Seguridad y usuarios finales

Escuela Técnica Superior de Ingeniería de Telecomunicación

http://gsyc.urjc.es

Septiembre de 2016

Ataques basados en ingeniería social

Algunos ataques se basan no tanto en *hardware* y *software* (que también) sino en ingeniería social: *engañar a una persona*

- Obviamente, la formación del usuario es especialmente importante
- Algunos de ellos son simples timos con siglos de historia, adaptados a internet
- Otros se basan en la inclinación natural de las personas a colaborar con otros o a evitar situaciones molestas

Ingeniería social básica

La paciencia y habilidad del atacante tratando con personas es con frecuencia un arma más eficaz que sofisticadas técnicas puramente tecnológicas

- Familiaridad y confianza
  Invertir tiempo en parecer familiar e inofensivo. Un completo desconocido provoca recelos
- Crear situaciones hostiles
  Fingir un gran enfado, incluso cierta agresividad. Pero nunca contra la víctima, esto suele ser contraproducente
  La hostilidad se dirige contra un (fingido) tercero, para que la víctima busque *quitarse de enmedio*

- Recopilación de información, con diversos grados de agresividad
  - Google, linkedin, facebook
  - Posters, libros o fotos que pueda tener la víctima en su lugar de trabajo. (Permite deducciones sobre sus gustos, sus herramientas, su capacidad...)
  - Fingir ser un responsable de una empresa colaboradora, cliente, o de otra rama de la misma empresa
  - Recopilar y analizar la basura (papeleras tradicionales)
  - Asaltar coches en el parking, otras oficinas, robar maletines, ordenadors, móviles... buscando documentación y material diverso

- Conseguir un trabajo en la empresa de la víctima
  Si el objetivo lo merece, colocar un trabajador dentro de la organización víctima conseguirá una enorme cantidad de información y accesos
- Lectura del lenguaje corporal
  De la misma forma que un buen *adivino* practica la *lectura fría* sobre sus *clientes*, un atacante educado y correcto (sin excesos) que aparentemente empatice con la víctima puede conseguir grandes resultados
- Coqueteo
  Si el atacante es una mujer atractiva y la víctima un hombre, la biología lo pone todo a favor del ataque

Spam

Envío indiscriminado de mensajes no solicitados

- No solo en correo electrónico: también en mensajería instantánea, grupos de news, blogs, wikis, sms, telefonía IP, fax
- Originalmente, SPAM es una marca de carne de cerdo en lata. Toma el significado actual a partir de un *sketch* de los Monty Python
- Es legal en ciertos casos, dependiendo de las legislaciones

- El spam puede anunciar productos o servicios reales (sean legales o ilegales), aunque en su gran mayoria se trata de estafas, *cartas nigerianas*, *phising*, etc
- Se estima que el volumen de spam en el correo actualmente es superior al 90 %, 95 % o incluso 97 %
- Los spammers obtienen las direcciones procesando masivamente páginas web (propias o ajenas), cadenas de correo, directorios, fuerza bruta o mediante ingeniería social
- Los mensajes suelen ofuscar su contenido, para dificultar su detección por parte de los filtros

Cadenas de correo

Reenvía esto a 20 amigos o tendrás 20 años de mala suerte
Anónimos e intemporales, *para que duren*
También pueden estar aparentemente bienintencionados (aviso de virus, actividad criminal)

- Puede ser más o menos dañino, pero es un tipo de spam. Debemos formar a nuestros usuarios para que no las sigan. Nunca. No es posible determinar su autenticidad
- Se pueden emplear para conseguir direcciones de correo
- Frecuentemente incluyen bulos (*hoax*)
- Pueden incluir falsos avisos de virus
  - jdbgmgr.exe, *virus del osito*
- No es cierto que Coca Cola dará un céntimo a los niños pobres de Uganda por cada correo reenviado
  - Además ¿cómo podría saberlo?
- En las contadas ocasiones en que el hecho es cierto, la situación puede haber cambiado, pero la cadena sigue

En Internet, cualquiera puede decir cualquier cosa, un cierto escepticismo es imprescindible
Antes de dar por cierta una afirmación, debemos evaluar qué confianza nos merece su autor. Y si su verdadero autor es quien dice ser. Ejemplos:

- El autor del *virus de la policía* no es la policía
- En 2011 se hizo muy popular un artículo titulado *¿sois idiotas?*, falsamente atribuido a Arturo Pérez-Reverte
- *Mañana Facebook va a cambiar su configuración para permitir que Isabel Pantoja entre en tu casa en cuanto te duermas y te cante "Marinero de luces" toda la noche. Para evitar ésto, entra en: Cuenta,Configuración de Privacidad, Invasión Doméstica, Pantoja,Copla y quita las comillas a "Marinero" Por favor, copia y pega esto en tu muro*

Legislación española sobre Spam

Ley 34/2002, de 11 de Julio de Servicios de la Sociedad de Información y Comercio Electrónico, art 21

1. Queda prohibido el envío de comunicaciones publicitarias o promocionales por correo electrónico u otro medio de comunicación electrónica equivalente que previamente no hubieran sido solicitadas o expresamente autorizadas por los destinatarios de las mismas.
2. Lo dispuesto en el apartado anterior no será de aplicación cuando exista una relación contractual previa, siempre que el prestador hubiera obtenido de forma lícita los datos de contacto del destinatario y los empleara para el envío de comunicaciones comerciales referentes a productos o servicios de su propia empresa que sean similares a los que inicialmente fueron objeto de contratación con el cliente.

En todo caso, el prestador deberá ofrecer al destinatario la posibilidad de oponerse al tratamiento de sus datos con fines promocionales mediante un procedimiento sencillo gratuito, tanto en el momento de recogida de los datos como en cada una de las comunicaciones comerciales que le dirija.

La ley estadounidense (*CAN-SPAM Act, 2003*) es más laxa

CAPTCHA

CAPTCHA: *Completely Automated Public Turing test to tell Computers and Humans Apart*

- Test de Turing inverso
- Lo más habitual es mostrar Texto o audio deformado de forma que solo puede ser reconocido por una persona, no por un programa
- Empiezan a aparecer test basados en realizar alguna pregunta que a una persona le tiene que resultar sencillo contestar, pero no a un programa
- En la actualidad, cualquier blog, wiki, formulario etc donde sea sencillo escribir se llenará rápidamente de Spam, a menos que se proteja con algo como un CAPTCHA
  - Problemático para personas con deficiencia visual

El CAPTCHA es vulnerable a

- Mejoras en los OCR
- Defectos en la implementación que permitan puentearlo
- Su resolución por verdaderos humanos
  - Pagados, en paises de muy baja renta
  - Engañados

Técnicas anti-spam

- Son preferibles los falsos negativos antes que los falsos positivos
- El usuario debe evitar publicar su correo de forma capturable por los spammers
  - Usando imágenes
  - Alterando el correo de forma legible por un humano.
    es mejor
    `juan.perez@empresa.QUITAESTO.com`
    que
    `juan.perez.QUITAESTO@empresa.com`
    Mejor aún:
    `juan.perez [arroba] empresa [punto] com`
    `juan.perez [at] empresa [dot] com`
- El usuario nunca debe responder al spam, ni para solicitar la baja

- Filtro reto-respuesta (*challenge-response spam filtering*)
  Técnica anti-spam que solicita al origen de correo dudoso una confirmación (reenvío, respuesta a pregunta, CAPTCHA)
  Muy controvertida:
  - Si el origen del spam es falso, se molesta a un usuario legítimo
  - Puede verse como *mala educación* con el emisor
  - Muy problemático con emisores no humanos, legítimos

- DNSBL (*DNS-based Blackhole*)
  Lista negra de posibles spammers
  Muy problemático
  - La dirección IP incluida puede ser dinámica
  - La dirección IP incluida puede ser la de un administrador algo descuidado, víctima de un *Open Relay*
- Listas grises
  Los correos dudosos se retrasan unas horas
  Técnica bastante eficaz
- Filtros bayesianos
  Análisis estadistico del contenido, basado en aprendizaje a partir de ejemplos
  Técnica bastante eficaz

Técnicas Anti-Spam propuestas para el futuro

- Autenticación del emisor
- Sistemas basados en coste
  - El bitcóin puede aportar soluciones, basadas en micropagos. El modelo actual de internet, donde casi todo es gratis, resulta muy caro porque hay que controlar todo tipo de abusos, en el correo y en cualquier otro protocolo. Con bitcóin se pueden pagar cantidades minúsculas por los servicios, p.e. millonésimas de euro. Esto es imperceptible para un uso legítimo, pero hace inviable el abuso

Phising

Actividad delictiva consistente en capturar información especialmente sensible como nombres de usuario, contraseñas y números de tarjeta de crédito

- Basado fundamentalmente en ingeniería social (e-mail o mensajería instantánea)
- Suplantación de páginas web de proveedores de correo, entidades financieras etc
- Frecuentemente basado en la manipulación de enlaces html

Cartas nigerianas

El timador

- Solicita ayuda para supuestamente sacar fondos del pais
- Solicita ayuda para pagar una fianza (*spanish prisioner*, *letter from Jerusalem*. s. XVIII)
- Comunica un supuesto premio de loteria o herencia
- Compra un artículo subastado y falsifica su pago
- Finje una relación amorosa (*romance scam*)
- Se hace pasar por una ONG y pide donativos para alguna causa
- Ofrece mercancía, alquiler o empleo
    - Tal vez por ebay

En ocasiones la víctima acaba secuestrada o asesinada

Scamb baiting: anzuelos para timadores

El timador ofrece enviar un dinero que la víctima debe reenviar, guardando una comisión

- El dinero puede ser real (para borrar el rastro de otras actividades, o emplear cuantas bancarias *respetables*)
- O puede ser dinero proveniente de cheque sin fondos o similar: figura en la cuenta, pero luego no se consolida

Calidad de las contraseñas

Las contraseñas son un elemento fundamental en cualquier mecanismo de autenticación, su calidad es de vital importancia

- Es imprescindible emplear palabras clave seguras, que no aparezcan en diccionarios, evitando nombres o fechas significativas, combinando símbolos, y de la mayor longitud posible.
- No solo nuestras contraseñas deben ser seguras, también las de nuestros usuarios
  - Se pueden probar con *password crackers*, p.e. *John the ripper*
  - Se puede revisar su calidad cuando el usuario las está definiendo

- Ejemplos de malas contraseñas:

  `123456`
  `4312`
  `toby`
  `r2d2`
  `tornillo`
  `fromage`
  `Fuenlabrada06`

- Contraseñas que parecen buenas, pero son malas:

  `XCV330`
  `NCC-1701-A`
  `ARP2600V`

- Buenas contraseñas
  Esto serían buenas contraseñas (si no estuvieran publicadas aquí)

Contraseña	Nemotécnico
QuReMa:	Queridos Reyes Magos:
3x4doze	3x4=doce
1pt,tp1	uno para todos,todos para uno
lh10knpr	le hare una oferta que no podrá rechazar
19dy500n	19 dias y 500 noches
waliaYS	we all live in a Yellow Submarine
R,cmqht?	Rascayú, cuando mueras que harás tú?

- Es conveniente que busquemos e inutilicemos las contraseñas débiles de nuestros usuarios, ya que suponen un primer punto de entrada en nuestro sistema
- En Unix, el root no puede leer las contraseñas. Pero en otros entornos sí. Y muchos usuarios emplean siempre la misma contraseña
  Ejemplo:
  1. Juan Torpe usa como contraseña dgj441iU en juan.torpe@hotmail.com
  2. Juan Torpe se registra en `www.politonosdebisbalgratis.com`, con su cuenta de correo y su contraseña de siempre
  3. El administrador malicioso de este web ya conoce el nombre de Juan, su cuenta de correo y su contraseña.
     - Además, puede usar la función *¿contraseña olvidada?* y colarse en cualquier otra cuenta de Juan

  Debemos instruir a nuestros usuarios sobre esto

- Los usuarios sin duda olvidarán en ocasiones su contraseña y tendremos que generarles una nueva, de forma segura. Problema de la *password fatigue*
- Pero es muy poco profesional que nosotros como administradores olvidemos una contraseña. Debemos usar diferentes contraseñas en diferentes servicios, y guardarlas de forma medianamente segura

Herramientas para almacenar contraseñas

- gpg
  Razonablemente seguro
  En Linux y OS X podemos usarlo directamente, en Windows es más conveniente un *fron end* como p.e. kleopatra
- LastPass
  Plugin para Internet Explorer, Chrome, Safari y Firefox, en Windows, Linux y OS X. Seguro si confiamos en su desarrollador.
- KeePassX
  Razonablemente seguro. Disponible para Windows, Linux, OS X
- KeePass
  Razonablemente seguro. Disponible para Windows. La versión 1.x es compatible con KeePassX (la versión 2.x, no)