# Seguridad en Sistemas de Información

Curso en Tamaulipas [Q2 2014]


Luis J. Dominguez Perez

*Cinvestav*, Junio 16 de 2014 - L8

# Contenido, sección 1

# Introducción

- El cómputo en la nube es un pradigma que está basado en un modelo de prestación de servicios a gran escala disponibles a través de la internet, donde, de manera flexible, los usuarios pueden disponer de una gran cantidad de recursos de cómputo bajo un modelo de pago por consumo, y en función de la demanda.
- Con la finalidad de proteger la información que está en la nube, algunos usuarios cifran la información, limitando sus capacidades de uso.

Presentación del Dr. Francisco Rodríquez-Henríquez

# Características de la nube

Las cinco características esenciales de una infraestructura de nube son:

- Autoservicio por demanda
- Amplio acceso a red
- Agrupación de recursos
- Rápida elasticidad
- Servicio medido

# Modelos de servicio

Existen diversos tipos de servicios provistos a un consumidor:

- Software com Servicio (SaaS)
- Plataforma com Servicio (PaaS)
- Infraestructura como Servicio (IaaS)

# SaaS

- En este modelo, las aplicaciones se ejecutan en una infraestructura de nube
- Las aplicaciones se acceden a traves de un navegador web, y cualquier dispositivo del cliente
- El consumidor no administra los recursos de la infraestructura, aunque puede controlar algunas características específicas

Ejemplos: email, salesforce, CRM, etc.

# PaaS

- En este modelo, el consumidor puede proporcionar a sus clientes aplicaciones sobre las bibliotecas y herramientas soportadas por el proveedor, pero que estén disponibles para el consumidor.
- El consumidor tampoco administra los recursos de la infraestructura; sin embargo, establece qué aplicaciones están disponibles en todo momento.

Ejemplos: Google App Engine, Windows Azure, soporte para .NET, Java, Python, PHP.

# IaaS

- En este modelo, el consumidor dispone del uso del procesamiento, almacenamiento, redes y otros recursos de cómputo.
- Se puede instalar aplicaciones, softwae, e incluso el sistema operativo que se desee mediante esquemas de virtualización de servidores.

Ejemplos: Google Compute Engine, Amazon Elastic Compute Cloud.

# Seguridad

Dependiendo del nivel de control sobre las aplicaciones o la infraestructura, la seguridad de la información recea en diferentes grados de responsabilidad sobre el consumidor.

- **SaaS**. El proveedor provee controles de seguridad al software, protege la red, y cuida el acceso desde sitios prohibidos
- **PaaS**. El proveedor provee controles para que no se mezcle la información entre usuarios y aplicaciones, así como de actualizaciones a las bibliotecas de funciones; sin embargo, el consumidor es responsable de cualquier código malicioso en sus programas.
- **IaaS**. El proveedor solamente provee garantías de que su información no se verá comprometida por otro consumidor abusando de equipos comprometidos dentro del mismo equipo físimo, el resto, es responsabilidad del consumidor.

# Contenido, sección 2

Cloud Security

Cifrado en bases de datos

Cifrado en disco

Wireless Sensor Networks

Bitcoins

TrueCrypt

Privacidad

# Cómputo sobre datos cifrados

- ¿No sería bonito poder...
  - Cifrar mis queries a la nube?
  - y que la nube aún así las pueda procesar?
  - y que la nube responda datos cifrados (que yo pueda decifrar)

# Presentación de Lil María Rodríquez-Henríquez

# Contenido, sección 3

# Introducción

- El cifrado de disco es una tecnología que permite proteger la información a bajo nivel.
- El cifrado de disco permite cifrar cada bit de información que va al disco, o a un volúmen de disco.
- El cifrado del sistema de archivos cifra cada archivo por separado.
- *Full disk encryption* normalmente include a la partición que inicia el sistema operativo, y en algunos casos el Master Boot Record (MBR) si el sistema lo ocupa.

# Presentación del Dr. Cuauhtemoc Mancillas

# Contenido, sección 4

# Introducción

- Las redes de sensores inalámbricos son una serie de dispositivos interconectados que recolectan información sensible, normalmente en ambientes hóstiles, o de difícil acceso.
- Poseen poder de cómputo modesto, poco espacio de memoria y almacenamiento, su red de conexión es de bajo ancho de banda, y tienen limitaciones de energía.
- Sus principales aplicaciones van desde la domótica, monitoreo ambiental (incluyendo gran profundidad marítima), y aplicaciones médicas.

# Presentación del Dr. Piotr Szczechowiak

# Contenido, sección 5

# El dinero de la antigua Roma

http://eldinerodelaantiguaroma.blogspot.mx/2012/01/el-dinero-de-la-antigua-roma.html

# Breve historia del dinero

Edición especial de la IEEE: `http://spectrum.ieee.org/at-work/innovation/a-brief-history-of-money`

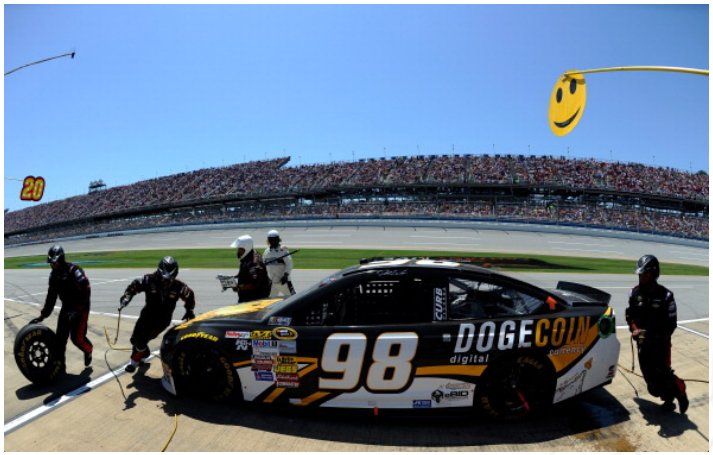
# Bitcoin

Funcionamiento del Bitcoin `http://spectrum.ieee.org/img/06Bitcoin-1338412974774.jpg`

# Otras monedas virtuales

- **Zerocoin**. Es una cryptomoneda propuesta como una extensión de Bitcoin para garantizar la anonimidad de las transacciones debido a ciertos fallos en Bitcoin.

- **Dogecoin**. Es una cryptomoneda que busca acercarse a la gente, y alejarse del pasado oscuro de Bitcoin (el mercado de la seda virtual). Actualmente patrocina a un equipo de la Nascar.



# Contenido, sección 6

# Introducción

Truecrypt is dead, Long live Truecrypt...

# Introducción

Truecrypt is dead, Long live Truecrypt... Este espacio estaba reservado para Truecrypt.

# Re-introducción

- Con las recientes declaraciones de que la NSA podría estar afectando al software de cifrado, crece la preocupación de los *netcitizens* sobre la privacidad y seguridad de su información
- Existe además poco software de alta calidad que provea cifrado utilizable por el usuario
- En algunos casos, proveedor tiene que cerrar por presiones de gobierno

# Casos

- PrivateSky de Certivox.
- Lavabit
- Truecrypt(?)

# PrivateSky

- Una versión beta del servicio PrivateSky de CertiVox (UK) cerró a principios del 2013 por una orden gubernamental.
- El servicio de cifrado seguro de correo, que trabajaba para webmail como Outlook tenía “miles de usuarios altamente activos” antes de ser objetivo del gobierno británico.
- Brian Spector, CEO de CertiVox, “Hacia finales del 2012, escuchamos por parte de la National Technical Assistance Centre (NTAC), una división del GCHQ y de enlace con la Secretaría de Gobernación, [que] querían las llaves para descifrar los datos de los usuarios.”.

# PrivateSky

- Dado que PrivateSky parte la llave con el cliente, es necesario que el cliente provea su parte de la llave para que se le espíe anónimamente, por lo que el requerimiento no se pudo satisfacer. La solución era proveer al gobierno con una puerta trasera, lo que iba en contra de la finalidad del producto, por lo que se decidió cerrar el sistema.
- La empresa sobrevive debido a que PrivateSky solamente era uno de sus productos que intentaba comercializar.

# Lavabit

- Lavabit proveía un servicio de criptografía que dada la tecnología actual era imposible de romper aún por las agencias gubernamentales.
- Bajo sospechas de posesión de contenido delicado por parte de algunos usuarios, el Gobierno de los EEUU solicitó las llaves privadas para poder leer los correos.
- En este caso, la empresa cerró operaciones casi de inmediato.

# Truecrypt

- Truecrypt era un servicio de cifrado de disco para sistemas windows.
- Tenía sospechas de posibles vulnerabilidades a partir de las revelaciones de que la NSA podía estar saboteando estándares de cifrado, y de internet.
- Se inició un proceso externo de auditoría, el cual no reveló nada crítico en su primera etapa; sin embargo, cerró operaciones abruptamente durante el proceso, alegando que sus principales clientes eran clientes de Windows XP, y que dado que este ya no tiene soporte, recomendaron a sus usuarios migrar a BitLocker.

# Truecrypt

- La controversia radica en que no se terminó el proceso de auditoría, y no fueron muy claros en el porqué.
- Argumentaron que se descubrió una falla de seguridad grave, y que no valía la pena arreglarla para sus clientes.
- La auditoría continua, pero su sitio git (para descargar el código fuente) fue saboteado por ellos mismos para forzar su migración. Se generaron rumores al respecto, mismos que no han sido contestados.

# Contenido, sección 7

# Echelon

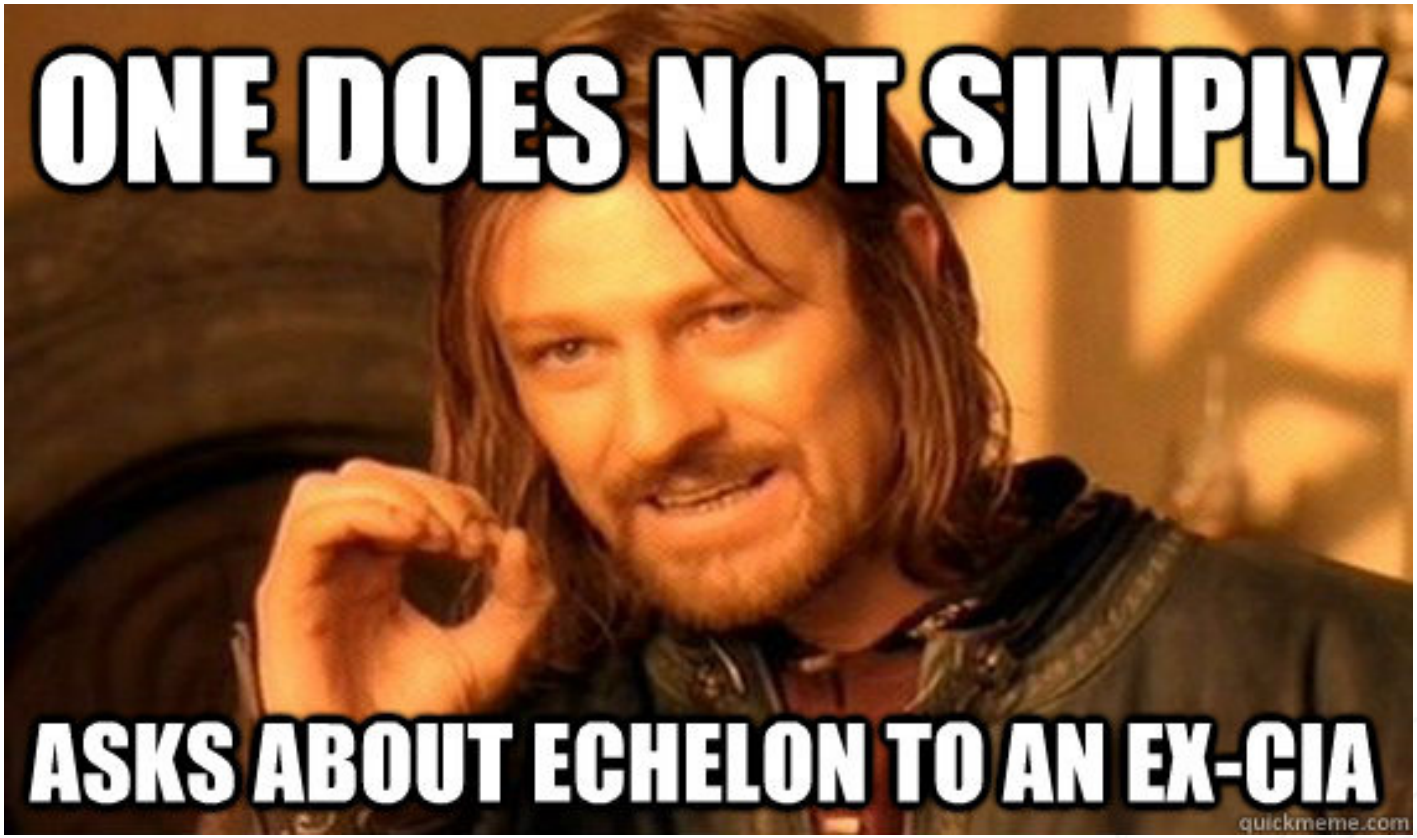
- Echelon es el nombre utilizado en los medios internacionales y en la cultura popular para describir una red de recolección y análisis de señales de inteligencia para los firmantes del acuerdo UKUSA de Seguridad (Australia, Canada, Nueva Zelanda, el Reino Unido, y los E.E. U.U.)

- 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

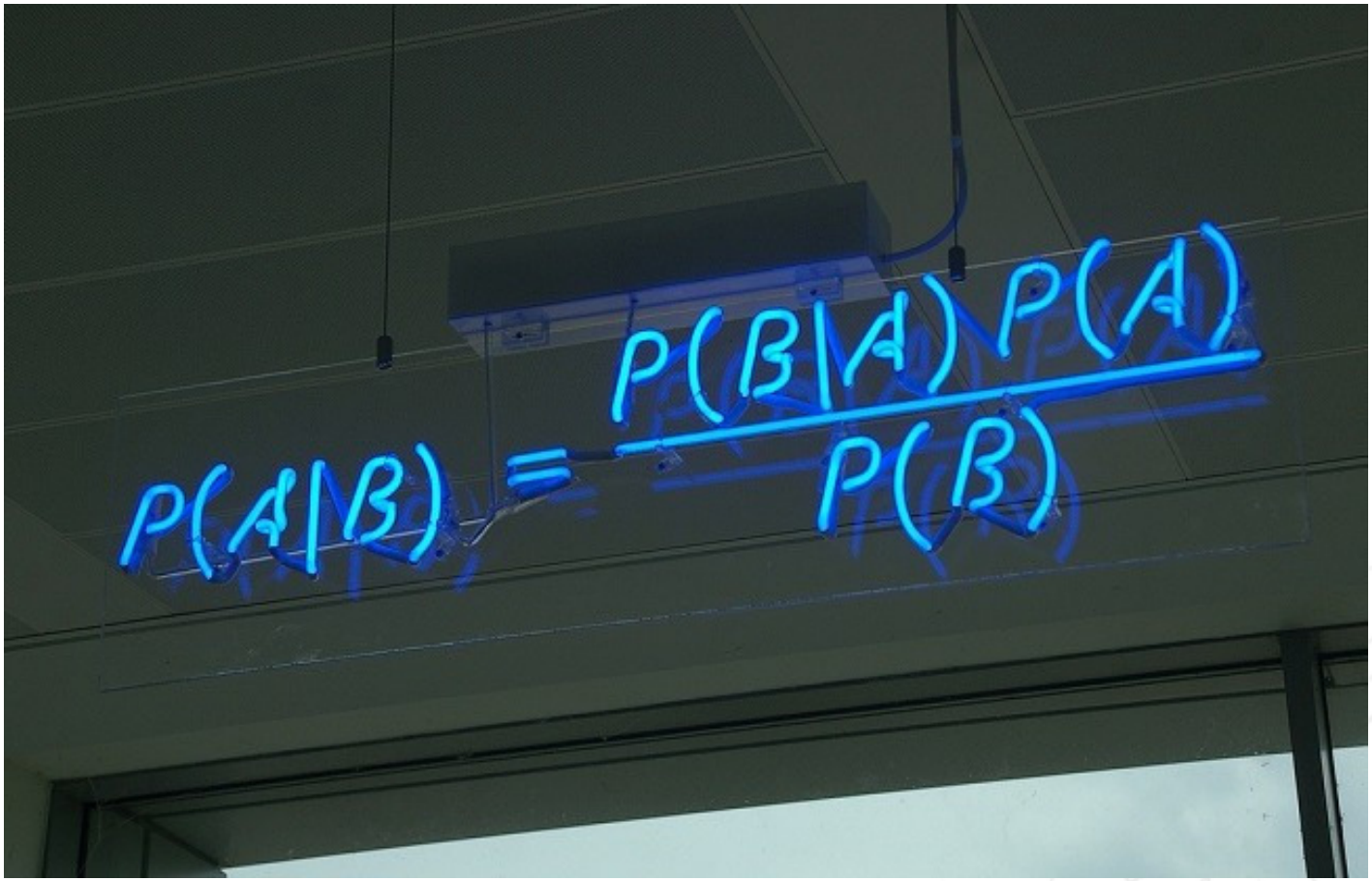
  All of them use the cheapest connection, which means, going through the USA

# 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!)

# End

There's part II!!!