Algunas perspectivas acerca de la ciberseguridad: 2012

1 Introducción

Ciberseguridad, como palabra clave, es un término terriblemente inexacto que puede cubrir una lista interminable de distintos problemas de seguridad, desafíos técnicos y "soluciones" de varios ámbitos, desde lo técnico hasta lo legislativo. Aunque palabras de moda como ciberseguridad son ideales para los titulares, cuando nos adentramos en discusiones serias sobre seguridad e Internet es necesario que se comparta el mismo significado para el término ciberseguridad.

El alcance del término ciberseguridad abarca muchos tipos de problemas e incluso un mayor número de soluciones. Algunas de esas soluciones son técnicas, otras no lo son y se pueden resolver a través de la educación, la política o la regulación. Como resultado del alcance y ámbito de las soluciones, hay muchos interesados involucrados en resolver problemas de ciberseguridad incluyendo usuarios individuales, organizaciones para el desarrollo de estándares y políticas, desarrolladores de productos, empresas, organizaciones no gubernamentales y gobiernos. Todos estos interesados deben colaborar de forma conjunta para lograr el objetivo de un Internet seguro y robusto.

El modelo de Internet de desarrollo colaborativo de estándares y políticas dentro de un proceso abierto, de consenso en manos de expertos internacionales es uno de los mejores vehículos para conseguir una seguridad real. Este modelo ha recogido sus frutos a la hora de mejorar la ciberseguridad gracias a la implementación de redes privadas virtuales (VPN) seguras, protocolos de cifrado, extensiones de seguridad de DNS (DNSSEC), protocolos seguros para el intercambio de datos y sistemas de enrutamiento más seguros a través del desarrollo de las mejoras de seguridad en BGP. Este modelo de consenso y cooperación internacional inspirará confianza y creará un entorno con pleno convencimiento a la hora tratar los numerosos desafíos que supone mejorar la ciberseguridad. Desafortunadamente, existen amenazas potenciales para este modelo de consenso abierto, incluyendo corporaciones que ejercen presión para que se usen soluciones con derechos de propiedad y la presión de los gobiernos para contar con mecanismos de acceso alternativo.

El objetivo de este artículo no es "resolver" la ciberseguridad sino desglosar algunos de los diferentes elementos que componen el problema de la ciberseguridad e identificar la labor continuada que realizan diferentes organizaciones e interesados a la hora de abordar estos elementos diversos. Tenemos la esperanza de que al tratar este problema desde esta perspectiva, el lector obtendrá una mayor comprensión de las diferentes maneras de enmarcar el problema y pensar en soluciones. También tenemos la esperanza de que este marco de trabajo

ofrezca a los lectores un conocimiento profundo sobre la extensa gama de organizaciones que colaboran conjuntamente para tratar los temas técnicos de la ciberseguridad.

1.1 Antecedentes

Internet ha transformado la esencia de nuestra sociedad y nuestra economía. A medida que Internet se vaya convirtiendo en una auténtica herramienta global y accesible desde cualquier punto de la tierra, su impacto, influencia e importancia irán en aumento. Además, existe una nueva generación de ciudadanos que conocen bien Internet ya que crecieron con la red y se sienten cómodos con sus numerosas dimensiones. Esta gente impulsa nuevas aplicaciones, servicios y usos.

El Internet abierto que conocemos hoy en día ha supuesto toda una revolución para la humanidad. No sólo ha permitido que negocios de todo tipo sean más eficientes, sino que también ha habilitado nuevas formas de producción y distribución, modelos económicos como software de código abierto y marketing basado en clics. También tiene el potencial de ser un instrumento relevante a la hora de tratar enfermedades sociales y otros tipos de desafíos significativos (como la diseminación de información durante los desastres naturales), supervisar el cambio climático y ayudar a la gente a reducir su consumo energético a través de “medidores inteligentes”.

Pero existe un lado oscuro en esta revolución digital, uno que podría alejar a individuos y negocios o que podría permitir restricciones en el uso de Internet impuestas por los gobiernos. El fraude en línea y el robo de identidad son comunes, además existe el desafío constante de tratar con flujos de información ilegal y datos incorrectos. Estos puntos negativos contrarrestan los beneficios de Internet con costes reales y directos. Y sin embargo, el resultado final de este cálculo de equilibrio no obtiene un consenso universal.

Aunque los firewalls, los antivirus, las medidas contra el correo electrónico no deseado y las prácticas de seguridad de Internet actuales pueden mejorar la ciberseguridad, la creciente complejidad del sistema y su naturaleza abierta van planteando nuevos desafíos. Como informa New Security Paradigms Workshop (NSPW, Taller de nuevos paradigmas de seguridad), una variedad de medidas preventivas que parecen sencillas, como contar con contraseñas fuertes, nos han dado una falsa sensación de protección contra ataques potenciales. De hecho, comenta el informe, no estamos prestando la suficiente atención a amenazas más serias. Descubrimientos recientes muy publicitados de “redes fantasmas” mundiales, fallos fundamentales en la infraestructura de seguridad de Internet como muestra el incidente Diginotar [DIGINOTAR], ataques cibernéticos contra compañías como Google [NYT-GOOGLE] o naciones como Estonia [WIKI-ESTONIA2007] indica que aún existen vulnerabilidades serias que se deben tratar y nuevas que aún no hemos imaginado. Si los ataques grandes fuesen algo común, y aparentemente imparables, nuestra confianza en Internet se reduciría de manera significativa o desaparecería de forma abrupta.

Para evitar esta situación, será necesario aumentar el uso de medidas pensadas para mejorar la confianza y la seguridad. Desafortunadamente, algunas de las propuestas actuales para mejorar la seguridad resultan ser un peligro para un Internet abierto y generativo. Algunos gobiernos nacionales están erigiendo fronteras en el ciberespacio. No todos estos esfuerzos tienen como objetivo imponer un control político; algunos tienen como objetivo mejorar la ciberseguridad pero, no obstante, amenazan el Internet abierto y su funcionalidad. Por ejemplo, el gobierno australiano consideró y abandonó posteriormente una propuesta que requería que los ISP

implementasen filtros que usaran una lista controlada por el gobierno. El objetivo es bloquear "imágenes de abusos infantiles, bestialidad, violencia sexual, instrucciones detalladas para cometer crímenes, violencia, uso de drogas o material que propugne llevar a cabo actos terroristas." [AUSTRALIA-DBCDE][AUSTRALIA-UPDATE] Más de una docena de países tienen planes para desplegar mecanismos cuyo objetivo es bloquear contenido de Internet por razones políticas, sociales y de seguridad [BORDER]. Estos planes suponen un riesgo significativo para la interoperabilidad global y el objetivo de un Internet abierto, accesible y generativo.

Existe una creciente necesidad de realizar una labor capital que afronte los problemas englobados en el término "ciberseguridad". Para que sea una labor constructiva y efectiva, es esencial empezar por entender lo que significa ciberseguridad.

1.2 Definición de ciberseguridad en constante evolución

Ciberseguridad es un amplio término que ha evolucionado con el paso del tiempo sin alcanzarse un consenso claro sobre su significado exacto. Su significado puede estar relacionado con una lista casi interminable de temas relacionados con la seguridad de Internet, incluyendo vulnerabilidades y problemas técnicos, problemas sociales y de comportamiento, y actividades criminales. Las posibles soluciones incluyen estándares y productos técnicos, prácticas operativas, educación del usuario, políticas, regulación y legislación.

Para este documento, ciberseguridad se define como todo lo que conlleve problemas de seguridad específicos de Internet, sus soluciones técnicas y no técnicas. No todos los delitos que se producen en Internet están cubiertos por el término ciberseguridad. Un delito es un delito, y extrapolarlo a Internet no lo hace especial. Cuando se comenten delitos usando Internet, resulta algo novedoso que ofrece buenos titulares, pero hacer un pedido a un vendedor e intentar pagar con una tarjeta de crédito robada es un mero fraude a través de Internet, no ciberfraude.

Algunos tipos de problemas legales y de seguridad que no son específicos de Internet, como la reproducción no autorizada o distribución de material con copyright como películas, el contenido ilegal como imágenes de abuso infantil, aunque son importantes, no se han incluido aquí. Aunque Internet puede ser un canal que facilite estas actividades, se han omitido para mantener el enfoque en soluciones tecnológicas a problemas de seguridad comunes, en vez de incluir "todo lo malo que puede suceder en Internet".

Tanto los problemas de ciberseguridad específicamente como otros tipos de actividades delictivas que se llevan a cabo usando Internet no se van a resolver exclusivamente mediante la tecnología, sino a través de una cooperación y coordinación entre todos los interesados de Internet, incluyendo empresas, usuarios organizativos e individuales, agencias gubernamentales y de cumplimiento legal y dirigentes políticos de todo el mundo. Todo ello se debe combinar con esfuerzos activos centrados en educar a los usuarios de Internet, incluyendo padres, niños y educadores. El componente social del cibercrimen no se puede erradicar sin la participación de los usuarios.

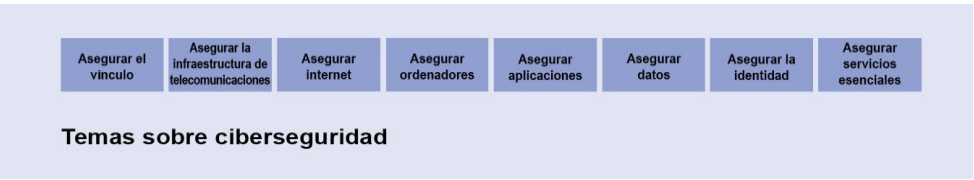

Figura 1: Temas de ciberseguridad

2 Temas de ciberseguridad

El gráfico de la Figura 1 es un desglose sencillo de muchos de los elementos que constituyen la ciberseguridad. El diagrama no pretende ser exhaustivo, sino ofrecer un marco para discutir los numerosos aspectos de la ciberseguridad. Cada bloque del diagrama representa una categoría general de los servicios de seguridad. Como el alcance de la ciberseguridad es tan amplio, resulta de ayuda el desglosarlo en estas categorías generales o temas. Las siguientes secciones se adentran con más detalle en cada uno de los temas.

2.1 Asegurar el vínculo

Los paquetes de Internet no cuentan con ninguna seguridad inherente. Con completamente abiertos y cualquiera con una simple herramienta de software puede inspeccionar fácilmente el contenido de los paquetes que se transmiten por la red. Es uno de los pilares básicos de la arquitectura de Internet. Para evitar *sniffing* o intercepción no autorizada, se reconoció con enseguida que era necesario contar con una manera de cifrar la transmisión de datos confidenciales. Existen varios enfoques para hacerlo, incluyendo cifrado en la capa del vínculo de datos (MACSec y acceso protegido para Wi-Fi), cifrado en la capa de la IP (IPSec) y cifrado en la capa de la aplicación (SSL/TLS y SSH, entre otros). Estas soluciones técnicas se discuten en la sección *Sniffing* de este documento.

Aunque interceptar comunicaciones por Internet puede ser técnicamente difícil en despliegues residenciales y comerciales normales, el uso creciente de Wi-Fi y otras tecnologías inalámbricas ha dejado claro que la intercepción es un problema continuado. Por ejemplo, en octubre de 2012, Eric Butler comercializó una herramienta llamada “Firesheep” para demostrar lo sencillo que es interceptar comunicaciones sin cifrar en el tráfico de Facebook en redes públicas inalámbricas. El objetivo mencionado por Butler era alentar a los sitios Web a usar más el cifrado (como SSL/TLS) para proteger los datos del usuario en circulación, un desafío que Facebook aceptó, pero que no cambió el comportamiento del resto de Internet. [FIRESHEEP]

IPsec, SSL, SSH y otros protocolos de cifrado de la capa IP y de aplicación vienen especificados por la Internet Engineering Task Force (IETF) en una serie de documentos de Request for Comment (RFC) que tratan los diversos componentes y extensiones. El Comité de Normalización IIEEE 802 LAN/MAN trata el asunto de la seguridad para redes con cable e inalámbricas locales y metropolitanas, entre los que se incluye Ethernet, Bluetooth, Wi-Fi y WiMax. La Wi-Fi Alliance, un consorcio de la industria, también participa en la definición de la seguridad inalámbrica a través de su norma de Acceso Wi-Fi Protegido (WPA y WPA2), un perfil basado en los estándares IEEE 802.11.

2.2 Asegurar la infraestructura de telecomunicaciones y la infraestructura de Internet

La seguridad de Internet y de las telecomunicaciones se ha diferenciado tradicionalmente una de la otra a la hora de definir el término ciberseguridad, ya que cada una de ellas tiene su propia infraestructura tecnológica y organizaciones de estándares relacionadas. Agruparlas juntas puede enturbiar los problemas, ya que las soluciones para asegurar la infraestructura de telecomunicaciones nacionales (sistemas cerrados muy regulados con pocos participantes destacados de cada mercado, organizados de manera jerárquica, monopolios naturales y plantas físicas en envejecimiento) son diferentes de las soluciones necesarias para asegurar la infraestructura de Internet; sistemas abiertos más bien no regulados, que se crean por encima de infraestructuras nacionales e internacionales múltiples sin un centro organizativo claro.
Cada vez más, los problemas de ciberseguridad incluyen problemas con las redes de telecomunicaciones como teléfonos móviles, satélite, instalaciones de emisión y microondas.

Conforme las tecnologías de Internet van usándose con mayor frecuencia para desplegar servicios de telecomunicaciones tradicionales, tales como entrega de servicio de telefonía a suscriptores de Internet en casa, la cooperación y colaboración son cada vez más importantes para llegar a mejorar con éxito el estado de la seguridad de Internet.

Cuando los políticos hablan de la falta de estándares para ciberseguridad, normalmente se refieren a los problemas relacionados con la infraestructura de Internet y seguridad informática, ya que esta infraestructura está en manos del sector privado y, por lo tanto, no está regulada o está autorregulada. La infraestructura de telecomunicaciones es la excepción, ya que siempre ha estado bajo la supervisión de varias agencias nacionales reguladoras de telecomunicaciones o proveedores de servicios gubernamentales de telefonía móvil. Debido a la antigua tradición de desarrollo y regulación de las telecomunicaciones, la mayoría de las redes de telecomunicaciones se consideran como entidades independientes, en lo que a seguridad se refiere. Por ejemplo, el enfoque de Angola para asegurar su infraestructura de telecomunicaciones nacionales no está vinculado a la seguridad de la infraestructura de Zambia ni a la de Argelia. En estos casos, las agencias internacionales de estándares de telecomunicaciones como la Unión Internacional de Telecomunicaciones (UIT) de la ONU son responsables de desarrollar recomendaciones y estándares efectivos. La IETF, aunque no es una organización dentro del tratado, también participa activamente en el desarrollo de estándares de seguridad para la red de telecomunicaciones, particularmente porque esas redes usan varios protocolos que normalizaron la IETF. Las agencias de cumplimiento legal también pueden cooperar con la UIT y la IETF a la hora de diseñar estándares para cumplir con sus propios requisitos, como la intercepción legal (grabación) de señales telefónicas y tráfico de audio.

La seguridad en la infraestructura de Internet es diferente a la seguridad en la infraestructura de telecomunicaciones nacionales o la seguridad empresarial corporativa, ya que debe enfrentarse al desafío de una red de redes global, en vez de a un conjunto redes nacionales o empresariales. Internet es una red global superpuesta de protocolos acordados, en la que la infraestructura subyacente y las redes individuales conectadas están gestionadas y controladas por organizaciones independientes, tanto públicas como privadas. Esto implica que los mayores desafíos a los que se enfrentan aquellas personas que trabajan en la seguridad de Internet surgen desde la autonomía y la diversidad organizativa y comercial de las redes individuales interconectadas que constituyen Internet.

La principal organización encargada de desarrollar estándares de seguridad para Internet es la IETF. Existen numerosos grupos de trabajo en la IETF que tratan específicamente el desarrollo de protocolos de seguridad como IPSec o TLS. Además, la IETF ha ordenado que todos los documentos de protocolos tengan una sección sobre “Consideraciones de seguridad” que traten las implicaciones de seguridad de ese protocolo. Se puede encontrar información adicional en www.ietf.org.

La IETF ha establecido un grupo de trabajo para la seguridad operativa, OPSEC, que planea producir documentos de prácticas recomendadas sobre más de una docena de problemas de seguridad operativa. Estos documentos capturarán prácticas actuales relacionadas con operaciones seguras basándose en experiencias del mundo real. Cada documento incluirá una lista de:

- Amenazas tratadas;
- Prácticas actuales para tratar la amenaza;

- Protocolos, herramientas y tecnologías existentes en ese momento para tratar la amenaza; y
- La posibilidad de que no exista una solución que haga uso de las herramientas y tecnologías existentes.

El resultado de OPSEC ofrecerá directrices a la comunidad de operadores de telecomunicaciones, la comunidad de desarrolladores de protocolos de la IETF y los implementadores de esos protocolos. Seis de los documentos de prácticas recomendadas propuestos se han publicado como RFC en noviembre de 2012, con otros seis documentos adicionales sobre prácticas recomendadas en desarrollo activo. Además de estas encuestas, OPSEC está produciendo una taxonomía de los diferentes estándares de ciberseguridad que están desarrollando las organizaciones de estándares de todo el mundo. [OPSEC-TAXONOMY]

2.3 Asegurar ordenadores

Asegurar ordenadores Cada vez que un dispositivo se conecta a Internet es susceptible de sufrir intrusiones. Aunque pueda sorprendernos, los ataques más exitosos de piratas, criminales y otros dudosos participantes se han efectuado contra servidores y ordenadores del usuario final que están conectados a Internet. Muchas organizaciones se esmeran en instalar firewalls y sistemas de seguridad de punto final, normalmente llamados “anti malware” o “antivirus”. Al mismo tiempo, los piratas están realizando pruebas continuamente y buscan debilidades en firewalls y ordenadores en red. El resultado es un creciente conflicto entre los propietarios de ordenadores, que quieren mantener el control de sus sistemas, y piratas, que quieren esos ordenadores y datos para alcanzar sus propios objetivos.

Nadie sabe con seguridad cuánto éxito tienen los piratas en su misión. Muchos ataques nunca se denuncian. Las presiones competitivas a menudo evitan que se compartan los datos de intrusión entre organizaciones e impide la colaboración acerca de diferentes enfoques relacionados con la seguridad. Sigue discutiéndose en varios foros sobre cómo recoger y compartir estos datos de una manera eficaz.

Las razones por las que los piratas han querido controlar ordenadores han variado con el tiempo. Hace quince años, el principal motivo del cibercrimen era puro vandalismo. Esto evolucionó a criminales que usaban Internet para extorsionar por dinero, robar contraseñas e información financiera (como números de tarjetas de crédito) y crear redes Bot para enviar spam, cometer fraude, robar información de identidad y lanzar ataques de denegación de servicio contra sitios web específicos. Algunas de estas técnicas las usan de manera más sofisticada gobiernos nacionales y otros mercenarios criminales para espiar, interrumpir comunicaciones y servicios y otros objetivos ofensivos.

Las herramientas que se usan para atacar ordenadores incluyen malware, troyanos, botnet, suplantación de identidad, ataque de denegación de servicio (DDoS) y ataques con intermediarios. Todo esto se discute en mayor detalle, junto con algunas tecnologías protectoras, en la sección “Problemas de ciberseguridad y tecnologías protectoras” de este artículo.

Mantener los ordenadores seguros, ya sean servidores o PC de usuario, portátiles y teléfonos inteligentes, es el objetivo de una amplia variedad de grupos dentro de las comunidades de TI e Internet. La tabla siguiente ayuda a identificar algunos de los principales participantes y sus áreas de interés.

Organización	Área de interés
Empresas de software, como Eset, F-Secure, Kaspersky, McAfee, Sophos, Symantec y Trend Micro	Producción de herramientas anti malware para servidores, ordenadores de usuario y portátiles. También se pueden usar en dispositivos integrados como firewalls.
Empresas de Firewalls, como por ejemplo Check Point Software, Cisco Systems, Juniper Networks y SonicWALL	Producción de dispositivos de firewalls de redes para asegurar las redes organizativas añadiendo una frontera entre la red e Internet.
Empresas de hardware, como AMD o Intel.	Producción de ordenadores con seguridad integrada (como discos duros con cifrado automático y el Módulo plataforma de confianza) para prevenir la ciberintrusión.
Trusted Computing Group (un consorcio industrial)	Desarrollo de estándares para la protección de dispositivos finales, como discos duros con cifrado automático, dispositivos de autenticación de hardware y control de acceso a redes.
IETF	Desarrollo de estándares para Evaluar los puntos finales de redes y asegurar la "salud" de los dispositivos antes de que se conecten a las redes e Internet.

2.4 Asegurar aplicaciones de Internet

Cualquier aplicación en un dispositivo, como un ordenador personal o teléfono inteligente por ejemplo, conectado y comunicando con Internet es "una aplicación de Internet". A modo de ilustración, dos de las aplicaciones más comunes de Internet: correo electrónico (email) y navegación por Internet, se examinan en esta sección. Sin embargo, existen muchas aplicaciones de Internet y el número sigue creciendo conforme se aceptan nuevos usos de Internet. Proteger estas aplicaciones entraría dentro de una categoría general de seguridad a nivel de aplicación, una faceta más de la ciberseguridad.

2.4.1 Asegurar el correo electrónico

Cualquier persona que use el correo electrónico estará familiarizado con un problema de seguridad: spam o correos electrónicos comerciales masivos no deseados. La protección de los correos electrónicos para no recibir spam se realiza mayoritariamente a nivel de compañías de software comercial y vendedores de dispositivos, como Barracuda Networks, Cisco/IronPort, McAfee, Proofpoint, Symantec y Trend Micro. Proveedores de servicios como Google/Postini y Microsoft han creado soluciones "en la nube" para ayudar a asegurar el correo electrónico frente al correo no deseado, y un número de compañías como Spamhaus ofrecen listas negras y servicios de reputación.

La principal organización de estándares que trabaja específicamente contra el spam es MAAWG, el Grupo de trabajo contra los mensajes abusivos, que mantiene una relación de coordinación con la IETF, otras organizaciones pequeñas de estándares y alianzas industriales. Basándose en la labor de MAAWG, la IETF formó un grupo de trabajo para ayudar a estandarizar los informes de spam. Los servicios de operaciones contra los mensajes abusivos entre servicios

independientes a menudo requieren que se envíen informes sobre fraudes que se hayan observado, spam, virus u otros tipos de abusos. Un formato normalizado del informe permite que se automatice el proceso. El grupo de trabajo MARF (formato de informe de mensajes de abuso) de la IETF ha desarrollado una serie de RFC que detallan un método y formato que pueden usar las organizaciones interesadas para informar sobre spam de manera normalizada. [MARF]

El correo electrónico es susceptible de una segunda amenaza, la suplantación de identidad. Debido al hecho de que el diseño de los protocolos de Internet no previó su uso por parte de una gran comunidad que podría ser susceptible de suplantación de identidad a gran escala, estos ataques aún son fáciles de realizar. La IETF ha desarrollado DKIM (Domain-Keys Identified Mail), una serie de estándares que ayudan a detectar correos electrónicos suplantados. DKIM también puede ayudar a bloquear ciertos tipos de spam que están relacionados con la suplantación de identidad, como correos de suplantación de identidad que pretenden provenir de bancos[1] [DKIM]

2.4.2 Asegurar las aplicaciones Web

Las aplicaciones Web, como la red social de Facebook, las subastas de eBay y Yahoo! Mail representan el uso más común de Internet para muchos consumidores. Para las empresas, las aplicaciones de comercio electrónico generales y especializadas como herramientas de autorización de tarjetas de crédito o gestión del inventario en línea ostentan un puesto más destacado. En cualquier caso, los servidores web y el software que suministra estas aplicaciones pueden usar seguridad especializada. Esos productos se conocen como firewalls para aplicaciones Web y los opera el dueño de la aplicación web, no el consumidor.

El principal objetivo de los firewalls de las aplicaciones Web es proteger a los usuarios de la Web y servidores Web frente a fallos de seguridad que podrían estar ocultos en la aplicación. Por ejemplo, un tipo de ataque en particular conocido como “Inyección SQL” se puede usar contra aplicaciones Web susceptibles para saltarse la aplicación y hablar directamente con la base de datos de la misma. Los ataques de inyección de SQL, cuando tienen éxito, pueden darle al atacante la posibilidad de descargarse información privada desde las bases de datos de las aplicaciones Web (como nombres de usuarios, direcciones, contraseñas e incluso números de tarjetas de crédito) o cargar contenido a un sitio Web de confianza que podría introducir malware en el ordenador de un usuario sin que éste lo sepa. Los firewalls de aplicaciones Web (y hasta cierto punto, los sistemas de prevención de intrusión) pueden ayudar a detectar y bloquear este tipo de ataques, ofreciendo una capa adicional de seguridad.

El World Wide Web Consortium (W3C) es el principal responsable de la administración de todos los estándares Web. El W3C ha creado dos grupos de trabajo relacionados con las aplicaciones y la seguridad, el Grupo de trabajo de aplicaciones Web [W3C-APP] y el Grupo de trabajo de seguridad en aplicaciones Web [W3C-SEC]. La IETF también creó un grupo de trabajo sobre seguridad Web en 2010, para ayudar a ofrecer estándares y consejos a los desarrolladores de software y reducir la incertidumbre. La mayor parte de la labor específica sobre firewalls de aplicaciones Web la han realizado vendedores de esos productos y desarrolladores de navegadores populares, en particular Microsoft y Mozilla. Debido a la gran cantidad de actividad dentro del campo de la seguridad de aplicaciones Web, muchos miembros de la comunidad

[1] “Phishing” es la creación de sitios Web que tienen el aspecto de sitios legítimos. Se dirige al usuario a estos sitios a través de un mensaje de correo electrónico, con nombres similares o grafía similar a otros lugares conocidos. Allí se les pide que escriban contraseñas, números de cuentas u otro tipo de información personal.

técnica creen que sería útil contar con una mayor coordinación dentro de marco de trabajo. [HODGES]

2.5 Asegurar los datos

La seguridad y privacidad de los datos (incluyendo el consentimiento) son dos áreas que se suelen incluir comúnmente en el término ciberseguridad.

Seguridad de datos es cualquier estrategia, ya sea legal, técnica, social o de otro tipo; que se use para proteger los datos. Como el mejor salvoconducto de datos entre fronteras, Internet permite a personas de todo el mundo enviar y recibir datos desde cualquier parte. Diferentes protocolos de Internet ofrecen grados diversos de seguridad en los datos. En algunas situaciones, los usuarios de Internet esperan que los datos que envían y reciben sean seguros, por ejemplo, cuando se comunican con su banco, gobierno o centro de salud. En otras situaciones, los datos que envían y reciben pueden no estar seguros durante el tránsito, por ejemplo, el contenido de Wikipedia.

Los usuarios de Internet también querrán proteger los datos almacenados para que un tercero no pueda acceder ni los manipule. Estos datos puede guardarlos localmente el usuario de Internet (por ejemplo en su ordenador o teléfono inteligente) o los puede guardar un proveedor de servicios (por ejemplo un banco, agencia gubernamental, proveedor de redes sociales, proveedor de almacenamiento de archivos, etc.) El aspecto de la **seguridad de datos** de la ciberseguridad trata el hecho de asegurar estos datos en tránsito y mientras están almacenados.

Privacidad, en el entorno en línea, trata la protección de datos personales. Recientemente ha surgido una definición moderna de privacidad centrada en la idea de compartir datos privados en línea:

> *Privacidad es el hecho de compartir datos de manera consensual en un contexto explícito con la expectativa de alcance*

Los marcos de trabajo sobre políticas y legalidad para la privacidad y protección de datos tienden a centrarse en datos personales (o información personal), que las directrices de privacidad de la OCDE definen como “cualquier información relacionada con un individuo identificado e identificable”. [OECD] Los datos sobre corporaciones, organizaciones e individuos que ya no existen suelen estar excluidos. Tradicionalmente, los marcos técnicos para el intercambio de datos a través de Internet se concentraban en la **seguridad de datos** más que en la **privacidad**. Sin embargo con la relativamente reciente explosión del intercambio de datos entre usuarios de Internet impulsada por herramientas más accesibles y fáciles de usar (por ejemplo dispositivos más baratos, sitios Web de redes sociales, blogs, acceso móvil, aplicaciones, etc.), la comunidad técnica de Internet está invirtiendo recursos considerables en desarrollar herramientas técnicas que respeten la privacidad y mejoras en la privacidad para los protocolos de Internet.

Las principales organizaciones que trabajan en esta área son poderes legislativos nacionales y cuerpos gubernamentales. La privacidad de la información personal ha sido objeto de legislación en todos los continentes. En Estados Unidos, la legislación ha sido normalmente débil a nivel federal con algunas excepciones notables, como la privacidad en temas de salud (HIPAA, ley de responsabilidad y portabilidad de los seguros médicos). Con lo que los estados deben intervenir para ofrecer mayor protección a los consumidores. California fue uno de los primeros líderes en esta área, legislando muchas áreas relacionadas con la protección de datos. Muchos otros

estados de Estados Unidos también han desarrollado su propia legislación, aunque esto ha dejado a Estados Unidos con un mosaico de regulaciones y requisitos muy diversos. Como respuesta a la preocupación acerca de la falta de normas de privacidad en línea a nivel federal, el Departamento de comercio de Estados Unidos está realizando una revisión exhaustiva del nexo entre políticas de privacidad e innovación en la economía de Internet. Además ha iniciado un proceso público y una serie de talleres con esa finalidad. [US-NTIA]

En la tabla de siguiente se muestran algunos ejemplos de normas de protección de datos. Nombre Portadas

Nombre	Cubre
Directiva de protección de datos europea	Cubre la transparencia, uso legítimo y proporcionalidad del uso de información personal de todos los ciudadanos europeos. También trata sobre cómo se pueden transferir los datos dentro y fuera de la UE.
Ley de privacidad de la Commonwealth en Australia	Recopilación adecuada, guardado, uso, corrección, divulgación y transferencia de información personal por parte de organizaciones del sector público y privado.
Ley de protección de información personal y los documentos electrónicos de Canadá	Trata sobre la recopilación no gubernamental, uso y divulgación de información personal, el derecho individual a la privacidad y la idoneidad de la recopilación organizativa, uso y divulgación de información personal.
Ley de protección de datos de Taiwán	Cubre el uso de datos personales por parte del sector público (gubernamental) y no público (sector privado), incluyendo la idoneidad, permisos, divulgación y castigos por el mal uso de datos personales.
Directrices de la OCDE sobre protección de la privacidad y flujos transfronterizos de datos personales	Cubre un consenso internacional sobre la recopilación y gestión de información personal. Ayuda a los gobiernos y empresas ofreciendo directrices sobre la protección de la privacidad y datos personales, además de flujos de datos transfronterizos.
Marco de privacidad de APEC (Foro de Cooperación Económica Asia-Pacífico)	Trata el tema del consenso regional sobre el desarrollo de la protección de privacidad, al mismo tiempo que se evita poner barreras al flujo de información.

2.6 Asegurar la identidad

Cuando Internet estaba en sus comienzos, se reconoció con rapidez que para que muchas aplicaciones comerciales tuviesen éxito, era necesario crear mecanismos basados en principios de confianza y gestión de identidad segura para autorizar y autenticar a los usuarios de Internet.[2] Un vínculo seguro sólo es bueno si se considera que los puntos finales son entidades legítimas que están autorizadas a llevar a cabo una transacción determinada. Originalmente, la expresión

[2] Identificación significa añadir una etiqueta a una entidad, como el nombre de usuario de una persona que está escribiendo en un ordenador. La autenticación es el proceso mediante el cual se verifica que la entidad que se identifica es quien dice ser, normalmente con técnicas tales como contraseñas secretas.

ciberseguridad se consideraba en estos términos; como una frase positiva para habilitar los servicios y capacidades de Internet.

Los mecanismos para aumentar la confianza y validar la identidad permitirían que Internet proveyese canales para comunicaciones seguras, fiables y privadas entre entidades, que se pueden autenticar claramente de forma ambas partes la entiendan. Estos mecanismos deberían ofrecer maneras razonables para que las entidades gestionen y protejan los detalles de su identidad.

Aunque muchos de los problemas relacionados con asegurar la identidad son legislativos, existen protocolos de privacidad y seguridad que pueden ayudar a asegurar el proceso de autenticación y autorización de usuarios finales. Las organizaciones que más participan en soluciones de identidad y confianza incluyen gobiernos nacionales y sus agencias, como por ejemplo US NIST, organizaciones del sector privado y público incluyendo OASIS, W3C, OpenID, la iniciativa Kantara y la IETF, todas ellas mencionadas a continuación.

OASIS (Organization for the Advancement of Structured Information Standards) [Organización a favor del avance de estándares de información estructurada] es un consorcio sin ánimo de lucro que se fundó originalmente para trabajar en SGML (Estándar de Lenguaje de Marcado Generalizado). Aunque SGML no tuvo mucho éxito, un estándar descendiente del mismo, XML (Lenguaje de marcas extensible) ha sido ampliamente adoptado. El Comité de Servicios de seguridad de OASIS desarrolló SAML (Lenguaje de marcado de aserción de seguridad) que es una base ampliamente usada para muchos protocolos avanzados de identidad. [OASIS]

El Instituto Nacional de Estándares y Tecnología (NIST) de EE.UU. ha preparado una Estrategia Nacional para Identidades confiables en el Ciberespacio [NSTIC]. Esta estrategia patrocinada por el gobierno “propone un cibermundo, el Identity Ecosystem, que mejora las contraseñas que se usan actualmente para conectarse en línea. Incluiría un mercado vibrante que permite que la gente escoja entre diferentes proveedores de identidad, tanto privados como públicos, que suministrarían credenciales de confianza que demuestren la identidad”.

La Fundación OpenID, otra organización activa en el área de asegurar la identidad, se fundó en 2007. OpenID es una organización internacional sin ánimo de lucro formada por individuos y compañías comprometidos por habilitar, promover y proteger tecnologías OpenID. [OPENID]

La iniciativa Kantara se fundó en 2009. Tiene el objetivo de ser el punto focal de la colaboración para tratar problemas compartidos en la comunidad de identidad. Su misión es “fomentar la armonización de la comunidad de identidades, la interoperabilidad, la innovación y su amplia adopción a través del desarrollo de especificaciones abiertas de identidad, marcos operativos, programas de educación, despliegue y uso de las prácticas recomendadas para el acceso seguro a los servicios en línea desde el respeto a la seguridad”. [KANTARA]

El grupo de trabajo de la IETF OAuth también trabaja de manera activa en la normalización de protocolos de confianza e identidad, y continúa con el desarrollo de OAuth, un “protocolo abierto que permite la autorización de seguridad con un método sencillo y estándar para aplicaciones de escritorio, web y móvil”. La versión 2 del protocolo OAuth se publicó como un estándar propuesto en octubre de 2012. [OAUTH-V2], [LYNCH2011], [CERF2011], [GRANT2011]

2.7 Asegurar servicios esenciales

Servicios esenciales, tales como suministro eléctrico y sistemas de agua municipal, dependen cada vez más de las redes de datos, llamadas SCADA (Supervisión, Control y Adquisición de Datos) para su funcionamiento normal. Cuando se ataca a servicios esenciales, el daño potencial va más allá de los daños que causa el envío de spam anunciando relojes o medicamentos que aumentan la potencia sexual.

Las consecuencias de un ataque exitoso contra un ordenador que opera o controla estos tipos de infraestructuras críticas son nefastas. Inhabilitar un servidor Web puede ser inconveniente y resultar en pérdida de ingresos y costes extras, pero derrocar el suministro eléctrico tiene consecuencias más serias y de gran alcance para la seguridad pública. Por ello es importante prestar particular atención a la amenaza que representan tales ataques y lo que representarían las respuestas asociadas para la gobernanza y funcionamiento adecuado del Internet global.

Estas amenazas son nuevas, y mayoritariamente, teóricas. Sin embargo, los sistemas SCADA no se ejecutan de la misma manera que las redes empresariales típicas, con revisiones de seguridad programadas regularmente y tiempo de desconexión para actualizaciones y mantenimiento. Las redes SCADA están equipadas con ordenadores internos programados para realizar tareas muy especializadas de forma muy fiable. Estos ordenadores, sin embargo, ponen menor énfasis en protegerse de ataques. La principal forma de protección de las redes que controlan servicios esenciales es doble: rendijas de aire y seguridad por anonimato.

La frase “seguridad de rendija de aire” se refiere a una práctica común de seguridad con sistemas críticos de control. La seguridad de la red y el sistema se piensa que es algo sencillo: sólo hay que asegurarse de que no haya conexión física entre el sistema de control e Internet. Sin conexión física, es decir, con una rendija de aire, significa que ningún malware puede infectar un sistema desconectado del resto y que nadie puede tomar el control de un sistema sin conexiones a la red. Aunque este tipo de seguridad era fácil de seguir hace algunos años, se está haciendo cada vez más difícil asegurar estas rendijas de aire, teniendo en cuenta la omnipresencia de Internet en muchos aspectos de nuestra vida y empresas, incluyendo las compañías de agua, luz y gas. Puesto que los sistemas esenciales están conectados entre sí, todo lo que se necesita es que haya un sistema comprometido en la periferia para derrocar a la cadena completa. Por ejemplo, se cree que el gusano Stuxnet que desconectó cientos de centrífugas en la planta iraní Natanz de enriquecimiento de combustible fue capaz de pasar la rendija de aire cuando un técnico conectó un ordenador infectado en la red de la planta. [STUXNET-NYT]

Un segundo tipo de seguridad, “seguridad por anonimato” sugiere que las redes que soportan servicios esenciales están protegidas de manera inherente porque muchos de los sistemas de control y protocolos son desconocidos para los posibles atacantes. Pero como estos sistemas se han convertido en objetivos valiosos para los criminales, existe un incentivo adicional para aprender más, y penetrar, en sistemas anónimos. Algo cada vez más cierto conforme se van sustituyendo los sistemas operativos personalizados que funcionan en tiempo real por software de bajo coste, genéricos como Windows o Linux, que tienen vulnerabilidades de seguridad conocidas que no se podrían revisar debido a la naturaleza de esas redes.

Las organizaciones militares, al igual que organizaciones de estándares, como NIST en EE.UU., están empezando a tratar el desafío de ofrecer seguridad a los sistemas que soportan la infraestructura nacional crítica.

3 Problemas de ciberseguridad y soluciones tecnológicas

La ciberseguridad es un área activa en la investigación y desarrollo dentro de la comunidad de tecnología de la información, con participantes de todas las áreas del ecosistema de TI. Muchos de los temas de ciberseguridad discutidos anteriormente tienen problemas de seguridad comunes que deben resolverse para propiciar la continuada maduración de Internet como una parte segura y de confianza de nuestras vidas.

La Figura 2 resume algunas de las principales áreas problemáticas de la ciberseguridad e indica dónde pueden encontrar soluciones tecnológicas esas áreas problemáticas, soluciones que han desarrollado entidades comerciales, organizaciones de estándares y usuarios de Internet.

Encontrar una solución tecnológica a un problema de ciberseguridad no hace que el problema desaparezca; sólo ofrece la posibilidad de resolverlo. Por ejemplo, el cifrado extremo a extremo mediante SSL/TLS es una conocida tecnología que se puede usar como parte de la respuesta a muchos de los temas mencionados anteriormente. Sin embargo, no se ha adoptado de forma universal, en parte por razones históricas e inercia organizativa, y en parte por ignorancia o por información errónea. Contar con soluciones conocidas para problemas conocidos no aporta mucho valor si las soluciones no se utilizan.

Las secciones siguientes ofrecen una visión general entre secciones de algunos de los principales problemas de ciberseguridad y las soluciones que se están desarrollando y manteniendo en la comunidad de Internet. En muchos casos, las soluciones listadas son conocidas y maduras; en el resto, las soluciones son áreas de investigación y desarrollo activo en toda la comunidad. Debido a que muchos de estos problemas de ciberseguridad se pueden usar en múltiples temas sobre ciberseguridad, no se asignan directamente en la lista de temas que se han mencionado anteriormente en el documentos, ya que son comunes a todo el área de ciberseguridad.

3.1 Resolver las intercepciones con cifrado

El problema de intercepciones se puede resolver con cifrado (y autenticación) de mensajes.

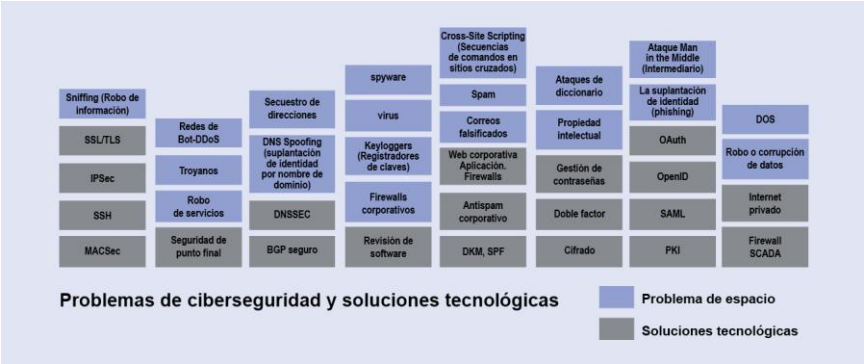

Figura 2: Problemas de ciberseguridad y soluciones tecnológicas

Este cifrado puede producirse a varios niveles de la red. En muchos casos, se pueden usar múltiples esquemas de cifrado a la vez, dependiendo de la red y la arquitectura de la aplicación. Los enfoques comunes son:

Capa	Solución
Más baja (vínculo físico y de datos)	Cifrado propietario del vínculo; Estándar inalámbrico IEEE 802.11; estándar de cableado MACSec IEEE 802.3
Red (a nivel de IPv4 e IPv6)	Los estándares IP Security IPSec de la IETF (e IKE, Intercambio de claves por Internet).
Aplicación	SSL, TLS, SSH, PGP, S/MIME

Se puede suministrar cifrado en la capa del vínculo con el estándar maduro inalámbrico IEEE 802.11 (y el perfil industrial llamado Acceso protegido Wi-Fi, WPA) o el nuevo estándar de cifrado de enlaces de datos IEEE 802.1 llamado MACSec. Aunque 802.11 y WPA se implementan en la actualidad de forma habitual, MACSec no se usa porque es un estándar nuevo y requiere contar con un nuevo equipo de redes. Herramientas antiguas de cifrado en la capa del vínculo, como dispositivos de cifrado punto a punto, se han desplegado en entornos de Red de área extensa (WAN), especialmente por parte de los servicios financieros y la comunidad militar.

El cifrado en la capa de red es común en muchas empresas que usan los estándares IPSec [IPSEC] e IKE. El término general para este tipo de cifrado es VPN, redes privadas virtuales, ya que el uso de estos protocolos puede crear una red protegida y cifrada dentro de una red. Estos estándares los desarrolló la IETF basándose en la labor ya realizada por otras organizaciones de seguridad y estandarización. Las empresas que necesitan vincular sucursales en Internet son los usuarios más frecuentes de IPSec, pero este estándar también se puede usar para el acceso remoto, permitiendo a los usuarios individuales entrar a la red corporativa a través de un cliente VPN de cifrado que se instala en su ordenador portátil o de escritorio.

El cifrado en la capa de la aplicación lo pueden suministrar muchos protocolos diferentes. El ejemplo más conocido es SSL (capa de conexión segura), reemplazado recientemente por Seguridad de la capa de transporte [TLS]. SSL/TLS es el protocolo de cifrado en la capa de la aplicación más común que usan la mayoría de transacciones financieras y basadas en la seguridad. En el mundo de la Web, se marca con el prefijo web “https:”. Además de SSL/TLS, existen otros protocolos de cifrado de seguridad para las aplicaciones como SSH (Intérprete de órdenes segura) [SSH] para conexiones remotas y S/MIME [SMIME-MSG] [SMIME-CERT] para cifrar el correo electrónico. Todos estos protocolos de seguridad usan certificados X.509 [X509] para la infraestructura de claves públicas. Varios incidentes relacionados con la emisión de esos certificados ilustran algunos de los fallos inherentes de este enfoque [COMODO] [DIGINOTAR]. Existen esfuerzos dentro de las organizaciones técnicas para tratar algunos de esos problemas.

Todos estos protocolos tienen un largo pasado de desarrollo a través de varias organizaciones de estándares técnicos. Muchos han generado desarrollos en otras organizaciones para buscar variaciones más seguras. IPsec, por ejemplo, es el sucesor del estándar ISO Protocolo de seguridad de capa de red (NLSP) basado en el protocolo SP3 que publicó NIST, pero que diseñó el proyecto de sistema de datos seguros en red de la Agencia de Seguridad Nacional (NSA) de EE.UU.

3.2 Resolver el malware usando un firewall y herramientas de seguridad de punto final

Una de las áreas de mejora potencial en la ciberseguridad es la protección de los ordenadores. Estas por lo general se denominan soluciones de seguridad de “punto final”, debido que el

equipo, ya sea si se tratara de un servidor web, un teléfono inteligente, un ordenador portátil o de escritorio ubicado en la casa de alguien o en la oficina, es uno de los dos extremos de una conexión a través de Internet.

3.2.1 Tipos de Malware

El término general para virus, spyware, troyanos y keyloggers es “malware”, diminutivo de “software malicioso”. Malware es un software que se descarga el usuario, a menudo involuntariamente, al hacer clic en lo que parece ser un sitio Web inocuo, una publicidad o abrir un mensaje de correo electrónico. El software se integra en el sistema operativo del ordenador con un amplio rango de efectos posibles. Puede ser una simple molestia que bombardea constantemente al usuario con ventanas indeseadas emergentes de publicidad. Por otro lado, el software puede ser más siniestro; por ejemplo, a través de los “keyloggers” se pueden escuchar las contraseñas y otra información personal que se escribe con el teclado. Este proceso también las guarda para que los delincuentes las obtengan más adelante.

Otro uso del malware es la creación de botnets, abreviatura de *Ro**bot Net**works*. Botnets las crean tipos de malware sofisticados diseñados para infectar muchos sistemas a la vez y dar el control de los sistemas a un humano que puede usarlos para crear una red masiva de procesamiento paralelo. Las botnets se pueden usar para enviar correos electrónicos comerciales no solicitados (spam), para actuar como falsos servidores Web para robar credenciales y otro tipo de información de los usuarios finales y para atacar otros ordenadores para inactivar o abrumarles (Denegación de servicio distribuida, ataques DDoS).

Investigaciones recientes indican la magnitud del problema. Una botnet típica creada para reclutar máquinas empresariales tiene unas 1000 máquinas, mientras que una gran botnet de espameo puede tener entre 50 000 a cientos de miles de máquinas. Según Dark Reading [DR] el número medio de botnets encontradas en las empresa ha sido constante durante los últimos dos años, with as much as 5 to 7 percent of all corporate systems infected by botnets, con un 5 a un 7 por ciento de todos los sistemas corporativos infectados por botnets.

Asegurar los ordenadores conectados a Internet para protegerlos de malware se ha dividido en dos principales áreas: firewalls, que crean un anillo protector alrededor de la red de la organización, y software y hardware de seguridad de punto final, que se centra en detectar y bloquear el software malicioso para que no tome control del punto final.

3.2.2 Usar firewalls

Un enfoque común para asegurar los puntos finales es crear una frontera alrededor de la red organizativa usando un firewall. Para la mayoría de ordenadores, el firewall actúa como una válvula de una dirección que permite al sistema de dentro conectar hacia fuera con Internet mientras que evita las conexiones que provienen desde fuera hacia dentro. Para algunos sistemas, como por ejemplo el correo electrónico y los servidores Web, se deben permitir las conexiones entrantes, pero estas conexiones se restringen a aplicaciones particulares en servidores concretos. Esto crea un desafío de configuración y control, en especial con las nuevas aplicaciones multimedia. Por ejemplo, Voz sobre IP (VoIP) y las conferencias Web no funcionan si el firewall las ahoga, de modo que el grupo de TI debe añadir normas para permitir el paso de tráfico a través del firewall para acomodarse a estos servicios tan complejos. Si el grupo de TI o el vendedor del firewall ha cometido un error al diseñar las funciones de VoIP o vídeo conferencias del firewall, se podría permitir la entrada de tráfico no deseado a la red corporativa.

Con el tiempo, el crecimiento del número de reglas y excepciones se ha convertido en objeto de preocupación. Puesto que cada regla se considera como “hacer un agujero” en el firewall, los firewalls organizativos se consideran “quesos suizos” y su eficacia a la hora de proteger ordenadores se cuestiona.

Además, la mayoría de firewalls permiten que los ordenadores internos tengan accesos sin restricciones a los navegadores Web de Internet y a leer el correo electrónico. Debido al hecho que el software malicioso se puede enviar al ordenador del usuario final a través de estos canales tan comunes, el firewall en sí no es muy eficiente para bloquear amenazas. Los firewalls y las tecnologías de inspección de paquetes coexisten mal con otras medidas de protección como contenido cifrado, VPN/tunelización y SOAP. Es así porque todos ellos abren caminos para que pasen cargas maliciosas. Esto ha llevado a la creación de un ecosistema de tecnologías de asistencia, entre las que se incluye:

- Firewalls con herramientas anti malware integradas (llamados usualmente “UTM,” Mitigación de amenazas unificada);
- Firewalls que detectan aplicaciones (normalmente llamados firewalls de la próxima generación) que integran herramientas anti malware y son capaces de controlar el uso de aplicaciones de Internet como Facebook y Skype, algo que un firewall tradicional no puede hacer; y
- Puertas de enlace Web seguras (también conocido como servidores proxy) con herramientas anti malware integradas.

3.2.3 Usar software y hardware de seguridad de punto final

El malware puede llegar a los ordenadores de muchas maneras. Uno de los más comunes es cuando un usuario descarga involuntariamente software de un sitio Web infectado o de dudosa reputación, o reciben el software como parte de un mensaje de correo electrónico.
Malware también se puede pasar a redes corporativas y del hogar (que suelen tener poca seguridad) compartiendo dispositivos USB. Los cibercriminales han desarrollado maneras innovadoras de atacar a los sistemas de los usuarios finales, como a través de conexiones Wi-Fi públicas [WIFI].

Existe malware para todo tipo de ordenador de uso común, incluyendo Macintosh OS X, Unix y sistemas Linux, además de teléfonos inteligentes y otro tipo de dispositivos como reproductores digitales de música y tabletas ordenador con sistemas operativos integrados.

Es un problema tan extendido que los empleados de TI organizativo suelen recomendar el uso de software de seguridad de punto final (a menudo llamado antivirus o anti malware) en todo tipo de dispositivos. Es común que las empresas exijan que cualquier ordenador conectado a su red tenga instalada una herramienta de seguridad de punto final configurada con los estándares corporativos. Esto es así para casi todas las esferas, desde educación superior y el gobierno, hasta los militares y las redes corporativas.

Las herramientas de seguridad de punto final pueden tener varios componentes para ayudar a proteger contra el malware, incluyendo:

Herramientas	Descripción
Anti malware	Protege contra virus y spyware (malware) detectando el malware cuando se descarga o se ejecuta.
Prevención de intrusión	Protege al detectar el comportamiento del malware, más que el malware en sí, cuando intenta infectar el sistema operativo, infectar otros sistemas o unirse a una botnet.
Firewall del anfitrión	Bloquea conexiones entrantes y salientes de un sistema final basándose en las políticas de seguridad.

3.3 Soluciones técnicas para asegurar la estructura de Internet

Aunque se considera que Internet es ubicuo y fiable, su propia infraestructura es vulnerable a ataques. Sin embargo, un ataque contra la infraestructura de Internet es una espada de doble filo para muchos criminales potenciales, una interrupción exitosa de la infraestructura de Internet descartaría su uso para cualquier otro objetivo, incluyendo comunicaciones de los "malos" o como plataforma para más ataques. Un ataque contra la infraestructura de Internet interrumpiría extensamente las comunicaciones comerciales en todo el mundo (aunque no es probable que interrumpa los servicios de comunicación militares), de modo que ese enfoque atraería a individuos o grupos que desean hacer declaraciones políticas muy destructivas. Como se ha visto con las ciberprotestas que han acompañado a eventos tales como la divulgación de cables diplomáticos clasificados por parte de Wikileaks, esos ataques pueden provenir de fuentes inesperadas en momentos inesperados.[3]

Algunos puntos clave de vulnerabilidad de Internet son los protocolos núcleo de enrutamiento de la red (BGP) y el sistema de nombres de Internet (DNS). La labor técnica continuada para mayor seguridad de BGP y DNS se discute abajo, en las secciones 3.3.1 y 3.3.2. Los enrutadores físicos, además de los planos de reenvío y gestión de Internet, son susceptibles a ciberataques, pero normalmente son problemas de seguridad internos de un solo dominio de un operador de redes de modo que normalmente se tratan a nivel organizativo o como problemas de seguridad de las telecomunicaciones.

Estos problemas no se han ignorado. El Departamento de Seguridad Nacional de EE.UU. ha publicado un roadmap for fixing the Internet's protocols [ROADMAP]. Aquellos lectores interesados en más detalles sobre problemas de seguridad relacionados con DNS y BGP pueden consultar [NIST-BGPSEC], una publicación del Instituto nacional de estándares y tecnología (NIST) de EE.UU.

Sin embargo, históricamente hablando han habido pocos ataques generalizados contra la infraestructura de Internet. Los ataques a DNS son los más frecuentes, pero no afectan a toda la infraestructura. En su lugar, se utilizan para atacar a individuos y organizaciones específicos. Los incidentes de BGP no son poco comunes, pero normalmente son causados por errores humanos y errores de configuración más que actores maliciosos o interrupciones intencionadas.

[3] Hay que tener en cuenta que las ciberprotestas relacionadas con las divulgaciones de Wikileaks no se consideran ataques a la infraestructura de Internet, tal y como se entiende en este escrito, sino ataque de denegación de servicios contra organizaciones que apoyan la posición del gobierno estadounidense sobre Wikileaks.

3.3.1 Asegurar los datos DNS con DNSSEC

El sistema de nombres de dominio (DNS) es una parte muy exitosa e importante de la infraestructura de Internet. Sin él, Internet no funcionaría. DNS permite que la gente use nombres fáciles de recordar y reconocibles para sitios Web y direcciones de correo electrónico, que luego se convierten en el formato numérico que usan los protocolos internos de Internet.

Se han descrito múltiples ataques potenciales a DNS, tanto en teoría como en demostraciones prácticas:

- DNS es una base de datos distribuida internacionalmente cuyo funcionamiento depende principalmente del uso de caché. Desafortunadamente se descubrió que las implementaciones comunes de software de DNS son vulnerables a ataques de suplantación de identidad en los que el atacante puede engañar a una caché para que acepte datos DNS falsos.
- Se pueden lograr ataques de intermediario cuando se puede insertar un dispositivo en el camino entre los clientes DNS y los servidores DNS (o dos servidores DNS) y redirigir o modificar información de DNS.
- Los ataques administrativos a DNS se pueden usar para redirigir el tráfico DNS de una organización averiguando las contraseñas de los registros de nombre de dominio o convenciendo a los registros a dar acceso personal no autorizado.

Los ingenieros de Internet se dieron cuenta hace tiempo que existía un fuerte incentivo para que DNS fueran seguros debido a la importancia de función para traducir direcciones que reconocen los humanos a las direcciones que usan los enrutadores y ordenadores conectados a Internet.

A principios de 1995, se inició una investigación [ATKINS2004] para encontrar un sustituto más seguro a DNS y DNSSEC se convirtió en un grupo de trabajo de la IETF. DNSSEC es una extensión de los DNS que ofrece comprobación de autenticación e integridad de los datos DNS. En 1997, se desarrolló el primer estándar DNSSEC, conocido como RFC2065. Se completó una especificación revisada de DNSSEC en 2005, con algunas funcionalidades adicionales estandarizadas en 2008.

La autenticación en DNSSEC asegura que el administrador de zona puede suministrar información autoritativa sobre un dominio DNS en particular, mientras que la comprobación de integridad asegura que la información de DNS no se pueda modificar (de manera accidental o maliciosa) mientras está en tránsito o almacenada. Eso significa que DNSSEC, entre otras cosas, ayuda a proteger contra los ataques que insertan información falsa en los DNS para redirigir a los usuarios de Internet a sitios Web engañosos o criminales, también conocido como “secuestro” de sitios Web.

Tras varios años de intenso estudio técnico y testeo, la primera producción de despliegue de DNSSEC se completó para un dominio de nivel superior en Suecia en 2007. Tras alcanzar un acuerdo sobre cómo se desplegaría globalmente, DNSSEC se está desplegando en todo el mundo. En julio de 2010 se firmó la zona raíz DNS.

Es importante tener en cuenta que la Extensión de seguridad en el Sistema de nombres de dominio (DNSSEC) no se ha diseñado para terminar con los ciberataques contra DNS sino para que se detecten esos ataques. Un despliegue a gran escala de DNSSEC también podría ayudar

a resolver muchos otros problemas de seguridad, como por ejemplo distribución segura de claves para las direcciones de correo electrónico.

Debido a cómo está implementado DNSSEC, éste permite que otras tecnologías usen el mismo conjunto de protocolos de seguridad para distribuir con seguridad la clave de cifrado necesaria para un amplio rango de objetivos, como SSH e IPSec. De modo que DNSSEC no sólo ofrecerá una base para tratar la seguridad de los desafíos de DNS; sino que fortalecerá otras partes importantes de Internet. [DANE]. Dicho esto, DNSSEC deberá tratar los mismos problemas asociados con el compromiso CA que se ilustraban con los incidentes de Diginotar y Comodo que se han referenciado anteriormente.

3.3.2 Seguridad BGP

El Protocolo Border Gateway (BGP), que es el protocolo de enrutamiento interdominio de Internet, es la cola que mantiene pegado Internet. Pero la principal limitación de BGP es que no trata la seguridad de manera adecuada. Interrupciones recientes en perfiles altos han demostrado con claridad que la infraestructura de enrutamiento de Internet es susceptible a ataques que tienen impacto global.

Las tablas de enrutamiento que mantienen los Proveedores de servicios de Internet (ISP) y que actualiza dinámicamente BGP son la base de todo el enrutamiento inter organizativo. Puesto que BGP es inherentemente inter dominio y no está bajo el control de una sola autoridad de gestión, es posible que se inserten errores de enrutamiento de forma deliberada o accidental por parte de organizaciones incluyendo tanto ISP y cualquier organización que tienen bastante presencia en Internet como para participar en el protocolo BGP, como por ejemplo una compañía con dos conexiones independientes a Internet. Los errores pueden resultar en interrupciones graves de Internet. Informes semanales producidos por numerosas organizaciones incluyendo APNIC (el Centro de información de Asia Pacífico) y la Universidad de Oregón, junto con investigadores de Internet como Geoff Huston, demuestran que los errores de configuración afectan al 1% a las entradas de la tabla de enrutamiento en cualquier momento, lo que subraya una vez el hecho que el sistema actual es muy vulnerable a errores humanos y un amplio rango de ataques maliciosos. Sin embargo, BGP ha demostrado ser muy resistente a la vez.

Una de las malas configuraciones de los enrutadores de Internet que ejecutan BGP, a menudo llamadas “secuestro de BGP”, no es nueva. Sucede frecuentemente aunque el secuestro no es intencional. No obstante, tales errores pueden tener como resultado en un extenso ataque de denegación de servicio o interrupción, como sucedió cuando Pakistan Telecom inadvertently secuestró el tráfico de YouTube.

En ese incidente, la compañía de telecomunicaciones pakistaní pretendía bloquear el acceso de los pakistaníes a Youtube para evitar que viesen contenido que el gobierno de Pakistán consideraba inaceptable. En su lugar, la compañía y su proveedor de canal de subida aconsejaron erróneamente a los enrutadores que esa era la mejor ruta a través de la cual enviar tráfico de YouTube. Durante casi dos horas navegadores de muchos sitios de Internet que intentaron alcanzar YouTube entraron en un agujero negro en Pakistán. [BGPHIJACK]

El secuestro de BGP es la inserción de rutas IP no autorizadas a las tablas de enrutamiento de BGP. En estos momentos, no existe una sola base de datos no ambigua que vincule las rutas IP a las organizaciones que tenga capacidad de insertar, o anunciarlas. El actual proceso de autorización es esencialmente manual, ya que cada organización que se une a Internet tiene la

responsabilidad de aprobar el conjunto de rutas IP que se pueden publicitar a sus pares. Mientras que las mejores prácticas de la IETF sugieren que cada par BGP debería permitir sólo rutas específicas que se hayan aprobado administrativamente, esta práctica no se sigue mucho. Además, conforme uno se separa de la organización conectada y va hacia el núcleo de Internet, la habilidad para autorizar y autenticar actualizaciones se hace tremendamente compleja. Herramientas basadas en políticas, como el Registro de enrutamiento de Internet (irr.net), que intenta suministrar con listas autoritativas de redes autorizadas y proveedores de servicios de red, han tenido éxito pero no se adoptan universalmente y requieren bastante intervención manual en la configuración de enrutamiento.

El grupo de trabajo de la IETF Enrutamiento seguro inter dominio (SIDR) se formó en noviembre de 2005 para reducir las vulnerabilidades del sistema de enrutamiento BGP de Internet. SIDR tiene el objetivo de reducir el riesgo que los proveedores de servicios secuestren redes publicitando rutas IP no autorizadas y creará estándares para una infraestructura de certificación llamada Recurso PKI (RPKI). Esta infraestructura de certificación verifica las designaciones de los Recursos de números de Internet (INR) incluyendo bloques de direcciones IP y Números de sistemas autónomos (ASN). Esta infraestructura sigue la estructura de distribución de INR que está en IANA, los Registros Regionales de Internet (RIR) y los Proveedores de Servicios de Internet (ISP), para emitir certificados a los recursos relevantes. Esto permite a las organizaciones que son dueñas de direcciones IP específicas autorizar a una red específica (marcada por ASN) publicitar estas direcciones. Esta autorización se publica usando un objeto firmado digitalmente, llamado Autorización de Ruta de Origen (ROA), que terceros pueden validar usando RPKI, lo que ofrece la posibilidad de comprobación automática, incluso en el núcleo de Internet y todas las actualizaciones de enrutamiento. Si una organización intentase inyectar una ruta IP no autorizada en las tablas de enrutamiento de BGP, se detectaría. [SIDR]

El grupo de trabajo SIDR ha publicado varios documentos detallando el marco de RPI y ROA. Las especificaciones se estandarizan y publican como RFC y todos los Registros Regionales de Internet (RIR) están desplegando servicios en estos momentos para soportar RPKI. Sin embargo, será necesario que todas las organizaciones que participan en el enrutamiento BGP de Internet (en estos momentos más de 37 000 organizaciones) hagan un esfuerzo significativo para usar estas nuevas capacidades en su infraestructura de gestión de enrutamiento.

3.4 3.4 Soluciones técnicas para asegurar los sistemas de autenticación

La autenticación de los usuarios finales de Internet basadas en aplicaciones representan una tensión continua entre el sector público y privado. Los objetivos de la seguridad, privacidad y usabilidad a menudo se enfrentan unos con otros. Cuánto más fácil es autenticar, más fácil es que alguien intercepte o robe información de autenticación y la use para suplantar a un usuario válido. Por otro lado, si la autenticación es onerosa y lleva demasiado tiempo, incluso cuando aumenta la seguridad, los usuarios finales no usarán la aplicación porque es demasiada molestia. O, frente a sistemas de autenticación difíciles de usar, los usuarios podrían crear sus propios desvíos y atajos para que el proceso de autenticación sea más sencilla, y a la vez, menos seguro.

Proteger la autenticación entra en dos amplias categorías: proteger la información en sí y facilitar a los usuarios una autenticación segura.

3.4.1 Proteger las bases de autenticación

Las bases de datos que guardan información de autenticación se llaman sistemas de identificación de la identidad (IdM) [IDM]. Es común que exista un subconjunto de muchas bases de datos que tienen grandes conjuntos de datos personales y que normalmente contienen la información de nombre del usuario y la contraseña necesaria para la autenticación. Estas bases de datos también pueden contener otra información pertinente relacionada con la autenticación, por ejemplo, si el usuario tiene autorización a ver cierto contenido desde una conexión remota. Los protocolos más populares que se usan en estos sistemas son sistemas de directorio como por ejemplo LDAP [LDAP] y X.500 [X500]. Los servidores RADIUS [RADIUS] que usan LDAP y X.500 son herramientas comunes para simplificar el acceso a la información de autenticación al ofrecer una sencilla Interfaz de Programación de Aplicaciones (API) para los sistemas de directorios más complicados.

Cualquier ruptura de la base de datos IdM abre todo el conjunto de datos personales que están almacenados en la base de datos a un atacante. En algunos casos, también permitiría al atacante suplantar a un usuario legítimo para autenticarse en otros sistemas de todo el mundo. Como resultado, los ataques contra sistemas IdM suelen ser uno de los métodos preferidos para romper la seguridad de una aplicación Web.

Las personas con acceso a IdM son normalmente el eslabón más débil a la hora de mantener la seguridad de los sistemas IdM. Enfoques de fuerza bruta como “ataques de diccionario” en los que los atacantes prueban nombres y contraseñas comunes para obtener acceso al sistema IdM se encuentran entre los enfoques más populares y exitosos para los atacantes externos.

Las defensas contra los ataques diccionario incluyen pedir a los usuarios que cambien sus contraseñas cada pocas semanas o meses y usar contraseñas complejas que consisten en caracteres numéricos y alfabéticos que no se encontrarían en nombres o contraseñas comunes. En el lado del servidor, la principal defensa es cifrar la base de datos de contraseñas para protegerla contra acceso no autorizado. En algunos casos, el cifrado ha demostrado ser inefectivo e incluso bases de datos cifradas han tenido como resultado contraseñas comprometidas.

Un enfoque más práctico, aunque más caro, para proteger las contraseñas es añadir una autenticación de dos factores. La autenticación de dos factores añade otro factor más además del nombre de usuario y contraseña. Este factor es necesario para que se complete la autenticación. Por ejemplo, se puede asignar una pequeña ficha a un usuario con una “contraseña del minuto” que se debería combinar con la contraseña normal del usuario. Otras técnicas innovadoras, tales como enviar una contraseña a un teléfono móvil, añadir herramientas biométricas tales como huellas dactilares o mostrar un código de Respuesta Rápida (QR) como parte del diálogo también se usan. [TIQR]

3.4.2 Usar estándares abiertos de autenticación y PKI

Como ha crecido el número de aplicaciones de Internet que requieren autenticación, también han crecido el número de bases de datos de autenticación. Como ya se ha mencionado anteriormente, en algunos casos el cifrado de estas bases de datos ha demostrado no ser efectivo con el resultado de contraseñas comprometidas. Un área de mucho interés en ciberseguridad es intentar reducir el riesgo de tener estas bases de datos reduciendo la cantidad de datos almacenados en esas bases de datos, mientras que a la vez se desarrollan protocolos abiertos que permiten que la información de autenticación pase entre aplicaciones con seguridad.

Se usan varias técnicas para robar información de autenticación directamente del usuario final, incluyendo ataques de suplantación de identidad e intermediario.
La suplantación de identidad es una actividad en la que los piratas establecen una identidad falsa en Internet, pretendiendo ser un banco y un sitio Web de almacenamiento, donde atrapan visitantes confiados para que hagan transacciones comerciales y les engañan para que el usuario les provea con información personal detallada como cuentas bancarias y contraseñas. Los ataques de "intermediario" son ordenadores desplegados en Internet que pueden interceptar consultas comunes y mensajes de un usuario, y luego redirigirlas a otro sitio u ofrecer datos erróneos como respuestas a la petición de un usuario. Una amenaza frecuente que suponen los ataques de intermediario es el robo de información de autenticación.

Tanto los ataques de suplantación y de intermediario se pueden vencer a través de la identificación y autorización de ambos puntos finales de la comunicación, lo que permite a ambas partes tener una certeza razonable que son quienes afirman ser.

Se ha realizado bastante investigación y desarrollo en la labor de establecer la identidad y confianza bajo la rúbrica de ciberseguridad. Ahora estamos empezando a ver la emergencia de los primeros productos y servicios de parte de organizaciones de estándares y organizaciones de investigación. En el mundo académico Shibboleth [Shibboleth] es la herramienta preferida para las identidades federadas, mientras que en el mundo comercial herramientas tales como OpenID [OPENID] y OpenAuth [OPEN AUTH] están consiguiendo mayor aceptación. El Lenguaje de etiquetas de aserción de seguridad (SAML) [SAML] es la tecnología subyacente que usan muchas aplicaciones de autenticación que usan OpenID y OpenAuth. Es un estándar basado en XML diseñado para intercambiar datos de authentication, authorization y otros atributos del usuario. SAML permite a las empresas hacer afirmaciones relacionadas con la identidad, atributos y derechos de un sujeto (a menudo un usuario humano) a otras entidades, como por ejemplo una compañía asociada u otras aplicaciones empresariales. SAML es un producto de OASIS Comité de servicios técnicos de seguridad [OASIS].

4 Pensamientos finales

Ciberseguridad es un amplio término que ha evolucionado con el paso del tiempo sin alcanzarse un consenso claro sobre su significado exacto. La concienciación pública sobre el estado de la ciberseguridad se ve teñida por los lapsus, normalmente sensacionales, en seguridad que copan los medios de comunicación. La divulgación de información personal, datos financieros robados y difusión de malware y virus, dan la impresión de peligro y caos, del colapso inminente de Internet. De hecho, no se nos cae el cielo a la cabeza; pero hay tormentas en el horizonte. Existen razones para tener cuidado, pero el balance general se decanta bastante por el lado del valor. Internet se ha convertido en una herramienta de conocimiento, comunicación, expresión y comercio, un recurso de confianza y una fuerza potente para la libertad personal.

Este artículo ha demostrado que las soluciones de ciberseguridad son extensas y complejas. Conforme caminamos hacia delante para enfrentarnos a nuevos desafío, debemos asegurarnos que el espíritu abierto e innovador de Internet no se ve comprometido. Las soluciones a los problemas de la ciberseguridad deben también fomentar la meta de todos los usuarios de Internet: un Internet abierto, accesible y confiable. Que Internet sea abierto es uno de sus principales valores, lo que lo convierte en la principal fuente mundial de creatividad, innovación y crecimiento. A fin de cuentas, el éxito para tratar los problemas de ciberseguridad está en la cooperación y colaboración de múltiples interesados y no en nuevos sistemas de control.

Referencias:

[ABAR] American Bar Association-appointed special cyber-prosecutors http://www.cfr.org/publication/22832/internet_governance_in_an_age_of_cyber_insecurity.html

[ALBRIGHT] Remarks of Madeleine K. Albright at the meeting of the North Atlantic Council with the Group of Experts on NATO's New Strategic Concept, May 17, 2010 http://www.nato.int/cps/en/natolive/opinions_63678.htm

[ATKINS] Atkins, D. and Austein R. (2004). RFC 3833, "Threat Analysis of the Domain Name System (DNS)", August, 2004 Available: http://www.rfc-editor.org/rfc/rfc3833.txt.

[AUSTRALIA-DBCDE] Australian Government Department of Broadband, Communications, and the Digital Economy. (2011). *Internet Service Provider (ISP) filtering.* Available: http://www.dbcde.gov.au/all_funding_programs_and_support/cybersafety_plan/internet_service_provider_isp_filtering. Last accessed 25 March 2012

[AUSTRALIA-UPDATE] http://arstechnica.com/tech-policy/2012/11/australia-comes-to-its-senses-abandons-national-internet-filtering-regime/

[BGPHIJACK] YouTube Hijacking: A RIPE NCC RIS case Study (http://www.ripe.net/internet-coordination/news/industry-developments/youtube-hijacking-a-ripe-ncc-ris-case-study)

[BORDER] Reporters without Borders http://en.rsf.org/internet.html

[CECC] Council of Europe Convention on Cybercrime http://www.coe.int/t/dc/files/themes/cybercrime/default_en.asp

[CERF2011] Cerf, V. (2011). The Battle for Internet Openness. *IEEE Internet Computing*. 15 (5), 104.

[CLARKE] Richard A. Clarke *Cyber-War* http://www.wired.com/threatlevel/2010/04/cyberwar-richard-clarke/

[COICA] Wikipedia, "Combating Online Infringement and Counterfeits Act" http://en.wikipedia.org/wiki/Combating_Online_Infringement_and_Counterfeits_Act

[COMODO] Leonhard, Woody. "Weaknesses in SSL certification exposed by Comodo security breach." InfoWorld Tech Watch. InfoWorld, 24 Mar. 2011. Web. Web. 27 Jul. 2012. <http://www.infoworld.com/t/authentication/weaknesses-in-ssl-certification-exposed-comodo-security-breach-593>.

[CYBERCOM] Burghardt, Tom, "The Launching of U.S. Cyber Command (CYBERCOM), Center for Research on Globalisation, Quebec, Canada, http://www.globalresearch.ca/index.php?context=va&aid=14186

[DANE] DNS-based Authentication of Named Entities Working Group - http://tools.ietf.org/wg/dane

[DIGINOTAR] Whitney, Lance. "Comodohacker returns in DigiNotar incident." CNET: News: Security & Privacy. CNET, 6 Sep. 2011. Web. Web. 27 Jul. 2012. <http://news.cnet.com/8301-1009_3-20102027-83/comodohacker-returns-in-diginotar-incident/>.

[DKIM] http://tools.ietf.org/wg/dkim/

[DR] Dark Reading – http://www.darkreading.com/index.jhtml

[FBI] 2005 FBI survey http://i.cmpnet.com/gocsi/db_area/pdfs/fbi/FBI2005.pdf

[FIRESHEEP] http://codebutler.com/firesheep/?c=1

[GRANT2011] Grant, J.A. (2011). The National Strategy for Trusted Identities in Cyberspace: Enhancing Online Choice, Efficiency, Security, and Privacy through Standards. *IEEE Internet Computing*. 15 (6), 80-84.

[HERSH] Seymour Hersh, "The Online Threat" http://www.newyorker.com/reporting/2010/11/01/101101fa_fact_hersh

[HODGES] Hodges and Steingruebl, "The Need for a Coherent Web Security Policy Framework", Web 2.0 Security and Privacy 2010 Conference, http://w2spconf.com/2010/papers/p11.pdf

[IC3] Internet Crime Complaint Center Report http://www.ic3.gov/default.aspx

[IDM] Identity Data Management systems (IdM) http://en.wikipedia.org/wiki/Identity_management

[IPSEC] IPsec http://datatracker.ietf.org/wg/ipsec/charter/

[IWM] Information Warfare Monitor http://www.infowar-monitor.net/

[KANTARA] The Kantara Initiative http://kantarainitiative.org/

[LDAP] Zeilenga, K. (ed) (2006). RFC 4510, "Lightweight Directory Access Protocol (LDAP): Technical Specification Road Map," June, 2006. Available: http://www.rfc-editor.org/rfc/rfc4510.txt.

[LOPPSI] http://fr.wikipedia.org/wiki/Loi_d'orientation_et_de_programmation_pour_la_performance_de_la_s%C3%A9curit%C3%A9_int%C3%A9rieure

[LYNCH2011] Lynch, L. (2011). Inside the Identity Management Game. *IEEE Internet Computing*. 15 (5), 78-82.

[MARF] http://tools.ietf.org/wg/marf/

[NIST-BGPSEC] http://csrc.nist.gov/publications/nistpubs/800-54/SP800-54.pdf

[NSPW] New Security Paradigms Workshop http://www.nspw.org/

[NSTIC] National Institute of Standards and Technology. (2011). *Making Online Transactions Safer, Faster, and More Private.* Available: http://www.nist.gov/nstic/. Last accessed 22 March 2012.

[NYT-ENERGY] http://www.nytimes.com/2010/01/26/world/26cyber.html

[NYT-GOOGLE] http://www.nytimes.com/2010/01/13/world/asia/13beijing.html

[OASIS] OASIS Security Services Technical Committee http://www.oasis-open.org/committees/tc_home.php?wg_abbrev=security

[OECD] Organization for Economic Cooperation and Development. (1980). *Guidelines on the Protection of Privacy and Transborder Flows of Personal Data.* Available: http://www.oecd.org/document/18/0,3746,en_2649_34255_1815186_1_1_1_1,00&&en-USS_01DBC.html. Last accessed 25 March 2012.

[OPENID] http://openid.net/

[OAUTH V2] Hardt, D. RFC 6749, "The OAuth 2.0 Authorization Framework", October 2012. Available: http://www.rfc-editor.org/rfc/rfc6749.txt Last accessed 23 October 2012.

[OPSEC] Internet Engineering Task Force. (2012). *Operational Security Capabilities for IP Network Infrastructure (opsec).* Available: http://datatracker.ietf.org/wg/opsec/. Last accessed 25 March 2012.

[OPSEC-TAXONOMY] C. Lonvick and D. Spak. (2011). *Security Best Practices Efforts and Documents (Internet Draft).* Available: http://tools.ietf.org/html/draft-ietf-opsec-efforts-18. Last accessed 25 March 2012.

[PATHWAYS] Seventh Worldwide Security Conference International Pathways to Cybersecurity http://www.ewi.info/international-pathways-cybersecurity-0

[PGP] Callas, J., Donnerhacke, L., Finney, H., Shaw, D., and Thayer, R. (2007). RFC 4880, "OpenPGP Message Format", November, 2007. Available: http://www.rfc-editor.org/rfc/rfc4880.txt. Last accessed 25 March 2012.

[RADIUS] Rigney, C., Willens, S., Rubens, A., Simpson, W. (2000). RFC 2865, "Remote Authentication Dial In User Service (RADIUS)," June, 2000. Available: http://www.rfc-editor.org/rfc/rfc2865.txt. Last accessed 25 March 2012.

[REVIEW] Defense Department's Quadrennial Defense Review http://www.defense.gov/qdr/

[ROADMAP] Department of Homeland Security's roadmap for fixing the Internet's protocols http://www.cyber.st.dhs.gov/docs/DHS-Cybersecurity-Roadmap.pdf

[SAML]Security Assertion Markup Language (SAML) http://en.wikipedia.org/wiki/Security_Assertion_Markup_Language

[SHADOWS] http://www.scribd.com/doc/29435784/SHADOWS-IN-THE-CLOUD-Investigating-Cyber-Espionage-2-0

[Shibboleth] http://shibboleth.internet2.edu/

[SIDR] http://tools.ietf.org/wg/sidr/charters

[SKYPE] Ten countries threatening to block Skype and Google http://www.voip-sol.com/10-isps-and-countries-known-to-have-blocked-voip/

[SMIME-MSG] Ramsdell, B., Turner, S. RFC 5751, "Secure/Multipurpose Internet Mail Extensions (S/MIME) Version 3.2 Message Specification," January 2010. Available: http://www.rfc-editor.org/rfc/rfc5751.txt.

[SMIME-CERT] Ramsdell, B., Turner, S. RFC 5750, "Secure/Multipurpose Internet Mail Extensions (S/MIME) Version 3.2 Certificate Handling," January 2010. Available: http://www.rfc-editor.org/rfc/rfc5750.txt.

[SSH] Ylonen, T., Lonvick, C. (ed). (2006). RFC 4251, "Secure Shell (SSH) Protocol Architecture," January, 2006. Available: http://www.rfc-editor.org/rfc/rfc2865.txt. Last accessed 25 March 2012.

[STUXNET] Falliere, Nicolas; Murchu, Liam; Chien, Eric (Symantec Security Response) W32.Stuxnet Dossier (Feb, 2011) http://www.symantec.com/content/en/us/enterprise/media/security_response/whitepapers/w32_stuxnet_dossier.pdf

[STUXNET-NYT] http://www.nytimes.com/2012/06/01/world/middleeast/obama-ordered-wave-of-cyberattacks-against-iran.html

[TIQR] Jan Michielson. (2011) *TIQR User Manual.* Available: https://tiqr.org/wp-content/uploads/2011/05/tiqr_manual_v1.0.pdf. Last accessed 25 March 2012.

[TLS] Dierks, T., Rescorla, E. (2008). RFC 5246, "The Transport Layer Security (TLS) Protocol, Version 1.2," August, 2008. Available: http://www.rfc-editor.org/rfc/rfc5246.txt. Last accessed 25 March 2012

[US-NTIA] http://www.ntia.doc.gov/category/privacy

[W3C-APP] Web Applications Working Group Charter, World Wide Web Consortium. http://www.w3.org/2010/webapps/charter/

[W3C-SEC] Web Application Security Working Group, World Wide Web Consortium, http://www.w3.org/2011/webappsec/

[WIFI] http://www.esecurityplanet.com/views/article.php/3869221/Top-Ten-Wi-Fi-Security-Threats.htm

[WIKI-ESTONIA2007] 2007 Cyberattacks on Estonia (from Wikipedia) http://en.wikipedia.org/wiki/2007_cyberattacks_on_Estonia

[X500] X.500, "Information technology - Open Systems Interconnection - The Directory: Overview of concepts, models and services." http://en.wikipedia.org/wiki/X.500

[X509] X.509, "Information technology - Open systems interconnection - The Directory: Public-key and attribute certificate frameworks." http://en.wikipedia.org/wiki/X.509

Internet Society
Galerie Jean-Malbuisson 15
CH-1204 Ginebra, Suiza
Tel: +41 22 807 1444

Fax: +41 22 807 1445
1775 Wiehle Ave.

Suite 201
Reston, VA 20190
USA
Tel: +1 703 439 2120
Fax: +1 703 326 9881

Correo electrónico: info@isoc.org
www.internetsociety.org