de la firma electrónica - 2

- Se renombra la FEA por "FIEL" (2007)
- Entran la Secretaría de Economía, la Secretaría de la Función Pública, y el Servicio de Administración Tributaria (2008 – 2012)

Legislación

- Ley Federal de Protección de Datos en Posesión de los Particulares
  - **Año:** 2010
  - **Reforma:** 2010
  - **Alcance:** Particulares
  - **Aspectos relevantes:** Establece que para el caso de las solicitudes en general, la firma electrónica u otro medio se pueden utilizar para las autorizaciones.

Legislación - 2

- Ley Federal de Transparencia y Acceso a la Información Pública
  - **Año:** 2002
  - **Reforma:** 2010
  - **Alcance:** Agencias gubernamentales
  - **Aspectos relevantes:** Exige mecanismos de verificación de la integridad de la información, se puede hacer uso de la firma electrónica para tal efecto.

Legislación - 3

- Código de Comercio
  - **Año:** 1889
  - **Reforma:** 2012
  - **Alcance:** Operaciones mercantiles
  - **Aspectos relevantes:** Contiene un título extensivo sobre el comercio electrónico, que incluye el uso de la firma electrónica

Legislación - 4

- Código Fiscal de la Federación
  - **Año:** 1984
  - **Reforma:** 2005
  - **Alcance:** Operaciones fiscales
  - **Aspectos relevantes:** Establece cómo se rigen los procedimientos relacionados a los impuestos

Legislación - 5

- Ley de Firma Electrónica Avanzada
  - **Año:** 2012
  - **Reforma:** 2012
  - **Alcance:** Particulares, operaciones no fiscales ni mercantiles
  - **Aspectos relevantes:** Hace equivalente a la firma digital con la firma autógrafa. Define las características de los certificados digitales

Legislación - 6

- Decreto de Austeridad 2012
  - **Año:** 2012
  - **Reforma:** 2012
  - **Alcance:** Gobierno federal, operaciones no fiscales ni mercantiles
  - **Aspectos relevantes:** Hace obligatorio y extensivo el uso de la firma electrónica, y busca reducir el consumo del papel

Infraestructura Extendida de Seguridad

- El Banco de México, como Banco Central del país, establece los mecanismos de comunicación para las transacciones financieras
- Define una infraestructura PKI que hace uso extensivo de los certificados digitales
- Delega ciertas actividades a los diferentes actores del mercado financiero

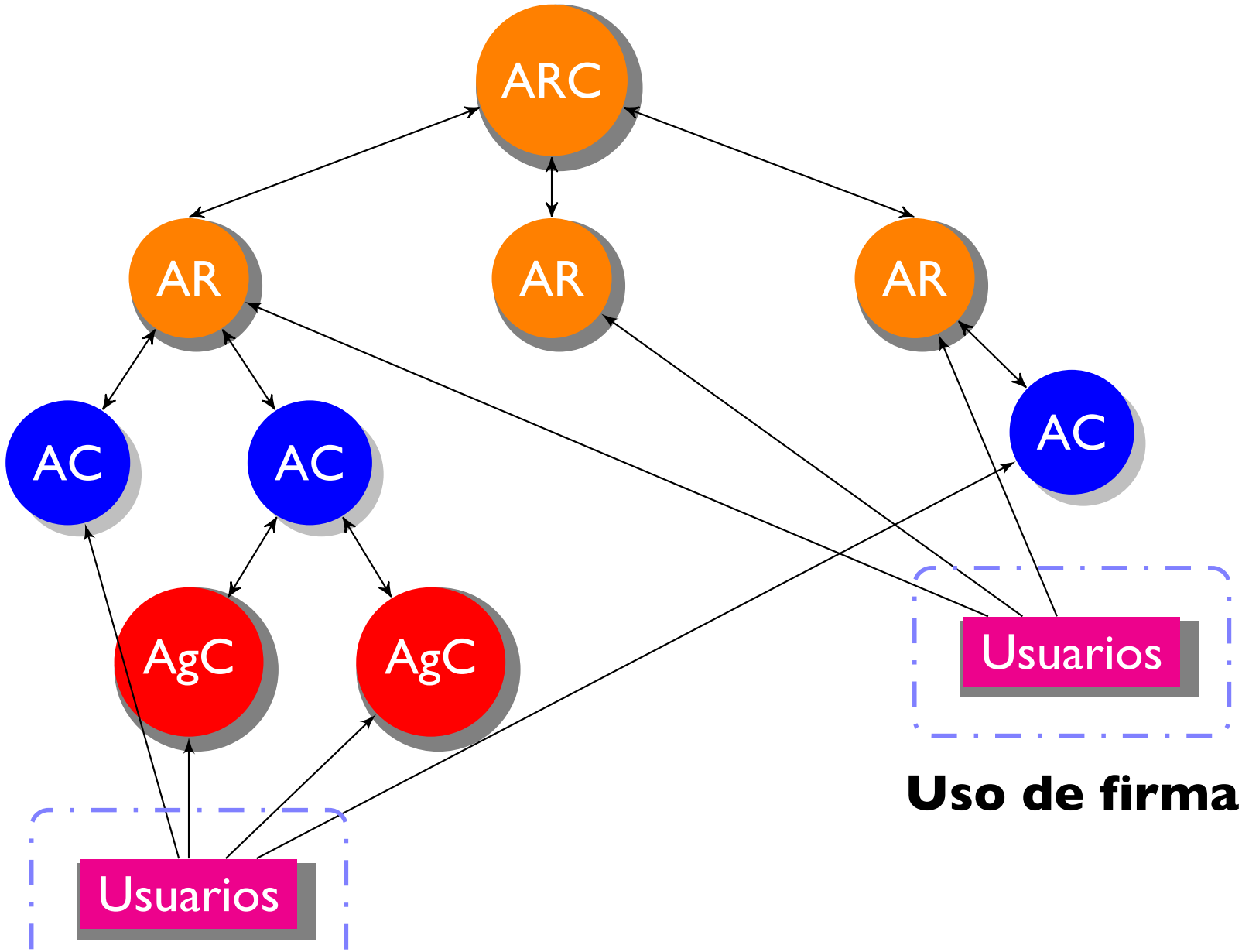
Elementos en la infraestructura de Banxico

La IES, infraestructura extendida de seguridad, contiene los siguientes actores:

- ARC - Agencia Registradora Central
- AR - Agencia Registradora
- AC - Agencia Certificadora
- AgC - Agente Certificador
- Usuario

Diagrama IES

Infraestructura IES



Elementos en la infraestructura de Banxico

- ARC - Agencia Registradora Central
  - Establece la normatividad y administra la IES
  - Autoriza su inclusión a la IES a otros elementos, y define sus funciones
  - Administra el esquema de PKI

- AR - Agencia Registradora
  - Registra los certificados digitales, previa autorización de la ARC
  - Administra los certificados a su cargo

Elementos de la IES - 2

- AC - Agencia Certificadora
  - Emiten los certificados digitales
  - Son el intermedio entre los Usuarios y los Agentes Certificadores (AgC), y la Agencia Registradora (AR)

- AgC - Agente Certificador
  - Realiza labores de certificación y revocación de firmas digitales

- Usuario
  - Es quien requiere un certificado
  - Puede ser persona física o moral, nacional o extranjera

Operaciones en la IES

Existen dos protocolos de comunicación:

- Entre la Agencia Registrador (AR) y la Agencia registradora Central (ARC):
  - Conexión
  - Desconexión
  - Alta de Certificado
  - Consulta de Certificado
  - Revocación de Certificado
  - Aviso de Revocación de Certificado

Operaciones en la IES - 2

- Entre el Usuario y las diferentes entidades de la IES:
  - Conexión
  - Desconexión
  - Consulta de Certificados
  - Revocación de Certificado propio

Caso Colima

- El caso de la firma electrónica del Estado de Colima es interesante ya que se tenía un serio problema de productividad y un evidente retraso en la operación de partes clave en el estado

- El Registro Público de la Propiedad y del Comercio del Estado de Colima (RPPC) requirió que el estado hiciera cambios en la legislación, e hizo uso de la firma electrónica como solución a sus problemas

- El Estado de Colima recibió un reconocimiento por parte de la OECD por sus avances en esta materia

Legislación afectada del Estado de Colima

- Se creó la Ley de Firma Electrónica para el Estado de Colima (2009)
- Se modificaron las siguientes leyes:
  - Código Civil
  - Código de Procedimientos Civiles
  - Código Penal
  - Código de Procedimientos penales
  - Ley de Catastro
  - Ley del Notariado del Estado de Colima
  - Reglamento del Registro Público de la Propiedad y del Comercio del Estado de Colima

Resultados en el Estado de Colima

- Reducción dramática de los procesos relacionados con el RPPC
- Eliminación o absorción de procedimientos redundantes
- Automatización de ciertos procesos
- Generación de nuevos y ágiles servicios
- Aumento de la productividad
- Reconocimiento de la OECD

Distrito Federal

- En el Distrito Federal también se generó una Ley en materia de firma electrónica (2009). En este caso se buscó:
  - Transparentar la función pública
  - Combatir la corrupción
  - Eficientizar la gestión administrativa
  - Brindar mejores servicios

- En este caso, se dejó a la Asamblea Legislativa hacer los ajustes pertinentes en materia legal
- También se dispuso al Departamento de la Administración Pública de proveer los medios a la ciudadanía (incluyendo la brecha digital)

- Otro caso interesante es el de la UNAM. (2005)
  - El objetivo de la firma electrónica es facilitar la autenticación de los miles de alumnos que se tienen
  - Facilitar el resguardo de la documentación (digitalización de documentos)
  - Incrementar la seguridad de los datos

- Dado que no existe urgencia del cambio en este caso, se ha ido incorporando el uso de la firma electrónica a diversos módulos de atención a alumnos, pero ha sido uno a uno, y no se procede a incluir otro hasta que se haya terminado el cambio en el módulo anterior.

Módulos UNAM

Los módulos a los que se le incluyeron la firma electrónica son:

- 2005 - Actas de calificaciones de bachillerato, vale de abastecimientos, presupuestos, mantenimiento, viáticos
- 2006 - Firma de actas de calificaciones
- 2007 - Programación de eventos culturales
- 2011 - Cartas de no adeudo para titulación, calificaciones extracurriculares, Archivo General
- 2012 - Sistema interno

Diferencias

- Caso Colima
  - Mejora de productividad
  - Nuevas leyes
  - Contratación de personal
- Caso UNAM
  - Autenticar y digitalizar
  - Aviso en la Gaceta universitaria
  - Cambio escalonado
- Caso D.F.
  - Corrupción y mejores servicios
  - Nuevas leyes
  - Delegación de trabajo

Diferencias - 2

- Caso SAT
  - Productividad y mejor recaudación
  - Nuevas leyes
  - Cambio escalonado

- Caso Banxico
  - Proporcionar una infraestructura
  - Nuevas leyes
  - Concientizar al gobierno

Situación legal de la firma electrónica en México

- Categoria 1. Existe una ley, CA, portal y/o aplicaciones
- Categoria 2. Existe una ley
- Categoria 3. No existe una ley, pero la usan, o planean
- Categoria 4. No hay avance

Cortesia:Miguel Morales

Presentación Notaria Digital de Vladimir González García

Contenido, sección 2

Presentación del Dr. Francisco Rodríguez-Henríquez

Perfect Forward Secrecy

- Si alguna de las llaves utilizadas en la comunicación entre dos partes se conoce, se presenta una catástrofe, ya que se puede decifrar la comunicación futura entre las partes.

- Sin embargo, si un escucha estuvo guardando la comunicación cifrada entre las partes, dicha comunicación puede ser descifrada, y se tendría acceso a la información anterior.

Perfect Forward Secrecy 2

- Un protocolo criptográfico tiene **perfect forward secrecy** si al comprometer llaves de uso a largo plazo (cifrado para almacenamiento), no se compromete la comunicación de las llaves de sesión anterior.
- La idea es que la llave utilizada para proteger la transmición de datos no se utilice para derivar llaves adicionales. Si la llave se derivó de otro material procedente de una llave, ese mismo material no debe ser utilizado para derivar más llaves.

Generación de llaves de sesión e intercambio

Cada conexión SSL pasa por un *SSL handshake* en donde se acuerda lo siguiente:

- Se comunican las habilidades de cada parte
- Se autentica
- Se acuerdan las *llaves de sesión* (intercambio de llaves)

La idea del intercambio de llaves es acordar las llaves de manera segura

Generación de llaves de sesión e intercambio 2

El método más común es RSA, sin embargo, cualquiera con acceso a la llave privada del servidor, puede obtener las llaves de sesión, y descifrar la comunicación

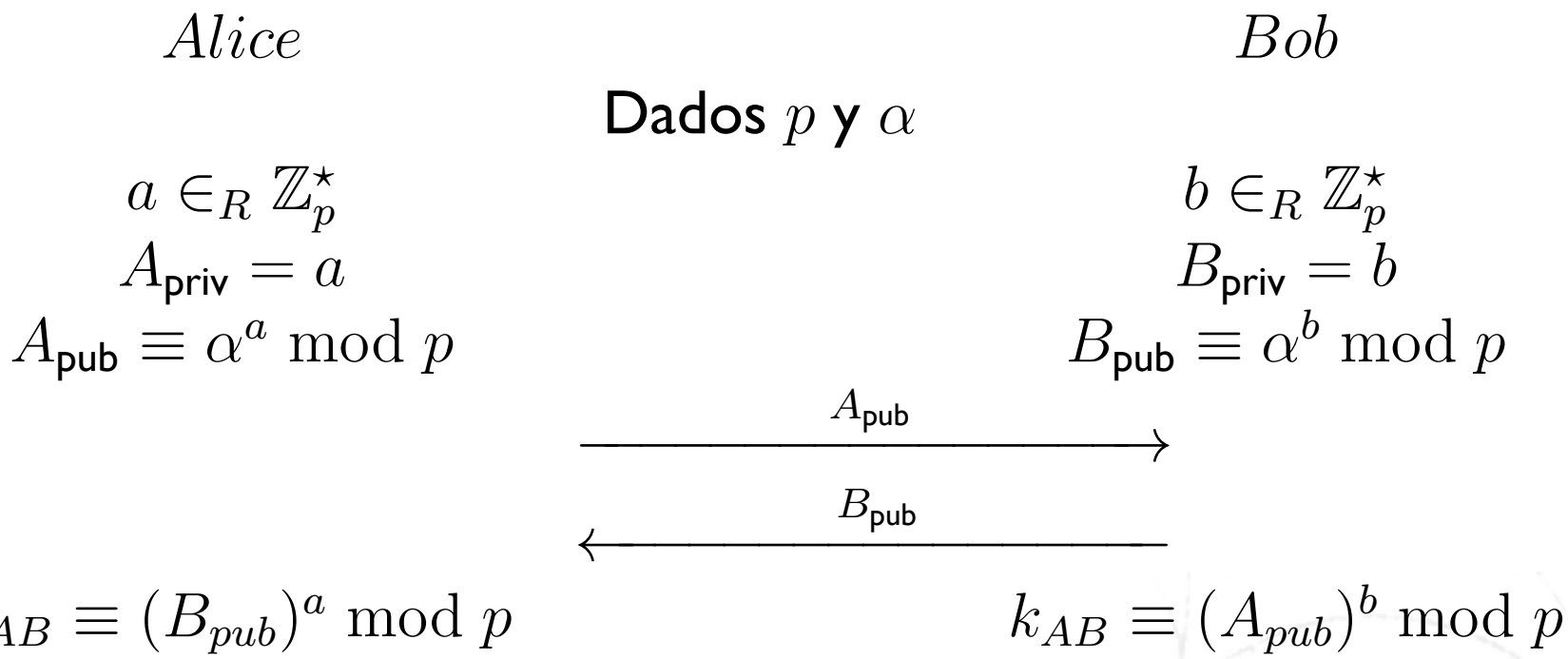
- Un dispositivo de seguridad podría descifrar la transmición y analizarla en busca de malware
- Un adversario podría guardar la transmición, y leerla después

SSL y PFS

SSL soporta forward secrecy con el Diffie-Hellman Exchange (DHE), y con el Elliptic Curve Diffie-Hellman Exchange (ECDHE):

- DHE es muy lento, por lo que los operadores de sitios web lo deshabilitan
- ECDHE también es lento, pero más rápido que el DHE

Diagrama DHE



Dado que siempre se utilizan valores aleatorios nuevos, a este algoritmo se le conoce como Ephemeral Diffie-Hellman (EDH, o simplemente DHE).

Diffie-Hellman con curvas elípticas

- El DHE puede ser acelerado si utilizamos su modalidad con curvas elípticas. En lugar de utilizar el problema del logaritmo discreto sobre la exponenciación modular, se utiliza la estructura algebraica de las curvas elípticas.

- Se puede obtener el mimo nivel de seguridad de RSA con llaves mucho menores...

Niveles de seguridad

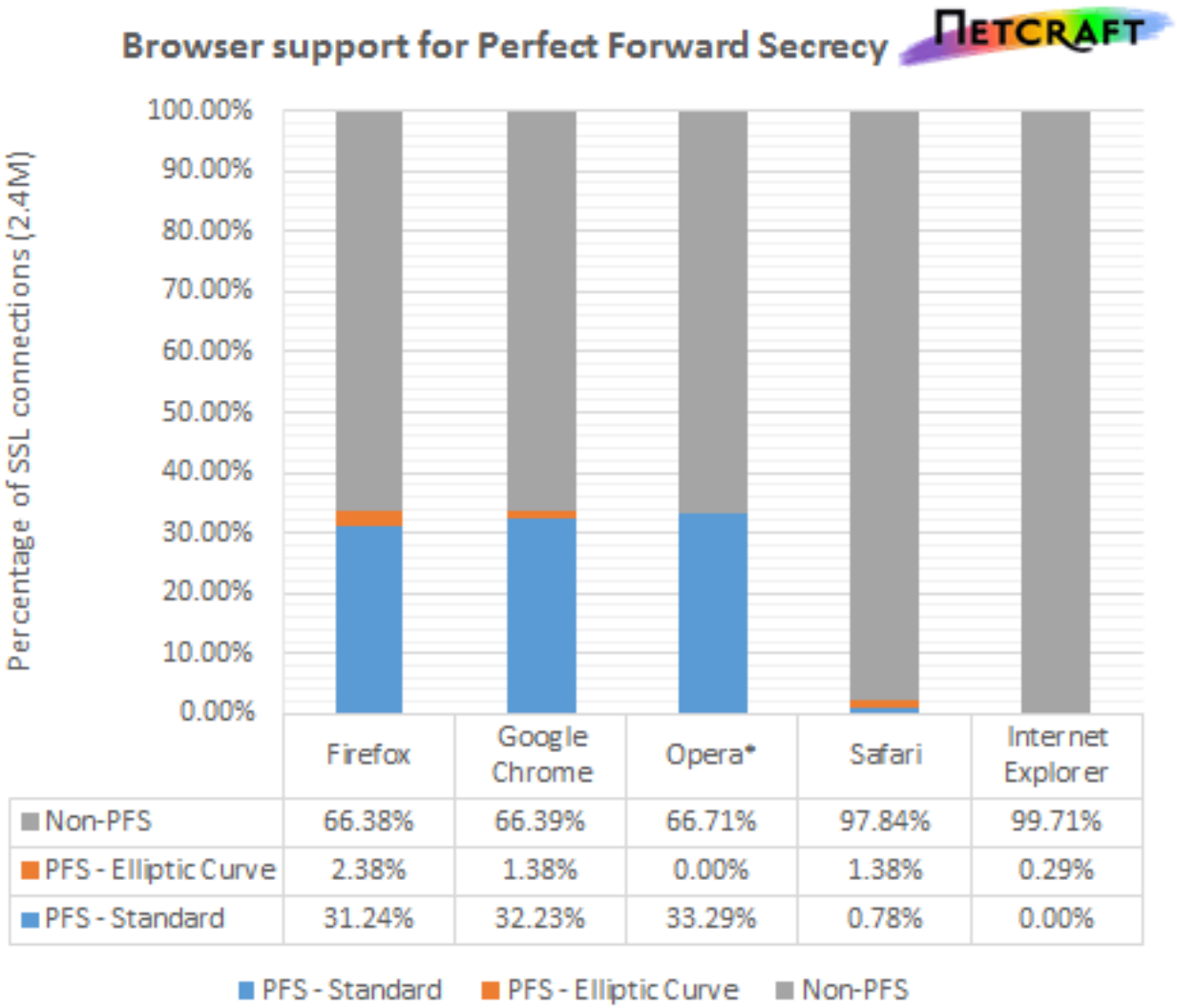
Familia	Criptosistema	Nivel de seguridad		
		128	192	256
Factorización entera	RSA	3072 bit	7680 bit	15360 bit
Logaritmo discreto	DH, DSA, Elgamal	3072 bit	7680 bit	15360 bit
Curvas elípticas	ECDH, ECDSA	256 bit	384 bit	512 bit
Clave simétrica		128 bit	192 bit	256 bit

Diffie-Hellman con curvas elípticas 2

- En lugar de definir p y α, se define una curva elíptica de la siguiente forma: $y^2 = x^3 + \alpha x + \beta$, un primo p, y un punto generador G.
- El RFC 4492 establece el uso de curvas elíptica en el TLS
- Existen unas curvas estandarizadas por el NIST: p-256, p-384, y p-521
- En lugar de exponenciaciones modulares, se utiliza la llamada multiplicación escalar-punto

Uso de PFS, navegador vs. sitio web

Netcraft hizo prueba de conectividad con los 5 navegadores principales, y 2.4 millones de sitios web con SSL. El gráfico muestra qué algoritmo de conexión utilizaron:



	Firefox	Google Chrome	Opera*	Safari	Internet Explorer
Non-PFS	66.38%	66.39%	66.71%	97.84%	99.71%
PFS - Elliptic Curve	2.38%	1.38%	0.00%	1.38%	0.29%
PFS - Standard	31.24%	32.23%	33.29%	0.78%	0.00%

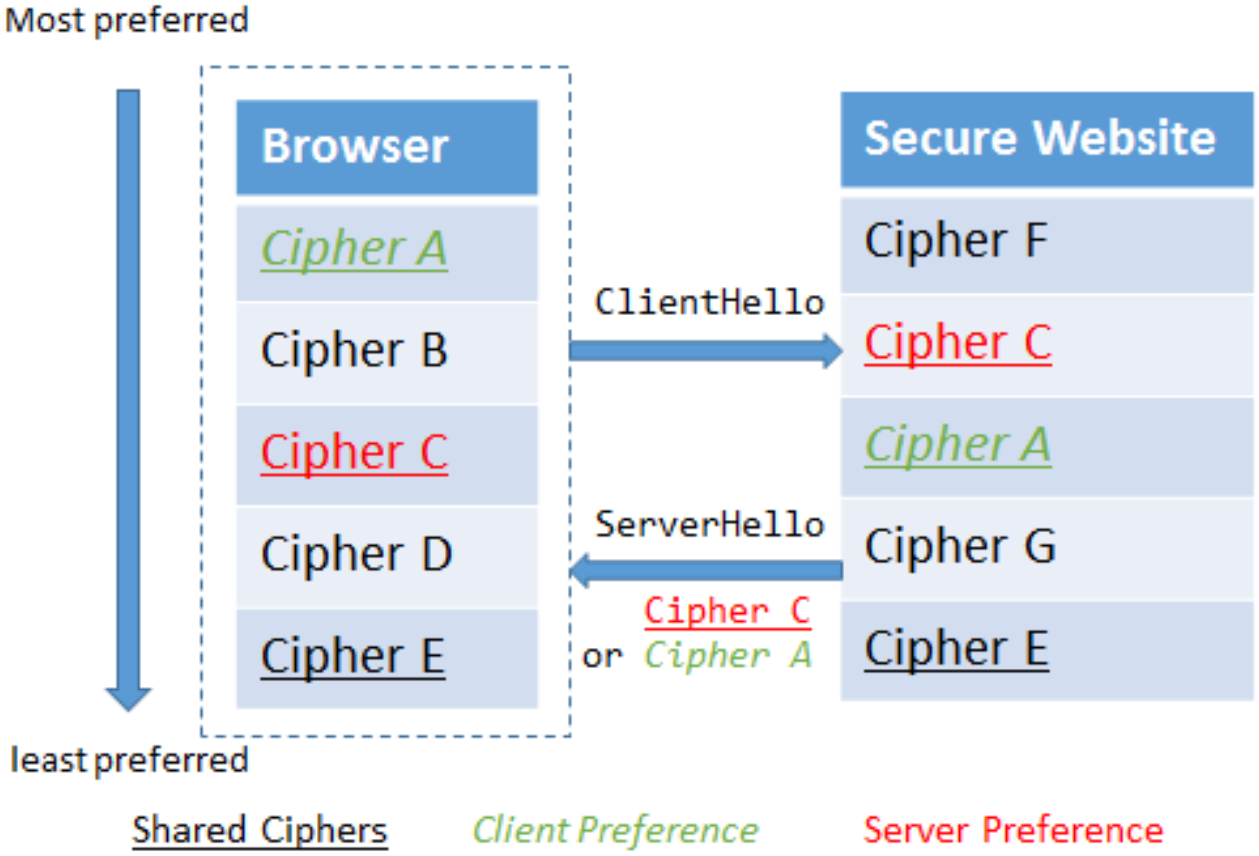
Desglose del Internet Explorer

Netcraft presenta el uso de lo cifradores en el Internet Explorer al conectare a lo 2.4 millones de sitio web SSL más populares:

Prioridad	Método	Uso
1	AES128-SHA	63.52%
2	AES256-SHA	2.21%
3	RC4-SHA	17.12%
4	DES-CBC3-SHA	0.41%
5	ECDHE-RSA-AES128-SHA	0.08%
6	ECDHE-RSA-AES256-SHA	0.21%
7	ECDHE-ECDSA-AES128-SHA	0.00%
8	ECDHE-ECDSA-AES256-SHA	0.00%
9	DHE-DSS-AES128-SHA	0.00%
10	DHE-DSS-AES256-SHA	0.00%
11	EDH-DSS-DES-CBC3-SHA	0.00%
12	RC4-MD5	16.46%

Algoritmos de conexión

Dramatización de la negociación de los algoritmos de cifrado



Contenido, sección 3

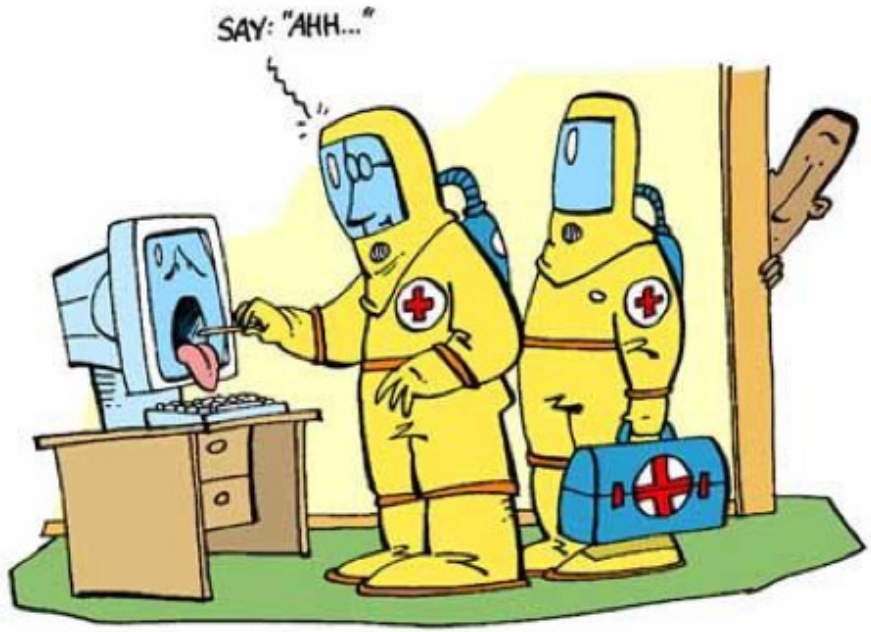
Definiciones

Abreviación de software o código maliciose. Es un software create para alterar la operación normal de una computadora, obtener información privada, u obtener acceso a otros equipos informáticos.

El Malware es una categoría de software que incluye: virus computacionales, gusanos, trojanos, spyware, a la mayoría de los rootkits, y otros programas maliciosos.

Virus computacional

Es una pequeña pieza de software que se trepa en programas reales o documentos para explotar algún error en el programa o programa de lectura con el propósito de destruir información.



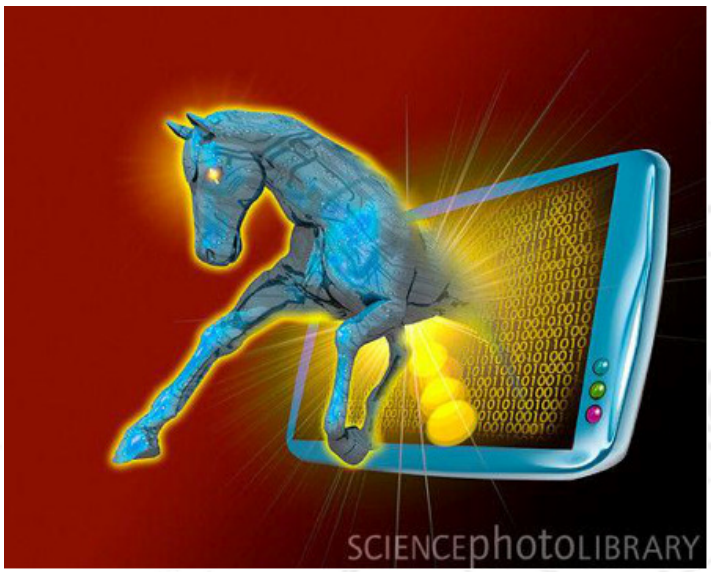
Gusano informático

Un programa computacional diseñado para auto replicarse y propagarse. Causan severos transtornos en el tráfico de las redes cuando atacan a gran escala.

La computadora se convierte en zombie si el gusano está utilizando la mayoría de sus recursos. Pueden proveer acceso remoto a un atacante.

Trojano

Un programa computacional que pretende ser otro. Se pueden replicar, robar información, o dañar el equipo computacional. Usualmente son utilizados para dar acceso remote al que lo envió.



Botnet

Es un conjunto de computadoras comprometidas con algún malware, el cual generalmente se comunica con su central a la espera de instrucciones para lanzar un ataque remoto en general o a algún objetivo.

Los bots (computadoras) son también llamados zombies ya que no tienen cerebro (no atacan hasta que son instruídos a hacerlo).

Spyware

Es un programa oculto que recolecta información del usuario, ya sea al leer archivos, capturando tecleos, o alguna otra técnica.

Por otro lado, también pueden ser utilizados por los propietaros de los recursos computacionales para fines legítimos de supervisión.

Adware

Es un programa que despliega un anuncio no requerido por el usuario, o por el generador de contenidos. En algunos casos, se agregan a sí mismos a las páginas web para generar ganancias. Son usualmente spyware que se enmascara como un anuncio. Por ejemplo, Wikipedia no tiene anuncios, por lo que...

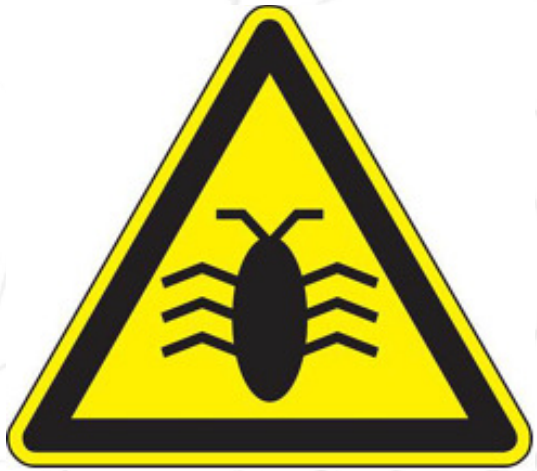
Rootkit

Es un software malicioso oculto que se ejecuta con permisos especiales. En una computadora comprometida, un atacante inserta un rootkit que se auto oculta manteniendo sus permisos especiales para su futura ejecución.

Una nota sobre el malware

En programa con errores haciendo cosas malas no es considera un malware, pero se puede abusar de él para hacer acciones malas.

La mayoría del malware tiende a ser un trojano o un virus de computadora convencional.



Inicio

- La noción de virus fue diseñada por John von Neumann en 1949.
- El primer autómata autoreplicable fue creado por Veith Risak en 1972, el cual fue escriteo en ensamblador y se ejecutaba en un sistema SIEMENS 4004/35
- En 1984, Fred Cohen bautizó a los programas autoreplicables como virus. En 1987 él creo el primer detector de virus.
- También, en 1984, J. B. Gunn describió los usus prácticos de los virus.

Malware famoso

- 1970. Creeper apareció en ARPANET, infectando computadoras PDP-10
- 1981. Elk Cloner, el primer virus "in the wild". Apple DOS 3.3 usando un disco flexible.
- 1986. Brain boot sector virus, 1ro sobre IBM
- 1987. Jerusalem, atacaba cada Friday 13 (principal ataque el 13 de Mayo de 1988).
- 1988. Morris, buffer overrun en Unix (explotaba 3 vulnerabilidades simultáneas)
- 1992. Michelangelo, creó psicosis colectiva.

Malware famoso

- 1995. Concept, el primer macro virus como adjunto en documentos de Microsoft word (trojan).
- 1996. Ply, virus polifmórfico.
- 1999. Happy99 worm. (1ro en correos)
- 1999. Melissa macro virus. Borraba documentos de MS Office (decepción).
- 1999. Kak, gusano javascript.
- 2000. Gusano ILOVEYOU, (decepción)
- 2001. Anna Kournikova, (decepción)
- 2001. CodeRed, servidores IIS (buffer overflow). Nimbda

Malware famoso

- 2002. Beast, trojano con back door
- 2003. Gusano SQL slammer
- 2004. MyDoom, el gusano más rápido en esparcirse. (ataque a SCO?)
- 2004. Gusano Sasser, reiniciaba PCs
- 2007. Storm, creaba una botnet (correo)
- 2007. Zeus, trojan capturador de teclado (MITM, phishing)
- 2009. Inicio de la cyber guerra
- 2010. Gusano Stuxnet...
- 2012. Gusano Flammer...

Phishing

Definición. Es un método para robar información personal a través de spam o métodos engañosos.

Existen muchísimas técnicas para este f la tecnología, surgen nuevos métodos.

Clasificación de phishing

- Correos engañosos
- Malware vía correo
- Malware vía web
- Keyloggers
- Suplantación de sesión
- Repositorios envenenados
- Robo
- Barras de herramientas/rootkits
- Buscadores apócrifos
- Tabbing
- Pharming
- Man-in-the-middle
- Spoofing

Descripciones de tipos de phishings 1/7

Correos engañosos. Son correos que contienen información falsificada y pretenden ser alguna autoridad. Normalmente solicitan información confidencial como contraseñas o números de tarjetas bancarias bajo la amenaza de perder algún servicio, o con la excusa de una pérdida o confirmación de datos.

Malware vía correo. Son archivos adjuntos infectados o virus disfrazados, provienen de un correo legítimo o de terceros. Buscan ser ejecutados manualmente por el recipiente mediante errores en los programas o vía engaños.

Descripciones de tipos de phishings 2/7

Malware vía web. Son programas maliciosos que son ejecutados al entrar a sitios web infectados, o mediante servicios malicioso de terceros en sitios de confianza.

Keyloggers. Son dispositivos o programas que capturan la interacción del usuario con la computadora, interceptando contraseñas o conversaciones con información sensible. Existe una modalidad llamada Screenlogger en la cual se toman capturas de la pantalla. Otra modalidad es vía webcam.

Descripciones de tipos de phishings 3/7

Suplantación de sesión. Algunos sitios web accesan a información privada del usuario a pesar de ya no estar el sitio web activo. En otros casos, enemigos sigilosos intentan continuar con una sesión abierta haciendo otras cosas, sin que se enteren las partes.

Repositorios envenenados. En algunas ocasiones, el malware ataca repositorios de archivos con la finalidad de introducir código que robe información. Pueden ser sobre sitios corporativos o públicos.

Descripciones de tipos de phishings 4/7

Robo. Robo físico de equipos de cómputo. Se da a nivel industrial y gubernamental. En la inmensa mayoría de los casos los datos no están cifrados. Al final, se vende el equipo en la calle.

Barras de herramientas/rootkits. En algunas ocasiones, los proveedores de servicios incluyen como parte de su equipo o de software, algún *crapware* (y en algunas ocasiones el mismo servicio lo es), el cual contiene código malicioso como keyloggers.

Descripciones de tipos de phishings 5/7

Buscadores apócrifos. Parcialmente como rootkits, aunque sin llegar a serlo (ya que no se instala ningún software en el equipo). Los buscadores apócrifos pretenden ser una opción fresca a los bucadores habituales, sin embargo, lo que buscan es redirigir tráfico de red hacia páginas fraudulentas o de captura de información; además de dedicarse a recabar información de comportamiento del usuario con o sin su consentimiento explícito.

Tabbing Son páginas maliciosas que si son cargadas como una pestaña y hay muchas más, se impersonan como otro sitio web para que en un momento de distracción capturen información de acceso accidentalmente.

Descripciones de tipos de phishings 6/7

Pharming. Un efectivo método para realizar phishing es mediante el ataque a los servidores de DNS. Los servidores de DNS asocian un nombre de dominio con una dirección de IP de la página. Si en lugar de redirigir al sitio oficial, se redirige a uno fraudulento, un atacante podría obtener información muy valiosa mediante un engaño transparente al usuario.

Main-in-the-middle Buscan impersonar ya sea a los servicios ofrecidos en internet, o a los clientes, de tal manera que las partes no se den cuenta y faciliten información sensible al atacante pensando que solo fue entre sí.

Descripciones de tipos de phishings 7/7

Spoofing. Buscan engañar a los clientes o servidores al falsificar las direcciones de origen o destino, realizando consultas sensibles o captura de información en tránsito.

Descripciones de tipos de phishings 7/7

Spoofing. Buscan engañar a los clientes o servidores al falsificar las direcciones de origen o destino, realizando consultas sensibles o captura de información en tránsito.

Ingeniería social. Busca engañar a las personas mediante técnicas verbales e histriónicas para obtener información sensible de una compañía o persona. Es de lo más efectiva y sencilla.

Stuxnet

Originalmente de origen desconocido, era un gusano de Windows que atacaba a equipo Siemens con el propósito de espiar y destrozar industrias.

Atacaba a la industria Iraní poco después del nerviosismo acerca de enriquecimiento de Uranio, que podía utilizarse para propósitos militares.

http://pastebin.com/a1DeRyFN

Stuxnet

Un año después del ataque inicial, cerca de 1,000 centrífugas en las instalaciones eléctricas de Natanz fallaban o estaban descompuestas.

El gusano modificaba la velocidad de operación de muy rápido a despacio, y viceversa.

Actualmente se conoce como un prototipo entre agencias ligadas a los gobiernos de Israel y los EEUU que "accidentalmente" se salió de control.

Infección

El gusano afectó equipos Windows con el software Siemens instalado.

Entonces, atacaba a los sistemas PLC que tuvieran en la configuración guardada la opción para cambiar la frequencia de las turbinas.

En algunos bloques de memoria cambiaba la velocidad del dispositivo a tiempos aleatorios, además de instalar un rootkit para esconderse, y para que los cambios no se registraran en las bitácoras.

Duqu

En 2011, un gusano idéntico fue liberado, pero como un spyware para cachar el teclado y otra información privada.

Ambos gusanos se cree que fueron creados en el 2007. Algunas otras variantes están ahí en internet.

Flame

Atacaba equipos Windows, se utilizó para el cyber espionaje en países del medio oriente.

Tomaba screenshots, el teclado, actividad de red, podía espiar conversaciones de Skype, y utilizar la conexión bluetooth para obtener información de contacto de dispositivos cercanos.

Se le ordenó remotamente autodestruirse una vez que fue descubierto.

Instalación

Básicamente, el gusano Flame utilizaba una vulnerabilidad de los servicios de Windows de algunos clientes, y abusaba de un error en la configuración de los Servidores de Microsoft, permitiendo a un atacante falsificar una actualización de Windows.

Microsoft Security Advisory (2718704)

Certificados digitales podrían permitir spoofing.

Los ataques activos utilizaban certificados digitales no autorizados, pero derivados de una Autoridad de Certificados de Microsoft. Un certificado no autorizado podría ser utilizado para falsificar contenidos, ejecutar ataques de phishing, o ejecutar ataques man-in-the-middle. Este problema afectó a todas las versiones distribuidas de Microsoft Windows.

Acerca del aviso

Esencialmente, la actualización revocaba un par de certificados del servicio de Licencia de Servidor de Terminales

El servicio de Terminal autoriza a una computadora que pertenezca al sistema a utilizar los recursos computacionales del servidor: interfaz, el Office, etc.

Esto permite tener terminales tontas en equipo viejo de bajo perfil, o para compartir licencias de software.

¿Porqué la revocación?

Estos certificados estaban pensados para autorizar clientes de terminal, sin embargo, estaban ligados al mismo certificado raíz utilizado para firmar, por ejemplo, para firmar actualizaciones de Windows.

Esencialmente, cualquiera que tuviera una licencia de Terminal de windows podría no solo firmar certificados de clientes de terminal en su red, sino que también tenían activada la opción de firmar código (por lo que se podrían firmar actualizaciones de Windows).

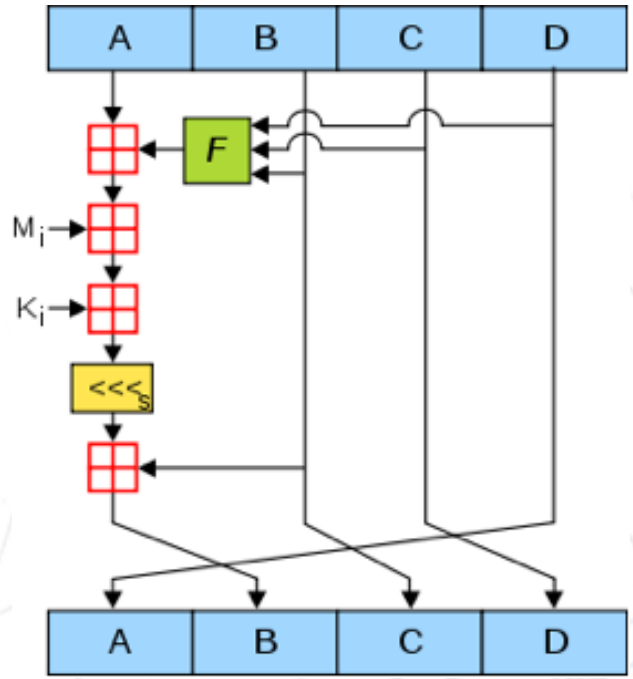
Actualización sobre el aviso 2718704

El malware Flame utilizaba un ataque de colisión criptográfica en combinación con los certificados del servidor de licencias de terminal, para firmar código malicioso que pareciera ser de Microsoft. Sin embargo, la firma de código sin colisión también es posible.

El ataque con colisión fue posible, debido a que el certificado del 2009 ¡seguía utilizando un resúmen MD5!

Ataques de colisión MD5

1996. ”El presente ataque no presenta aplicaciones prácticas sobre MD5, pero son claramente próximas en el futuro, MD5 no debería de ser implementado cuando una función picadillo resistente a colisiones sea requerida.”



¿Porqué la colisión?

Los certificados de las licencias del cliente de terminal funcionaban para firmar código para las versiones de Windows Vista o anteriores.

Las versiones actuales de Window se quejaban de las extensiones del certificado del servidor de Terminal, por lo que crearon un certificado con una colisión MD5, ¡pero sin las extensiones! //con eso, podían validar malware como software Microsoft en Windows 7.

El costo de la colisión

En el 2008, un grupo de científicos encontró una colisión en 1 día utilizando un clúster de PS3.

Cualquier agencia gubernamental con fondos suficientes puede hacer un certificado con una colisión…¿pero quién?

Ahora, el resto de los certificados Microsoft expirarán en el 2020…¡tal vez sea redituable intentarlo!

Detalles

Para mayores detalles, nos cambiaremos a la presentación de Alex Sotirov's.

Analizando la colisión MD5 en el gusano Flame

También vea: http://blog.didierstevens.com/2012/06/04/flame-before-and-after-kb2718704/

¿Porqué está cambiando la seguridad en las TI?

Basicamente, el gusano Flame estuvo cerca de dos años en la red, ¡sin que nadie lo detectara!

Una vez detectado, se autodestruyó para evitar un análisis forense, sin embargo, algunas firmas de seguridad consiguieron obtener una copia.

¡Se necesitan más maneras para detectar malware!

Time-to-live

Durante la guerra Vietnam-EEUU, un soldado tenía una expectativa de vida de menos de 15 segundos cuando saltaba desde un helicóptero bajo fuego (en la práctica era más si no estabas en el primer grupo).

Las amenazas actuales son los malware en la red. ¿Cuánto tarda un computadora sin protección estar a salvo antes de recibir un ataque exitoso por parte de un malware?

Tiempo antes de un ataque/infección

- En el 2003, un equipo windows sin protección podía estar limpio por 40 minutos.
- En el 2004, se redujo a 20 minutos.
- En el 2008, un equipo Windows XP podía estar seguro por 16 minutos (ese es el tiempo que uno disponía para bajar e instalar un antivirus en una máquina nueva)

Windows 7 es un mejor producto, puede sobrevivir de 40 a 200 minutos en internet (Linux entre 400 y 1400, no hay dato para una Mac, pero se presume que es alrededor del mismo)

Lo importante

¡Ese es el tiempo para los ataques detectables!

Un ataque sofisticado como el gusano Flame estuvo grabando conversaciones en Rusia, Irán, Israel, Egipto, Pakistán, Afganistán, y quién sabe qué otros países sin que nadie lo notara.

Es la pieza más sofisticada de malware a la fecha, y no sabemos quién la hizo.

La parte fea

Obama ordenó incrementar los atauqes a las computadoras Iraníes que tuvieran relación con la industria nuclear, y el enriquecimiento de Uranio.

Ahora se sabe que el gusano Stuxnet que destruyó las centrífugas en Irán y el gusano Flame comparten parte del código.

Un nuevo gusano se ha detectado, este estuvo recolectando archivos de AutoCAD (planos de instalaciones) y correos de China.

Seguridad Nacional

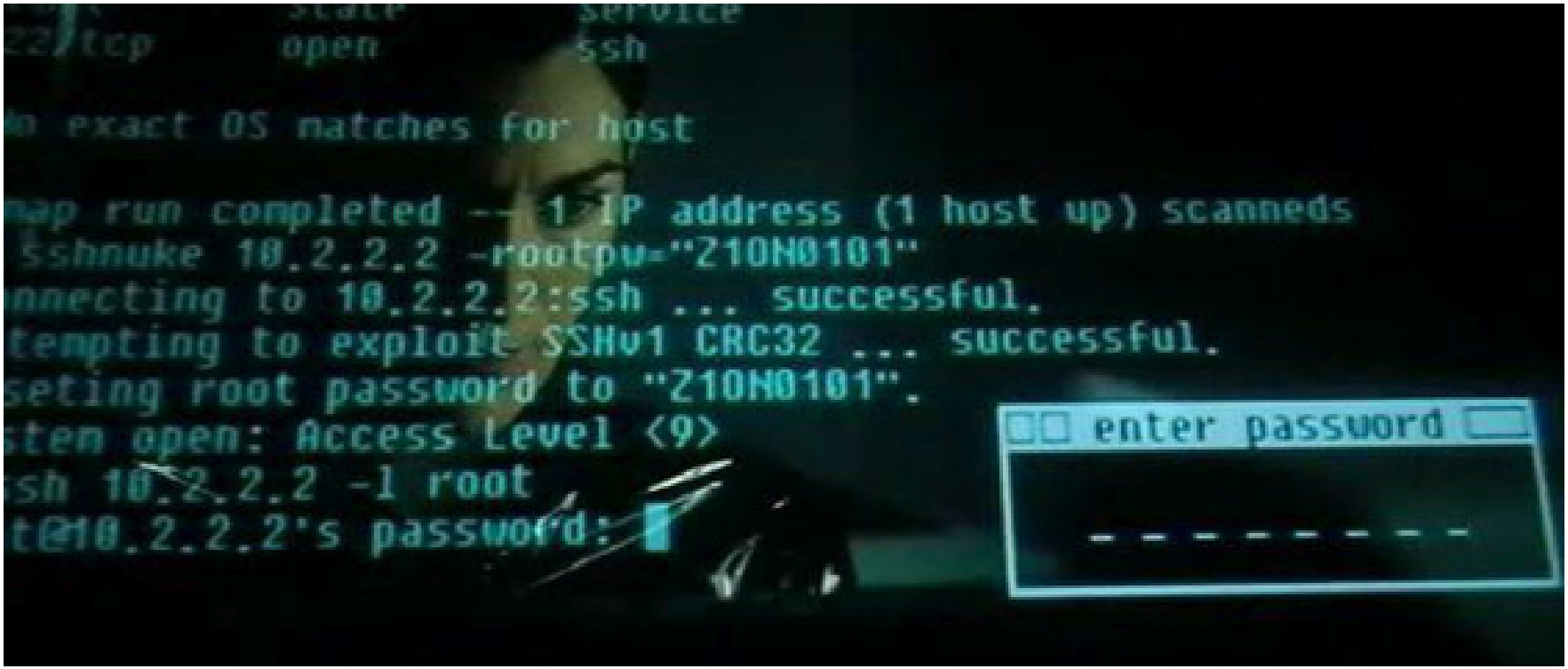
- En el pasado, algunos científicos Iraníes han sido asesinados o han muerto en circunstancias cuestionables.
- Es bien sabido que Israel realizó algunos de estos asesinatos dado que se sienten amenazados por las fuerzas Iraníes.
- Lo mismo pasa entre los EEUU y China (aunque en este caso no ha habido muertes).

Algunos piensan que están protegiendo sus propios intereses, otros piensan que sólo son pro-activos.

Definición

- Una vulnerabilidad en el sistema, cuando es explotada, reduce la confianza de un sistema computacional.
- Un lenguaje de programación o biblioteca dificil de usar presenta una tendencia a proveer vulberabilidades.
- Un programa con permisos elevados son objetivos comunes. Otros programas con acceso a permisos también son un objetivo.

Definición


open ssh
exact OS matches for host
run completed -- 1 IP address (1 host up) scanneds
sshnuke 10.2.2.2 -rootpw="Z1ON0101"
nnecting to 10.2.2.2:ssh ... successful.
tempting to exploit SSHv1 CRC32 ... successful.
seting root password to "Z1ON0101".
sten open: Access Level <9>
sh 10.2.2.2 -l root
t@10.2.2.2's password:
enter password

¿Porqué hay vulnerabilidades?

- Software
  - falta de pruebas
  - falta de auditoría
- Red
  - texto plano en la red
  - errores de diseño de en la red
- Gente
  - entrenamiento inadecuado
  - inconsciencia sobre la seguridad
- Administración del sistema
  - falta de auditoría
  - inexistencia de política de seguridad
  - administración del recurso humano

Vulnerabilidades Zero-day

Es un ataque que utiliza una vulnerabilidad desconocida públicamente. No hay mecanismo conocido para defenderse de ella, salvo que siga algún patrón anterior.

Los atacantes utilizan vulnerabilidades zero-day ara entrar en sistemas remotos o locales, ganando permisos sobre el sistema objetivo para lanzar otro ataque.

¿Quién es susceptible a los 0-day?

Todos y cada uno de los sistemas computacionales posiblemenete tengan una vulnerabilidad zero-day.

Mientras más complejo sea el sistema, más costosa de comprar es una vulnerabilidad de este tipo.

Cada malware entra a un sistema mediante una vulnerabilidad zero-day. Los espías modernos utilizan sus propias vulnerabilidades zero-day para espiar sistemas nacionales o extranjeros.

Smartphones

Hoy en día las tendencias en tecnología se concentran en la movilidad de los recursos computacionales.

Esta una época que comenzó con un "mientras más chico mejor", y de pronto súbitamente se transformó en una que buscaba lo más grande dentro de lo pequeño.

De un diminuto teléfono de pulsera o un váder, pasó a teléfono con pantalla ancha de 4 pulgadas, de un lector de 6 pulgadas a una tablet de 10.

Smartphones

Este cambio en los dispositivos, también tuvo un cambio en requerimientos: De poder leer un correo o leer un libro, ahora que busca que se pueda escribir el libro, escribir el correo, hcaer miles o millones de cálculos por segunto, e incluso jugar y ver películas.

Toda esta potencia en recursos no solamente ha hecho que la gente lleve sus equipos al trabajo y los use como herramienta, sino que ha hecho que la gente lleve su trabajo a sus equipos.

En algunos países ha creado una tendencia conocida como "trae tu propio dispositivo" (BYOD)...

Bring your own device

Con esta nueva tendencia, de llevar sus propios dispositivos como requisito (al igual que es el coche en algunos casos), se crea en el teléfono una extensión de la oficina, conviertiéndose en el nuevo SOHO de 24 horas.

En este caso, tiene una gran ventaja en cuanto a costos para la empresa, al requerir que los usuarios lleven sus propios equipos, es el usuario el que termina gastando sus propios planes de datos.

Tu teléfono, tu recibo

Al comprar un Smartphone, es normalmente un requisito contratar costosos planes de pago. Aún al haber pagado una gran suma de dinero, la primer sorpresa para los primerizos, es que además necesitan de un plan de datos para sacarle jugo a su equipo [1].

Es precisamente este plan de datos lo que hace atractivo un smartphone, y en su conjunto, atractivo para la empresa.

[1] Algunas empresas manejan esto como una prestación

Acceso a información desde un Smartphone

Una de las principales ventajas de un Smartphone, es que se puede acceder a un tipo de información empresarial mucho más compleja, al grado de poder hacer modificaciones o transmitirla al dispositivo.

Desgraciadamente, una de las principales ventajas de un Smartphone es precisamente un catalizador para su principal desventaja: son muy atractivos tanto para la competencia como para los ladrones convencionales.

Esta desventaja es crítica ya que en caso de caer en las manos adecuadas, puede revelar planes y estrategias de la empresa, además de posibilitar un ataque desde el exterior.

Otros dispositivos

Los smartphones no son el único elemento atractivo para el robo de información. Las computadoras portátiles, dispositivos USB o memorias en general, son tnato fuente de información como punto de acceso remoto para un atacante. Cada año alguna gran empresa sufre un robo de información masivo o sensible.

Para proteger estos equipos, normalmente es sencillo al establecer un mecanismo de cifrado, y llevar una política que obligue a introducir credenciales de acceso manualmente.

Espionaje

El espionaje ha existido desde tiempos ancestrales. El espionaje busca la obtención de datos o información confidencial.

En el siglo pasado tuvo su climax, principalmente durante la segunda guerra mundial y la guerra fría. Una serie de industrias se crearon o florecieron a su alrededor. En fechas recientes el espionaje se ha centrado sobre los secretos industriales.

Espionaje moderno

En la era moderna, los datos e información se almacenan en dispositivos electrónicos. Los dispositivos electrónicos tienen la facilidad de que los datos son muy fáciles de copiar.

Es precisamente esta facilidad que hace el contra espionaje particularmente difícil hoy en día.

Cyberguerra

Un concepto que ha tomado auge en estos últimos años es el de cyberguerra.

En esta guerra de espías electrónicos, grupos secretos financiados por los gobiernos (o parte del gobierno), entablan entre sí ataques en internet, esto con la finalidad de ganar acceso a las redes privadas de otros países.

¿Porqué los ataques?

Si nadie China no está en guerra con los EEUU, ni otros países que tienen cyber ataques entre sí, ¿porqué se atacan?

¿Porqué los ataques?

Si nadie China no está en guerra con los EEUU, ni otros países que tienen cyber ataques entre sí, ¿porqué se atacan?

Afección a los usuarios

Con la excusa de detectar posibles sabotajes, ya sea contra la integridad del presidente, del país o de ciertos intereses, existen políticas para garantizar la estabilidad de un país.

Dichas prácticas tienen a violar la privacidad y anonimidad de los usuarios de internet.

¿Qué se puede hacer?

- Ser respetuoso de las leyes de cada país

¿Qué se puede hacer?

- Ser respetuoso de las leyes de cada país
- Cifrar archivos o información personal o importante

¿Qué se puede hacer?

- Ser respetuoso de las leyes de cada país
- Cifrar archivos o información personal o importante
- Utilizar anonimizadores, como Tor.

¿Qué se puede hacer?

- Ser respetuoso de las leyes de cada país
- Cifrar archivos o información personal o importante
- Utilizar anonimizadores, como Tor.
- Estar al día ante amenazas computacionales.

¿Qué se puede hacer?

- Ser respetuoso de las leyes de cada país
- Cifrar archivos o información personal o importante
- Utilizar anonimizadores, como Tor.
- Estar al día ante amenazas computacionales.

¿Con esto es suficiente?

¿Qué se puede hacer?

- Ser respetuoso de las leyes de cada país
- Cifrar archivos o información personal o importante
- Utilizar anonimizadores, como Tor.
- Estar al día ante amenazas computacionales.

¿Con esto es suficiente? No, ciertos gobiernos tienen muchísimo dinero y tecnología, además es conveniente no llamar la atención si no se quiere perder la privacidad.

Contramedidas a las vulnerabilidades

El libro naranja de Criterios de Evaluación de Sistemas Computacionales Confiables (Trusted Computer System Evaluation Criteria) establece diversos niveles de seguridad.

- D - Protección mínima del sistema
- C - Protección discrecional
- B - Protección obligatoria
- A - Protección verificada.

Sistemas nivel D

El sistema ha sido evaluado pero ha fallado en proveer seguridad

Sistemas nivel C

Protección discrecional

- Protección de seguridad discrecional: Autenticación de usuario, separación de usuarios y datos, DAC - control de acceso discrecional, documentación del sistema
- Protección de acceso controlado: autenticación de usuario finamente granulada y DAC, pistas de auditoría, aislamiento de recursos, contabilidad de los procesos de autenticación.

Sistemas nivel B

Protección mandatoria

- B1 - Protección de seguridad basada en etiquedas: modelo de seguridad informal, etiquetas para datos privados, Control de Acceso Obligatorio sobre objetos seleccionados, especificaciones de diseño, y verificación
- B2 - Protección estructurada: DAC and MAC obligatoria para todos los objetos, controles de administración estrictos, confianza en la administración, y segregación de operadores
- B3 - Dominios de seguridad: excluya código que no sea esencial para la operación, diseñe para una complejidad mínima de los sistemas, auditoría a la emisión de alertas de seguridad importantes, definición de roles en la administración de la seguridad, dispositivos IDS/IPS automatizados

Sistemas nivel A

Protección verificada

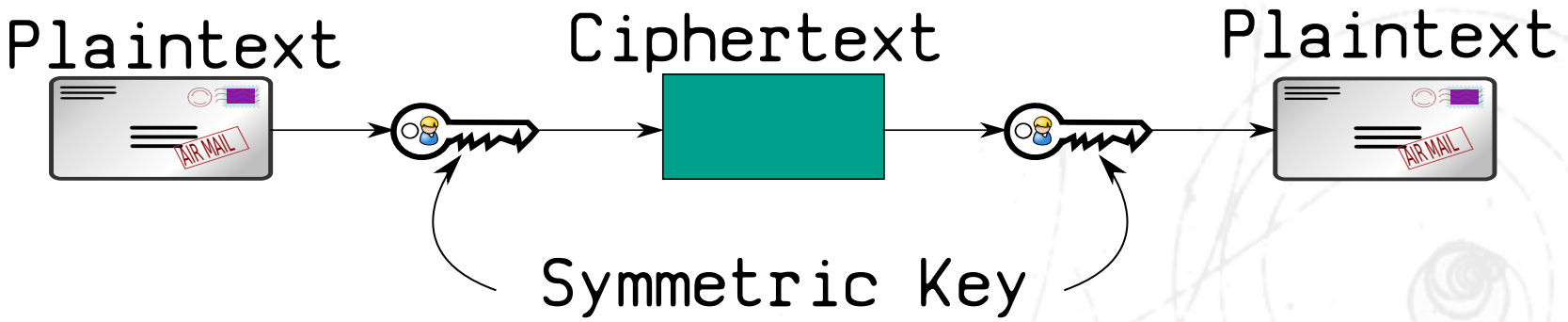
- A1 - Diseño verificado: diseño formal y procedimientos verificados, roles formales en la administración de la seguridad
- Más allá del A1: Sistemas autoprotegidos, diseño de confianza operado por elementos de confianza solamente, procedimientos de prueba de software completos de arriba hacia abajo, incluyendo las especificaciones de bajo nivel.

Contenido, sección 4

Cryptography basics

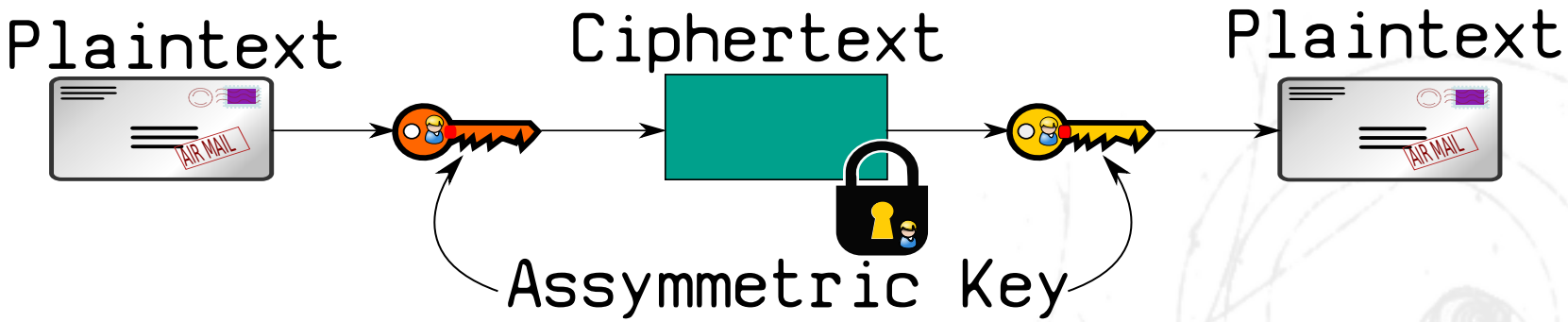
Cryptography supports *symmetric encryption* and *asymmetric encryption* for cryptographic functions:

- **Symmetric Encryption.** The same key is used for both encryption and decryption. The key has to be exchanged between the parties in a secure way.



Cryptography basics II

- **Asymmetric Encryption.** Two different, but mathematically related keys are used to encrypt and decrypt the information. Only the public key is needed for other parties. We can broadcast it, there is no need for an exchange protocol.



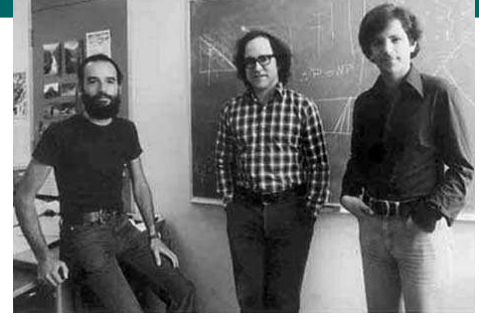
Asymmetric Key


The public release of the public key cryptosystem by Diffie and Hellman in 1976 not only created modern cryptography, but also concentrated the Computational Number Theory efforts in this direction.

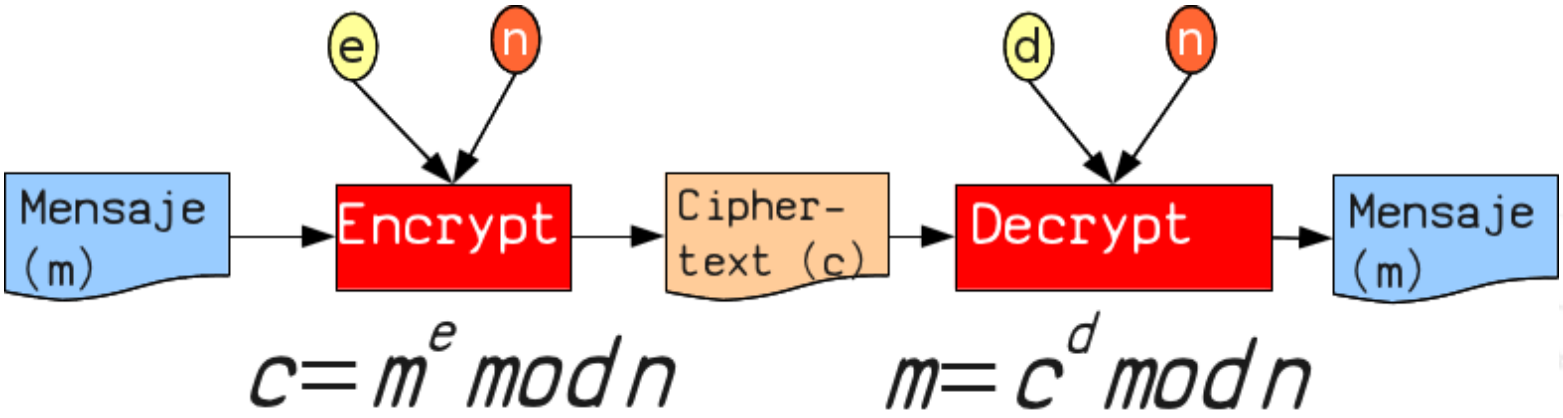
Given a (g, g^x, g^y) what is the value of g^{xy}?

This is meant to be infeasible for sufficiently large values.

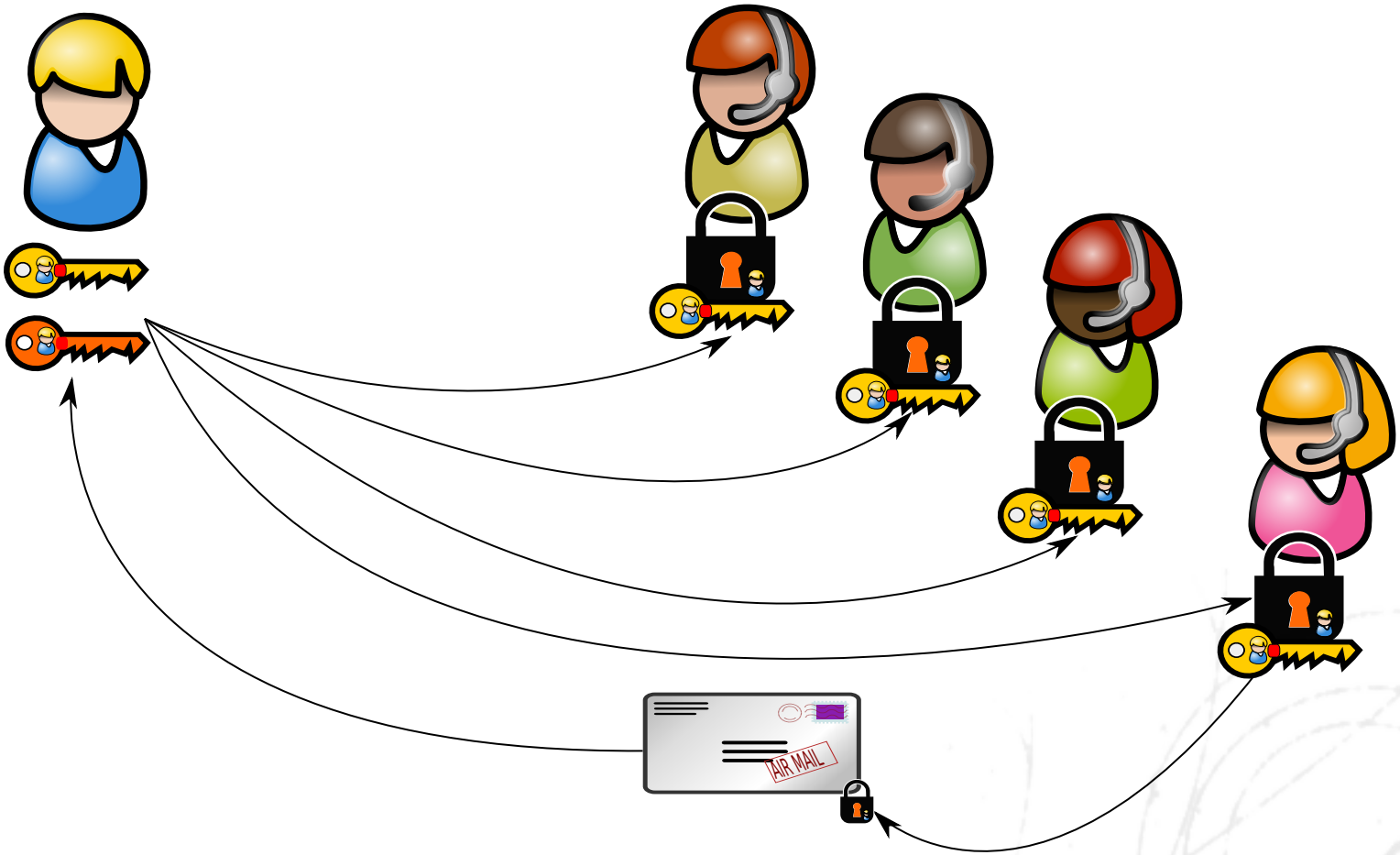
The RSA model



In 1978, the RSA scheme was introduced as the first usable public key cryptosystem. It was based on the problem of factoring large integers.

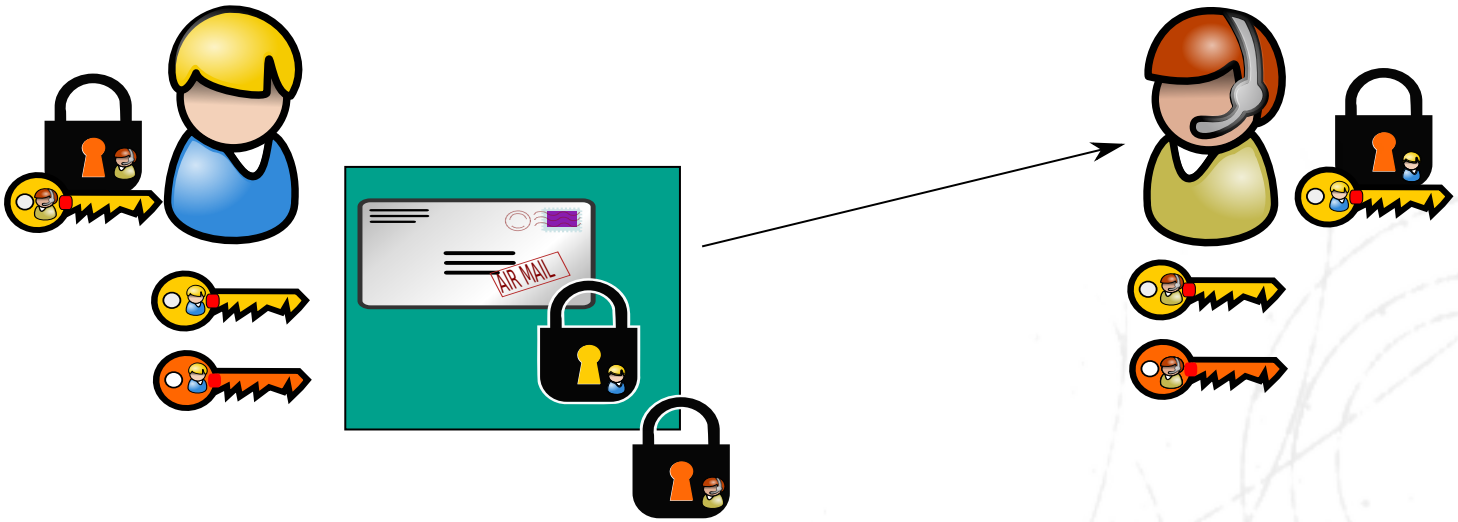


Secret and Public Key



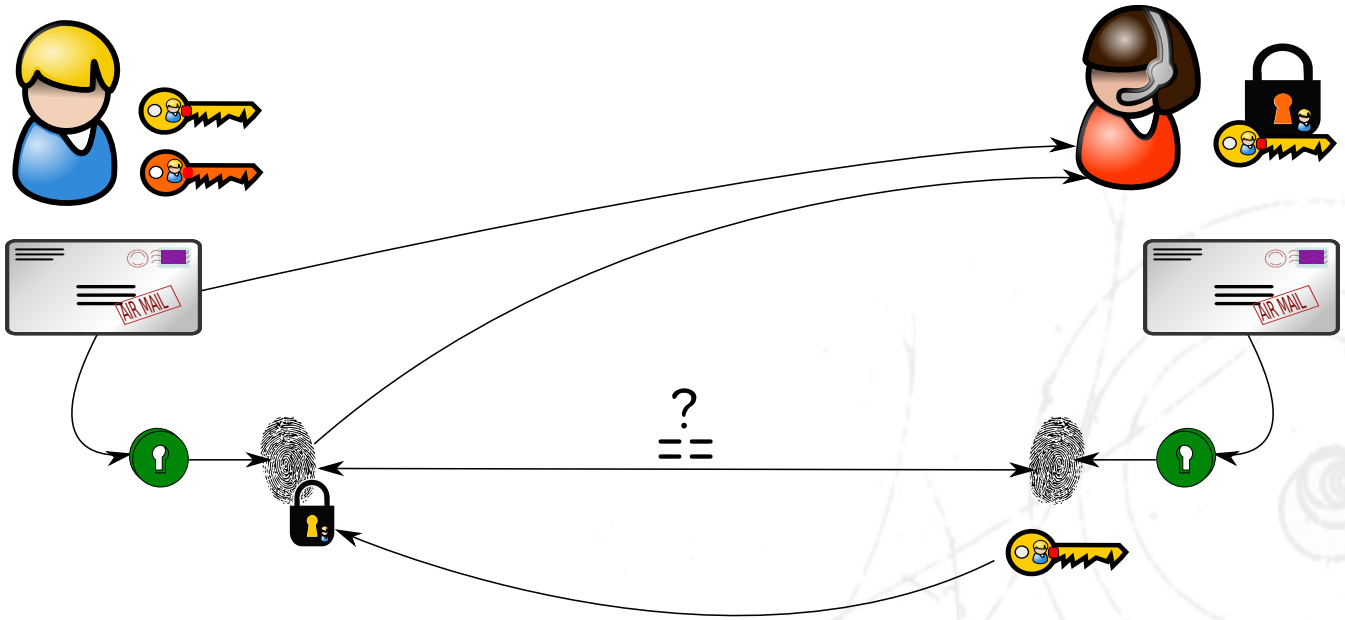
Protecting a message

- Protect the message with our private key so that, everybody will know I sent the message.
- Use recipient's public key so that, only the recipient (owning that private key) reads the message.



Signature of a message

- Sender: Gets the digest of our message
- Sender: Uses our private key on that, send both to the recipient.
- Recipient: Applies the public key of the sender on the message, compare.

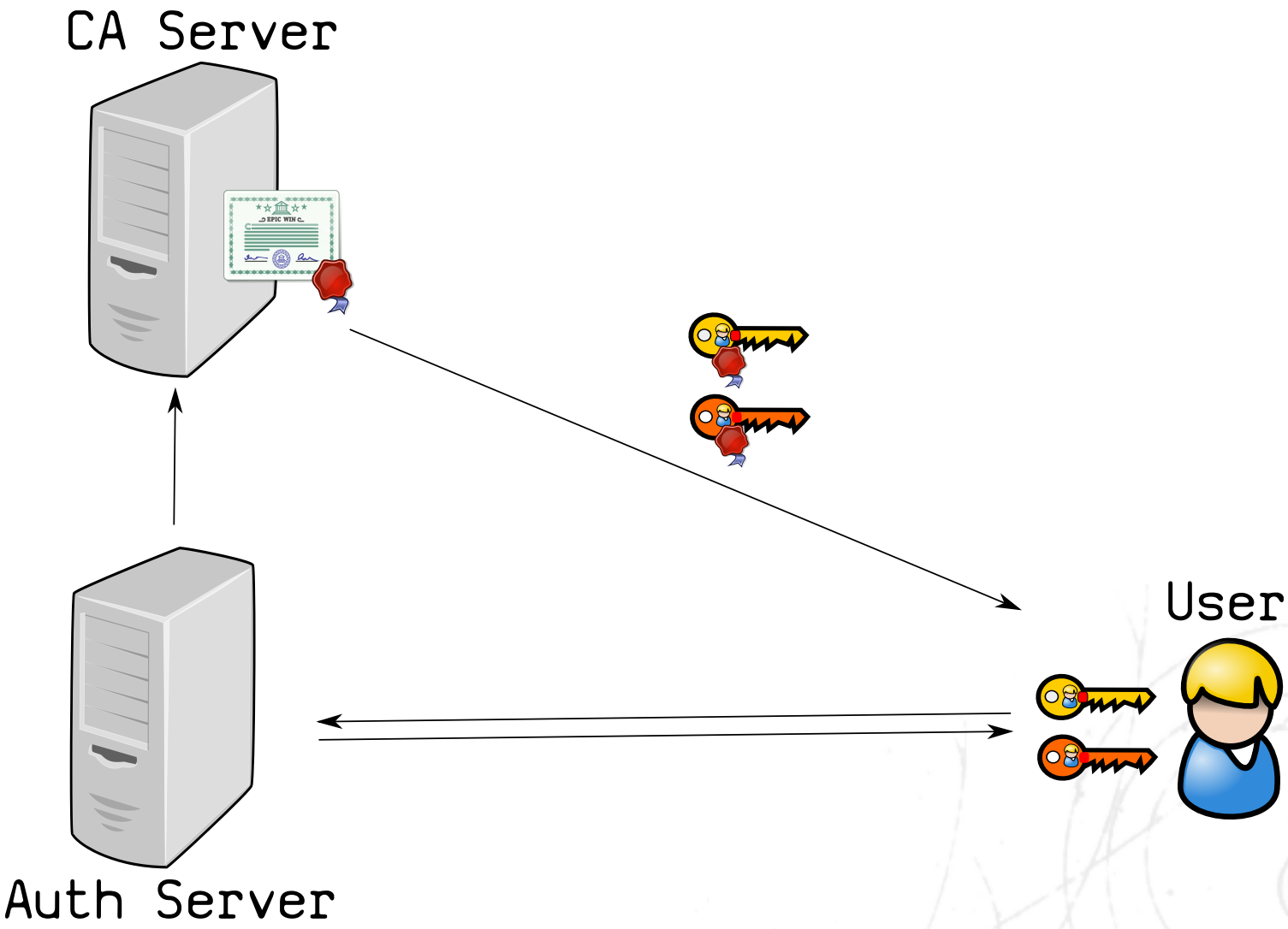


Public Key Infrastructure

- but how do I know the recipient is actually she?
- what about the sender?

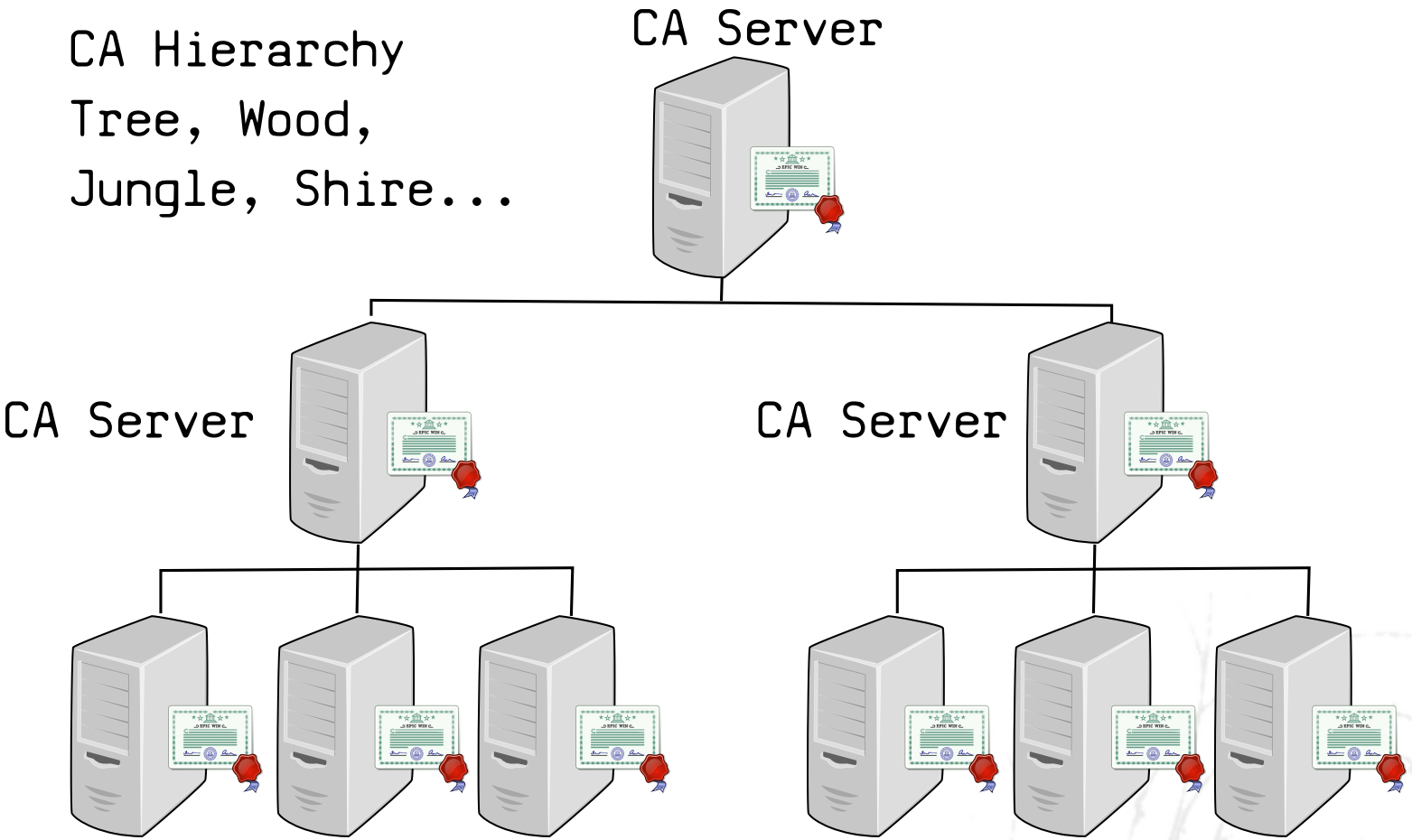
to solve this, we have Public Key Infrastructure...

Public Key Infrastructure



Public Key Infrastructure

CA Hierarchy
Tree, Wood,
Jungle, Shire...



Public Key Infrastructure

CA Hierarchy
Tree, Wood,
Jungle, Sh...

CA Server

CA Server

Even more servers...

Public Key Infrastructure

- To encrypt a message for a user, we get her public key (along with its certificate) in a quite similar process.

Public Key Infrastructure

- To encrypt a message for a user, we get her public key (along with its certificate) in a quite similar process.
- Nice, we have the keys and the certificates stored, how they look like?

They look like a really long sequence of numbers, letters and encoded symbols...

Public Key Infrastructure

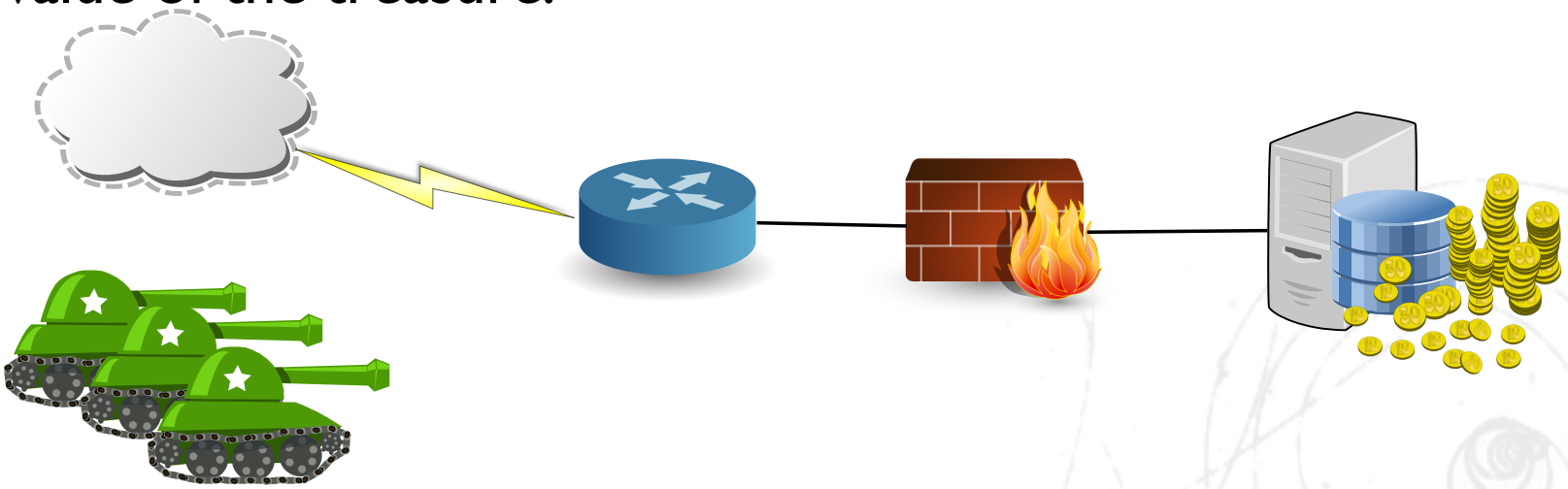
- To encrypt a message for a user, we get her public key (along with its certificate) in a quite similar process.
- Nice, we have the keys and the certificates stored, how they look like?

They look like a really long sequence of numbers, letters and encoded symbols... what do you mean with really long?

Key size and attacks

The main concern about the security of a system, is how long does an attacker need to break it, and how many resources are needed.

The cost of the attack should be balanced with respect to the value of the treasure:



Key size and attacks II

NIST states that an 80-bit symmetric key is equivalent to a 160-bit one using discrete logs subgroups and elliptic curve groups. This is defined as a 80-bit security level, and it is not recommended for use after 2012. An 128-bit security level is recommended therefore after that year.

Equivalent symmetric key size		80	112	128	192	256
NIST	RSA	1024	2048	3072	7680	15360
	EC	160	224	256	384	512
ECRYPT	RSA	1248	2432	3248	7936	15424
	EC	160	224	256	384	512

More complains

- and what happens if the user is not explicitly in the system?
- or what about giving access to a group of users with the same characteristics?

More complains

- and what happens if the user is not explicitly in the system?
- or what about giving access to a group of users with the same characteristics?

Wait!

More complains

- and what happens if the user is not explicitly in the system?
- or what about giving access to a group of users with the same characteristics?

Wait! Why would someone would like to encrypt something for a non-existant user?... That's non-sense!

or is it?

What's next?

Are there anything we can do to solve all of this?

What's next?

Are there anything we can do to solve all of this?

Yes! We can use the Pairing-Based Cryptography.

How does it started?

In 1984, Shamir posed a challenge:

"create a cryptographic system that permits any two users to comunicate securely and to verify each other's signatures without exchanging private or public keys, without keeping key directories, and without using the services of a third party."

How does it started?

In 1984, Shamir posed a challenge:

"create a cryptographic system that permits any two users to comunicate securely and to verify each other's signatures without exchanging private or public keys, without keeping key directories, and without using the services of a third party."

This sounds impossible!

How does it started? 2

However, in 2001, Boneh and Franklin, solved this challenge using cryptographic pairings. They presented what it is now called Identity-Based Encryption.

... also, in 2000, Antoine Joux presented a breaking-through paper involving pairings, but we are focusing in this talk on Identity-Based Encryption.

Pairing-Based Cryptography

Identity-Based Encryption is a type of the Pairing-Based Encryption, this is, we use some cryptographic function called the pairing.

In essence, a cryptographic pairing is a particular function of groups over elliptic curves.

$$\langle \cdot, \cdot \rangle : M \times M \longrightarrow R$$

The bilinear pairing can be used as a primitive to build cryptosystems with certain functionality. Examples of use:

The bilinear pairing can be used as a primitive to build cryptosystems with certain functionality. Examples of use:

- Short signatures schemes,

The bilinear pairing can be used as a primitive to build cryptosystems with certain functionality. Examples of use:

- Short signatures schemes,
- Identity-Based Encryption,

The bilinear pairing can be used as a primitive to build cryptosystems with certain functionality. Examples of use:

- Short signatures schemes,
- Identity-Based Encryption,
- Attribute-Based Encryption,

The bilinear pairing can be used as a primitive to build cryptosystems with certain functionality. Examples of use:

- Short signatures schemes,
- Identity-Based Encryption,
- Attribute-Based Encryption,
- and other protocols already deployed.

Some protocols are impossible with currently deployed technology, in other cases, they are faster.

Example of PBC

Identity-Based Encryption case:

- Enables any pair of users to communicate securely and to verify each others' signatures **without exchanging** private or public keys;
- Needs **no key server repositories**;
- Requires a trusted server for key generation **only**.
- **No certificate required** to bind the public key to the identity.

Implementation issues...

Pairing-Based Cryptography has become relevant in industry.

Although there are plenty of applications, however efficiently implementing the pairings function is often difficult as it requires more knowledge than previous cryptographic primitives.

There are many implementation issues just with the primitive itself!

... implementation issues

- **Non-familiar** technology;
- Lack of **programming framework**;
- More **difficult to understand** compared to the already deployed technology;
- **Unavailability** of implementations with novel (faster) computing methods;
- Complex area.

Depending on the scenario, a developer must choose from a selection of parameters and apply the corresponding optimizations for efficiency...

What to do when... ?

- **bandwidth** use is expensive;
- **low memory** is available;
- a **slow** processor is used (old);
- a **small** processor (in bits) is the only option;
- we have a **Desktop** environment;
- we have a device with **multiprocessors**;
- a **higher security** is required;

Some basic operations that are cheap in some environments are expensive in others!

Protocol primitives

The operations involved in a Pairing-Based protocol are:

- The pairing function
- Elliptic Curve point addition and point doubling
- Scalar-point multiplication
- exponentiation
- hash onto a curve
- hash into a subgroup
- matrix conversion
- boolean function analysis. . .

Many more!

Some background

Let do a bit of maths...

Scalar-point multiplication

Let P be a point in a curve E and $n \in \mathbb{Z}$, $n \geq 0$. Define $[n]P = P + P + \cdots + P$. The order of the point P is the smallest n such that $[n]P = \mathcal{O}$.

Denote $< P >$ the group generated by P. In other words,

$$< P >= \{\mathcal{O}, P, P+P, P+P+P, \ldots\}$$

Let $Q \in < P >$. **Given Q, find n such that $Q = [n]P$ is hard.**

Pairing definition

A **pairing** is a map: $\mathbb{G}_1 \times \mathbb{G}_2 \rightarrow \mathbb{G}_T$.

These groups are finite and cyclic. $\mathbb{G}_1$ and $\mathbb{G}_2$ are additively-written and at least one is of prime order r. $\mathbb{G}_T$, is multiplicatively-written and of order r.

Properties:

- *Bilinearity*
- *Non-degeneracy*
- *Efficiently computable*

Pairing properties

Properties:

- *Bilinearity*

$$e(P + P', Q) = e(P, Q) \times e(P', Q)$$

$$e(P, Q + Q') = e(P, Q) \times e(P, Q')$$

Pairing properties

Properties:

- *Bilinearity*

  $e(P + P', Q) = e(P, Q) \times e(P', Q)$

  $e(P, Q + Q') = e(P, Q) \times e(P, Q')$

- *Non-degeneracy*

  $\forall P \in \mathbb{G}_1, P \neq \mathcal{O}$: $\exists Q \in \mathbb{G}_2$ **s.t.** $e(P, Q) \neq 1$

  $\forall Q \in \mathbb{G}_2, Q \neq \mathcal{O}$: $\exists P \in \mathbb{G}_1$ **s.t.** $e(P, Q) \neq 1$ $\quad$ $e(P, Q) \neq 1$

Pairing properties

Properties:

- *Bilinearity*

  $e(P + P', Q) = e(P, Q) \times e(P', Q)$

  $e(P, Q + Q') = e(P, Q) \times e(P, Q')$

- *Non-degeneracy*

  $\forall P \in \mathbb{G}_1, P \neq \mathcal{O}$: $\exists Q \in \mathbb{G}_2$ **s.t.** $e(P, Q) \neq 1$

  $\forall Q \in \mathbb{G}_2, Q \neq \mathcal{O}$: $\exists P \in \mathbb{G}_1$ **s.t.** $e(P, Q) \neq 1$ $\quad$ $e(P, Q) \neq 1$

- *Efficiently computable*

(Ab)Using the pairing

The most important property of a pairing is:

$$e([a]Q, [b]P) = e([b]Q, [a]P) = e(Q, [ab]P) = e(Q, P)^{ab}$$

where $Q \in \mathbb{G}_2$, $P \in \mathbb{G}_1$, and the result is in $\mathbb{G}_T$.

In our context, the $\mathbb{G}_2$ group is larger than $\mathbb{G}_1$. The group $\mathbb{G}_T$ is also larger and has a different set of operations.

(Ab)Using the pairing II

- Since $\mathbb{G}_2$ is larger than $\mathbb{G}_1$, it is wise to exchange operations from one group to the other.

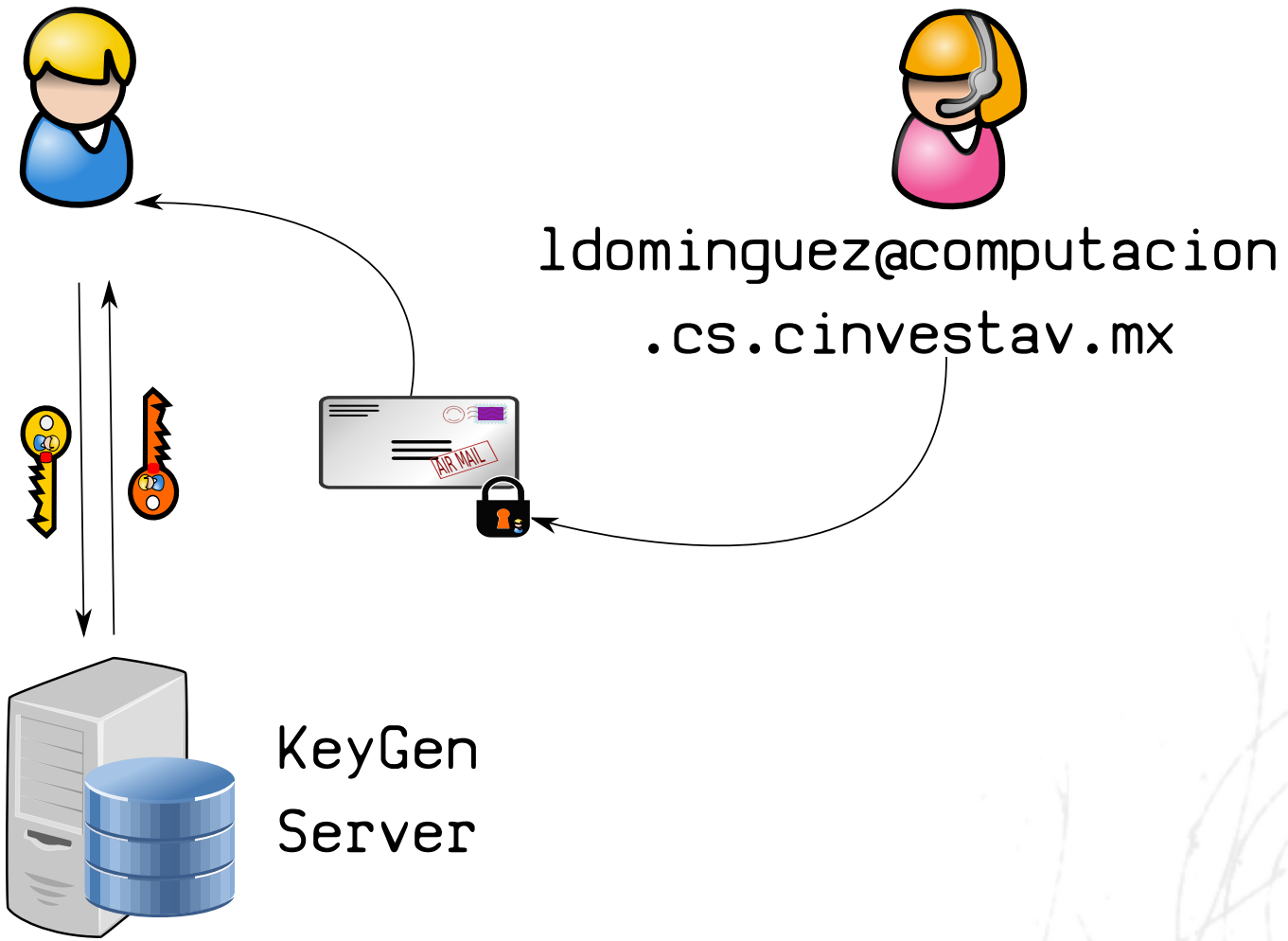
- $\mathbb{G}_T$ is significantly larger and has a different set of operations, we also try to avoid it, but we keep it handy, because...

(Ab)Using the pairing II

- Since $\mathbb{G}_2$ is larger than $\mathbb{G}_1$, it is wise to exchange operations from one group to the other.
- $\mathbb{G}_T$ is significantly larger and has a different set of operations, we also try to avoid it, but we keep it handy, because...
- An operation in $\mathbb{G}_T$ is cheaper than computing the pairing itself.

In short, we use the groups at will.

Encryption for an identity

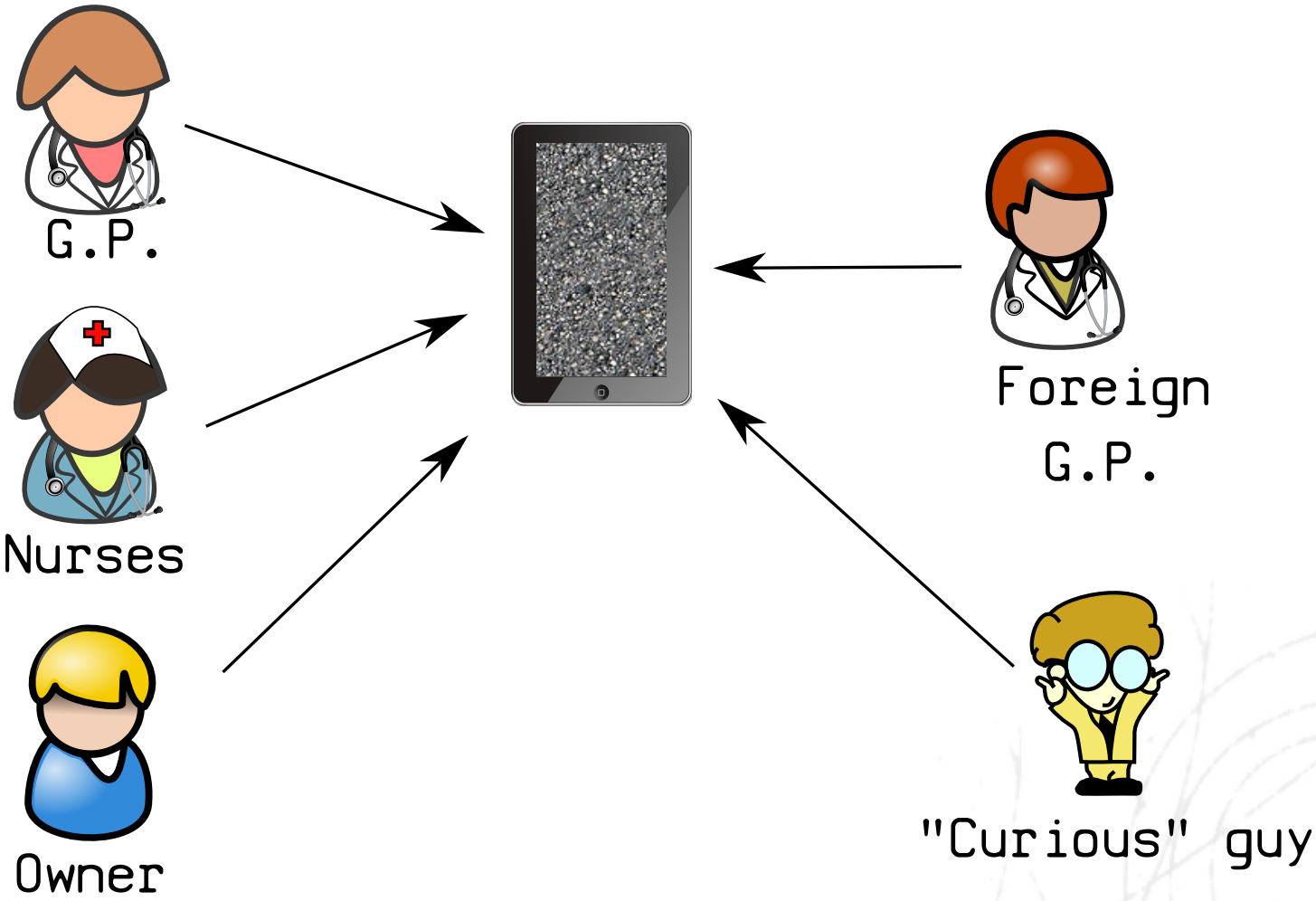


Attribute-Based Encryption

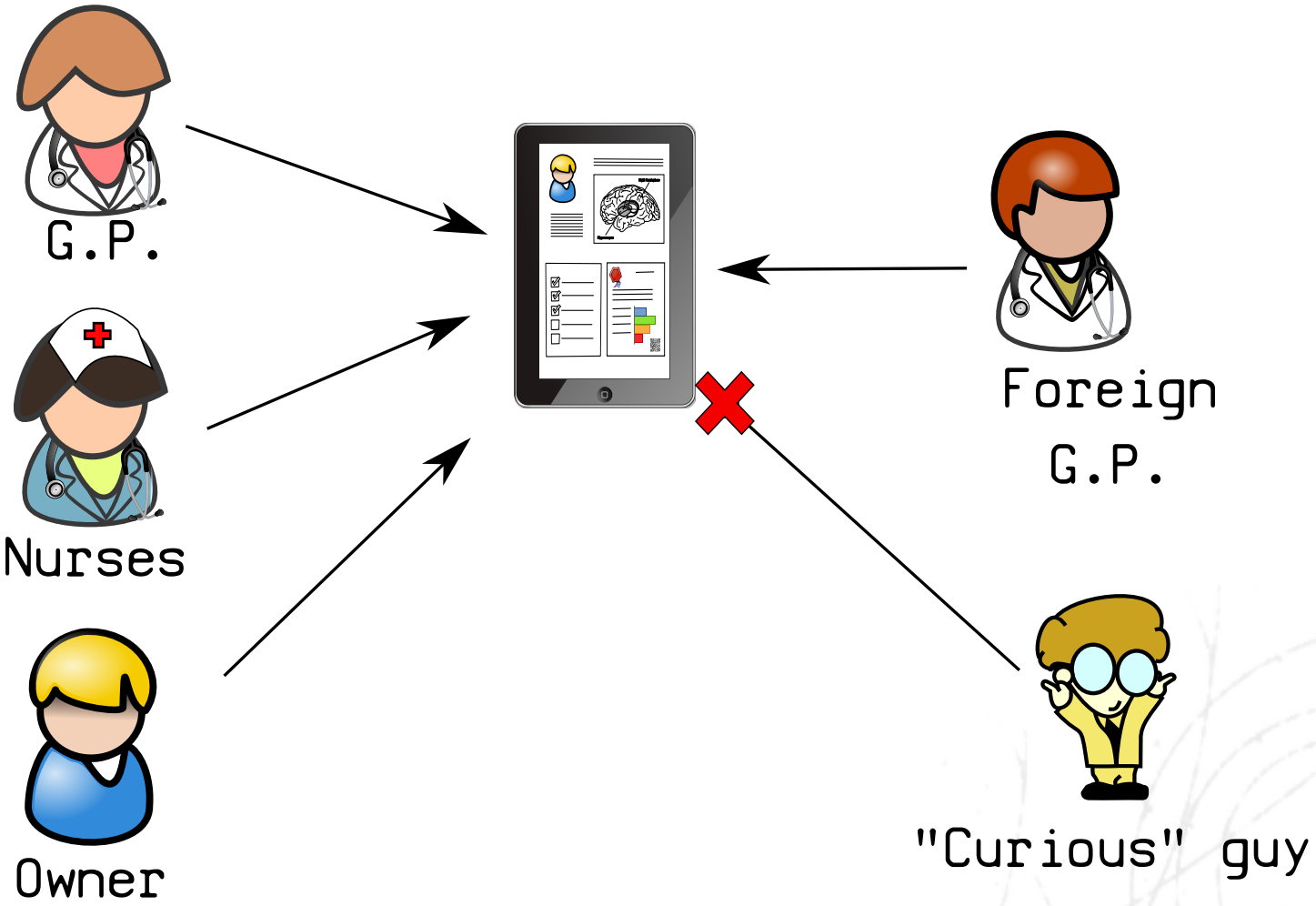
Fuzzy Identity-Based Encryption. Also known as Attribute-based encryption.

- An identity is a set of attributes
- An entity is valid if it presents a minimum number of attributes
- Better for sharing a small secret: a symmetric key.

Attribute examples



Attribute examples



Boneh's short signatures

Boneh's short signatures are based on the mathematical problem:

Given $(P, [a]P, Q, [b]Q)$, it is hard to decide if $a = b$

The computational variant of this hard problem is:

Given $(P, Q, [n]Q)$, compute $[n]P$

Boneh, Lynn and Shacham constructed a short signature scheme based on this problem as follows:

... the steps

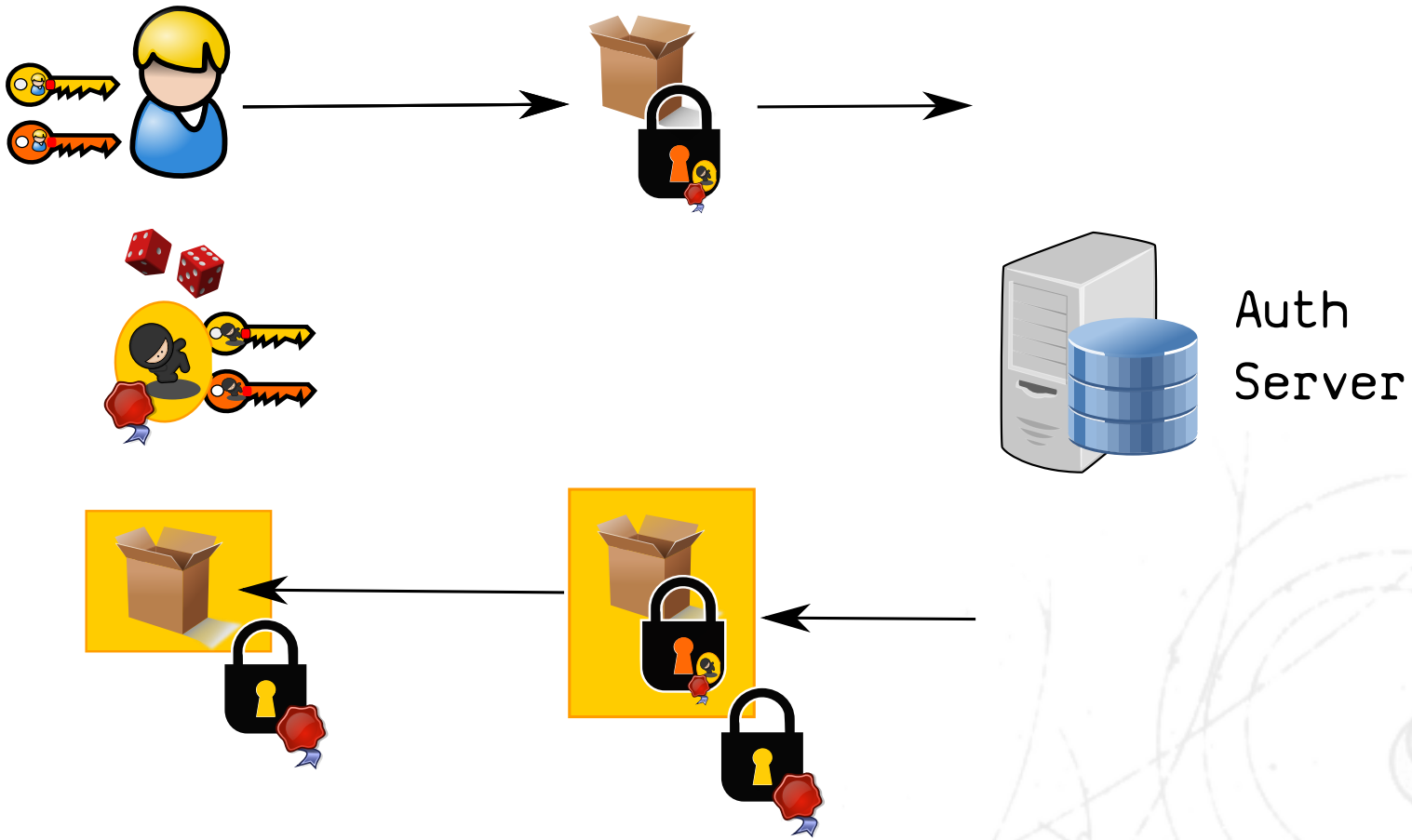
Key generation. Choose $n \in_R \mathbb{Z}_r$, set $R \leftarrow [n]Q$. The public key is: Q, R. The secret key is n

Sign. Map to a point the message to sign as P_M, set $S_M \leftarrow [n]P_M$. The signature is the x-coordinate of S_M.

Verify. Given the x-coordinate of S_M, find $\pm S$. Decide: $e(Q, S) \stackrel{?}{=} e(R, h(M))$

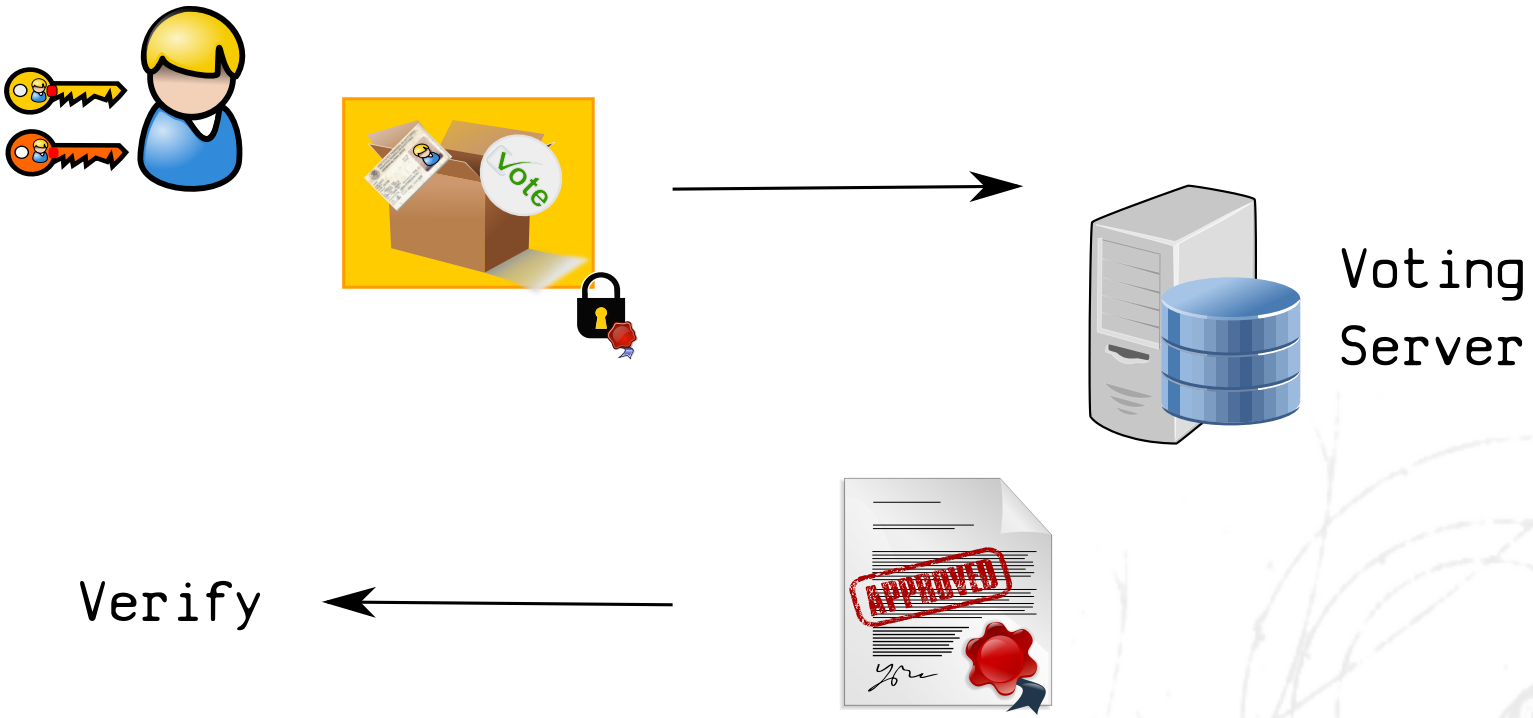
e-voting system based on pairings

An e-voting system based on short and blind signatures by Lopez-Garcia and Rodriguez-Henriquez.



e-voting system based on pairings

With a blind signature, we can cast our vote in the blank ballot.



Detailed e-voting system... 1/2

An e-voting system based on short and blind signatures by Lopez-Garcia and Rodriguez-Henriquez.

Authentication phase

Voter		Authentication Server (AS)
$b, d_t \in \mathbb{Z}_r$		
$V_t = [d_t]Q \in \mathbb{G}_2$		
$m = m2s(V_t) \in \{0,1\}^{1016}$		
$\tilde{M} = [b]H_1(m) \in \mathbb{G}_1$		
$S_{\tilde{M}} = [d_V]\tilde{M} \in \mathbb{G}_1$		
	$\{ID_V, t, \tilde{M}, S_{\tilde{M}}\}$ $\longrightarrow$	
		$e(Q, S_{\tilde{M}}) \stackrel{?}{=} e(V_V, \tilde{M})$
		$\tilde{S} = [d_{AS}]\tilde{M} \in \mathbb{G}_1$
	$\{t, \tilde{S}\}$ $\longleftarrow$	
$S_{V_t} = [b^{-1}]\tilde{S} \in \mathbb{G}_1$		

... detailed e-voting system 2/2

Voting phase

Voter		Voting server (VS)
$S_v = [d_t]H_1(v) \in \mathbb{G}_1$		
$B = \{V_t, S_{V_t}, v, S_v\}$	$\xrightarrow{\{B\}}$	$m = m2s(V_t)$
		$e(Q, S_{V_t}) \stackrel{?}{=} e(V_{AS}, H_1(m))$
		$e(Q, S_v) \stackrel{?}{=} e(V_t, H_1(v))$
		$a \in \mathbb{Z}_r$
		$ACK = H(V_t\|\|S_{V_t}\|\|v\|\|S_v\|\|a)$
		$S_{ACK} = [d_{VS}]H_1(ACK)$
	$\xleftarrow{\{ACK, S_{ACK}\}}$	
$e(Q, S_{ACK}) \stackrel{?}{=} e(V_{VS}, H_1(ACK))$		

Timings of the e-voting protocol

Scheme	# Cryptographic operation	# Cycles
Kharchineh & Ettelace	4 RSA-public	6,053,528
	6 RSA-private	253,251,894
	4 DLP-exponentiations	87,135,920
	Total	**346,441,342**
Li et al.	15 RSA-public	22,700,730
	9 RSA-private	379,877,841
	Total	**402,578,571**
Chung & Wu	5 RSA-public	7,566,910
	4 RSA-private	168,834,596
	Total	**176,401,506**
The proposed scheme	1 scalar multiplication in $\mathbb{G}_2$	380,000
	6 scalar multiplications in $\mathbb{G}_1$	1,800,000
	6 map-to-point functions H_1	1,890,000
	8 bilinear pairings	14,630,000
	Total	**18,700,000**

Contenido, sección 5

Echelon

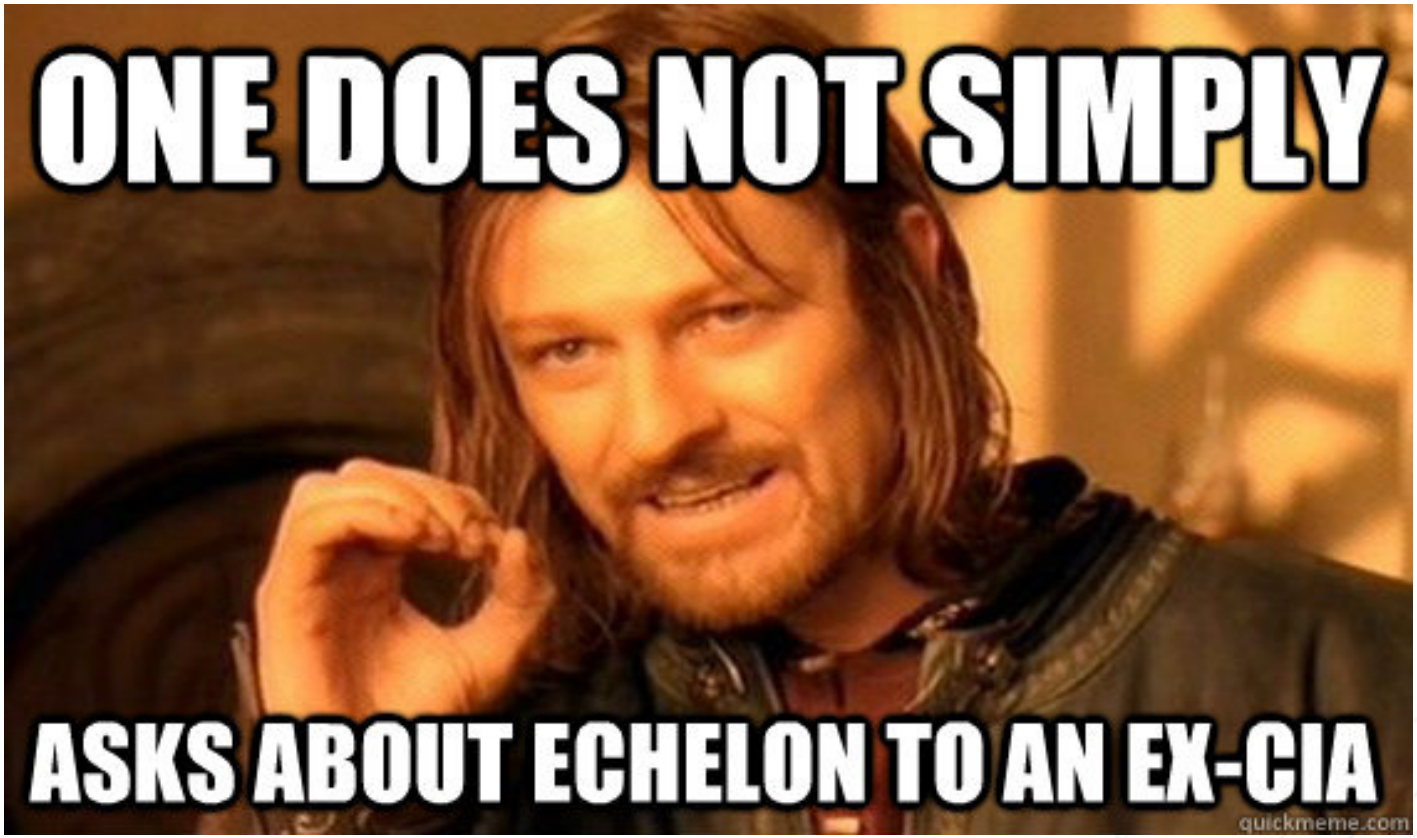
- Echelon es el nombre utilizado en los medios internacionales y en la cultura popular para describir una red de recolección y análisis de señales de inteligencia para los firmantes del acuerdo UKUSA de Seguridad (Australia, Canada, Nueva Zelanda, el Reino Unido, y los E.E. U.U.)

- También se le ha descrito como el software que controla la descarga y diseminación de los troncales de comunicación satelital comercial (no-militar).

Sobre su existencia

- Hay un documento del Parlamento Europeo titulado: ”Sobre la existencia de un sistema global para la intercepción de comunicaciones comerciales y privaadas (ECHELON)”

- Ahi se establece que un sistema fue creado para monitorear las comunicaciones militares y diplomáticas de la Unión Soviética y sus aliados del Bloque del Este durante la Guerra Fría, al principio de la década de los 1960s.


ONE DOES NOT SIMPLY
ASKS ABOUT ECHELON TO AN EX-CIA
quickmeme.com

PRISM

- The top-secret PRISM program allows the U.S. intelligence community to gain access from nine Internet companies to a wide range of digital information, including e-mails and stored data, on foreign targets operating outside the United States

- The program is court-approved but does not require individual warrants

- It operates under a broader authorization from federal judges who oversee the use of the Foreign Intelligence Surveillance Act (FISA)

PRISM 2

- It is needed because the USA government is under constant thread from foreign agents.

- However, most of the world's communication flow through the USA
  - Phone calls
  - e-mail
  - chat

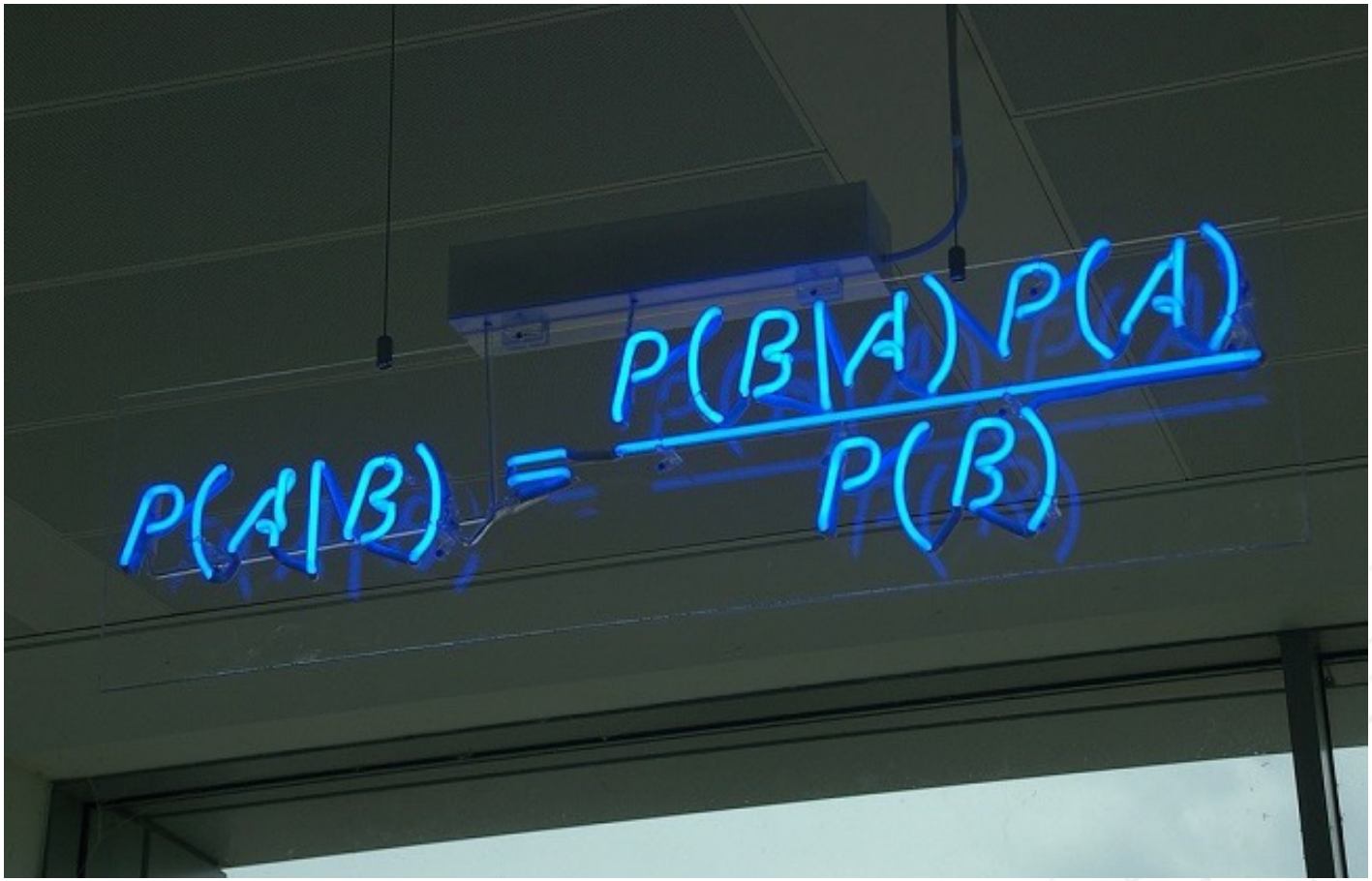
  All of them use the cheapest connection, which means, going through the USA

PRISM 3

- Main providers:
  - Microsoft (Outlook, Skype, etc.)
  - Google
  - Yahoo!
  - Facebook
  - YouTube
  - Apple
  - AOL
  - Twitter
  - etc.
- They provide:
  - Email conversations
  - Chat - voice and video
  - Videos
  - Photos
  - Stored data in the cloud
  - File Transfers
  - Videoconferences
  - Login notifications
  - Social Network details
  - etc.

PRISM 4

- *I don't have anything to hide*



PRISM 5

- In a country with 10 mill ppl., and with a very precise system, we can get 99.9% probablìlity to catch a criminal, and only 1% of chance of a false positive
- If we have 100,000 criminals, we can get 99,900 criminals, not bad at all.
- unfortunately, it has caught 100,000 innocent ppl.!

I don't have anything to hide, and that's why I am not showing you anything

Protecting

How can I protect my privacy from the NSA?

- Use PFS connections to websites
- Use Full-disk Encryption
- Use Open-PGP for personal communication
- Off-the-record chat
- TOR network
- Change your passwords frequently
- - Avoid email servers in the USA

The downside of protecting yourself

If you encrypt your data, the NSA will store your files for the future, when they can decrypt them.

- This does not applies to PFS, as the recovered key would only work per message
- If you have a long-term protection system, it will add an extra layer of encryption when new algorithms arrive
- Being anonymous now, does not mean you will always be anonymous
- *we are not sure what does the NSA is able to decrypt now, and in the short future* (military encryption is ahead of commercial and academic encryption, but we don't know how much!)