La agencia que no es, quiere ser el aleph

Francisco Rodríguez-Henríquez
Departamento de Computación
CINVESTAV-IPN

"Sí, el Aleph.
El lugar donde están, sin confundirse,
todos los lugares del orbe,
vistos desde todos los ángulos.
[...]
Lo que vieron mis ojos fue simultáneo:
lo que transcribiré, sucesivo,
porque el lenguaje lo es."
El aleph, Jorge Luis Borges.

Seminario del Departamento de Computación
CINVESTAV-IPN
Lunes 24 de febrero de 2014

Noticias del imperio

- A partir del 5 de junio de 2013, el ex-empleado de la Agencia Nacional de Seguridad estadounidense (NSA por sus siglas en inglés), Edward Snowden, ha ido revelando a través de los periódicos The Guardian y The Washington Post, documentos clasificados como de alto nivel de seguridad

Noticias del imperio

- A partir del 5 de junio de 2013, el ex-empleado de la Agencia Nacional de Seguridad estadounidense (NSA por sus siglas en inglés), Edward Snowden, ha ido revelando a través de los periódicos The Guardian y The Washington Post, documentos clasificados como de alto nivel de seguridad
- Los documentos filtrados describen una serie de programas de espionaje que la NSA aplica desde hace varios años con el objetivo de vulnerar los servicios de seguridad que deberían de proporcionar aplicaciones informáticas de uso masivo.

Noticias del imperio

- De esta manera, la NSA ha almacenado una cantidad de información que le permite ejercer una incesante vigilancia de cientos y quizás miles de millones de personas [sin precendentes en la historia de la humanidad]

Noticias del imperio

- 5.junio.2013: Trasciende que la NSA recopila llamadas de Verizon

Noticias del imperio

- 5.junio.2013: Trasciende que la NSA recopila llamadas de Verizon
- 6.junio.2013: PRISMA
  - permite acceder a datos de Apple, Google y Microsoft
  - Se insinúa que existe complicidad de dichas empresas con la NSA

Noticias del imperio

- 5.junio.2013: Trasciende que la NSA recopila llamadas de Verizon
- 6.junio.2013: PRISMA
  - permite acceder a datos de Apple, Google y Microsoft
  - Se insinúa que existe complicidad de dichas empresas con la NSA
- 9.junio.2013: Boundless Informant
  - En febrero de 2013, la agencia recopiló 3.000 millones de datos relacionados con ciudadanos estadounidenses

Noticias del imperio

- 5.junio.2013: Trasciende que la NSA recopila llamadas de Verizon
- 6.junio.2013: PRISMA
  - permite acceder a datos de Apple, Google y Microsoft
  - Se insinúa que existe complicidad de dichas empresas con la NSA
- 9.junio.2013: Boundless Informant
  - En febrero de 2013, la agencia recopiló 3.000 millones de datos relacionados con ciudadanos estadounidenses
- 27.junio.2013: Evil Olive y Shell Trumpet
  - Se procesan miles de millones de meta-datos por Internet
  - Usando Stellar Wind, la NSA recopila datos de los SMS de los celulares

Noticias del imperio

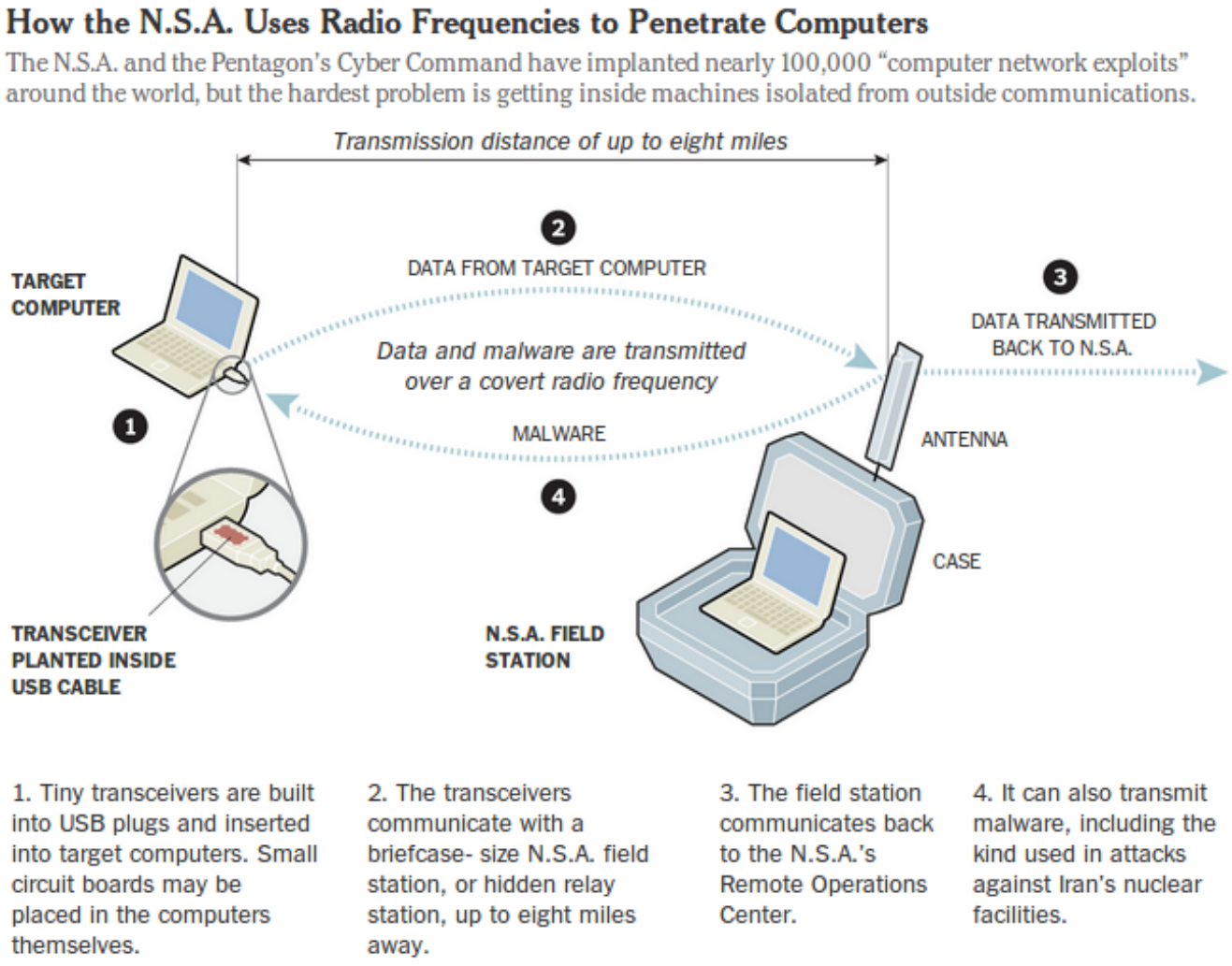
- 5.junio.2013: Trasciende que la NSA recopila llamadas de Verizon
- 6.junio.2013: PRISMA
  - permite acceder a datos de Apple, Google y Microsoft
  - Se insinúa que existe complicidad de dichas empresas con la NSA
- 9.junio.2013: Boundless Informant
  - En febrero de 2013, la agencia recopiló 3.000 millones de datos relacionados con ciudadanos estadounidenses
- 27.junio.2013: Evil Olive y Shell Trumpet
  - Se procesan miles de millones de meta-datos por Internet
  - Usando Stellar Wind, la NSA recopila datos de los SMS de los celulares
- 1.septiembre.2013: Espionaje a Dilma Rousseff y a Enrique Peña Nieto
- 23.octubre.2013: La NSA ha vigilado a 35 líderes políticos a nivel mundial
- 14.enero.2014: La NSA puede acceder a computadoras sin necesidad de que estos estén conectados

Noticias del imperio

- 5.junio.2013: Trasciende que la NSA recopila llamadas de Verizon
- 6.junio.2013: PRISMA
  - permite acceder a datos de Apple, Google y Microsoft
  - Se insinúa que existe complicidad de dichas empresas con la NSA
- 9.junio.2013: Boundless Informant
  - En febrero de 2013, la agencia recopiló 3.000 millones de datos relacionados con ciudadanos estadounidenses
- 27.junio.2013: Evil Olive y Shell Trumpet
  - Se procesan miles de millones de meta-datos por Internet
  - Usando Stellar Wind, la NSA recopila datos de los SMS de los celulares
- 1.septiembre.2013: Espionaje a Dilma Rousseff y a Enrique Peña Nieto
- 23.octubre.2013: La NSA ha vigilado a 35 líderes políticos a nivel mundial
- 14.enero.2014: La NSA puede acceder a computadoras sin necesidad de que estos estén conectados

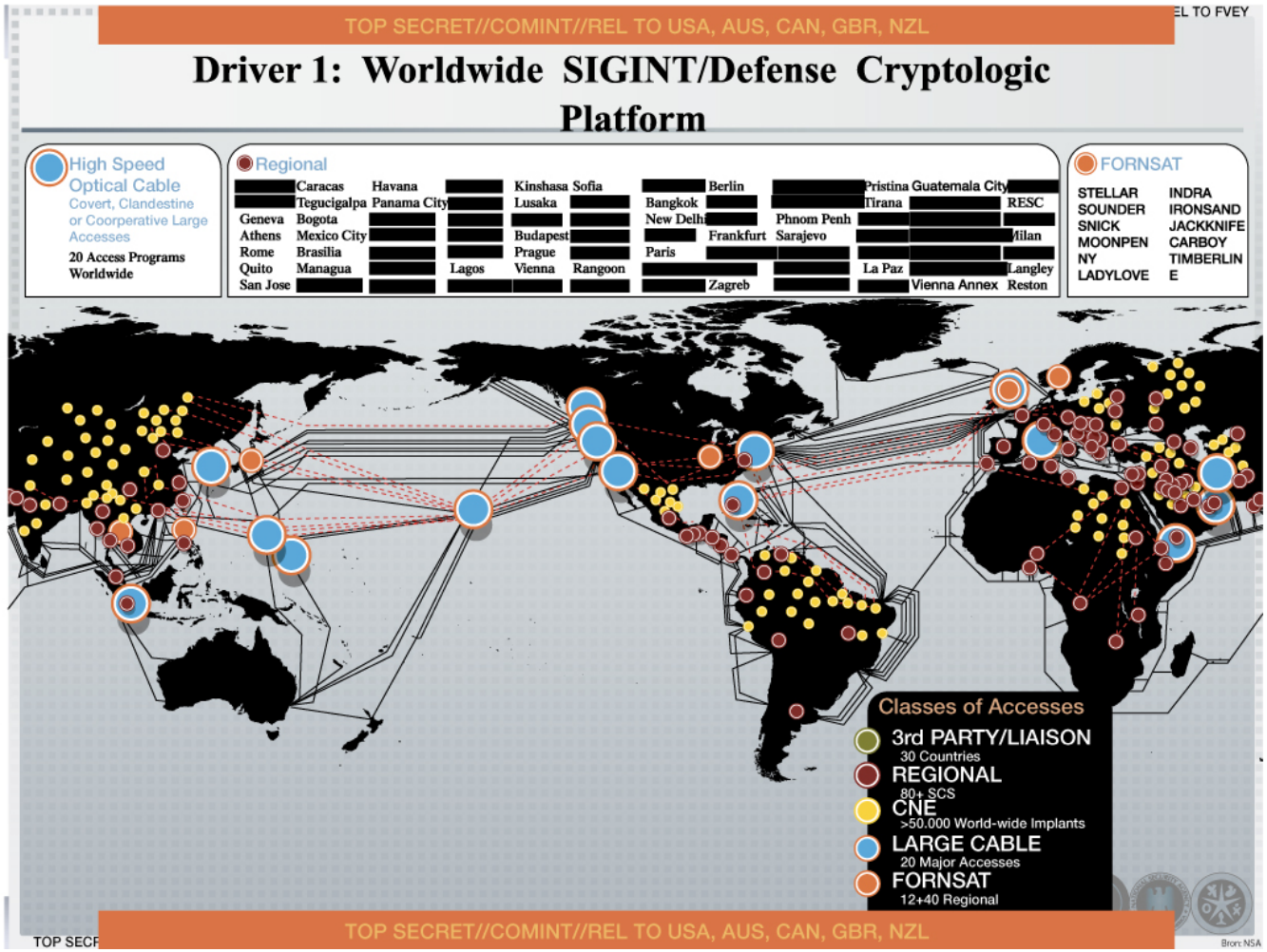
Se especula que menos del 1% de los aproximadamente 1,7 millones de documentos confidenciales de la NSA acopiados por Snowden han sido revelados a la fecha.

¿Cómo inyecta/extrae información la NSA de computadoras que no están conectadas a Internet?



Fuente: The New York Times

¿En dónde inyecta/extrae información la NSA de computadoras que no están conectadas a Internet?



Fuente: Periódico holandés nrc.nl

Edward Snowden

Edward Snowden

"En tanto el individuo objetivo tenga una cuenta de correo electrónico, es posible espiarlo sin importar si se trata de ti, de tu conocido, de un juez, o incluso, del presidente."

Breve contexto criptográfico y de seguridad informática

Tres leyes de la seguridad informática

Figure: Primera ley: Los sistemas absolutamente seguros no existen

Tres leyes de la seguridad informática

Figure: Segunda ley: Disminuir las vulnerabilidades de un sistema a la mitad implica duplicar los costos de seguridad

Tres leyes de la seguridad informática

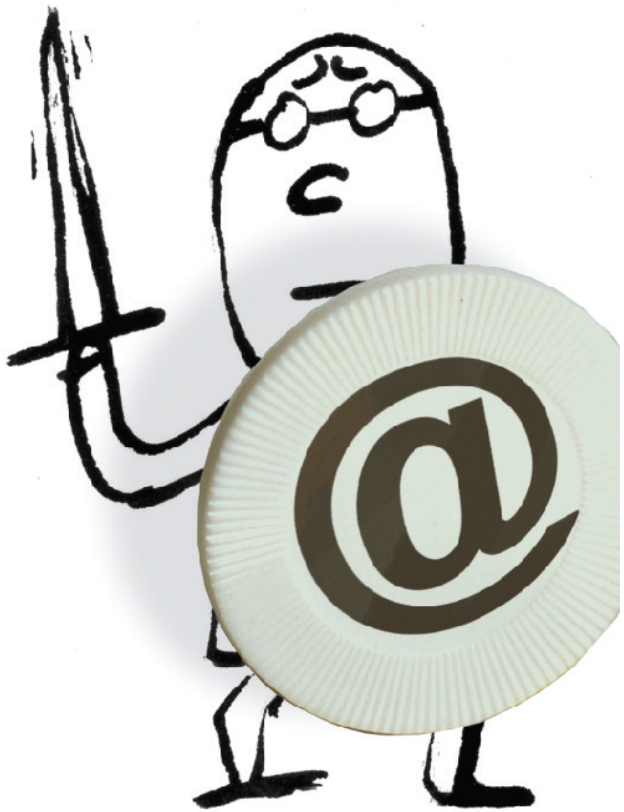


Figure: Tercera ley: Típicamente la criptografía no es vulnerada sino más bien brincada

De la importancia del sigilo en la criptografía

- En criptografía y en seguridad informática los secretos arduamente obtenidos no suelen revelarse

De la importancia del sigilo en la criptografía

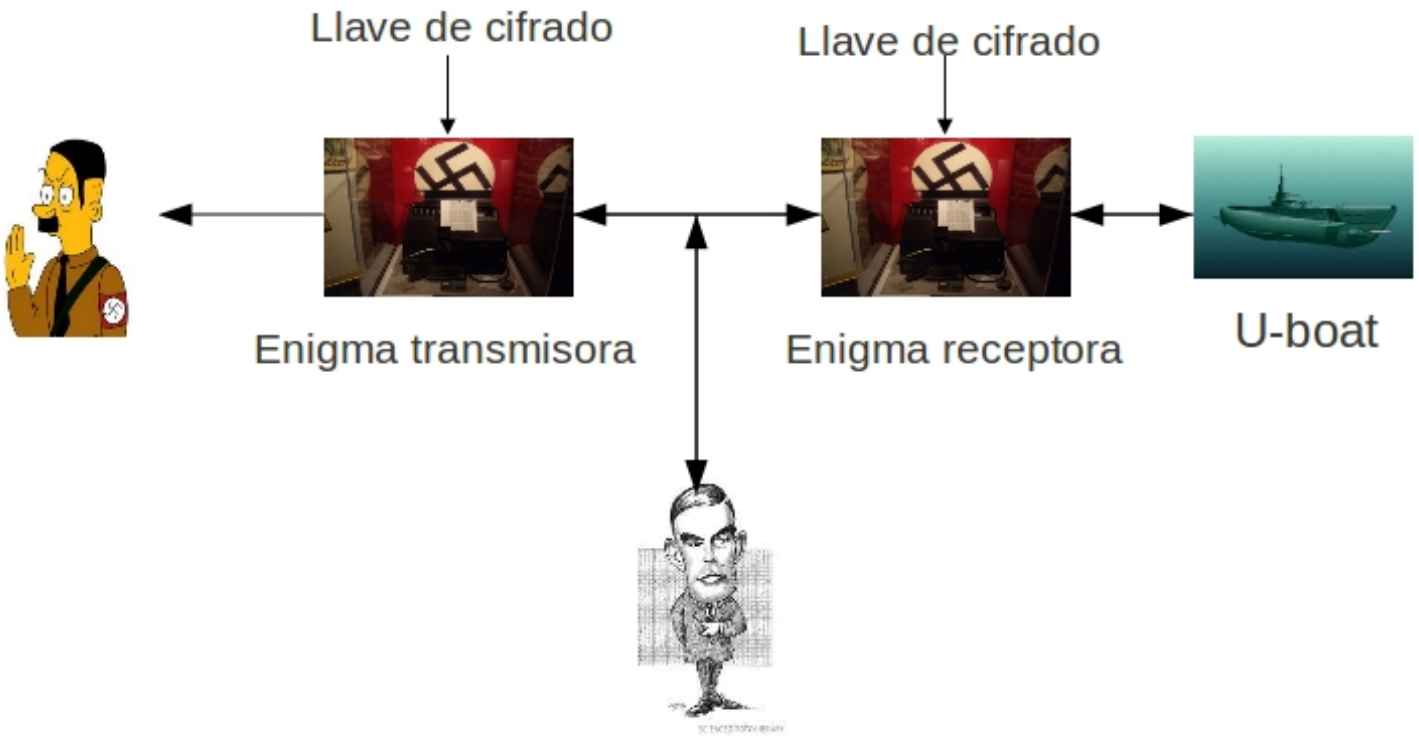
- En criptografía y en seguridad informática los secretos arduamente obtenidos no suelen revelarse
- Innumerables ejemplos en que el crédito de vulnerar un criptosistema no se le otorga a los atacantes sino muchos años después [y a veces nunca]

De la importancia del sigilo en la criptografía

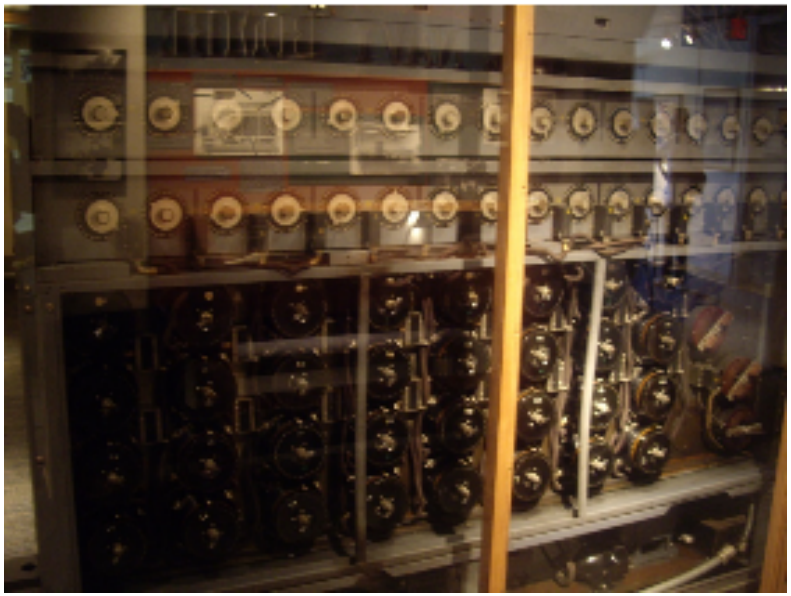
- En criptografía y en seguridad informática los secretos arduamente obtenidos no suelen revelarse
- Innumerables ejemplos en que el crédito de vulnerar un criptosistema no se le otorga a los atacantes sino muchos años después [y a veces nunca]
- Ejemplo paradigmático: Alan Turing y el éxito de su equipo para "romper" la máquina de cifrado Enigma durante la segunda guerra mundial

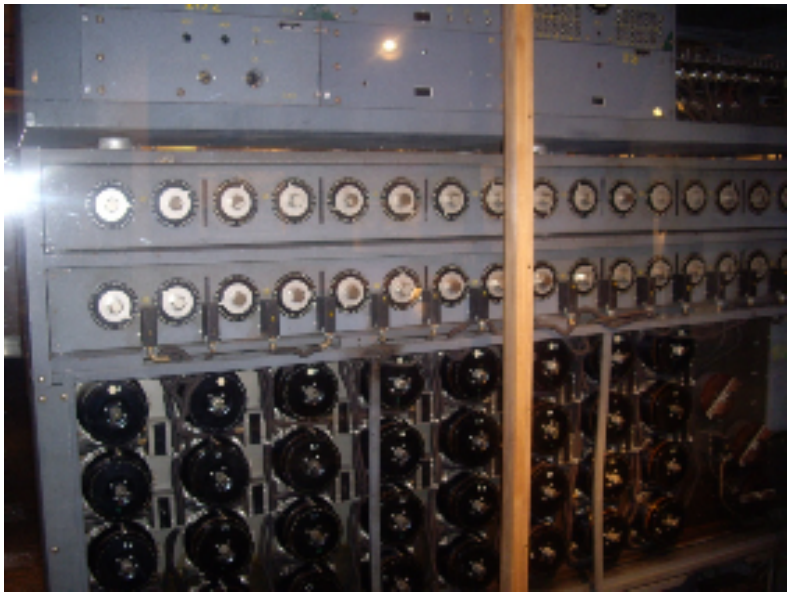
La máquina de escribir Enigma

Modelo de seguridad de Enigma



La Bomba de Turing





Turing y Enigma

Turing y Enigma

- Se considera que el rompimiento de Enigma fue una de los principales razones por las cuales las fuerzas aliadas de Estados Unidos, Inglaterra y Francia lograron vencer junto con la ayuda del poderoso ejército rojo de la Unión Soviética, a la Alemania nazi de Adolf Hitler

Turing y Enigma

- Se considera que el rompimiento de Enigma fue una de los principales razones por las cuales las fuerzas aliadas de Estados Unidos, Inglaterra y Francia lograron vencer junto con la ayuda del poderoso ejército rojo de la Unión Soviética, a la Alemania nazi de Adolf Hitler
- Más de 20 años después de su muerte, documentos desclasificados del sistema de inteligencia militar inglés mostraron que Turing fue el principal criptógrafo de su país durante la segunda guerra mundial

¿Qué es la NSA?


Fear now,
but one day
we,ll be
in charge and
you shallhave
PEACE

¿Qué es la NSA?

- En la cultura popular, se sabe relativamente poco sobre la NSA

¿Qué es la NSA?

- En la cultura popular, se sabe relativamente poco sobre la NSA
- Significativamente, incluso en los propios Estados Unidos se suele decir que el verdadero significado de las siglas NSA es,

No Such Agency

¿Qué es la NSA?

- En la cultura popular, se sabe relativamente poco sobre la NSA
- Significativamente, incluso en los propios Estados Unidos se suele decir que el verdadero significado de las siglas NSA es,

No Such Agency

- Lo cual podría traducirse como:

"*la agencia que no es*"

¿Qué es la NSA?

- En la cultura popular, se sabe relativamente poco sobre la NSA
- Significativamente, incluso en los propios Estados Unidos se suele decir que el verdadero significado de las siglas NSA es,

No Such Agency

- Lo cual podría traducirse como:

"la agencia que no es"

- Características generales de la NSA:
  - fue fundada en 1952
  - Cuenta con un presupuesto de $\approx 10,8$ mil millones de dólares anuales y $\approx$ 40K empleados
  - Máximo empleador de matemáticos en el mundo

Computadora Bluffdale

- Tiene una capacidad de almacenamiento de 12 exabytes [$= 12 \cdot 2^{60}$ bytes $= 12 \cdot 2^{20}$ TBytes]
- el costo de construcción fue de $2,000$ millones de dólares y se estima que su mantenimiento costará otros $2,000$ millones de dólares
- Consume 65 Mega vatios de potencia (Suficiente para alimentar una ciudad de 50,000 habitantes), lo cual cuesta 40M de dólares anuales
- Ha sido identificada como el símbolo del programa de vigilancia de la NSA

Computadora Bluffdale

- Tiene una capacidad de almacenamiento de 12 exabytes [$= 12 \cdot 2^{60}$ bytes $= 12 \cdot 2^{20}$ TBytes]
- el costo de construcción fue de 2,000 millones de dólares y se estima que su mantenimiento costará otros 2,000 millones de dólares
- Consume 65 Mega vatios de potencia (Suficiente para alimentar una ciudad de 50,000 habitantes), lo cual cuesta 40M de dólares anuales
- Ha sido identificada como el símbolo del programa de vigilancia de la NSA

Figure: Computadora Bluffdale de la NSA (crédito de la fotografía: Rick Bowmer/AP)

Líneas de ataque de la NSA

1. Ataques a la criptografía
2. Ataques a la implementación del criptosistema
3. Ataques a las contraseñas ideadas por seres humanos
4. Ataques al generador de números aleatorios
5. Ataques al componente humano del criptosistema

NSA: 1. Ataques a la criptografía

- Existe consenso en que es computacionalmente muy costoso vulnerar los problemas matemáticos difíciles que protegen la seguridad de la mayoría de los algoritmos criptográficos utilizados hoy en día

NSA: 1. Ataques a la criptografía

- Existe consenso en que es computacionalmente muy costoso vulnerar los problemas matemáticos difíciles que protegen la seguridad de la mayoría de los algoritmos criptográficos utilizados hoy en día
- Sin embargo, hay un importante número de criptosistemas comerciales y gubernamentales que usan criptografía obsoleta y/o protocolos de intercambio de datos excesivamente complicados, cuyo nivel de seguridad real es difícil de determinar

NSA: 2. Ataques a la implementación del criptosistema

- La gran mayoría de implementaciones criptográficas en software y hardware son vulnerables a ataques especialmente diseñados para recuperar la información privada de un objetivo concreto.

NSA: 2. Ataques a la implementación del criptosistema

- La gran mayoría de implementaciones criptográficas en software y hardware son vulnerables a ataques especialmente diseñados para recuperar la información privada de un objetivo concreto.
- Tales ataques explotan canales colaterales de información que filtran parte de los datos secretos de una determinada aplicación.

NSA: 2. Ataques a la implementación del criptosistema

- La gran mayoría de implementaciones criptográficas en software y hardware son vulnerables a ataques especialmente diseñados para recuperar la información privada de un objetivo concreto.
- Tales ataques explotan canales colaterales de información que filtran parte de los datos secretos de una determinada aplicación.
- Sin embargo esta estrategia es difícil de escalar a un nivel de vigilancia masiva excepto que se agreguen puertas-trampa (trapdoor en inglés) en las aplicaciones de software comerciales y/o en los componentes de hardware

NSA: 3. Ataques a las contraseñas ideadas por seres humanos

- Los ataques de diccionario se han vuelto cada vez más sofisticados y permiten ahora adivinar virtualmente cualquier contraseña que sea memorizable por un ser humano, de manera casi instantánea.

NSA: 3. Ataques a las contraseñas ideadas por seres humanos

- Los ataques de diccionario se han vuelto cada vez más sofisticados y permiten ahora adivinar virtualmente cualquier contraseña que sea memorizable por un ser humano, de manera casi instantánea.
- Si el oponente conoce las contraseñas utilizadas por un individuo, normalmente puede no sólo tener acceso a todos sus datos informáticos si no también usurpar su identidad.

NSA: 4. Ataques al generador de números aleatorios

- Ningún criptosistema puede considerarse seguro si no tiene la disponibilidad de generar números aleatorios cuya secuencia sea imposible de predecir

NSA: 4. Ataques al generador de números aleatorios

- Ningún criptosistema puede considerarse seguro si no tiene la disponibilidad de generar números aleatorios cuya secuencia sea imposible de predecir
- Desafortunadamente, la gran mayoría de generadores de números aleatorios son sorprendentemente frágiles

NSA: 4. Ataques al generador de números aleatorios

- Ningún criptosistema puede considerarse seguro si no tiene la disponibilidad de generar números aleatorios cuya secuencia sea imposible de predecir
- Desafortunadamente, la gran mayoría de generadores de números aleatorios son sorprendentemente frágiles
- Probablemente, el principal reto para la NSA sea el de diseñar un generador de números aleatorios que no pueda ser trivialmente manipulado por *otros* atacantes

NSA: 5. Ataques al componente humano del criptosistema

- Muy frecuentemente, la manera más simple y efectiva de acceder a los datos confidenciales de un sistema es a través de sobornos y/o coerciones a las personas encargadas de guardar las contraseñas y llaves secretas

Líneas de ataque de la NSA

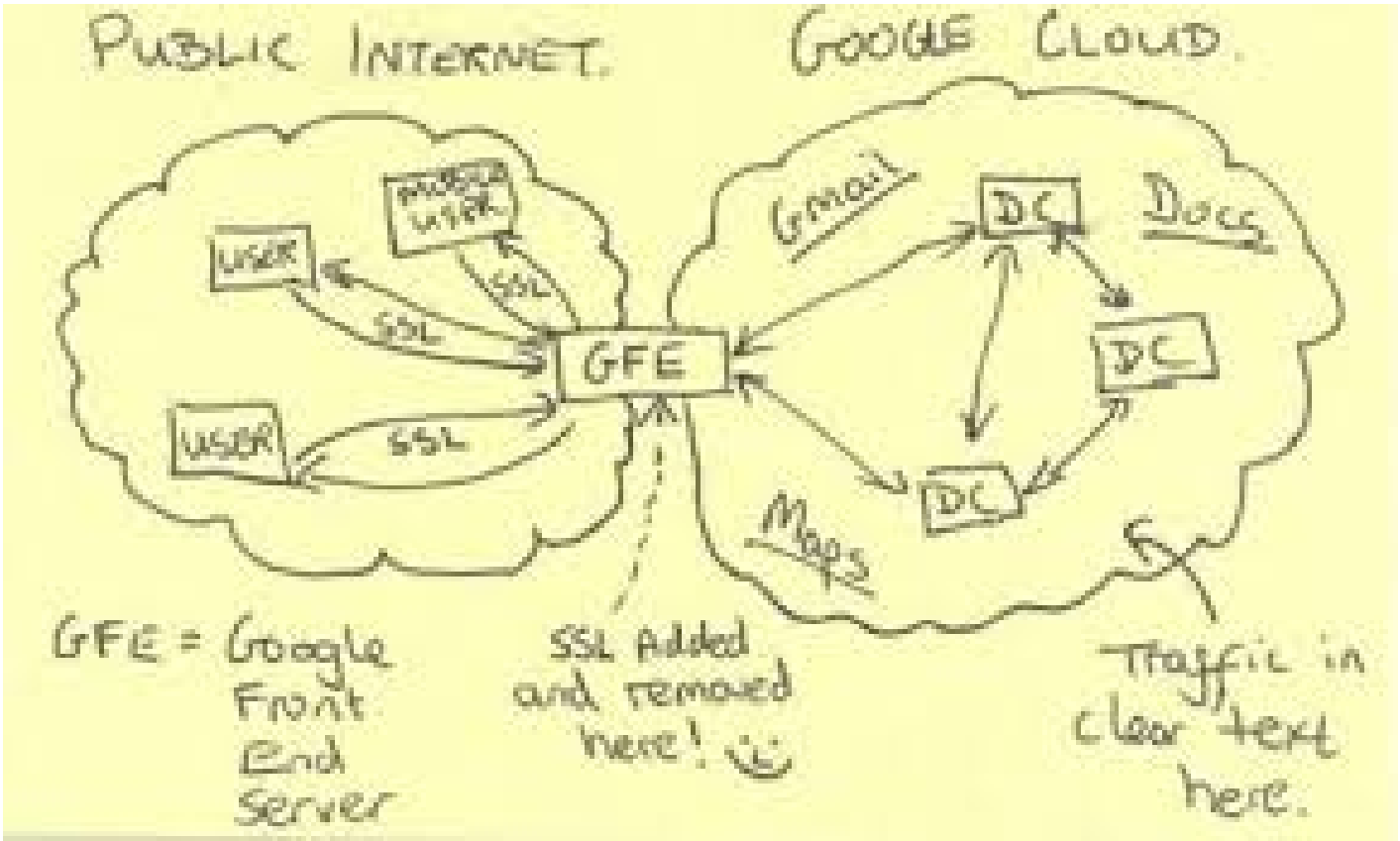
- De acuerdo a los documentos revelados por Snowden y a otros que él que todavía no ha publicado, la NSA ha utilizado principalmente las estrategias (2)-(5) para su programa de vigilancia masiva

Líneas de ataque de la NSA

- De acuerdo a los documentos revelados por Snowden y a otros que él que todavía no ha publicado, la NSA ha utilizado principalmente las estrategias (2)-(5) para su programa de vigilancia masiva
- A manera de ejemplo nótese la curiosa desfachatez de cómo concibió la NSA vulnerar (con éxito) la nube de servidores de Google.

Líneas de ataque de la NSA

- De acuerdo a los documentos revelados por Snowden y a otros que él que todavía no ha publicado, la NSA ha utilizado principalmente las estrategias (2)-(5) para su programa de vigilancia masiva
- A manera de ejemplo nótese la curiosa desfachatez de cómo concibió la NSA vulnerar (con éxito) la nube de servidores de Google.



Ataques de la NSA: Casos de éxito

- La NSA ha mantenido una política muy activa de sobornos e influencias en los comités que diseñan los estándares criptográficos internacionales, promoviendo el uso de algoritmos criptográficos débiles y vulnerables.

Ataques de la NSA: Casos de éxito

- La NSA ha mantenido una política muy activa de sobornos e influencias en los comités que diseñan los estándares criptográficos internacionales, promoviendo el uso de algoritmos criptográficos débiles y vulnerables.
- Se sabe además que la NSA se ha coludido con fabricantes de hardware y software para debilitar criptosistemas de cifrado y de autenticación de usuarios en esquemas conocidos como autenticación por dos factores.

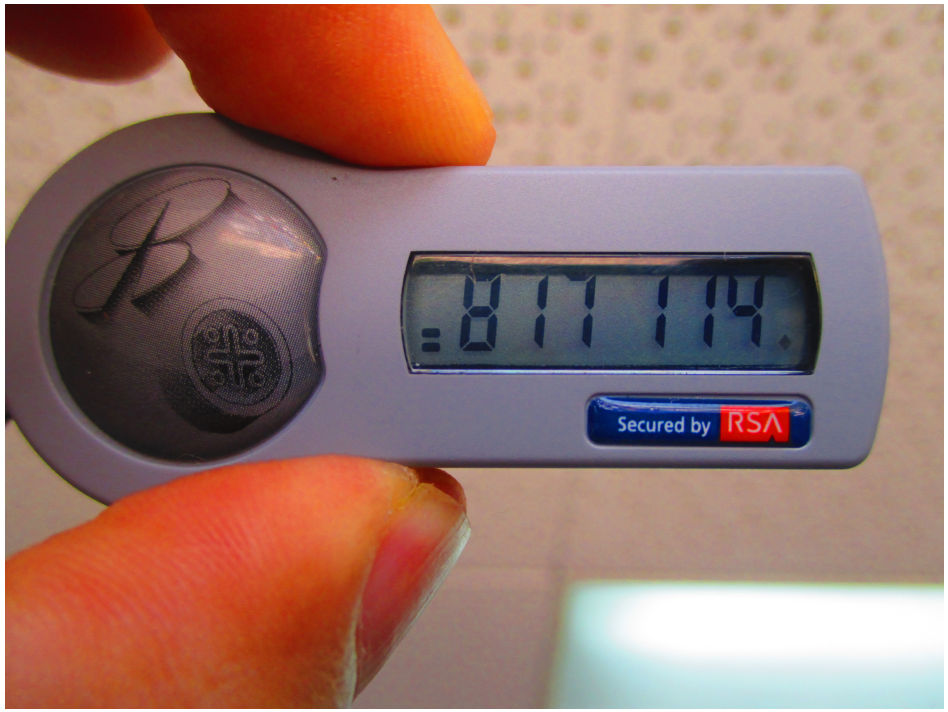
Ataques de la NSA: Casos de éxito

- La NSA ha mantenido una política muy activa de sobornos e influencias en los comités que diseñan los estándares criptográficos internacionales, promoviendo el uso de algoritmos criptográficos débiles y vulnerables.
- Se sabe además que la NSA se ha coludido con fabricantes de hardware y software para debilitar criptosistemas de cifrado y de autenticación de usuarios en esquemas conocidos como autenticación por dos factores.
- Probablemente el ejemplo más emblemático de estas políticas, es la implantación de una puerta-trampa en el generador de números aleatorios SecurID de la compañía RSA.

La compañía RSA

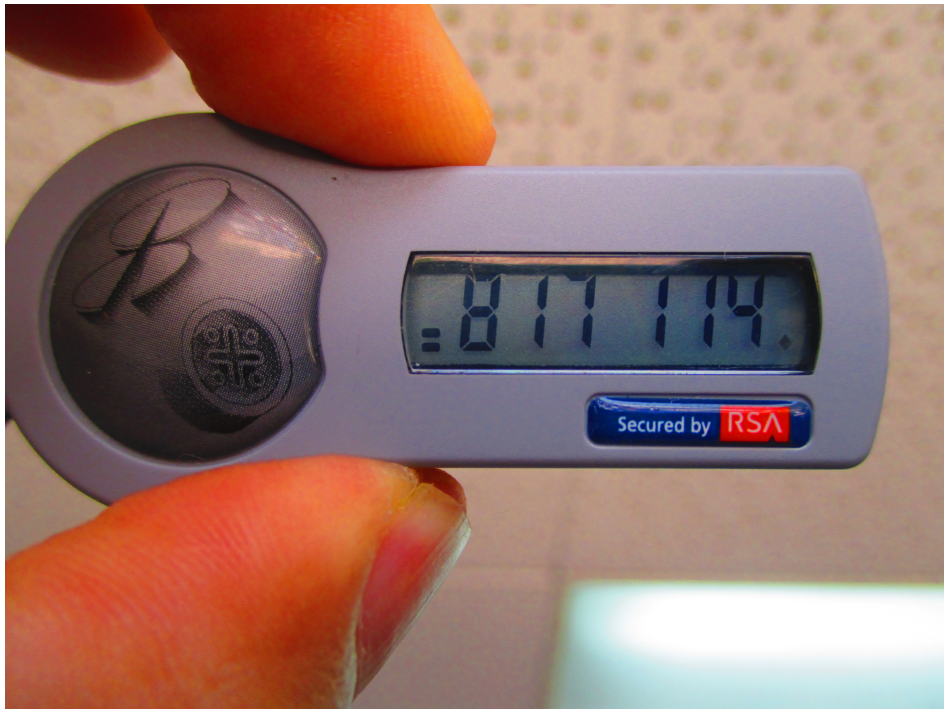
- La firma estadounidense RSA fue fundada en 1982 y desde entonces ha sido considerada una de las compañías pioneras en seguridad de la información
- En 2006, RSA fue comprada por EMC Corporation a un precio de 2,1 mil millones de dólares
- RSA organiza todos los años en San Francisco, la conferencia internacional más grande en seguridad informática

La compañía RSA



- El principal producto comercial de RSA, el generador de números aleatorios SecurID que permite autenticar usuarios electrónicamente para aplicaciones bancarias, gubernamentales, etc

La compañía RSA



- El principal producto comercial de RSA, el generador de números aleatorios SecurID que permite autenticar usuarios electrónicamente para aplicaciones bancarias, gubernamentales, etc
- SecurID controla el 70% del mercado mundial de autenticación por dos factores

dispositivo de autenticación por dos factores SecurID

- A cada usuario se le asigna un dispositivo SecurID conocido como token, el cual genera un número aleatorio que funciona como un código de autenticación y que se renueva cada 60 segundos.

dispositivo de autenticación por dos factores SecurID

- A cada usuario se le asigna un dispositivo SecurID conocido como token, el cual genera un número aleatorio que funciona como un código de autenticación y que se renueva cada 60 segundos.
- La secuencia de números aleatorios generados en cada token está sincronizada con un servidor central.

dispositivo de autenticación por dos factores SecurID

- A cada usuario se le asigna un dispositivo SecurID conocido como token, el cual genera un número aleatorio que funciona como un código de autenticación y que se renueva cada 60 segundos.
- La secuencia de números aleatorios generados en cada token está sincronizada con un servidor central.
- para garantizar su unicidad, se utiliza una semilla diferente, la cual es asignada de fábrica a cada token.

RSA se colude con la NSA

- En diciembre del año pasado, el periodista Joseph Menn de Reuters, publicó un artículo en el que se afirma que los directivos de RSA aceptaron un pago por diez millones de dólares por parte de la NSA

RSA se colude con la NSA

- En diciembre del año pasado, el periodista Joseph Menn de Reuters, publicó un artículo en el que se afirma que los directivos de RSA aceptaron un pago por diez millones de dólares por parte de la NSA
- A cambio RSA permitió que sus bibliotecas criptográficas utilizaran de manera predeterminada. El esquema de generador de números aleatorios Dual_EC_DRBG que fuera promulgado como estándar de ISO y de ANSI desde junio del 2004.

RSA se colude con la NSA

- En diciembre del año pasado, el periodista Joseph Menn de Reuters, publicó un artículo en el que se afirma que los directivos de RSA aceptaron un pago por diez millones de dólares por parte de la NSA
- A cambio RSA permitió que sus bibliotecas criptográficas utilizaran de manera predeterminada. El esquema de generador de números aleatorios Dual_EC_DRBG que fuera promulgado como estándar de ISO y de ANSI desde junio del 2004.
- El esquema Dual_EC_DRBG contiene una puerta-trampa introducida por la NSA, la cual permite predecir sin dificultades la secuencia generada por cualquier dispositivo de autenticación fabricado por la compañía.

Otros casos de *"éxito"* para la NSA

- Ataques al esquema de cifrado utilizado por la última generación de teléfonos 4G

Otros casos de *"éxito"* para la NSA

- Ataques al esquema de cifrado utilizado por la última generación de teléfonos 4G
- Acceso a los datos en claro de Skype de llamadas de voz a través de Internet

Otros casos de *"éxito"* para la NSA

- Ataques al esquema de cifrado utilizado por la última generación de teléfonos 4G
- Acceso a los datos en claro de Skype de llamadas de voz a través de Internet
- Colección de un millón de directorios personales por día de correos electrónicos de usuarios de Hotmail, Yahoo, Google y Facebook

Otros casos de *"éxito"* para la NSA

- Ataques al esquema de cifrado utilizado por la última generación de teléfonos 4G
- Acceso a los datos en claro de Skype de llamadas de voz a través de Internet
- Colección de un millón de directorios personales por día de correos electrónicos de usuarios de Hotmail, Yahoo, Google y Facebook
- Desciframiento de conexiones SSL (las cuales se utilizan en el 90% de las transacciones de comercio electrónico a nivel mundial)

Otros casos de *"éxito"* para la NSA

- Ataques al esquema de cifrado utilizado por la última generación de teléfonos 4G
- Acceso a los datos en claro de Skype de llamadas de voz a través de Internet
- Colección de un millón de directorios personales por día de correos electrónicos de usuarios de Hotmail, Yahoo, Google y Facebook
- Desciframiento de conexiones SSL (las cuales se utilizan en el 90% de las transacciones de comercio electrónico a nivel mundial)
- Establecimiento de una división de inteligencia cuyo objetivo es infiltrar la industria mundial de telecomunicaciones

Principales críticas al programa de espionaje de la NSA

- Críticas éticas: los programas de espionaje son ilegales

Principales críticas al programa de espionaje de la NSA

- Críticas éticas: los programas de espionaje son ilegales
- La vigilancia es inútil: Los beneficios reales del sistema de vigilancia son desdeñables o aun, inexistentes

Principales críticas al programa de espionaje de la NSA

- Críticas éticas: los programas de espionaje son ilegales
- La vigilancia es inútil: Los beneficios reales del sistema de vigilancia son desdeñables o aun, inexistentes
- Pérdida de imagen: La NSA ha creado un clima de total desconfianza hacia los Estados Unidos

Principales críticas al programa de espionaje de la NSA

- Críticas éticas: los programas de espionaje son ilegales
- La vigilancia es inútil: Los beneficios reales del sistema de vigilancia son desdeñables o aun, inexistentes
- Pérdida de imagen: La NSA ha creado un clima de total desconfianza hacia los Estados Unidos
- Pérdida de seguridad: Al debilitar deliberadamente la infraestructura de Internet, la NSA ha permitido que oponentes maliciosos puedan actuar con mayor facilidad

Principales críticas al programa de espionaje de la NSA

- Críticas éticas: los programas de espionaje son ilegales
- La vigilancia es inútil: Los beneficios reales del sistema de vigilancia son desdeñables o aun, inexistentes
- Pérdida de imagen: La NSA ha creado un clima de total desconfianza hacia los Estados Unidos
- Pérdida de seguridad: Al debilitar deliberadamente la infraestructura de Internet, la NSA ha permitido que oponentes maliciosos puedan actuar con mayor facilidad
- Pérdidas económicas: Se ha creado una resistencia mundial a utilizar productos estadounidenses de hardware/software

Reacciones internacionales al programa de espionaje de la NSA

- 5.julio.2013: la [sexy] ex espía rusa Anna Chapman le propone matrimonio a snowden a través de Twitter

Reacciones internacionales al programa de espionaje de la NSA

- 5.julio.2013: la [sexy] ex espía rusa Anna Chapman le propone matrimonio a snowden a través de Twitter
- 11.julio.2013: En Rusia, la KGB anuncia el regreso a las máquinas de escribir para enviar despachos oficiales confidenciales

Reacciones internacionales al programa de espionaje de la NSA

- 5.julio.2013: la [sexy] ex espía rusa Anna Chapman le propone matrimonio a snowden a través de Twitter
- 11.julio.2013: En Rusia, la KGB anuncia el regreso a las máquinas de escribir para enviar despachos oficiales confidenciales
- 14.octubre.2013: La presidenta de Brasil, Dilma Rousseff, anuncia la creación de un sistema nacional de correo electrónico cifrado, dependiente de una red local que *no* atravesará suelo estadounidense

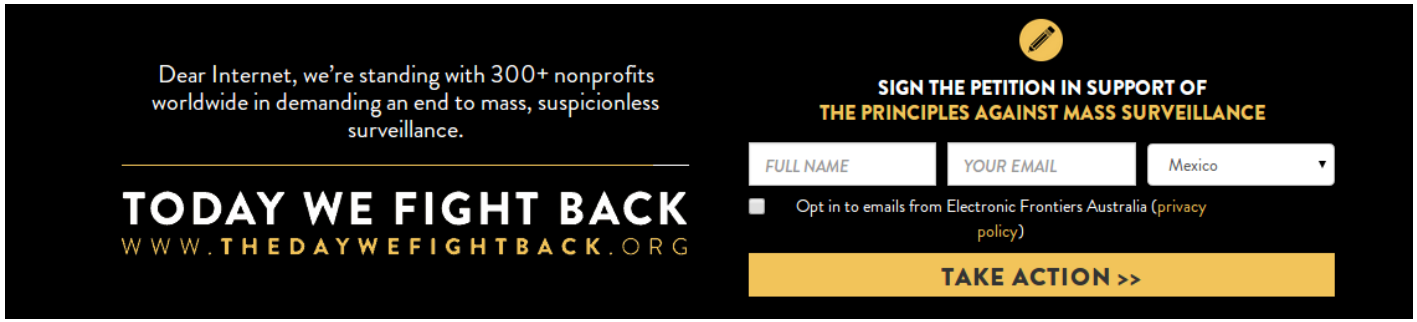
Reacciones internacionales al programa de espionaje de la NSA

- 5.julio.2013: la [sexy] ex espía rusa Anna Chapman le propone matrimonio a snowden a través de Twitter
- 11.julio.2013: En Rusia, la KGB anuncia el regreso a las máquinas de escribir para enviar despachos oficiales confidenciales
- 14.octubre.2013: La presidenta de Brasil, Dilma Rousseff, anuncia la creación de un sistema nacional de correo electrónico cifrado, dependiente de una red local que *no* atravesará suelo estadounidense
- 11.enero.2014: Snowden testificará ante a la Unión Europea con respecto al espionaje ejercido por la NSA a Europa

Reacciones internacionales al programa de espionaje de la NSA

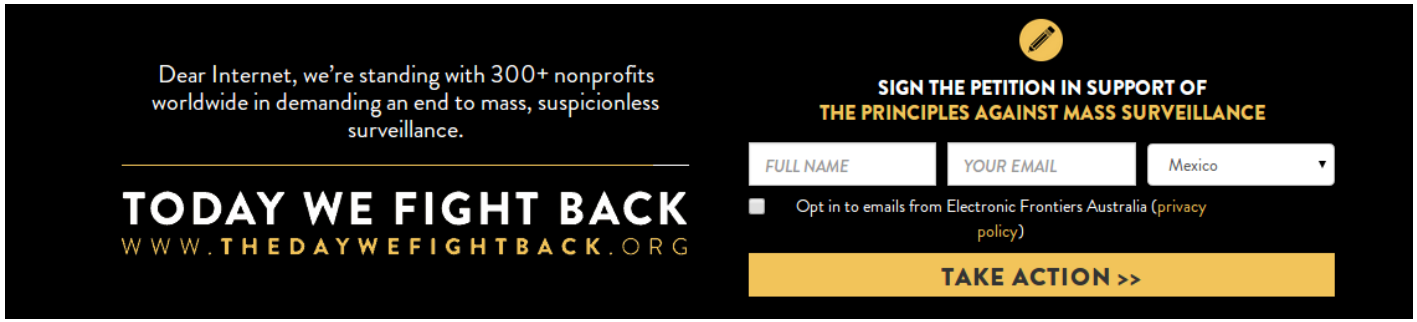
- 5.julio.2013: la [sexy] ex espía rusa Anna Chapman le propone matrimonio a snowden a través de Twitter
- 11.julio.2013: En Rusia, la KGB anuncia el regreso a las máquinas de escribir para enviar despachos oficiales confidenciales
- 14.octubre.2013: La presidenta de Brasil, Dilma Rousseff, anuncia la creación de un sistema nacional de correo electrónico cifrado, dependiente de una red local que *no* atravesará suelo estadounidense
- 11.enero.2014: Snowden testificará ante a la Unión Europea con respecto al espionaje ejercido por la NSA a Europa
- 29.enero.2014: Dos parlamentarios noruegos nominan a Snowden para el Nobel de la Paz

Reacciones en Estados Unidos al programa de espionaje de la NSA



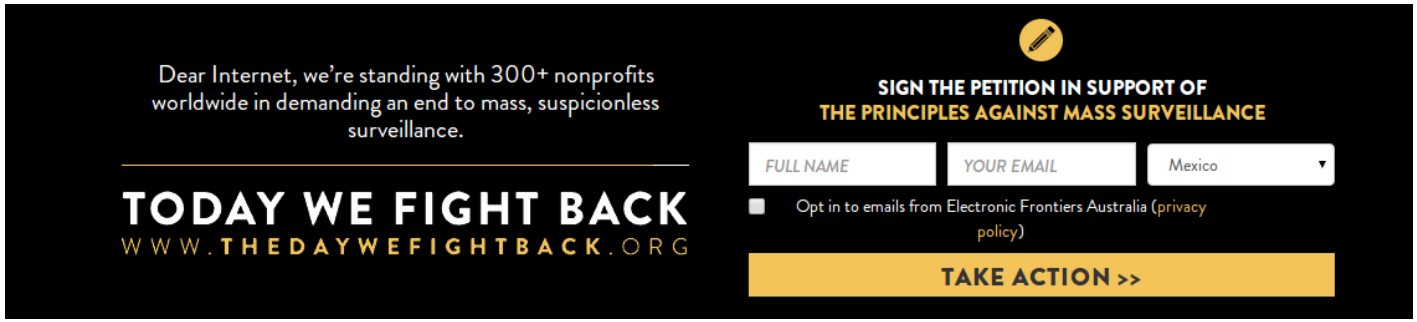
- 25.enero.2014: Más de 50 prominentes criptógrafos estadounidenses firmaron una carta protestando por la vigilancia masiva ejercidad por los Estados Unidos a través de la NSA

Reacciones en Estados Unidos al programa de espionaje de la NSA



- 25.enero.2014: Más de 50 prominentes criptógrafos estadounidenses firmaron una carta protestando por la vigilancia masiva ejercidad por los Estados Unidos a través de la NSA
- 31.enero.2014: El presidente Obama anuncia la designación de un nuevo director de la NSA

Reacciones en Estados Unidos al programa de espionaje de la NSA



- 25.enero.2014: Más de 50 prominentes criptógrafos estadounidenses firmaron una carta protestando por la vigilancia masiva ejercidad por los Estados Unidos a través de la NSA
- 31.enero.2014: El presidente Obama anuncia la designación de un nuevo director de la NSA
- 11.febrero.2014: Activistas del movimiento "The day we fight back" anuncian una campaña para detener el programa de espionaje de la NSA

Reacciones mexicanas al programa de espionaje de la NSA

Reacciones mexicanas al programa de espionaje de la NSA

Hasta el día de hoy no tengo conocimiento de ninguna postura oficial por parte del gobierno mexicano con respecto al espionaje ejercido por los Estados Unidos

A manera de conclusiones

- En su archifamoso cuento fantástico “El aleph”, el escritor argentino Jorge Luis Borges, planteó la existencia de un objeto esférico de unos dos o tres centímetros de diámetro en el cual

A manera de conclusiones

- En su archifamoso cuento fantástico “El aleph”, el escritor argentino Jorge Luis Borges, planteó la existencia de un objeto esférico de unos dos o tres centímetros de diámetro en el cual

  “están, sin confundirse, todos los lugares del orbe, vistos desde todos los ángulos”

A manera de conclusiones

- En su archifamoso cuento fantástico “El aleph”, el escritor argentino Jorge Luis Borges, planteó la existencia de un objeto esférico de unos dos o tres centímetros de diámetro en el cual

  “están, sin confundirse, todos los lugares del orbe, vistos desde todos los ángulos”

  y en el que el todo no es mayor que ninguna de las partes.

A manera de conclusiones

- En su archifamoso cuento fantástico “El aleph”, el escritor argentino Jorge Luis Borges, planteó la existencia de un objeto esférico de unos dos o tres centímetros de diámetro en el cual

  “están, sin confundirse, todos los lugares del orbe, vistos desde todos los ángulos”

  y en el que el todo no es mayor que ninguna de las partes.
- Borges (el personaje) nos refiere que en el aleph se ven a un tiempo, una infinidad de actos deleitables o atroces, todos ocupando un mismo punto, sin superposicíon ni transparencia

A manera de conclusiones

- En su archifamoso cuento fantástico “El aleph”, el escritor argentino Jorge Luis Borges, planteó la existencia de un objeto esférico de unos dos o tres centímetros de diámetro en el cual

  “están, sin confundirse, todos los lugares del orbe, vistos desde todos los ángulos”

  y en el que el todo no es mayor que ninguna de las partes.
- Borges (el personaje) nos refiere que en el aleph se ven a un tiempo, una infinidad de actos deleitables o atroces, todos ocupando un mismo punto, sin superposicíon ni transparencia
- Borges (el escritor) incluye una nota final en la que se afirma que en el inconcebible aleph se refleja el universo entero.

A manera de conclusiones

A manera de conclusiones

En su intento por vigilar al planeta,

A manera de conclusiones

En su intento por vigilar al planeta,
la NSA,

A manera de conclusiones

En su intento por vigilar al planeta,
la NSA,
la agencia que no es,

A manera de conclusiones

En su intento por vigilar al planeta,
la NSA,
la agencia que no es,
quiere ser el aleph.

Créditos de las ilustraciones

Imágenes de Internet tomadas prestadas de

- Banksy
- M. C. Escher
- Quino

Gracias
por su atención

prestado de Quino.

¿Preguntas?