No.19 / agosto-septiembre 2013 ISSN: 1251478,

# .Seguridad

Cultura de prevención para TI

19

# Vulnerabilidades de hoy


## Técnicas para quebrantar y proteger los activos de información

Donde colocar Seguridad | Criptografía cuántica | WPA y WPA2 | Explotación Kali | Seguridad y bioinformación | SCADA

# Contenido

.Seguridad
Cultura de prevención para TI

# Editorial

## Vulnerabilidades de hoy
## Técnicas para quebrantar y proteger los activos de información

Desde el inicio de nuestro caminar sobre la tierra nos hemos visto propicios a sufrir todo tipo de ataques, parte de nuestra naturaleza es ser débiles: vulnerables… ¿Cómo hemos logrado, entonces, llegar al punto actual de desarrollo como especie y como sociedad?

Una de las formas que mejor nos ha funcionado es la capacidad de aprender de los peligros, reaccionando ante ellos, enfrentándolos, evadiéndolos y resistiéndolos. A tal punto que las pestes de la Edad Media son solo recuerdos para la sociedad de la información actual.

Sin embargo, hoy nos enfrentamos a nuevos peligros, muy distintos a los de civilizaciones anteriores. Un claro ejemplo es el riesgo que significa el mal manejo de nuestra información, tanto a nivel personal, como ser víctima de algún fraude; a nivel de comunidad, como espionajes corporativos; y a nivel de humanidad, con resultados que no queremos imaginar.

En esta edición te invitamos a que conozcas algunas de las técnicas actuales utilizadas para quebrantar la protección de nuestra información, de la mano de algunos escritos sobre cómo aminorar esta realidad. Esperamos que los artículos que estás por leer te sean útiles, te generen inquietudes y compartas tus opiniones con nosotros. Deseamos que la lectura de la ediciónnúmero 19 de .Seguridad *Cultura de prevención para* TI te sea de gran ayuda en el arduo camino de hacer a nuestra sociedad menos vulnerable.

L.C.S Jazmín López Sánchez
Editora
Subdirección de Seguridad de la Información

.Seguridad
Cultura de prevención para TI

.Seguridad Cultura de prevención TI M.R. / Número 19 / agosto - septiembre 2013 / ISSN No. 1251478, 1251477 / Revista Bimestral, Registro de Marca 129829

# ¿Dónde colocamos al área de seguridad de la información?

Jeffrey Steve Borbón Sanabria

La asignación de recursos para crear un nuevo cargo o área que sea responsable de la gestión de la seguridad de la información es un reto que implica demostrar que la seguridad no es un gasto, por el contrario, es una inversión que genera valor al negocio, controla y previene diversos tipos de riesgos. También se requiere utilizar otros argumentos convincentes que permitan lograr el apoyo y compromiso de la dirección. Sin embargo, la historia no termina ahí, uno de los temas que la mayor parte de las empresas pasan de forma desapercibida es definir dónde estará ubicado este nuevo cargo o área dentro del organigrama o estructura de la organización.

## Una visión estratégica

A partir de experiencias propias y vivencias de algunos colegas, la imagen y percepción del personal del área de seguridad, o en general del área, puede impactar directamente la labor a realizar. Esto se debe a diversos factores: el más significativo de ellos es la visión como un área técnica enfocada a temas de tecnología, la cual, con el paso de los años, se ha ido cambiando para buscar un rol más estratégico y de apoyo en la toma de decisiones, por encima de la definición de reglas de firewall y gestión de antivirus, entre otras actividades.

Obtener este rol estratégico toma tiempo, además se basa en la generación de indicadores o métricas (relacionados con la gestión) que apalanquen las actividades del negocio, un ejemplo de esto puede ser la aparición y seguimiento de proyectos o actividades de seguridad de la información en el *Balanced Scorecard* (Cuadro de Mando Integral) o dentro de la planeación estratégica de la organización, de esta manera se logra trascender aquel estigma del área que da permisos, autoriza, detiene proyectos, etc., cambiando esa imagen

y permitiendo ser un actor importante en la toma de decisiones en la organización, con ese rol de consejero o asesor que se mencionó al inicio.

## Los esquemas tradicionales

Ahora bien, retomando la idea inicial, con respecto a la ubicación del área de seguridad de la información o del personal dedicado a estas funciones, hay varias opciones que a continuación se analizan de manera detallada con sus pros y contras.

### Al interior de tecnología

Esta posición es una de las más usuales y, en realidad, una de las más complejas de tratar. Aunque se trabaja de la mano con el personal responsable de las tecnologías de información de la organización, pasa directamente a ser parte de este equipo de trabajo, de tal manera que es común enfrentarse a situaciones en las que se presentan conflictos de intereses, un ejemplo de esto puede ser cuando se realiza un análisis de vulnerabilidades o pruebas de intrusión a la infraestructura tecnológica y los resultados obtenidos no son favorables para la imagen del área, por lo que será necesario ocultar información o presentarla de otra forma a la dirección, restándole importancia a los hallazgos identificados.Obviamente, esta situación se soluciona al buscar cómo proteger la imagen de la función del personal del área ante la dirección, esta situación resulta en ocasiones común.

Sin embargo, un punto a favor de esta ubicación es el conocimiento y participación activa dentro de las actividades que realiza el área, pudiendo así implementar controles y estrategias de seguridad de la información desde la fuente, lo que puede reducir las debilidades o fallos de la seguridad de tecnologías y, a final de cuentas llevar a entornos productivos. Un punto final y que resulta decisivo, consiste en que, bajo esta posición dentro de la organización, la percepción de la seguridad de la información se orienta a lo técnico y se presenta la situación mencionada hace algunos párrafos, donde no se ve la labor como se requiere que sea percibida.

### Al interior de auditoría

Un segundo caso o situación, es la existencia del área de seguridad de la información o ubicación del personal responsable de ésta al interior del área de auditoría. Bajo este esquema se cuenta con una percepción orientada al cumplimiento, en algunos casos, también policiva, lo cual es bueno en la medida en que se propongan y entran en vigor políticas, procedimientos y otras medidas necesarias, sin embargo, también hay conflictos de intereses en juego, dado que esta área usualmente es la responsable de validar que el resto de la organización cumpla con las reglas y normativas establecidas como marco interno de comportamiento o lineamientos.
Por consiguiente, desde esta posición no sería posible esperar que el área de seguridad implemente proyectos e iniciativas, dado que cae en el rol de juez y parte, contra uno de los principios de la auditoría y del control interno.

### Al interior de la unidad de riesgos

Las organizaciones que cuentan con un área establecida para la gestión de riesgos y el manejo del ciclo de vida de estos, tienen la posibilidad de estructurar proyectos e iniciativas en pos de la mitigación y con la responsabilidad del manejo de riesgos de seguridad de la información. Desafortunadamente, hay una posición a la que se puede enfrentar el área, verla como un obstáculo para el negocio. Lo anterior suele ocurrir cuando, desde el área de riesgos, se actúa de forma reactiva y se detienen iniciativas, proyectos o labores, al tratar de identificar riesgos que pueden tener un alto impacto y consecuencias adversas para la organización. Es decir, se puede terminar observando a la seguridad de la información como un obstáculo y se entraría en contra de una de las expectativas de la labor a desarrollar: Ser vistos como generadores de valor para el negocio.

### ¿Y entonces dónde?

Luego de visualizar cada escenario, podría concluirse que ningún espacio sirve, pero esto es falso, ya que hay una posición que

estratégicamente es la más óptima y, al mismo tiempo, la más compleja de lograr: depender directamente de la dirección, es decir, organizacionalmente sería un área independiente de otras y reportaría a los altos mandos.

Esta idea no es utópica, se conocen organizaciones que arduamente han logrado salir de roles técnicos y llegado a una posición de aporte y consejería para el negocio, que hace tangible la posición de un área consejera, de acompañamiento, estratégica e importante para el negocio. Bajo este esquema se evitan intermediarios y se alcanza una posición en la que acercarse a la dirección es más simple y se tiene más peso dentro de la organización.

## ¿Y el presupuesto?

Decir que la implementación de seguridad de la información se puede hacer sin presupuesto es una idea errónea, por más que se cuenten con recursos de acceso abierto a nivel tecnológico, existen factores como la pedagogía y la concienciación, por nombrar algunos, que implican contar con recursos para ejecución de campañas y generación de material. Por supuesto, es necesario contar con un músculo económico para inversión en soluciones, actividades y otros factores igual de relevantes.

La recomendación es responsabilizar a cada área transversal del negocio de contar con presupuesto para seguridad

de la información, esto se basa en una primera idea que es simple, el área de seguridad no cuenta con fondos abundantes, por el contrario, es un área que en muchos casos, por más que genere valor, aún es percibida como un gasto y no se dispondrá a manos llenas de presupuesto. Una segunda razón radica en que los servicios se prestan para el negocio, si éste aportará valor o brindará mejoras para unos procesos o actividades de un área, entonces el área correspondiente es la que lo debe costear, es decir, el usuario del mismo. Esto ayudará a cambiar la percepción de que el área de seguridad compite con la de tecnología por ser quien logra gastar másrecursos económicos, recursos humanos y por supuesto, físicos. Resumiendo, el área debe contar con presupuesto propio, pero no es quien debe costear los proyectos de seguridad asociados a las áreas del negocio, sino por el contrario, las mismas áreas deben aportar para estas inversiones, lo cual quiere decir que se deben hacer labores de planeación estratégica para determinar oportunamente qué proyectos tendrá el negocio y qué se requerirá en términos de seguridad y que así sean asignados recursos por la dirección y las áreas responsables.

Una última idea que apalanca lo anteriormente presentado es una frase coloquial que tiene mucho sentido: *"Si no le duele a las áreas la inversión en seguridad, no la valorarán igual"*, el principio es simple, si todo lo carga el área de seguridad, entonces a las demás no les implicará un esfuerzo técnico, físico, de recurso humano y, principalmente, económico, por lo que probablemente no valoren la inversión como debería ser.

En la actualidad, en mi labor como Oficial de Seguridad de la Información, trabajo en un área diferente a las anteriormente mencionadas, pero he percibido una estrategia provechosa y consiste en descentralizar la responsabilidad de la seguridad de la información en una estructura de roles que, a través de varias áreas del negocio, permitan hacer esos roles tácticos, operativos, de control, legales a lo largo de la empresa, contando con responsables en diferentes unidades organizacionales.
Esta visión ha permitido apalancar proyectos

de una manera más óptima, ayudando también a reducir tanta labor de lobby consiguiendo *"patrocinio"* área por área, que aunque es una labor necesaria, por momentos llega a ser desgastante. Al final, independientemente del lugar en el que se coloque el área o el personal, lo primero y más importante es contar con ese apoyo de la alta gerencia para contratar y dedicar recursos. Además, desde el principio es importante mostrar que *"no somos un gasto, somos una inversión que genera valor"* y no sólo con palabras, sino con hechos.

Jeffrey Steve Borbón Sanabria

Ingeniero de sistemas con estudios de máster en seguridad Informática y especialización en Gestión de Riesgos. Ha desarrollado roles en torno a la gestión de TI y de la seguridad de la información en diversos mercados tales como Energía, Educación, Financiero, entre otros. Actualmente se desempeña como oficial de seguridad de la información de un grupo em_ presarial del mercado energético. Cuenta con algunas certificaciones y estudios complemen_ tarios.

# Criptografía cuántica – Parte II

Paulo Santiago de Jesús Contreras Flores

## Implementación del algoritmo de Shor

Recordando el ejemplo de la aplicación teórica del algoritmo de Shor descrito en la anterior entrega de este artículo, el intruso Eve calculó los factores primos p = 5 y q = 3 para el producto de ellos n = 15 y de esta forma obtuvo la llave privada del remitente Bob y descifró el mensaje siguiendo el algoritmo RSA. Siete años después de que Peter Shor publicara su algoritmo[1], en 2001, científicos del Centro de Investigación Almaden de IBM, en San José California, Estados Unidos, consiguieron ejecutar el algoritmo de Shor en una computadora cuántica basada en Resonancia Nuclear Electromagnética, calculando correctamente los factores primos del producto n = 15, utilizando 108 moléculas, cada una de ellas de 7 átomos[2]. A continuación se explicará cómo es que con una computadora cuántica se pudo lograr este desarrollo.

## Los bits

La electrónica digital es la base de las computadoras actuales y a través de ésta, el procesamiento de la información se realiza sobre la unidad básica de información, el bit (binary digit o dígito binario), el cual almacena solamente dos posibles valores por unidad de tiempo, comúnmente interpretados como “0” o “1”, nunca los dos valores al mismo tiempo.A estos dos valores lógicos, dependiendo del contexto en que se trabaje, se les otorga una interpretación, por ejemplo, si se trabaja en un ambiente geofísico, el “1” podría interpretarse como el registro de un sismo detectado de ondas p, y el “0” como un registro de un sismo detectado de ondas s.

Es posible utilizar varios bits al mismo tiempo para así formar valores de mayor tamaño, por ejemplo, la siguiente tabla muestra la representación en bits de los números decimales 3 y 5:

| Número decimal | Representación en binario |
|---|---|
| 3 | 011 |
| 5 | 101 |

Las operaciones en una computadora están dadas por el uso de las proposiciones lógicas, por ejemplo la negación (not), la disyunción (or) o la conjunción (and)[3]. Si se quiere hacer el producto de 3 y 5, se hará uso de la proposición lógica conjunción.

| | Primer valor | Operación | Segundo valor | Resultado |
|---|---|---|---|---|
| Binario | 011 | And | 101 | 1111 |
| Decimal | 3 | * | 5 | 15 |

La computadora toma los valores en binario de ambos números, ejecuta sobre ellos la operación y obtiene el resultado.
Los procesadores solamente pueden ejecutar una operación a la vez por unidad de tiempo. Tomando el ejemplo anterior, supongamos que ahora queremos obtener el valor *q* de la ecuación 3*q = 15, con una computadora actual habría que encontrar los posibles valores de *q* probando cada valor posible a través de una operación lógica a la vez, en la siguiente tabla podemos observar los resultados para los posibles valores de *q*:

| P | operación | Q | resultado |
|---|---|---|---|
| 011 | And | 000 | 0000 |
| 011 | And | 001 | 0001 |
| 011 | And | 010 | 0110 |
| 011 | And | 011 | 1001 |
| 011 | And | 100 | 1100 |
| 011 | And | 101 | 1111 |

Se realizarían 6 operaciones, una por cada ciclo del procesador, para encontrar el resultado correcto; otra opción sería contar con un procesador para cada operación, por lo que se deberá considerar tener al menos 6 procesadores trabajando simultáneamente para obtener el resultado correcto en un solo ciclo del procesador. Es por eso que el cálculo de los factores planteados en el artículo anterior con uno o varios procesadores actuales tomaría un tiempo considerablemente grande.

## Los qubits

El término qubit proviene de quantum bit o bit cuántico. La alta velocidad de procesamiento de las computadoras cuánticas en comparación con las computadoras actuales, se debe al uso de propiedades descubiertas en partículas subatómicas que permiten tener a la vez, por ejemplo, todos los valores posibles para un cómputo dado.

Como los bits, un qubit puede tener dos posibles estados, 0 ó 1, para diferenciarlos de los bits clásicos (que se usan en la electrónica digital) se utiliza la notación de Dirac (usada para representar el estado físico de un sistema cuántico[4] ), quedando de la forma `|0>` o `|1>` (en alguna literatura relacionada se les suele nombrar como ket uno y ket cero); pero un qubit puede encontrarse en un estado de superposición arbitraria (combinación de sus dos posibles estados), es decir, el qubit puede almacenar tanto `|0>` o `|1>` al mismo tiempo durante el cómputo y antes de que se mida su valor[5], esto permitiría realizar múltiples operaciones simultáneamente, pero una vez medido el estado del qubit, éste permanecerá en ese estado.

El estado de superposición del qubit se puede representar por la función:

$$\Psi = a|0\rangle + b|1\rangle$$

En donde los coeficientes *a* y *b* son números complejos.

La probabilidad de que se encuentre con un valor `|0>` o `|1>` está dada por la norma al cuadrado, es decir:

$$|a|^2+|b|^2 = 1$$

Mientras no se mida el estado del qubit, éste puede permanecer en el estado de superposición, cuando el valor sea medido, el qubit saldrá del estado de superposición, entonces, se tendrá una cierta probabilidad de que se encuentre con un valor `|0>` o con un valor `|1>`. Esto se debe a que todo sistema cuántico posee como propiedad fundamental un carácter probabilístico[6].

De la misma forma que los bits clásicos, los qubits pueden formar arreglos para representar la información, si tomamos el ejemplo de la búsqueda del valor q para la ecuación 3*q = 15 de los bits clásicos anteriores, podemos tener en un solo procesador cuántico todos los posibles valores de *q* al mismo tiempo con solamente 3 qubits:

$$\Psi = x0|000> + x1|001> + \ldots + x5|101> + x6|110> + x7|111>$$

En donde la función Ψ representa el estado del qubit, los coeficientes $x_n$ son números complejos y la norma de $x_n$ corresponde a la probabilidad de que la computadora se encuentre en ese estado, es decir:

- la probabilidad de que la computadora se encuentre en el estado |000> es de |x0|2
- la probabilidad de que la computadora se encuentre en el estado |001> es de |x1|2
- …
- la probabilidad de que la computadora se encuentre en el estado |101> es de |x5|2
- …

Una vez que se realice la medición del resultado correcto y descartando las opciones erróneas[7], los qubits quedarán como:

$$\Psi = |101>$$

Y se romperá el estado de superposición, quedando el valor |101> definido. A este concepto se le conoce como paralelismo cuántico, en general la idea de paralelismo cuántico es recorrer al mismo tiempo todos los posibles valores que podría tomar un cómputo, en este caso un cálculo de una operación de multiplicación[8].La superposición cuántica da la posibilidad de que con un arreglo de *n* qubits se puedan representar $2^n$ valores simultáneos . Por ejemplo, un cómputo sobre 300 qubits lograría el mismo efecto que 2300 cómputos simultáneos sobre bits clásicos[10].

Con esta capacidad de cómputo de las computadoras cuánticas se podrá aplicar con eficiencia el algoritmo de Shor para encontrar en un tiempo razonablemente corto los coeficientes *p* y *q* necesarios para calcular las llaves de cifrado y descifrado del algoritmo RSA, el cual es el soporte para protocolos y esquemas de comunicación y cifrado como SSL o PKI.

## El espín

Una propiedad del mundo físico que puede ser utilizada para representar al qubit es el espín (del inglés *spin*, girar), es una propiedad intrínseca del electrón (tal como lo es la masa y la carga eléctrica). Es común encontrar en la literatura

relacionada la analogía entre la rotación de un objeto del mundo macroscópico, por ejemplo, un trompo o el movimiento de rotación de la tierra e imaginar al espín como una cantidad (momento magnético) del campo magnético que genera el electrón que gira sobre su propio eje; aunque esta propiedad debe considerarse como un concepto cuántico, sin una analogía detallada de la mecánica clásica.

Dependiendo de la orientación del campo magnético es como se representa el espín, siempre con una cantidad de este campo bien definida. Por ejemplo, el valor del espín del electrón es de ½, y dentro del átomo, si está alineado con el espín del núcleo, se dice que el espín tiene orientación hacia arriba ↑, y si está alineado en la dirección contraria tiene espín hacia abajo ↓. Esta propiedad del electrón se puede usar para representar el valor de un qubit, el valor de `|0>` puede ser orientación hacia arriba o si tiene orientación hacia abajo se dice que tiene el valor `|1>`. Se puede representar de la siguiente forma:

```
a|↑> + b|↓>
a|0> + b|1>
```

## Fortalecimiento en la distribución de claves, el protocolo BB84

Hasta el momento se ha hablado del tema, solamente desde el punto de vista de la resolución por medio de una computadora cuántica de un algoritmo de cifrado actual, como lo es RSA, pero con los descubrimientos sobre el comportamiento de las partículas, también se han planteado el uso de sus propiedades cuánticas para fortalecer las comunicaciones. Un ejemplo de esto es en el envío de claves a través del protocolo BB84, creado en 1984 por Charles Bennet y Gilles Brassard[11].

Una forma de implementación de los qubits es a través de fotones, con ellos se pueden obtener cuatro posibles polarizaciones horizontal, vertical, diagonal derecha o diagonal izquierda, es en esta partícula de luz en que se basa el planteamiento del protocolo BB84.

Consideremos de nuevo a tres actores, Alice, Bob y el intruso Eve. En el ejemplo del artículo anterior, Eve interceptaba ilegítimamente la conversación sin que Alice o Bob lo advirtieran.
Para este ejemplo, Alice envía a través de un canal cuántico a Bob un bit al que le aplicó una base, la cual es un estado de polarización de un fotón (polarización horizontal, vertical, diagonal derecha o diagonal izquierda) y es usada como un filtro; entonces Alice envía a Bob `|1>--`, un bit 1 con una polarización `"–"` (polarización horizontal, 0º sobre un plano), Bob aplicará una base elegida de forma previa y aleatoria al bit recibido de Alice, si Bob eligió una base con polarización horizontal, el resultado de aplicarla a lo recibido por Alice será un *1*, que es el bit enviado por Alice. En cambio, si aplica una base con polarización vertical, el resultado será *0*, que no corresponde al bit enviado por Alice, es decir se produjo un error, en cualquier caso Bob conservará su resultado en secreto.

Una vez que ha finalizado la transmisión de los datos por este canal cuántico, Alice y Bob comparan sus bases públicamente, es decir, por un canal clásico, se quedarán solamente con la información que obtuvieron cuando ambos midieron sobre la misma base, es decir, cuando no hubo errores, este dato será la clave entre ambos[12].

La siguiente tabla ilustrará mejor el concepto, fue tomada del trabajo realizado por Gustavo Rigolin y Andrés Anibal Rieznik. Las primeras cinco líneas corresponden a una transmisión a través de un canal cuántico, las siguientes cinco líneas corresponden a una transmisión por un canal clásico. Y la última es la clave compartida que usarán durante su comunicación. El ejemplo considera la pérdida de bits durante la transmisión.

La base A corresponde a una polarización horizontal, es decir que el fotón tiene una polarización de 0º respecto al plano y la base B corresponde a una polarización diagonal derecha, es decir que el fotón tiene una polarización de 45º respecto al plano.

Las mediciones de Bob hubieran salido erróneas, a pesar de haber elegido la misma base de Alice, si Eve hubiera interceptado los datos al utilizar este protocolo. Alice y Bob eligen unos datos

al azar, que anuncian públicamente, con el fin de calcular el porcentaje de error (razón de los datos que no coincidieron), si el error está por encima del 10%, eliminan sus datos y podrían volver a realizar el protocolo[13]. Con esto se tiene certeza sobre la privacidad de su clave secreta al percatarse si es que hubo un intruso durante la comunicación.

Con este planteamiento, se podrá resolver uno de los principales objetivos de la criptografía, la distribución segura de claves criptográficas entre dos partes que inicialmente no comparten ninguna información secreta[14].

| Secuencia de bits de Alice | 0 | 1 | 1 | 0 | 1 | 1 | 0 | 0 | 1 | 0 | 1 | 1 |
|---|---|---|---|---|---|---|---|---|---|---|---|---|
| Bases escogidas por Alice | B | A | B | A | A | A | A | A | B | B | A | B |
| Fotones enviados por Alice | $\|0\rangle_B$ | $\|1\rangle_A$ | $\|1\rangle_B$ | $\|0\rangle_A$ | $\|1\rangle_A$ | $\|1\rangle_A$ | $\|0\rangle_A$ | $\|0\rangle_A$ | $\|1\rangle_B$ | $\|0\rangle_B$ | $\|1\rangle_A$ | $\|1\rangle_B$ |
| Bases escogidas por Bob | A | B | B | A | A | B | B | A | B | A | B | B |
| Bits recibidos por Bob | 1 | | 1 | | 1 | 0 | 0 | 0 | | 1 | 1 | 1 |
| Bob informa de los fotones detectados | A | | B | | A | B | B | A | | A | B | B |
| Alice informa las bases correctas | | | OK | | OK | | | OK | | | | OK |
| Información compartida | | | 1 | | 1 | | | 0 | | | | 1 |
| Bob revela algunos bits de la clave | | | | | 1 | | | | | | | |
| Alice confirma estos bits | | | | | OK | | | | | | | |
| Bits restantes que serán la clave | | | 1 | | | | | 0 | | | | 1 |

## Las computadoras cuánticas

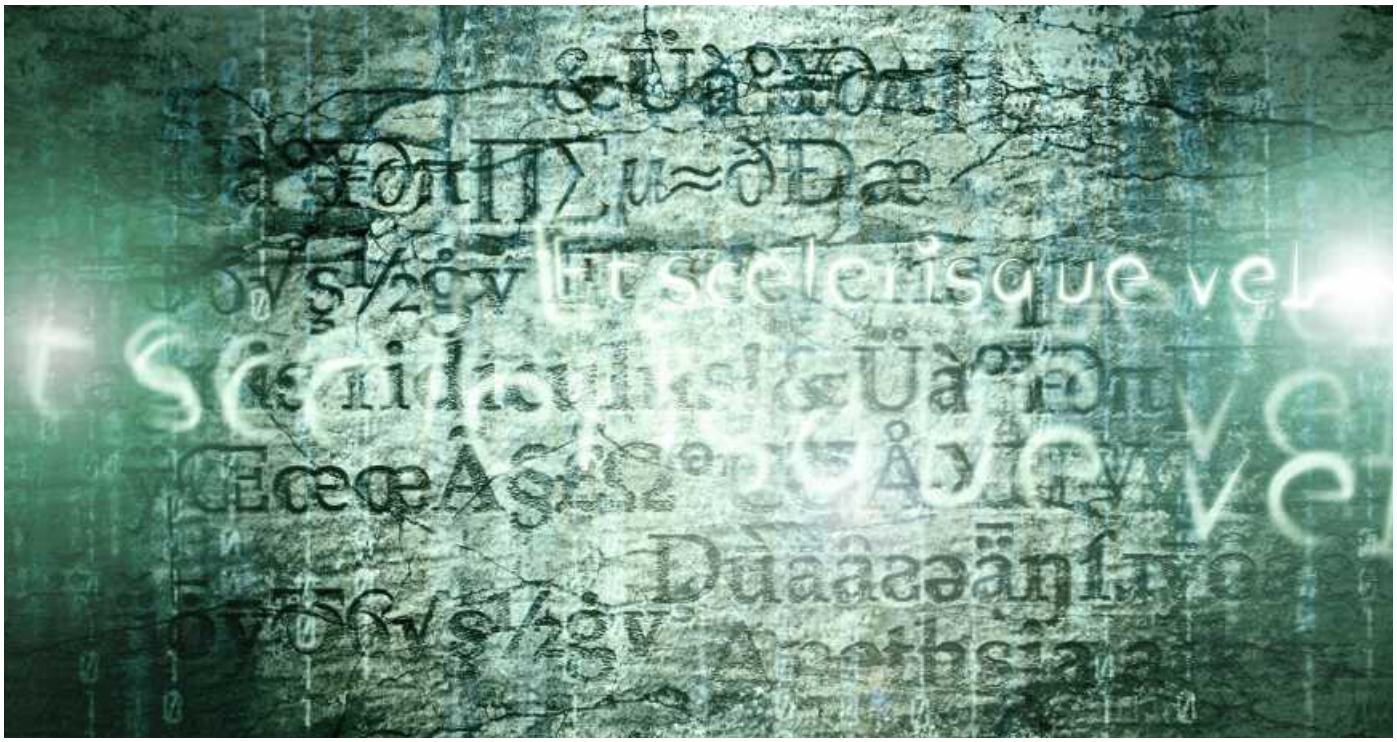
En la investigación científica con frecuencia existe una brecha entre el planteamiento de los estudios, los resultados teóricos y su recreación en el mundo real, porque cuando se trata de crear lo propuesto en la teoría, se encuentran complicaciones de tipo técnico. Y la búsqueda del desarrollo de una computadora cuántica no es la excepción.

Se han estudiado y probado diversas técnicas para la creación de una computadora cuántica. Pero, aunque exista esta diversidad de posibilidades de sistemas cuánticos, las computadoras cuánticas deberán cumplir con ciertas características para ser consideradas como tales. En el año 2000, David P. DiVincenzo, investigador de IBM, propuso cinco criterios principales para considerar un sistema cuántico como computadora cuántica[15].

1.Tener caracterizada la noción de qubit y poder ensamblar varios de ellos.
2.Contar con un conjunto de compuertas cuánticas primitivas que permitan realizar cualquier algoritmo.
3.Poder iniciar una lista de qubits en estados puros determinados.
4.Poder ejecutar la operación de toma de mediciones.
5.Que los tiempos de coherencia excedan los de aplicación de las compuertas cuánticas primitivas [16].

A partir del cumplimiento de estos criterios es que se han creado diversas propuestas. A continuación se enlistan algunas[17].

•Resonancia Nuclear Electromagnética



- Cavidad electrodinámica cuántica
- Trampas de iones
- Átomos neutros
- Técnicas ópticas
- Superconductividad
- Técnicas de estado sólido

Como se mencionó al principio, el desarrollo de la computadora cuántica en 2001, por científicos del Centro de Investigación Almaden de IBM, se basó en la Resonancia Nuclear Electromagnética. Este dispositivo está formado por moléculas que se encuentran en una solución líquida a temperatura ambiente, almacena los qubits en el espín de los átomos de cada molécula y las manipula a través de radiación electromagnética. Los núcleos de estas moléculas tienen espín ½ y tienen orientaciones hacia *"arriba"* o hacia *"abajo"*.

La factorización de 15 como el producto de 3 por 5 se logró con un conjunto de moléculas, siete espines en cada molécula actuando como siete qubits, sin embargo, el modelo no podría extenderse a más de 10 qubits 18.

Otra motivación para el estudio de la computación cuántica se debe a la creación de componentes electrónicos cada vez más pequeños, llegará el momento en que, por el tamaño de éstos, empezarán a aparecer fenómenos de la mecánica cuántica en esos desarrollos.

La computación cuántica es un área que irá en crecimiento, probablemente las primeras computadoras comerciales serán una combinación de la tecnología de la electrónica digital y de la computación cuántica. Con el desarrollo de esta área se abre un mundo de posibilidades, porque las implementaciones no se limitan a una sola técnica.

De la misma forma como avanzan las implementaciones de las primeras computadoras cuánticas, será necesario que la criptografía cuántica avance y pruebe los desarrollos actuales para que pueda ofrecer la confidencialidad y la integridad a este nuevo cómputo.

Por último, enlisto tres enlaces referentes a investigaciones de IBM con el cómputo cuántico.

*IBM Says Practical Quantum Computers are Close*

*IBM Paves The Way Towards Scalable Quantum Computing*

*IBM Research Advances Device Performance for Quantum Computing*

Quiero agradecer a Tonatiuh Sánchez Neri y a Félix Hernández Fuentes por sus acertados comentarios y observaciones a este trabajo,

a la editora de la revista Jazmín López Sánchez y al diseñador Abraham Ávila por su apoyo y paciencia para la publicación del mismo; también a la profesora M. en C. Ma. Jaquelina López Barrientos quien motivó durante mi formación académica mi interés por este tema.

[1]El desarrollo del algoritmo de Shor se encuentra disponible en http://arxiv.org/pdf/quant-ph/9508027v2 (ago-2013)
[2]IBM's Test-Tube Quantum Computer Makes History. IBM, 2001. Disponible en http://www-03.ibm.com/press/us/en/pressrelease/965.wss (ago-2013)
[3]TRELLES, ROSALES. Introducción a la lógica. Pontificia Universidad Católica del Perú. 2ª ed. 2002.
[4]LÉVY, ÉLIE. Diccionario Akal de física, Akal, España, 2008.
[5]ARREOLA, Verónica. Computación Cuántica, México, Universidad Nacional Autónoma de México, Facultad de Ciencias, 2004.
[6]KLIMOV, Andrei B. "Información cuántica: ideas y perspectivas", en Revista Cinvestav , México, IPN, v27, n1 enero-marzo, 2008.
[7]El descartar las opciones erróneas se logra con el concepto de interferencia, que es un caso particular de la superposición, se dejará al lector la tarea de profundizar con apoyo de las referencias.
[8]ARREOLA, Verónica. Computación Cuántica, México, Universidad Nacional Autónoma de México, Facultad de Ciencias, 2004.
[9]VARGAS, BRANCH. Quantum computing's state of the art. Revista Avances en Sistemas e Informática, Vol 6 Num 2. Colombia. 2009.
[10]ARREOLA, Verónica. Computación Cuántica. México, Universidad Nacional Autónoma de México, Facultad de Ciencias, 2004.
[11]El documento original puede consultarse en http://researcher.watson.ibm.com/researcher/files/us-bennetc/BB84highest.pdf (ago-2013)
[12]LÓPEZ, Barrientos Ma. Jaquelina. Criptografía, México, Universidad Nacional Autónoma de México, Facultad de Ingeniería, 2009.
[13]ARREOLA, Verónica. Computación Cuántica. México, Universidad Nacional Autónoma de México, Facultad de Ciencias, 2004.
[14]RIGOLIN, RDIEZNIK. Introdução à criptografia quântica. Revista Brasileira de Ensino de Física, v. 27, n. 4, Brasil. 2005. Disponible en http://www.scielo.br/pdf/rbef/v27n4/a04v27n4.pdf (ago-2013)
[15]DIVINCENZO, David P. The Physical Implementation of Quantum Computation. IBM, 2008. Disponible en http://arxiv.org/pdf/quant-ph/0002077v3 (ago-2013)
[16]MORALES-LUNA, Guillermo. "Computación cuántica: un esbozo de sus métodos y desarrollo". IPN, Revista Cinvestav. v26. 2007.
[17]Ibid.
[18]Ibid.

Paulo Santiago de Jesús Contreras Flores

Egresado de la carrera de Ingeniería en Computación de la Facultad de Ingeniería de la UNAM, cursando el módulo de especialización de redes y seguridad. Formó parte de la cuarta generación del Plan de becarios de seguridad en cómputo impartido por la Subdirección de Seguridad de la Información/UNAM-CERT a través de la DGTIC de la UNAM.

Actualmente colabora en la SSI/UNAM-CERT en el área de Detección de Intrusos y Tecnologías Honeypot, realizando pruebas en tecnologías honeypot y aplicaciones de detección de tráfico malicioso.

Cuenta con las certificaciones Certified Ethical Hacking (CEH) y Computer Hacking Forensic Investigator (CHFI) del ECCouncil.

# Redes inalámbricas WPA/WPA2 ¿La protección ya no es suficiente?

Erika Gladys De León Guerrero

Se tiene la idea de que las redes inalámbricas 802.11 cuentan con un nivel de protección alto cuando se encuentran configuradas mediante un cifrado WPA/WPA2, sin embargo, es importante hacer tres observaciones con respecto a este tema.

Por otro lado, la combinación de estos protocolos en conjunto con WPS ( Wi-Fi Protected Setup), no da el resultado esperado, sino que se expone información debido a que existen vulnera_ bilidades que eliminan la protección brindada por la fortaleza de estos protocolos.

La primera se relaciona con la protección establecida por estos protocolos, debido a que principalmente se refieren a la autenticación, por lo que otros elementos básicos de seguridad, como la disponibilidad, no son cubiertos por el control, lo que implica la implementación de un conjunto de medidas adicionales para proporcionar un nivel de seguridad aceptable.

De lo anterior se deriva la herramienta Reaver, muy popular en los últimos meses, la cual aprovecha la divulgación para vulnerar redes inalámbricas del tipo de cifrado WPA/WPA2.
Finalmente, la fortaleza per se que utiliza WPA/WPA2 está dada por el nivel de robustez de la contraseña, por lo que las contraseñas sin la fortaleza suficiente o configuradas por

defecto por los fabricantes, son vulnerables a ataques de fuerza bruta. A lo largo del artículo se expondrá principalmente el segundo punto, debido a que los otros son más triviales.

## ¿Qué es WPS?

Wi-Fi Protected Setup™ es un programa opcional de certificación que proporciona la Wi-Fi Alliance[1], diseñado para facilitar la ins_ talación y configuración de seguridad en redes inalámbricas de área local 802.11. Este programa fue presentado por la *Wi-Fi Alliance* a principios de 2007, proporciona un conjunto de soluciones de configuración de red para hogares y pequeñas oficinas. Permite administrar y configurar de manera segura los elementos de una red inalámbrica pequeña sin necesidad de tener conocimientos avanzados en el tema[2].

En WPS existen dos opciones principales de configuración de seguridad, *Personal Identification Number* (PIN) y *Push Button Configuration* (PBC), los *Access Point* deben ofrecer ambas opciones y los clientes deben of recer, al menos, la opción de seguridad PIN.


Imagen 1. . Logo WPS

## Método PIN

En este método se proporciona un PIN a los distintos dispositivos que se quieren integrar a la red con la finalidad de garantizar que dicho dispositivo es válido, previniendo la conexión accidental o maliciosa de dispositivos no deseados. El PIN suele estar impreso en el Access Point, como se muestra en la *figura 2*, y lo proporciona el proveedor de servicio de Internet. Este código debe ser ingresado por el usuario mediante una interfaz gráfica o una aplicación proporcionada por el *Access Point*.


Imagen 2. PIN impreso en AP

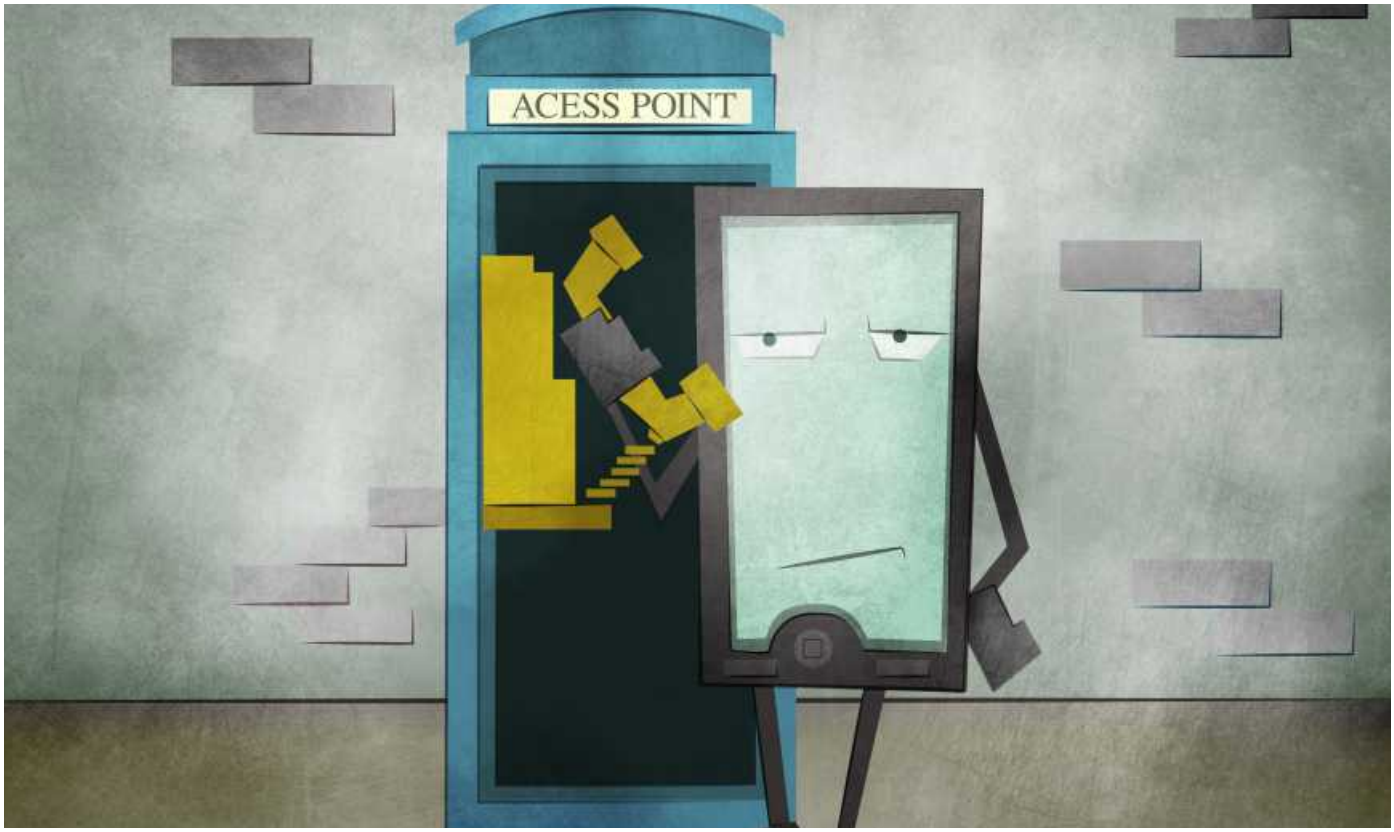
## Método PBC

Mediante el método PBC es posible aplicar cifrado de datos al presionar un botón físico o lógico situado en el Access Point y el cliente.

El uso de WPS simplifica algunas tareas requeridas al momento de configurar una red inalámbrica, por ejemplo, la generación de SSID y contraseña. Además, permite al usuario proteger la red automáticamente mediante los dos métodos mencionados previamente. Otro tipo de protecciones que ofrece este sistema consiste en revisar la configuración de la clave WPA2 y el SSID. Tiene una función tiempo de espera para cancelar el proceso de configuración si el intercambio de credenciales no se establece de manera oportuna. Para mejorar la complejidad de la contraseña, el sistema genera contraseñas robustas evitando que el usuario configure contraseñas fáciles de adivinar.

## ¿Cómo funciona WPS?

WPS proporciona un procedimiento simple y consistente para agregar nuevos dispositivos a redes Wi-Fi, este procedimiento está basado en un protocolo de detección homogéneo por parte de los fabricantes. El procedimiento utiliza automáticamente un elemento para expedir credenciales a los dispositivos que están asociados en la red. Todos los Access Point




certificados con WPS poseen capacidad de registro de nuevos dispositivos. Además, el elemento que registra puede residir en cualquier dispositivo de la red. Un elemento de registro que reside en el *Access Point* se conoce como *Internal Registrar* o elemento de registro interno. Un elemento de registro que reside en otro dispositivo de la red se conoce como *External Registrar* o elemento de registro externo. WPS puede admitir varios elementos de registro en una sola red[3].

El proceso para la configuración de un nuevo dispositivo en la WLAN comienza con una acción iniciada por el asistente de configuración e introduce el PIN o presiona el botón PBC. Ésta es la etapa donde el usuario pretende acceder a la red. WPS inicia el intercambio de información entre el dispositivo y el elemento de registro. Este último expide las credenciales de red (SSID y clave de seguridad) que autorizan al cliente a unirse a ésta. Una vez otorgado el acceso, el nuevo dispositivo puede comunicarse de forma segura transmitiendo datos a través de la red y evitando accesosno autorizados. Una vez que WPS ha finalizado y concede el acceso, la configuración es guardada, por lo que el usuario no tiene que realizar el procedimiento cada vez que quiera acceder. El dispositivo, una vez encendido, realizará una búsqueda automática para asociarse a la red.

WPS puede cifrar los datos y autenticar cada dispositivo, también puede ser utilizado en una red abierta, sin cifrado. El intercambio de credenciales de red e información inalámbricas se realiza mediante el protocolo de autenticación extensible (EAP-WSC), uno de los protocolos de autenticación utilizados en WPA. Se establece un handshake en el que los dispositivos se autentican mutuamente y de ese modo un cliente es aceptado en la red, pues el elemento de registro comunica el SSID y la clave WPA2 previamente compartida (PSK). El uso de un PSK al azar mejora la seguridad al eliminar el uso de contraseñas que pueden ser previsibles y fáciles de obtener. Por otro lado, en el método de instalación tradicional, el usuario debe configurar manualmente el *Access Point* para soportar el tipo de cifrado con PSK y, a continuación, debe introducir manualmente el SSID y PSK tanto en el AP como en el cliente. Este enfoque está sujeto a errores del usuario a través de una mala escritura de PSK y SSID. Con WPS, el proceso de intercambio de credenciales requiere poca intervención del usuario, solo hasta que se ha completado la primera acción de configuración (introducir el PIN o presionar el botón PBC),

ya que la red emite el nombre y PSK. La mayoría de los fabricantes, incluyendo Cisco/Linksys, Netgear, D-Link, Belkin, Buffalo, ZyXEL y Technicolor tienen dispositivos certificados en WPS, otros proveedores como TP-Link no están certificados pero cuentan con soporte para WPS.

## PIN Internal Registrar

Como se comentó anteriormente, el usuario debe ingresar el PIN en el adaptador de Wi-Fi dentro de una interfaz web del Access Point. El PIN puede estar impreso en el dispositivo (Access Point).

## PIN External Registrar

El usuario tiene que ingresar el PIN en el dispositivo del cliente, por ejemplo, en una computadora.

Una vez que se ha explicado teóricamente el funcionamiento de los dos métodos empleados por WPS, se explicarán las vulnerabilidades a las cuales está expuesto.


## Problema de seguridad en PIN External Registrar

Debido a que el método de PIN External Registrar no requiere ningún tipo de autenticación, independiente al acto de proporcionar el PIN, es potencialmente vulnerable a ataques de fuerza bruta.

El investigador Stefan Viehböck ha detectado una vulnerabilidad en el proceso de autenticación que permite a un atacante reducir el número de intentos y comprobaciones en un ataque de fuerza bruta para descubrir el PIN de acceso

a la red que usa el AP en el protocolo WPS[4]. El ataque es posible, debido a que el protocolo WPS no implementa la posibilidad de limitar el número de intentos posibles. Además, la vulnerabilidad detectada reduce el tiempo necesario para realizar este tipo de ataque a un intervalo de tiempo de 4 a 10 horas.

La vulnerabilidad ha sido detectada en los mensajes EAP-NACK que envía el Registrar (AP) al cliente y/o dispositivo con la primera y segunda mitad del PIN, al iniciar una autenticación externa mediante código PIN. Esta forma de autenticación reduce drásticamente el número de intentos necesarios para averiguar el PIN, disminuyéndolo de 10^8 (100.000.000) a ~ 20.000.

Un atacante puede obtener información acerca de la exactitud de los elementos del PIN basada en las respuestas del Access Point:

- Si se recibe un mensaje EAP-NACK después de enviar M4, se sabe que la primera mitad del PIN es incorrecta.
- Si se recibe un mensaje EAP-NACK después de enviar M6, sabe que la segunda mitad del PIN es incorrecta.

Así los intentos sufren un decremento de $10^8$=100 000 000 a $10^4 + 10^4$ =20 000.
Como el último dígito pertenece al *checksum* del PIN, los intentos se reducen a
$10^4 + 10^3$ =11 000.

La vulnerabilidad se puede resumir como la susceptibilidad a ataques de fuerza bruta de WPS, específicamente PIN WPS, esta vulnerabilidad es dada debido a que la implementación permite indicar cuándo la primera mitad del PIN es correcta lo que reduce considerablemente la cantidad de intentos al ejecutar un ataque de fuerza bruta. Para disminuir el grado de dificultad para la obtención del PIN mediante combinaciones reiteradas, el último dígito es conocido debido a que este dígito representa el *checksum* o suma de verificación del PIN. Estos dos factores dan como resultado un total de 10^8 a 10^4 + 10^3 lo que significa 11,000 intentos en total.

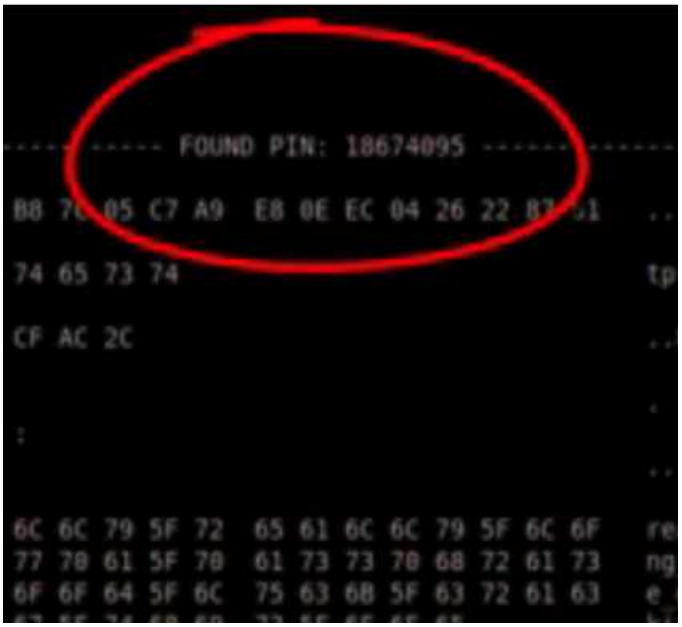
La siguiente tabla permite visualizar mejor lo explicado anteriormente:

| Autenticación | Acceso Físico | Interface WEB | Solo PIN |
|---|---|---|---|
| Push Button Connect | Requerido | | |
| PIN internal Registrar | | Requerido | |
| PIN External Registrar | | | Requerido |

Esta vulnerabilidad está referenciada bajo el identificador CVE-2011-5053[5], donde es posible ver los productos afectados y detalles extra.

Para casos más prácticos, existen herramientas como *Reaver*, las cuales son capaces de identificar la clave WPA/WPA2-PSK de cualquier Access Point que tenga activado WPS. Otra opción es el código[6] escrito de Stefan Viehböck, el cual está incluido en su artículo.

El resultado de la herramienta *Reaver* puede observarse en la siguiente imagen:




## Mitigación o solución

Se recomienda la desactivación de WPS para eliminar esta vulnerabilidad, algunos proveedores han desarrollado guías especiales para su desactivación, sin embargo, existen dispositivos que no lo permiten.

1 http://www.wi-fi.org/
2 https://www.wi-fi.org/knowledge-center/white-papers/wi-fi-certified-wi-fi-protected-setup%E2%84%A2-easing-user-experience-home-a-0
3 https://www.wi-fi.org/download.php?file=/home/webs/wifi/public_html/sit

es/default/files/downloads-registered/wp_20101216_Wi-Fi_Protected_Setup.pdf
4 http://www.seguridadparatodos.es/2012/01/vulnerabilidad-en-el-protocolo-wifi.html
5 http://web.nvd.nist.gov/view/vuln/detail?vulnId=CVE-2011-5053
6 http://sviehb.files.wordpress.com/2011/12/viehboeck_wps.pdf

## Referencias


*http://www.seguridadparatodos.es/2012/01/vulnerabilidad-en-el-protocolo- Wi-Fi.html*

*http://sviehb.wordpress.com/2011/12/27/wi-fi-protected-setup-pin-brute-force-vulnerability/*
*http://www.kb.cert.org/vuls/id/723755*

*https://www.wi-fi.org/knowledge-center/white-papers/wi-fi-certified-wi-fi-protected-setup%E2%84%A2-easing-user-experience-home-a-0*

*https://code.google.com/p/reaver-wps/*

*http://www.tacnetsol.com/news/2011/12/28/cracking- Wi-Fi-protected-setup-with-reaver.html*

*https://www.wi-fi.org/download.php?file=/home/webs/ Wi-Fi/public_html/sites/default/files/downloads-registered/wp_20101216_Wi-Fi_Protected_Setup.pdf*



Erika Gladys De León Guerrero

Recibió el título de Ingeniera en Computación en la Universidad Nacional Autónoma de México (UNAM). Más de 8 años de experiencia en Seguridad de la Información, participando como consultora, ponente, instructora y académica, implementando y ejecutando proyectos de gran importancia a nivel nacional. Cuenta con experiencia en Pruebas de Penetración (Pentest), Análisis forense, Análisis de Vulnerabilidades, Sistemas de Gestión de Seguridad de la Información (SGSI), Auditoría e Investigación sobre nuevas tecnologías de seguridad. Ha impartido cursos y talleres junto a expertos internacionales. Ha impartido conferencias y cursos a nivel nacional. Ha asistido a conferencias internacionales como BlackHat (Briefings) y Defcon, además de recibir capacitación internacional en 2012 y 2013 en BlackHat Training con los cursos SQL Injection y Advanced Windows Explotation (AWE).

Pasante de la Maestría en Ingeniería en Seguridad y Tecnologías de la Información (ESIME-IPN). Ex colaboradora de la Subdirección de Seguridad de la Información (SSI/UNAM-CERT). Auditor interno y líder. Académica en la maestría de redes en el Instituto Tecnológico Superior de Sinaloa.

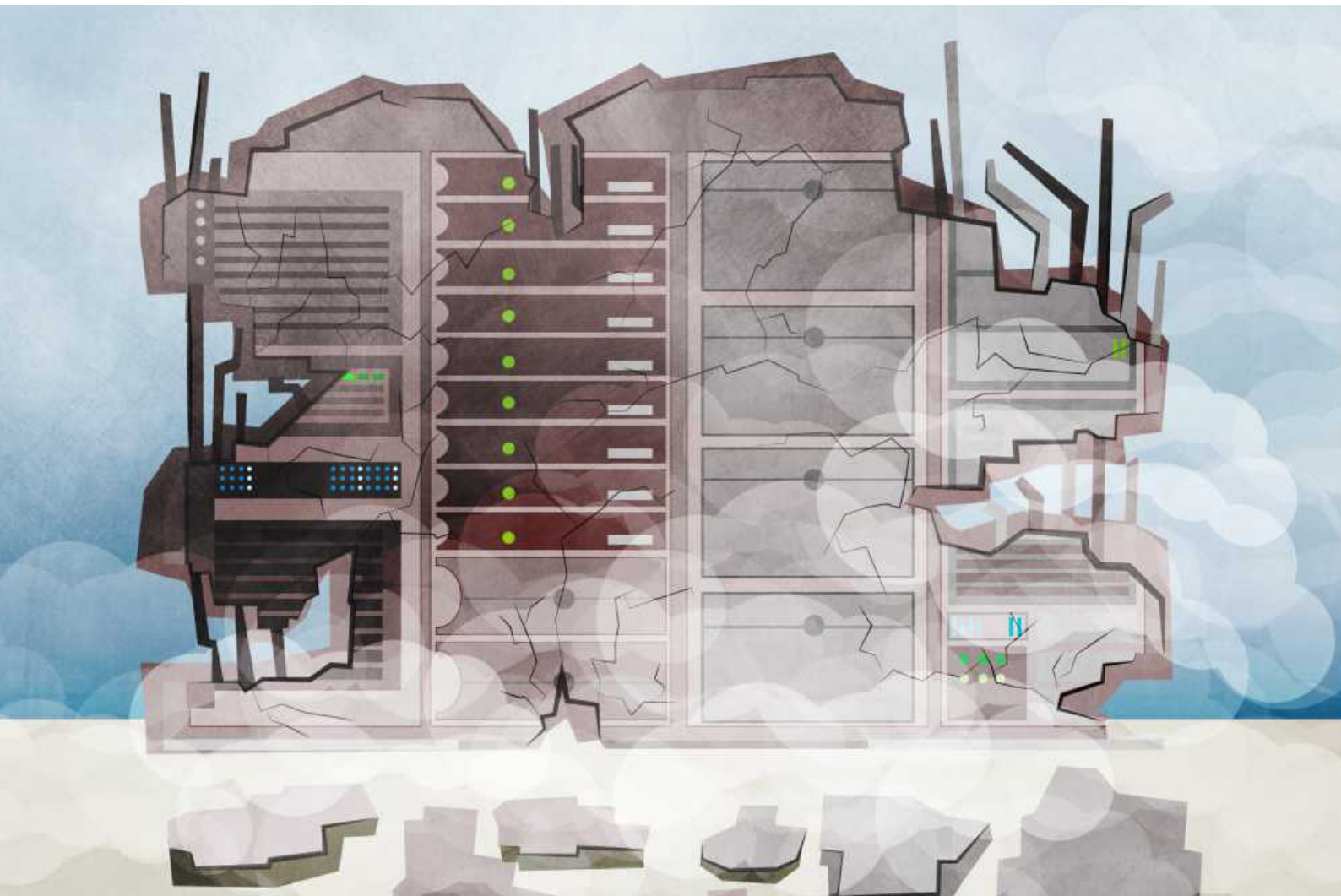
# Pruebas de penetración para principiantes: explotando una vulnerabilidad con Metasploit FrameworkLockpicking

Fernando Catoira

La versión gratuita y limitada de *Metasploit* framework Community es una herramienta que permite ejecutar y desarrollar exploits contra sistemas objetivos. Actualmente se encuentra integrado con *Kali Linux,* una distribución de Linux con diversas herramientas orientadas a la seguridad y es ampliamente utilizado para realizar pruebas de penetración. En la revista anterior mencionamos algunas de las *herramientas más importantes para adentrarse en el mundo de las pruebas de penetración.* Ahora, utilizaremos *Metasploit* para mostrar paso a paso **la explotación de un servidor vulnerable.**

## ¿Qué etapas se contemplan durante una prueba de penetración?

Para realizar una *prueba de penetración es necesario considerar diferentes etapas.* La primera de ellas consiste en recopilar información sobre el sistema objetivo y comúnmente se le conoce como etapa de reconocimiento. A partir de los datos obtenidos, se tomarán las decisiones acordes y los pasos a seguir en etapas posteriores. Una vez que los datos han sido recopilados y analizados, se procede a la instancia donde se realizará la explotación sobre el sistema objetivo.



La selección de los exploits que se utilizarán dependerá exclusivamente de la información obtenida en la etapa anterior. Finalmente, una vez realizado el ataque, se analiza el impacto, posiblemente, se realizarán nuevas acciones a partir de este último. La documentación y la generación de reportes concluyen las pruebas de penetración y suelen reflejar el trabajo completo por parte del *pentester* (persona que lleva a cabo la prueba de penetración).

Existen diferentes metodologías que pueden implementarse para realizar pruebas de penetración, donde cada una de las variantes difiere principalmente en las técnicas y métodos para llevar a cabo las respectivas tareas. Algunas metodologías son del tipo *blackbox,* donde básicamente no se conoce ningún tipo de información sobre el sistema objetivo. En contraposición, están las de *whitebox,* donde se tiene información sobre el sistema objetivo, como puede ser código fuente de aplicaciones, configuraciones, entre otras alternativas. A su vez, existen diferentes etapas de acuerdo a la metodología utilizada.

En este caso, sin realizar distinción de la metodología, haremos foco sobre la etapa de reconocimiento. Dentro de ésta existen dos formas de recopilar la información, ya sea de forma activa o pasiva. En el primer caso la información se obtiene directamente del sistema objetivo y en el segundo de forma indirecta. Finalmente ejecutaremos la etapa de explotación, ya que nos permitirá obtener un panorama general de lo que realmente involucra una prueba de penetración. Asimismo, un análisis completo involucra otras etapas, tales como la de enumeración, acceso, entre otras.

## ¿Cómo comenzar?

Para que los lectores puedan hacer el ataque paso a paso deberían instalar dos máquinas virtuales conectadas entre sí. Para ello es posible utilizar *VMWare* o en su defecto *VirtualBox*, en realidad existen otras alternativas, aunque estas dos son las más populares. Las dos máquinas virtuales que deben instalarse son las siguientes:

- Linux: como mencionábamos en el número anterior de la revista, es la distribución para pruebas de penetración por excelencia bajo la licencia GPL, se puede descargar desde: http://www.kali.org/
- Metasploitable 2: es una máquina creada con fines académicos, que ya posee varias vulnerabilidades que permiten que sea sencillo realizar pruebas sobre la misma, se puede descargar desde: http://sourceforge.net/projects/metasploitable/files/Metasploitable2/

Para continuar, es importante verificar que ambas máquinas tengan visibilidad entre sí (es decir, que puedan comunicarse). Esto puede corroborarse con un simple ping entre las dos. Después, desde la máquina en Kali Linux (todo el ejercicio se desarrolla en esta máquina, la segunda solo oficia como objetivo del ataque, pero no se realizarán acciones en ésta más allá de prenderla para "atacarla") utilizaremos la consola de Metasploit `(msfconsole)` de donde se lanzarán todos los comandos correspondientes sobre el servidor en el que se desea realizar la prueba de penetración. Para abrir la consola, solo hace falta el comando:

```
> msfconsole
```

## Information gathering

Para recopilar información es posible utilizar Nmap desde la propia consola de Metasploit. Para ello, basta con solo invocar el comando "`db_nmap`". Los parámetros que pueden utilizarse son los mismos que acepta Nmap. De esta manera, los resultados serán almacenados en la base de datos de Metasploit. Para obtener una observación rápida del sistema objetivo, se ingresa el siguiente comando:

```
> db_nmap {dirección ip} -p 1-65535
```

La dirección IP de la máquina objetivo es posible averiguarla mediante el comando *ifconfig* (este comando se utiliza en las distribuciones de Linux para conocer las direcciones IP de las diferentes interfaces de red).


Con el comando anterior se realiza un escaneo sobre todos los puertos del sistema objetivo.
De esta manera, tal como se especificó anteriormente, los resultados serán almacenados en la base de datos.
Para consultarlos, es necesario ingresar alguno de los siguientes comandos:

- **Hosts**: Imprime por pantalla información de todos los sistemas que fueron analizados.
- **Services**: Imprime por pantalla todos los puertos y servicios asociados que fueron descubiertos durante el análisis con Nmap.
- **Vulns**: Describe las vulnerabilidades que fueron descubiertas durante el análisis.

Sin embargo, en esta instancia es posible que no se cuente con demasiada información sobre los servicios descubiertos en el sistema objetivo. De esta manera, utilizando la misma herramienta (Nmap) es posible determinar, por ejemplo, la versión específica de un servicio. Esto se puede lograr mediante el siguiente comando:

```
> db_nmap -sV {dirección ip} -p {puerto de interés}
```

El parámetro "sV" indica que examine la versión específica del servicio. A modo de ejemplo, ejecutamos el siguiente comando para averiguar la versión sobre el servicio que se está ejecutando en el puerto 21, utilizado comúnmente por el servicio FTP.

```
> db_nmap -sV 172.16.1.119 -p 21
```

Si ahora se ejecuta el comando "**services**", nuevamente, se obtendrá información específica del servicio analizado.


## Explotación

Suponiendo que se ha encontrado información de un servicio en especial, es posible determinar a partir de ésta, si el mismo es vulnerable. Utilizando la consola, se realiza una búsqueda de un exploit en particular para ese servicio y luego se llevará a cabo la explotación del mismo.
Para realizar la búsqueda se ingresa el siguiente comando:

```
> search {cadena}
```

(para buscar una cadena específica que corresponda a un *exploit* en particular)

```
> search cve:{código CVE}
```

(para buscar un *exploit* en particular a partir del identificador CVE)

Asimismo, si se desea conocer todos los posible

parámetros de búsqueda, es posible acceder a la ayuda mediante el siguiente comando:

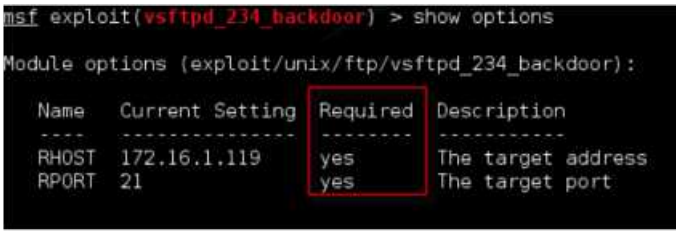
```
> help search
```

Tal como se muestra en el comando anterior, si se conociera el identificador OSVDB de una vulnerabilidad, entonces será posible buscar el exploit para dicho identificador. Esto también puede llevarse a cabo utilizando otros


identificadores, como por ejemplo, el CVE. Para seleccionar el *exploit* se introduce el comando "*use*" seguido de la ruta del *exploit* seleccionado. En este caso el comando sería el siguiente:

```
> use exploit/unix/ftp/vsftpd_234_backdoor
```

Una vez seleccionado el *exploit* que se va a utilizar, se deben configurar aquellos parámetros necesarios a través de la consola. Para ver las opciones, se debe ingresar el comando *"show options"*, el cual enumera todos los parámetros indicando si son opcionales u obligatorios mediante el campo *"required"*.

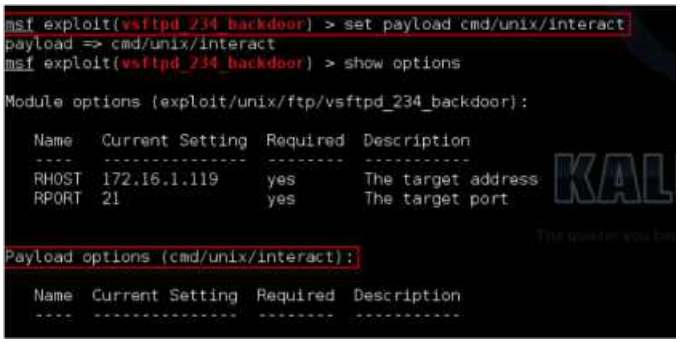



En esta instancia, ya es posible configurar los parámetros. Para realizar esta tarea se debe utilizar el comando *"set"* seguido del parámetro y el valor que se desea establecer. Para este ejemplo, el comando es el siguiente:

```
> set RHOST 172.16.1.119
```

## Payload

Básicamente, el *payload* es la secuencia de instrucciones que se ejecutarán una vez que se haya explotado con éxito la vulnerabilidad. Metasploit Framework posee diversos *payloads* con diferentes funcionalidades para cada tipo de arquitectura. Mediante el comando *"show payloads"* se pueden visualizar cuáles son compatibles. De esta forma, se utiliza el siguiente comando para establecer el *payload*:




En este caso hemos elegido el *payload cmd/unix/interact*. Sin embargo, para conocer todos los payloads que son compatibles con el exploit que se va a utilizar, existe un comando para realizar el listado correspondiente:

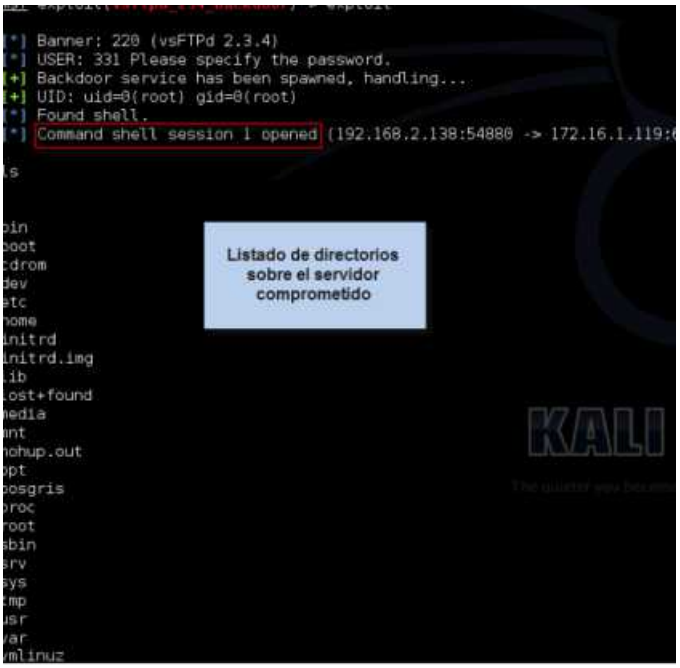
```
> show payloads
```

De la misma manera, si se desea conocer cuáles son los parámetros configurables del payload seleccionado, es posible ejecutar el comando:

```
> show options
```

Luego de que todos los parámetros ya han sido configurados, será posible llevar a cabo la explotación. Para ello, basta con ejecutar el comando *"exploit"* y esperar que *Metasploit* haga su trabajo.
En esta instancia, si todo ha resultado bien, se obtiene una *shell* de comandos sobre el sistema que ha sido atacado, permitiendo ejecutar cualquier comando en dicho sistema.

Por ejemplo, a continuación se puede observar un comando de listado de directorios:




En este caso se obtuvo acceso a un servidor a través de un servicio FTP vulnerable. Mediante la identificación de la versión del servicio se pudo encontrar el *exploit* adecuado. De la misma manera, se inyectó un *payload* capaz de disponer una *shell* de comandos a merced del atacante.

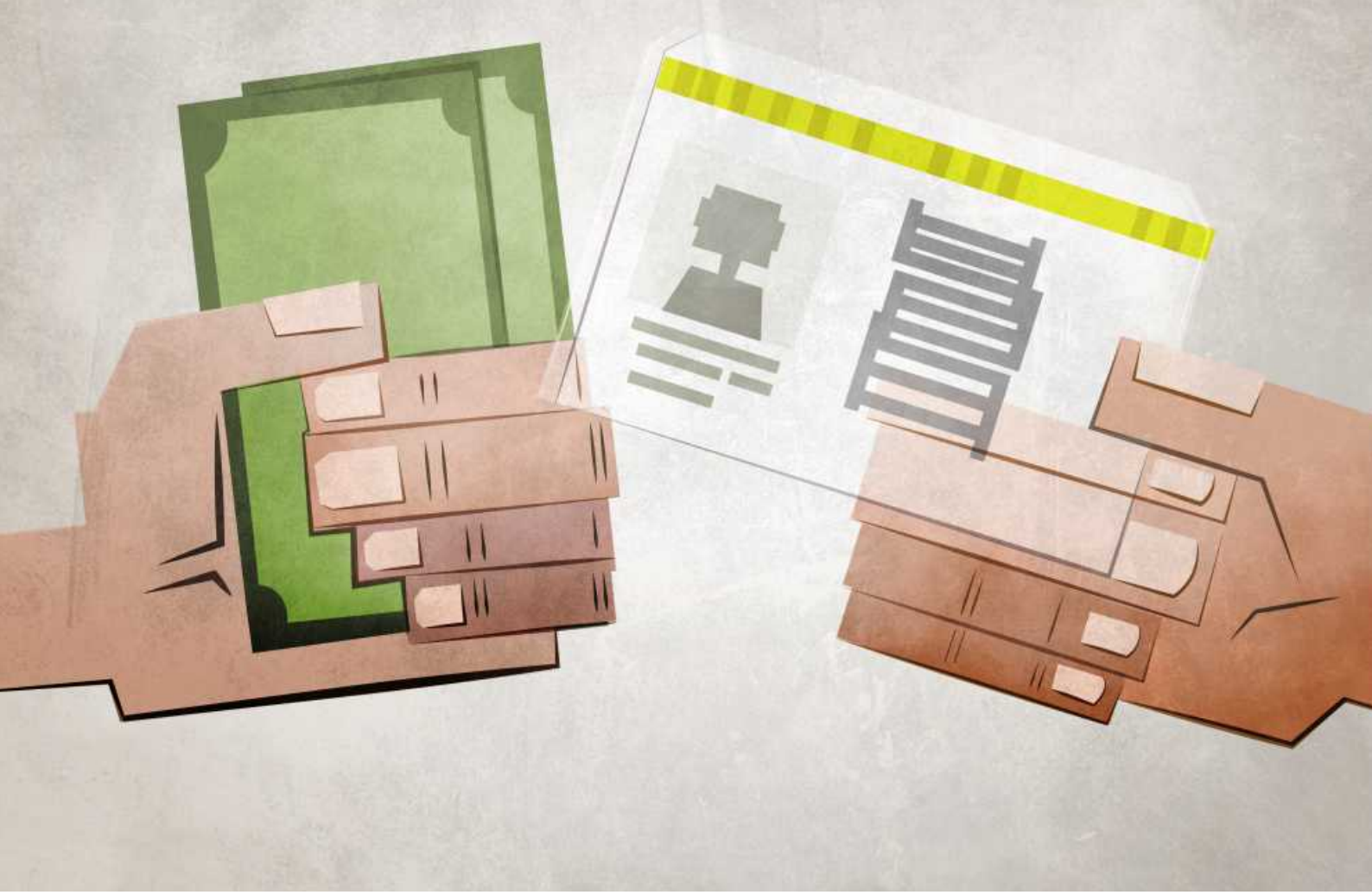
Si bien este es un ejemplo específico, donde el acceso se logró a través de una vulnerabilidad conocida por una versión antigua del software *Vsftpd*, también es posible que esto ocurra en un escenario real. Asimismo, los ataques reales pueden ser más complejos o combinados. Sin embargo, esto es un buen comienzo para tener noción sobre cómo se realizan ataques con *Metasploit*.

Finalmente, vale la pena destacar que no existe una herramienta capaz de ejecutar automáticamente una prueba de penetración de calidad. El auditor, es decir, quien realiza las pruebas de penetración *(pentester)*, siempre debe recurrir al uso de su imaginación y conocimiento, cualidades que pondrán a su disposición una gama de herramientas que le permitirán ejecutar una prueba precisa y contundente sobre el sistema para obtener

Fernando Catoira

Se desempeña actualmente como Analista de Seguridad en la empresa ESET Latinoamérica, dedicada al desarrollo, investigación y comercialización de soluciones de protección antivirus y seguridad informática.

Catoira trabajó de manera independiente como desarrollador de sistemas de información para distintas organizaciones. Por otra parte, posee conocimientos en los siguientes lenguajes de programación: Java, JavaScript, JSP, PHP, Python y cuenta con manejo de los sistemas operativos Windows y Linux.



# Implicaciones jurídicas y de ciberseguridad para la protección de bioinformación humana en su regulación legal, almacenamiento y uso – Parte I

Randall Barnett Villalobos

Hoy en día, la Ciberseguridad adquiere un papel preponderante respecto a la Bioinformática, pero al decantar más allá del tópico citado, se vislumbra otro punto importante: *¿Existe una regulación legal apropiada para la adquisición, almacenamiento, organización, gestión y distribución de ingentes cantidades de datos e información de carácter biológico?* Ecuya red de conocimiento integral se basa en ciencias como la Bioestadística, Medicina, Electrónica, Informática, Química o Matemática, entre otras.

Como se puede notar, es fundamental que todo ese conglomerado de conocimiento esté debidamente asegurado ante posibles amenazas más allá del robo o el acceso no autorizado, es decir, que sea utilizado con fines bélicos, como la creación de armas biológicas genéticamente modificadas para poblaciones particulares o bien, vigilancia intrusiva sobre núcleos poblacionales vulnerables a ciertas enfermedades. Parece que la barrera de lo inverosímil cada vez se hace más difusa ante un

mundo que no conoce límites y, que si bien muchos gobiernos realizan gestas para salvaguardar los datos privados a nivel legal, existen otros que saben que la información es el nuevo *"petróleo"* por el cual vale saltarse cualquier código moral o legal.

Basado en las proyecciones realizadas por EMC Corporation [NYSE:EMC][1], para el año 2020 la información digital manejada en el mundo entero alcanzará los 40 zetabytes. En términos de volumen, estos 40 ZB de datos son equivalentes a 5,247 GB de información elaborada y administrada por persona a nivel mundial. Haciendo una comparación más gráfica, esta cantidad de datos sería equivalente a 57 veces la cantidad de granos de arena que hay en todas las playas del mundo. Además, NYSE:EMC estimó que para ese mismo año, un 62% de este Universo Digital[2] será producido en los mercados emergentes, tal como las tecnologías móviles.

Ante este escenario, nuestra Latinoamérica ha optado por la creación y puesta en marcha de leyes de protección de los datos personales. Casos como México, Uruguay o Costa Rica cuentan con leyes que regulan el uso de los datos públicos y privados, sin embargo, son pocos los países que cuentan con una ley específica para la reglamentación del Banco Nacional de Datos Genéticos[3], ejemplo de ello, Argentina.

El análisis de ADN para indagaciones judiciales o científicas que permiten identificar a las personas a partir de variados rastros es comúnmente utilizado, pero para que esta poderosa herramienta rinda todo su potencial al servicio de la justicia o de la ciencia, se requiere disponer de bases de datos en las que figuren los perfiles genéticos de posibles estrellas del deporte, posibles científicos brillantes, soldados resistentes y, por qué no, perfiles genéticos de delincuentes.

*¿Estamos en franca desventaja como personas, ante una recolección de datos biológicos en medios informáticos privados y estatales?*
Pese a los congresos internacionales como el Congreso Latinoamericano de Genética Humana o locales como el Congreso Mexicano de Genética Humana, donde se promulga la importancia y uso de los datos biológicos en la genética clínica, tamizaje neonatal, enfermedades complejas, entre otros temas de relevancia, la respuesta es: sí.

Piensa por un momento en las grandes transnacionales que invierten millonarios capitales para alimentar a la llamada *"Guerra de Patentes"*, que a su vez, se alimenta de ese caldo de agujeros legales que tanto dañan nuestra Latinoamérica. Medita esta prerrogativa: si hipotéticamente sufrieras de una enfermedad particular, cuya investigación solo se puede realizar en decenas de humanos a nivel mundial, ¿sería algo por lo cual una compañía podría pagar grandes cantidades de dinero, con tal de obtener el mapa genético de la enfermedad y así patentizar una cura?

## Almacenamiento masivo de datos genéticos

Toda estrategia para el manejo de datos debe aplicar una gestión adecuada para la conservación y cuidado de éstos. Veamos:

1. Lo primero que deberíamos considerar es que sea un lugar seguro. Es decir, de acceso restringido, con respaldo redundante en conectividad, en fin, que este Centro de Datos cumpla con un TIER IV[4] para reducir casi a cero sus vulnerabilidades.

2. Sería necesario implementar una tecnología que permita administrar automáticamente datos de múltiples fuentes, así sea desde el ámbito de la nube, tecnología móvil u otro centro de datos.

—¿debería ser estatal?— Puesto que las instituciones autónomas, en general, son más reguladas que las privadas, sería lo más lógico.

5. No dejemos de lado la parte legal, que al fin y al cabo, es la que certificaría que toda la información suministrada o sustraída cumpla con un debido proceso, que a su vez tenga una regulación legal aprobada por cada país y exista difusión clara por medios de comunicación adecuados.

3. Debido a que existirían múltiples fuentes de datos posibles, también sería idóneo disponer de un medio para indexar el contenido de todos estos datos. Esto con el fin de que cualquier tipo de información sea localizable a través de una sola interfaz.

4. Otro punto importante sería la administración centralizada de los datos, que debería recaer en personal altamente capacitado, con valores éticos y con probidad comprobable. Además, el organismo que resguarda estos datos

Lo anterior parece una descripción básica y repetitiva de cualquier centro de datos de cualquier lugar del mundo —¿Cuál debería ser el factor diferenciador que constituye a un centro de datos genéticos, que no constituye a otro tipo de banco de información?—

Para darles una pista veamos dos casos.
El primero, Brasil. Para el 12 de marzo del 2013, se instituye por el decreto N° 7950 el Banco Nacional de Perfiles Genéticos y la Red Integrada de Bancos de Perfiles Genéticos de la República

de Brasil[4].Dicho banco tiene por objetivo principal, recolectar información de personas condenadas por asesinatos, homicidios y otros delitos de sangre a fin de reforzar el trabajo de la Policía Científica. El presidente de la Asociación Nacional de Peritos Criminales de la Policía Federal Brasileña, Hélio Buchm ller, consideró que ese banco de datos será una herramienta *"fundamental"* para reducir los índices de violencia y limitar la reincidencia en los crímenes de sangre.

El segundo caso es Argentina. El Banco Nacional de Datos Genéticos creado por la ley N° 26548 del 26 de noviembre del 2009[5], en su artículo N° 2, cita que el banco fue creado para: *"garantizar la obtención, almacenamiento y análisis de la información genética que sea necesaria como prueba para el esclarecimiento de delitos de lesa humanidad…".* Esta ley garantiza que la información genética que allí estuviere solo podrá ser suministrada por solicitud judicial, con el fin exclusivo de respaldar el debido proceso de dictámenes periciales. Esto se debió a un clamor político, ya que en tiempos convulsos de la República Argentina se dio el llamado "Terrorismo de Estado" y con esos rastros genéticos centralizados sería posible identificar a posibles víctimas.

Si ya les cruzó la idea por la cabeza, la respuesta sería: Derechos Humanos. Hoy en día, con lo revolucionado de las telecomunicaciones, estar a miles de kilómetros de un lugar y tener la posibilidad de saber quién fue tu madre, buscar a un hermano muerto durante un crimen en otro país o conocer las causas de una enfermedad particular, debería reducirse al hecho de que como personas, tenemos derechos inalienables y que ciencias como la Bioinformática y Ciberseguridad, son un puente amplio y seguro con el cual contar.

1 EMC Corporation (NYSE: EMC) es una empresa que integra la American Fortune 500 y S&P 500 fabricante de software y almacenamiento de información. http://bit.ly/13rg9Dj

2 Universo Digital es un servicio de información en línea gratuito fundado en 2006 por Joe Firmage, CEO de ManyOne.

3 El Banco Nacional de Datos Genéticos es un organismo autónomo y autárquico dentro de la órbita del Ministerio de Ciencia de Argentina. Ley: http://bit.ly/16QXcXJ

4 Existe un estándar llamado ANSI/TIA-942 Telecommunications Infrastructure Standard for Data Centers.

5 Documento resumen de legislación extranjera sobre Bancos de Datos Genéticos: http://bit.ly/17w7gFA

6 Ley de Regulación del Banco Nacional de Datos Genéticos de Argentina: http://bit.ly/1bExCrZ

## Referencias

*Durán Díaz, Edmundo, "Criminología y bioética. La manipulación genética", Revista Anual de la Asociación de Derecho de la Pontificia Universidad Católica del Ecuador, Quito, año XLV, núm. 37, t. I, Ecuador, 1994, pp. 46 y 47.*

*Matozzo de Romualdi, Liliana, "La biotecnología y el derecho a la identidad", Cuadernos de Bioética, Santiago, España, vol. VII, núm. 25, 1996, p.14 y 11.*

Rabdall Barnett Villalobos

Master en Informática y Computación de la Universidad de Costa Rica. Desarrollador y analista de bases de datos del Instituto Costarricense de Electricidad. Seis años de experiencia en desarrollo de software antifraude en telecomunicaciones y exprofesor de informática. Twitter: @elbartocr

# Sistemas SCADA, algunas recomendaciones de seguridad – Parte II

Eduardo Carozo Blumsztein,
Leonardo Vidal

En el número anterior describimos los problemas que enfrentan las implementaciones de seguridad que se aplican a las redes industriales (*ICS: Industrial Control System*). Históricamente, estos sistemas nacieron en una situación diferente a la que operan hoy en día: eran implementados en recintos cerrados, controlando dispositivos físicos cercanos (frecuentemente bajo línea de vista del operador) y bajo estrictos controles de acceso físico en el interior de la instalación industrial que debían medir o controlar. La seguridad se controlaba por *obscuridad*, dejando la red desconectada de su entorno y dando acceso a un número limitado de empleados especializados. Es frecuente encontrarse con estos sistemas operando sin interrupciones ni actualizaciones desde hace varios años.

Por esta forma de gestión, en el pasado los sistemas SCADA eran relativamente inmunes a las intrusiones y ataques que sufrieron las redes en el exterior, no por ser más resistentes, sino porque estaban desconectados y eran inaccesibles desde las redes administrativas o Internet.

Es importante aclarar que los operadores de estos sistemas de control industrial, siguen percibiendo y trabajando con estos sistemas como si fueran aislados e implícitamente seguros, aún cuando en la misma consola en la que gestionan las instalaciones, eventualmente puedan tener un cliente de correo electrónico corporativo o miren las noticias en un navegador con acceso a Internet.

Por otra parte, en los países con mayor cantidad de implementaciones de control industrial y desarrollo tecnológico, los referentes de seguridad han identificado este tema como un aspecto central a proteger, por ejemplo, citemos a Janet Napolitano del Departamento de Seguridad Interna de Estados Unidos: *"Un 9/11 cibernético, que podría paralizar las infraestructuras críticas, como las telecomunicaciones, el agua, la electricidad y el gas, pueden ser inminentes (sic). No debemos esperar hasta que haya un 9/11 en el mundo cibernético. Hay cosas que podemos y debe_ mos estar haciendo en este momento que, aunque no pueda evitarlo, puede atenuar la magnitud del daño…".*

Además, la cantidad de vulnerabilidades identificadas en infraestructuras críticas como la red de energía, instalaciones de suministro de agua, sistemas de telecomunicaciones y de transporte, se han disparado un 600% desde 2010, según los datos reportados en el *VulnerabilityThreatReport de NSS Labs*, en el trabajo de *DELL Security Works*. En la figura siguiente se muestra una comparación de la cantidad de vulnerabilidades identificadas en los navegadores más populares, en *"flash"* y en *"java"*, respecto de las vulnerabilidades identificadas en sistemas SCADA de amplia difusión.

## Entendamos al enemigo: "Advanced Persistent Threat (APT)", ¿qué son?

Existen múltiples grupos de técnicos que a nivel global ofrecen la capacidad e intención firme de lograr intrusiones a objetivos específicos, con la intención de, por ejemplo: robar secretos industriales, detener procesos críticos de naciones, empresas u organizaciones, extorsionar con base a liberar información confidencial o destruir información esencial, etc. Los incentivos económicos para la realización de estas actividades suelen ser muy altos y están financiando la instalación silenciosa de muchas herramientas de software malicioso en todo sistema de control industrial al que se tenga acceso.

Una vez que se accede a unos cuantos de estos sistemas, lo habitual sería analizar qué tipo de dominio se puede ejercer sobre los mismos y se ofrecen dichos activos como objetivos, a actores interesados en financiar el ataque a la organización en el momento oportuno.

Entonces es necesario desarrollar las APT para que sean indetectables, duraderas, adaptables y provoquen ataques tenaces a la infraestructura, pensando focalmente en una infraestructura crítica objetivo.

El primer APT ampliamente reconocido ha sido *Stuxnet,* un malware tipificado como gusano, desarrollado en 2010, que se dispersa en programas SCADA (WinCC) desarrollados por *Siemens.* Él mismo pudo ingresar a su objetivo (que era un sistema con un altísimo grado de aislamiento físico y lógico) presumiblemente a través de una memoria USB infectada.

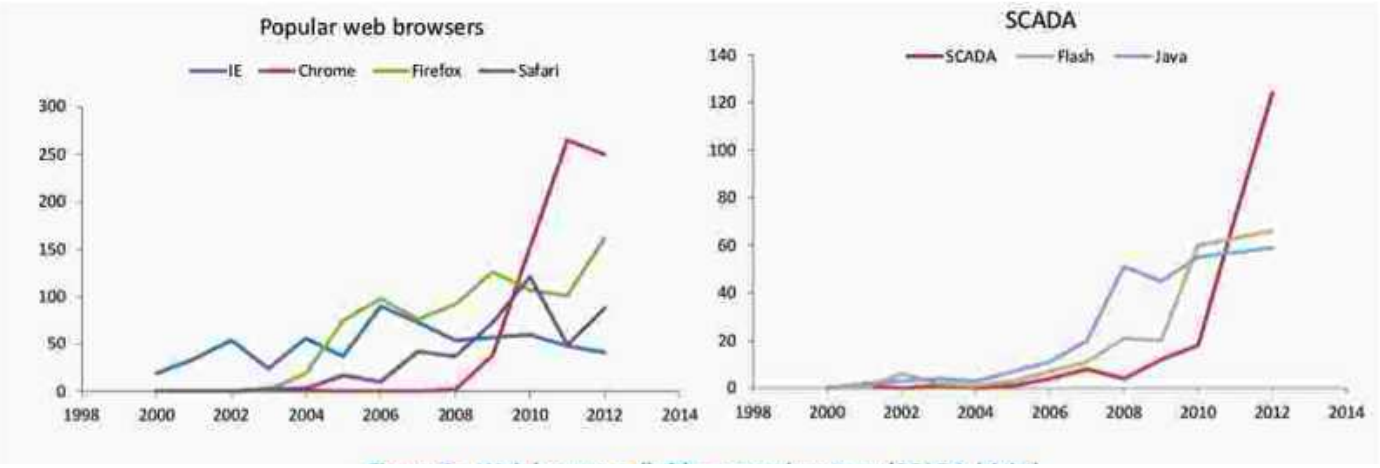
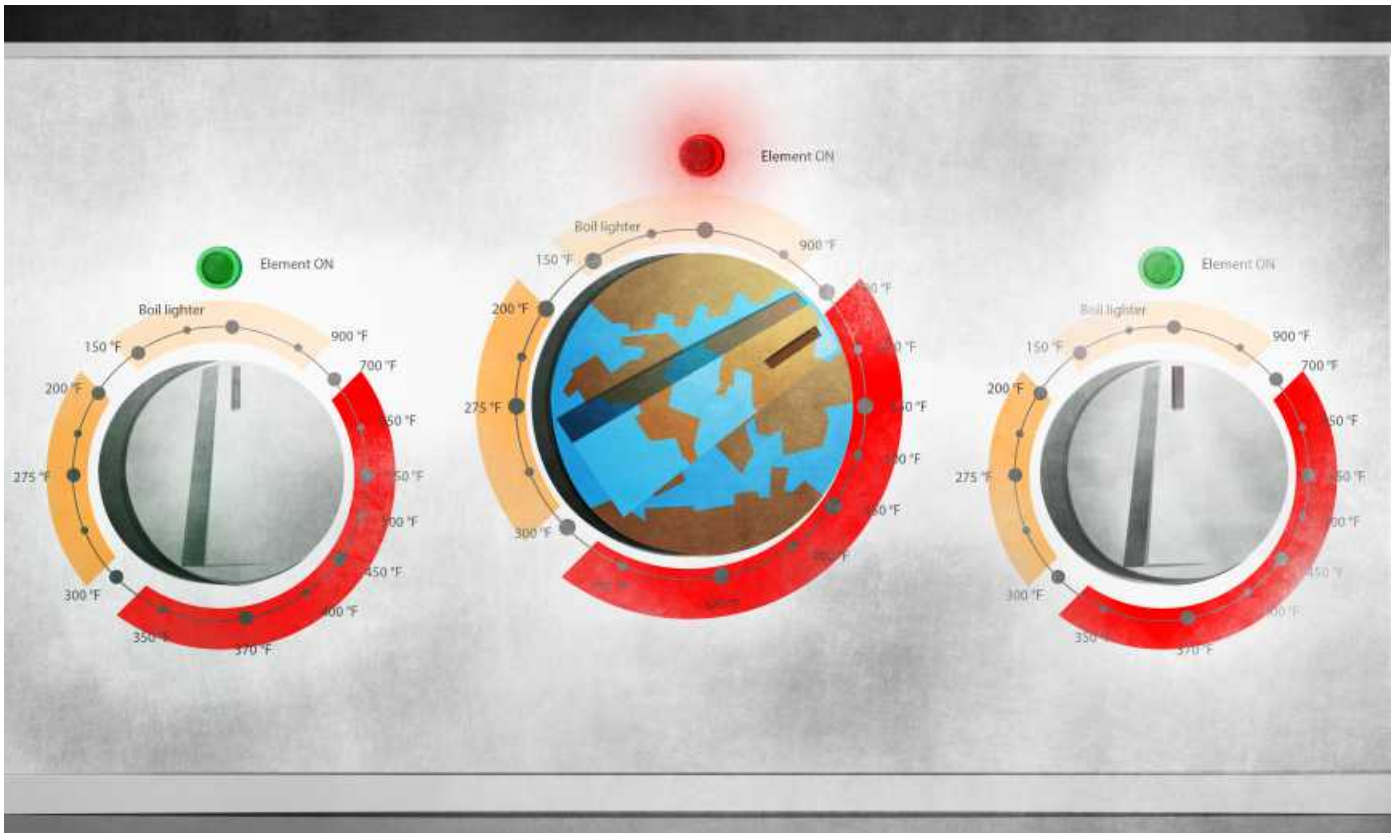



Imagen1. Navegador web(izq) – Sistemas de control SCADA (der)

Usted se preguntará: —¿cómo llega una memoria USB con malware, a una computadora dentro de una instalación aislada?—

Una forma podría ser ésta: en Internet busca e imprime el logo de la empresa u organización objetivo, ve a una tienda de regalos empresariales y compra 10 memorias USB de baja calidad que llevarán en el lomo el logo impreso que se obtuvo; luego incorpora a la memoria información aparentemente corporativa (un *Excel* o *Word* con datos inventados) y el malware que se necesita introducir a la red de la organización objetivo. A la mañana siguiente ve al estacionamiento de la organización víctima, estaciónate en un extremo alejado y cada 60 metros deja caer

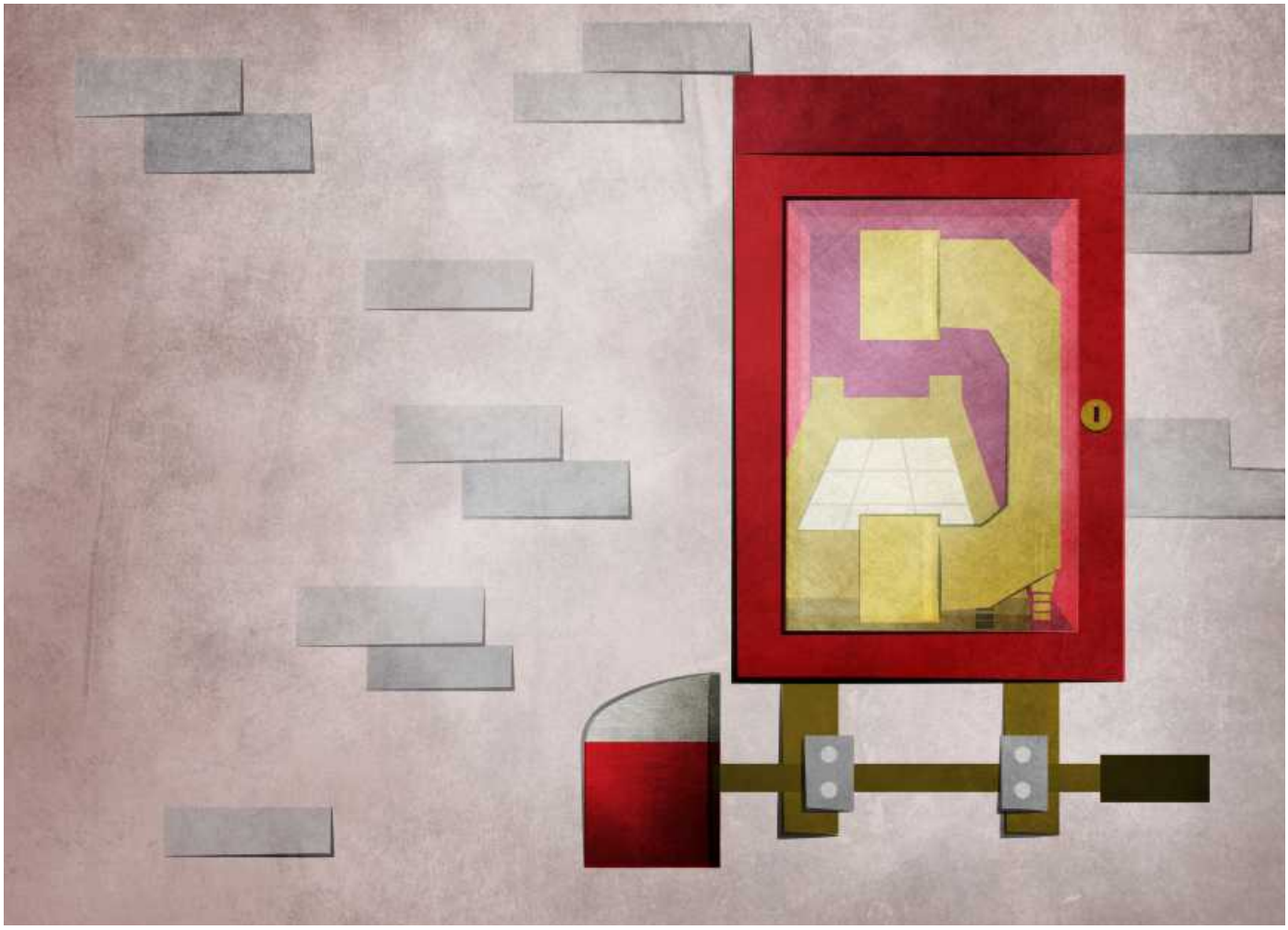



de a una, las memorias al suelo. Cuando lleguen los empleados de la organización a su jornada laboral harán el resto del trabajo que falta (conectando la memoria USB a su equipo de oficina) para brindarte un acceso remoto a diferentes equipos de la organización. Con menos de 30 dólares ya ingresaste a la red corporativa.

En el caso de *Stuxnet*, además de la organización de Irán que fue objetivo del ataque, se infectaron más de cien mil ordenadores de organizaciones (como *Chevron*) que usaban sistemas similares, generando una diversidad de daños colaterales, que aún continúan ocurriendo. Esta situación muestra que un actor en el ciberespacio puede causar graves daños a poblaciones enteras, atacando un objetivo específico sin medir consecuencias en otras infraestructuras que tengan componentes similares.

*Duqu, Flame y Gauss*, son otros ejemplos de malware catalogado como APT y que han provocado grandes daños físicos, inclusive han sido señalados como la causa de muerte de varias personas en explosiones provocadas en bases militares.

Con este panorama, —¿cómo sabemos si nuestro ICS está infectado?— Lamentablemente, lo más probable es que estés conviviendo con tu enemigo todos los días puesto que Internet está en todos lados, ya sea en tu equipo o en un pequeño *Smart-meter* que mide un tanque a distancia usando la red de datos celular, a través de un equipo de consulta en una remota instalación o por un estacionamiento *"sembrado"* con memorias USB que seguramente tengan alguna versión de estos gusanos instalada (si corres con suerte, lo más normal es que el mismo



se encuentre inactivo y posiblemente disfuncional por desconocer la topología de su red, o descansando hasta encontrar el momento adecuado para despertar).

Finalmente, para ilustrar el ciclo de vida de las APT, compartimos una imagen de *DELL SecureWorks:*


Como se puede observar, el trabajo realizado sobre cada objetivo implica enfoque y dedicación, por lo que de momento solo están siendo atacadas algunas organizaciones con alta exposición por razones específicas, generalmente económicas o políticas. Pero no debemos olvidar el daño colateral sufrido por otras organizaciones, sobre todo porque son actores pasivos y sin defensa frente a un ataque como los descritos, es decir, ataques con un alto grado de sofisticación.

## Temas urgentes a tratar para mejorar la seguridad de nuestro Sistema de Control Industrial

Las consideraciones anteriores están mostrando que la aparente tranquilidad de la que se disfrutó hasta el momento en la gestión de los ICS está por terminar. Para ello sugerimos algunas líneas de trabajo:

1. La necesidad de realizar un inventario detallado de todos los elementos que constituyen el ICS que tenemos que asegurar, conociendo estados de actualización, variables críticas y dispositivos claves para la continuidad.

2. Identificar roles de las personas y aclararlos explícitamente a todos los operadores del sistema ICS, dichos roles deben reflejarse en los privilegios de las personas para conel sistema.

3. La necesidad de describir detalladamente las políticas y procedimientos de uso de los sistemas y computadores asociados al ICS, sobre todo a las personas encargadas de diseño y despliegue de los dispositivos del sistema, así como del personal de reciente ingreso a la organización.

4. Disponer de un proceso sistemático de revisión de riesgo físico y tecnológico, basado en vulnerabilidades derivadas de alertas realizadas por:

a. Los proveedores de los equipos.
b. Centros de alertas especializados (ICS-CERT:http://ics-cert.us-cert.gov/, www.securityincidents.net).
c. Revisiones físicas completas del equipamiento del ICS, según un programa de revisión periódico diseñado con la gerencia de riesgo e ingeniería.

5. Proveer de entrenamiento y capacitación sobre conductas y detección de incidentes de seguridad en los sistemas de control industrial.

6. Diseñar la red basados en (IS-99), bajo la segmentación en "zonas" y "conductos", de forma que promuevan la defensa en profundidad.

7. Implantar controles exigentes de acceso físico y lógico a los elementos críticos del ICS.

8. Establecer un exhaustivo hardening de los componentes principales del sistema (muchos de los ataques son mitigados por esta actividad).

9. Utilizar componentes industriales robustos, con tasas de MTBF (Mean Time Between Failures, tiempo transcurrido entre una falla y otra) altas.

10. Diseñar la red que los soporta con redundancia.

11. Utilizar firewalls específicos para sistemas SCADA.

12. Establecer algún sistema de *DeepPacketInspection* (inspección profunda de paquetes), que genere alarmas por paquetes inusuales en la red.

13. Establecer una política de gestión de vulne_ rabilidades que incluya el concepto de *workarounds* (configuración que no corrige la vulnerabilidad, pero ayuda a bloquear el ataque mientras se puede realizar el cam_ bio/parche definitivo).

## Referencias


*Lifecycle of an Advanced Persistent Threat – DELL Secure Works*
*http://www.secureworks.com/assets/pdf-store/articles/Lifecycle_of_an_APT_G.pdf*

*Barack Obama Executive Order -- Improving Critical Infrastructure Cybersecurity*
*http://www.whitehouse.gov/the-press-office/2013/02/12/executive-order-improving-critical-infrastructure-cybersecurity*

*Guide to Industrial Control Systems (ICS) Security*
*http://csrc.nist.gov/publications/nistpubs/800-82/SP800-82-final.pdf*

*Recommendations of the National Instituteof Standards and Technology - NIST Special Publication 800-82 - June 2011*
*http://csrc.nist.gov/publications/nistpubs/800-82/SP800-82-final.pdf*

*Using ANSI/ISA-99 Standards to Improve Control System Security - Tofino Security, May 2012*
*http://web.tofinosecurity.com/download-the-white-paper-using-ansi-/-isa-99-standards-to-improve-control-system-security/*

*ANSI/ISA-99 Standards: Security for Industrial Automation and Control Systems*

*https://www.isa.org/Template.cfm?Section=Standards2&template=/Ecommerce/ProductDisplay.cfm&ProductID=10243*

*SCADA and CIP Security in a Post-Stuxnet World*
*http://www.tofinosecurity.com/professional/scada-and-cip-security-post-stuxnet-world*

*The Future of Critical Infrastructure SecurityEric Byres - Byres Security Inc – Tofino Security*
*http://www.tofinosecurity.com/professional/scada-and-cip-security-post-stuxnet-world*

*Vulnerability Threat Trends, Stefan Frei - NSS Labs, Feb 2013*
*https://www.nsslabs.com/system/files/public-report/files/Vulnerability%20Threat%20Trends.pdf*

*The Industrial Control Systems Cyber Emergency Response Team (ICS-CERT)*
*http://ics-cert.us-cert.gov/*
*https://ics-cert.us-cert.gov/ics-archive*

*Repository of Industrial Security Incidents - RiSi*
*http://www.securityincidents.net/*

Eduardo Carozo Blumsztein

Gerente de Comercialización de ITC SA
Director Equipo de Seguridad de la Información
Miembro del Comité Asesor del Proyecto AMPARO de LACNIC
Profesor de Posgrado en Seguridad de la Información en la Facultad de Ingeniería de la Universidad de la República, dependiente de su Instituto de Computación (INCO)


DGTIC

DIRECCIÓN GENERAL DE CÓMPUTO Y DE
TECNOLOGÍAS DE INFORMACIÓN Y COMUNICACIÓN


Revista .Seguridad Cultura de prevención para TI
No.19 / agosto-septiembre 2013 ISSN: 1251478, 1251477