Curso: (30227) Seguridad Informática

Fernando Tricas García

Departamento de Informática e Ingeniería de Sistemas
Universidad de Zaragoza
http://webdiis.unizar.es/~ftricas/
http://moodle.unizar.es/
ftricas@unizar.es

Tema Autentificación con clave

Fernando Tricas García

Departamento de Informática e Ingeniería de Sistemas
Universidad de Zaragoza
http://webdiis.unizar.es/~ftricas/
http://moodle.unizar.es/
ftricas@unizar.es

Autentificación mediante clave

- Es una de las formas mas populares
- No es un sistema muy seguro, pero es aparentemente sencillo
- Lo mejor es implantar varios métodos a la vez
- El usuario y el servicio comparten un secreto, la clave
- Hacer las cosas bien es más difícil de lo que parece!

http://www.flickr.com/photos/12129374@N00/3964214880/

Almacenamiento de claves

- Primero, la privacidad (nadie quiere que se conozcan sus claves)
- ¿Pedimos confianza en los administradores del sitio?
- ¿Cómo lo protegemos?

Las claves

- Una solución es cifrarlas
- Hace falta una clave (y el problema ahora es cómo almacenarla y utilizarla)
- Además, la clave gestionada por el programa (y entonces, un atacante ...)
- Esconderla lo mejor posible (¿seguridad por la oscuridad?)

Las claves: una solución

- Una solución mejor (y habitual): almacenar y utilizar un 'hash' criptográfico (iterando!).
  - Identifica igual al interesado, es fácil de comprobar y si la roban, 'no pasa nada'
  - No olvidar utilizar una semilla ('salt') para el 'hash'
    Problemas:
  - No podemos recordarle su clave al usuario.

Hay soluciones más complejas (criptografía de clave pública, por ejemplo)

Autentificación del usuario

'Olvidar' la clave lo antes posible.

Algoritmo:

1. Leer el nombre del usuario (identificador)
2. Calcular/obtener la semilla ('salt')
3. Leer la clave (sin que se vea en la pantalla)
4. Validar la clave (`crypt`, o el que se use) con la semilla
   - `bcrypt, PBKDF2,...`
5. Sobreescribir la clave
6. Comparar

Departamento de Informática e Ingeniería de Sistemas
Universidad Zaragoza

Un ejemplo

2011-12-08:

PuTTY vulnerability password-not-wiped

When PuTTY has sensitive data in memory and has no further need for it, it **should wipe the data out of its memory**, in case malware later gains access to the PuTTY process or the memory is **swapped out to disk or written into a crash dump file**. An obvious example of this is the **password** typed during SSH login; other examples include obsolete **session keys, public-key passphrases, and the private halves of public keys**.

`http://www.chiark.greenend.org.uk/~sgtatham/putty/wishlist/password-not-wiped.html`

Almacenando y usando claves

¡Cuidado!

- No mostrar las claves
- El uso de la función de hash con semilla
  - Si dos usuarios tienen la misma clave, la semilla lo 'esconde'.
  - Menos seguro que los métodos más modernos.
  - Un error (común): usar la clave como semilla. Tomará los dos primeros caracteres, se almacena en texto claro, eso da muchas pistas sobre la clave.
- Iterar la aplicación del hash
  - Ralentizar los cálculos
- Procurar que no se escriban al disco

Algunos problemas

¿Qué hacer con intentos repetidos?

- Como mínimo, contarlos y limitarlos (¿5?)
- Una vez superado el límite, bloquear el acceso (¿Seguro? Problema ... identificar al usuario de una cuenta bloqueada)
  - Denegación de servicio! (usar dos claves, la primera sin bloqueo)

Algunos problemas

¿Qué hacer con intentos repetidos?

- Como mínimo, contarlos y limitarlos (¿5?)
- Una vez superado el límite, bloquear el acceso (¿Seguro? Problema ... identificar al usuario de una cuenta bloqueada)
  - Denegación de servicio! (usar dos claves, la primera sin bloqueo)
- Mejor ralentizar el proceso con fallos sucesivos
- O añadir otras medidas
  - GMail añade un CAPTCHA

CAPTCHA

http://www.google.com/recaptcha

La imagen de http://www.blackhatworld.com/blackhat-seo/blackhat-lounge/423026-something-interesting-ive-noticed-recently-recaptcha.html

'Google Now Using ReCAPTCHA To Decode Street View Addresses'.

http://techcrunch.com/2012/03/29/google-now-using-recaptcha-to-decode-street-view-addresses/

Completely **A**utomated **P**ublic **T**uring test to tell **C**omputers and **H**umans **A**part

Departamento de Informática e Ingeniería de Sistemas
Universidad Zaragoza

Y algunas ideas

- Preguntar la clave...
- Poner un número alto de reintentos
- Ralentizar sucesivamente reintentos sucesivos
- Errores repetidos no cuentan (¿usabilidad?)
- Guardar también el número de reintentos globales (y obligar a cambiar, cuando es alto)

¡Y atentos a los reintentos probando nombres!

(`http://www.elladodelmal.com/2012/11/tus-passwords-son-suprayectivas.html`)

Elección de claves

- La gente no selecciona bien las claves
- Hay programas que ayudan a 'adivinarlas'
- Incluso 'a ojo' funciona, si se conoce un poco a la 'víctima'
- Conviene implantar un sistema que mida la calidad de las claves

Tiempos descubrimiento de claves

Clave de longitud 8

Clave	Car.	Comb.	Número de claves por segundo					
			10.000	100.000	1M	10M	100M	1000M
Números	10	100 M	2'75 h.	17 m.	1'5 m.	10 s.	Inmediato	Inmediato
Caracteres	26	200.000 M	242 d.	24 d.	2'5 d.	348 m.	35 m.	3'5 m.
May. y Min	52	53 MM	169œ a.	17 a.	1'5 a.	62 d.	6 d.	15 h.
Car. y Núm.	62	218 MM	692 a.	69.25 a.	7 a.	253 d.	25'25 d.	60'5 h.
Car., Núm. y Sím.	96	72.000 MM	22.875 a.	2.287 a.	229 a.	23 a.	2.25 a.	83'5 d.

- 100,000 Passwords/seg. Recuperación de contraseña Microsoft (Archivos .PWL)en un Pentium 100
- 1,000,000 Passwords/seg. Recuperación de contraseña de un archivo comprimido en ZIP o ARJ Pentium 100
- 10,000,000 Passwords/seg. Recuperación de cualquiera de las contraseñas anteriores con un PC (Monoprocesador +2Gh)
- 100,000,000 Passwords/seg. Recuperación de una contraseña con un cluster de microprocesadores o con multiples Pcs trabajando de manera simultánea.
- 1,000,000,000 Passwords/seg. Recuperación de una contraseña utilizando una supercomputadora o una red de ordenadores interconectados a gran escala, por ejemplo (160000 computadoras PII 266MHz 24/7)

`http://www.tufuncion.com/ataques-passwords-hacker-msn`

Más medidas

- Letras y números sin diferenciar mayúsculas de minúsculas
  - 6 caracteres: 2.24×10^9
    - En línea, 1000 intentos por segundo: 3.7 semanas
    - Fuera de línea, 100.000 millones de intentos por segundo: 0.0224 segundos
    - Fuera de línea, procesado masivamente paralelo, 100.000.000 millones de intentos por segundo, 0.0000224 segundos
  - 10 caracteres: 3.76×10^{15} de combinaciones
    - En línea, 1000 intentos por segundo: 1.2 siglos.
    - Fuera de línea, 100.000 millones de intentos por segundo: 10.45 horas
    - Fuera de línea, procesado masivamente paralelo, 100.000.000 millones de intentos por segundo, 37.61 segundos.

Más medidas

Si añadimos un símbolo

- 6 caracteres, 7.6×10^{12} combinaciones
  - En línea, 1000 intentos por segundo: 2.4 siglos.
  - Fuera de línea, 100.000 millones de intentos por segundo: 1.26 minutos
  - Fuera de línea, procesado masivamente paralelo, 100.000.000 millones de intentos por segundo, 0.0756 segundos.
- 10 caracteres, 1.71×10^{20} (171,269,557,687,901,638,419)
  - En línea, 1000 intentos por segundo: 54.46 millones de siglos.
  - Fuera de línea, 100.000 millones de intentos por segundo: 54.46 años.
  - Fuera de línea, procesado masivamente paralelo, 100.000.000 millones de intentos por segundo, 2.83 semanas.

`http://www.itworld.com/security/280486/how-long-would-it-take-crack-my-password`
`https://www.grc.com/haystack.htm`

`http://abclocal.go.com/kabc/story?section=news/consumer&id=8361856`

Y la gente?

Estudio informal, Liverpool Street station en Londres. Infosecurity 2004-2008.

`http://www.guardian.co.uk/technology/blog/2008/apr/16/woman4timesmorelikelythan`

Una encuesta, ofrecían una chocolatina por rellenar el cuestionario.

- 21 % de los encuestados dieron su clave. 45 % de las mujeres, 10 % de los hombres
- Sorteo de un viaje a París. Teléfono, nombre, fecha de nacimiento, ...
  - 60 % de los hombres, 62 % de las mujeres
- La mitad conocían claves de sus compañeros y el 58 % dijeron que le darían la clave a los del departamento de informática
- El 35 % sabía que la clave del jefe la conocía alguien más (asistentes, personal de IT, ...)
- 43 % la cambia raramente

¿Y la gente?

- Una persona dijo que trabajaba para un departamento del gobierno y que nunca daría su clave porque podría costarle el trabajo. 
- Otro dijo que parecían tan bien vestidos y honestos que era imposible que pudieran ser criminales. 

De años anteriores: (15 % nombres de la familia, 11 % equipos de fútbol, 8 % mascotas, ...)
Otro estudio, de RSA

- 79 % revela datos personales
- 33 % los compartía o los escribía

Más datos ...

Ataque de Phishing a MySpace (34.000 claves). 2006.

- 65 % de las claves tienen 8 caracteres o menos
- 17 % tienen 6 o menos

Longitud	Porcentaje
1-4	0.82 percent
5	1.1 percent
6	15 percent
7	23 percent
8	25 percent
9	17 percent
10	13 percent
11	2.7 percent
12	0.93 percent
13-32	0.93 percent

Composición	Porcentaje
numbers only	1.3 percent
letters only	9.6 percent
alphanumeric	81 percent
non-alphanumeric	8.3 percent

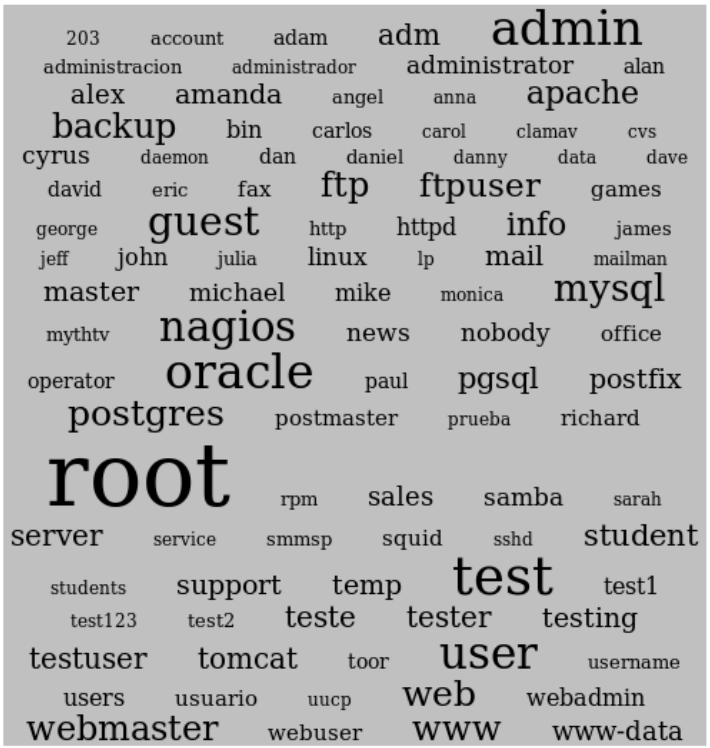
Claves más frecuentes

password1, abc123, myspace1, password, blink182, qwerty1, fuckyou, 123abc, baseball1, football1, 123456, soccer, monkey1, liverpool1, princess1, jordan23, slipknot1, superman1, iloveyou1 and monkey
(el más usado 0.22 % de las cuentas).

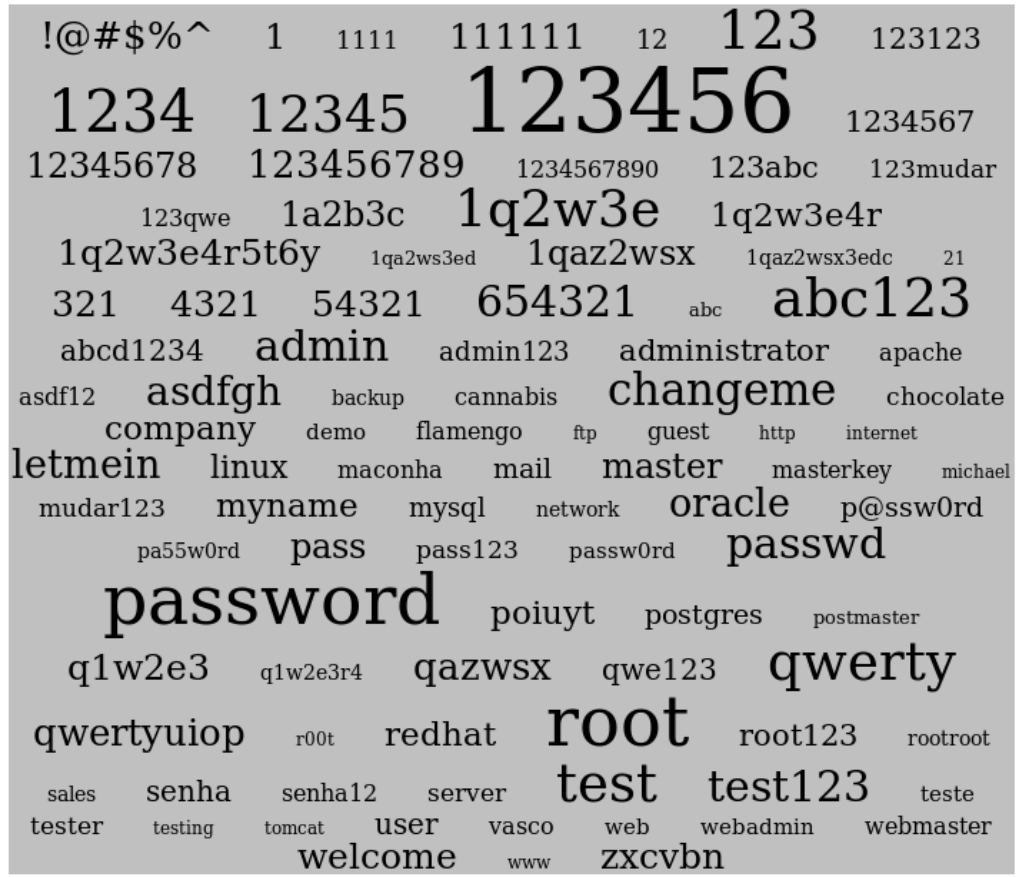
`http://www.schneier.com/blog/archives/2006/12/realworld_passw.html`

Most common usernames and passwords that have been tried in latest SSH brute force attacks.

most popular usernames



most popular passwords



http://www.dragonresearchgroup.org/insight/sshpwauth-cloud.html

Ideas

¿Qué tal?

- Dos palabras y un símbolo de puntuación en medio (buen!consejo)
- Fecha, símbolo de puntuación y una cadena (190345;ugh)
- Una frase fácil de recordar, la inicial de cada palabra, y algún signo de puntuación (el gato que está triste y azul $\longrightarrow$ Egqe'TYa;)

Mejor no dar ejemplos...

Explicar, no indicar

Clave: ftricas

- Mal! es su nombre

Clave: fernando

- Mal! es una palabra fácil de pensar

Clave: Gollum

- Mal! a mi también me gusta El señor de los anillos

Clave: a3f·

- Mal! esa clave es muy corta

¿Cuántas veces?

Departamento de Informática e Ingeniería de Sistemas
Universidad Zaragoza

Más consejos

- Suficientemente largas (10 caracteres)
- Incluso más!
- Evitar claves parecidas en distintos sitios
- Evitar palabras, títulos de libros, ciudades, ...
- Incluir símbolos de puntuación
- Cambiar letras por símbolos (pero que no sean parecidos: gato por g@to es un cambio trivial)

Más consejos

Michelle L. Mazurek, Saranga Komanduri, Timothy Vidas, Lujo Bauer, 'Measuring Password Guessability for an Entire University'. Octubre 2013

https://www.cylab.cmu.edu/research/techreports/2013/tr_cylab13013.html

- Claves largas
- Que contenga símbolos, dígitos, mayúsculas
  - En lugares no predecibles.
- ¡Cuidado con las políticas!

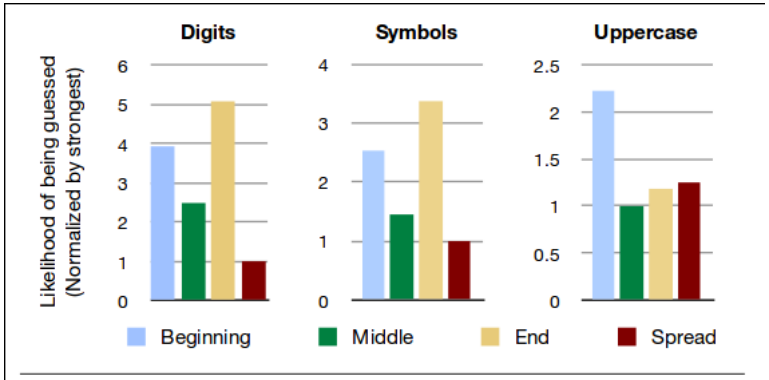


Figure 3: The relative likelihoods of passwords with digits, symbols, or uppercase letters in a given location being cracked. For example, a password with all its digits at the end is five times as likely to be cracked as a password with its digits spread throughout, other things being equal. The values are derived from the exponent of the regression coefficient, for the non-interaction model (Table 2). Each character class is normalized independently.

Más consejos

Michelle L. Mazurek, Saranga Komanduri, Timothy Vidas, Lujo Bauer, 'Measuring Password Guessability for an Entire University'. Octubre 2013

https://www.cylab.cmu.edu/research/techreports/2013/tr_cylab13013.html

- Claves largas
- Que contenga símbolos, dígitos, mayúsculas
  - En lugares no predecibles.
- ¡Cuidado con las políticas!
  Los usuarios disconformes tienen claves mucho peores (46 % más fáciles de adivinar)

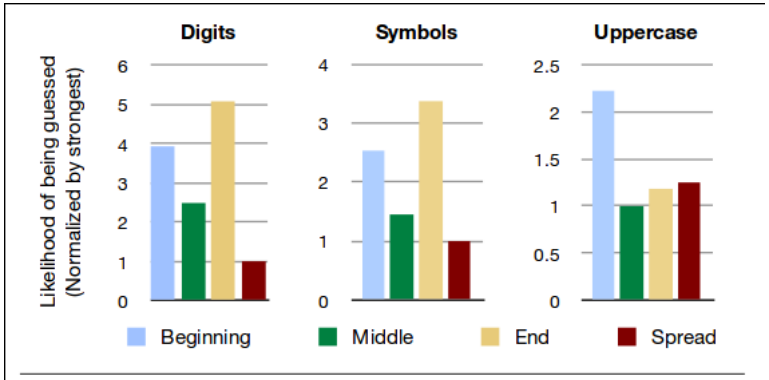


Figure 3: The relative likelihoods of passwords with digits, symbols, or uppercase letters in a given location being cracked. For example, a password with all its digits at the end is five times as likely to be cracked as a password with its digits spread throughout, other things being equal. The values are derived from the exponent of the regression coefficient, for the non-interaction model (Table 2). Each character class is normalized independently.

Echar los dados

- Nuevamente hemos encontrado un compromiso entre seguridad y comodidad
  - Lo 'mejor' es no rechazar ninguna clave!
- Una buena técnica es buscar una clave completamente aleatoria (pero es mucho trabajo!!!)
  - `mkpasswd` o programas similares.
- ¿Lo escribimos o no?

Echar los dados

- Nuevamente hemos encontrado un compromiso entre seguridad y comodidad
  - Lo 'mejor' es no rechazar ninguna clave!
- Una buena técnica es buscar una clave completamente aleatoria (pero es mucho trabajo!!!)
  - `mkpasswd` o programas similares.
- ¿Lo escribimos o no?
- Hay programas para guardar claves (y sólo hay que acordarse de la que protege al programa).
  - Utilizar `KeePass` o similares.

Departamento de Informática e Ingeniería de Sistemas
Universidad Zaragoza

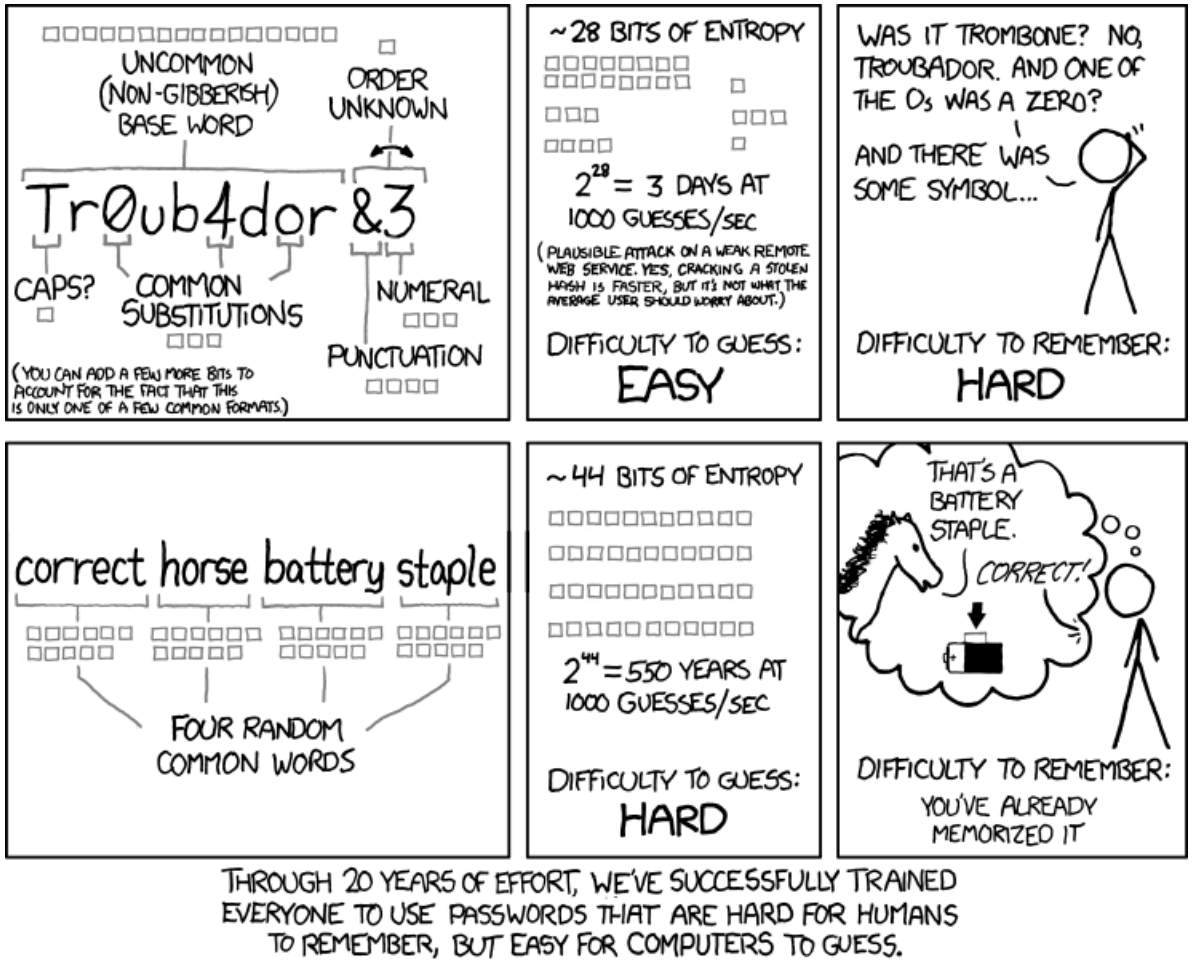
En lugar de claves, frases

- Interesante, el nombre ya ayuda a pensar en algo largo
- Nada impide (normalmente) que la frase sea una palabra
- Las frases también se pueden 'adivinar'
- Como mínimo 5 palabras, 13 caracteres

Departamento de Informática e Ingeniería de Sistemas
Universidad Zaragoza

Consejos

http://xkcd.com/936/



https://diogomonica.com/posts/password-security-why-the-horse-battery-staple-is-not-correct

¡Ojo! (2014-10-11)

¿Y si los elige el programa?

- Ver el tema sobre aleatoriedad
- Se pueden generar claves (con letras)
- Se pueden generar frases (con palabras)
- ¿Cómo informamos al usuario?

  Fuera de banda, si es posible.

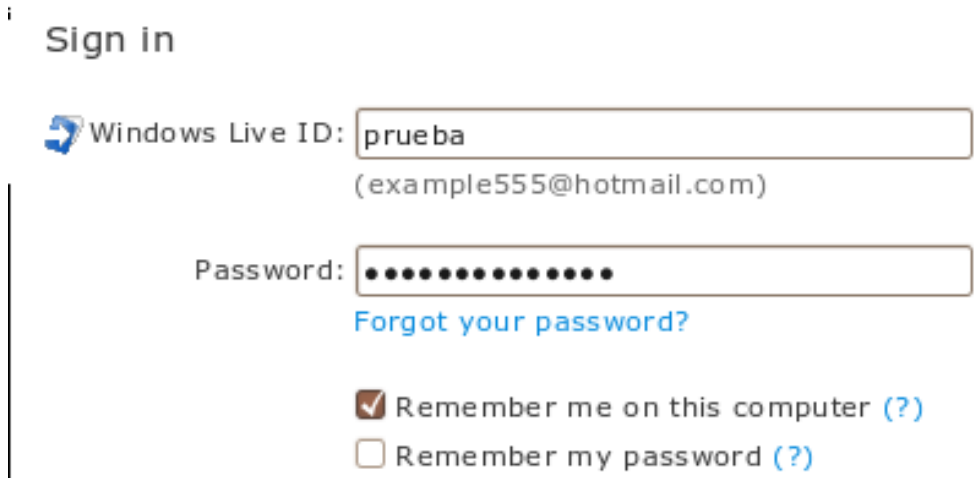
Departamento de Informática e Ingeniería de Sistemas
Universidad Zaragoza

Claves de un solo uso

- Las claves son fáciles de comprometer
- Si tienen un solo uso resuelven el problema
- Normalmente se basan en algún sistema de almacenamiento de las claves
- También en sistemas que calculan las claves de manera sucesiva
- Y en sistemas de autentificación con doble factor

Pedir la clave

- Si es web: siempre, en una página 'segura' (si no, no podemos estar seguros de que el sitio es quien dice ser).
- Si se transmite: siempre cifrada.
- Mostrar la clave (¡no! ... ¿no?)



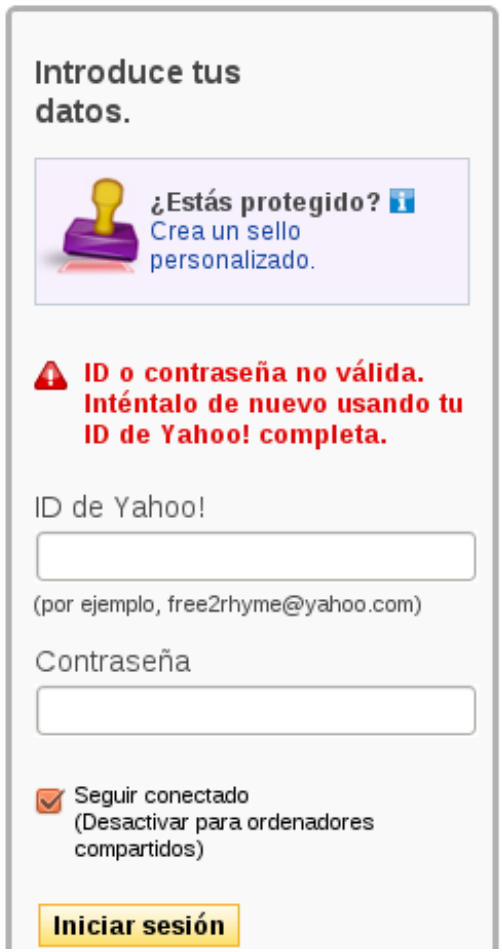
Opción mostrar la clave

Pedir la clave

- ¿Qué avisos?
  - ¿Usuario incorrecto?
  - ¿Clave incorrecta?
    - Según la decisión, tener en cuenta las consecuencias...

Prueba con estos consejos.

- **¿Están encendidos los indicadores "Bloq.Mayús" o "A" del teclado?**
  Si es así, presiona la tecla "Bloq Mayús" antes de continuar.
- **¿Has escrito bien tu ID o contraseña? ¿No te acuerdas de ellas?**
  Puedes recuperar tu ID y/o contraseña si nos confirmas algunos datos.
- **¿Sigues sin poder entrar?**
  Consulta nuestra ayuda de entrada.
- **¿Te olvidaste de introducir tu ID de Yahoo! completa?**
  De ser así, recuerda usar tu ID de Yahoo! completa (por ejemplo, free2rhyme@yahoo.com) para iniciar sesión.

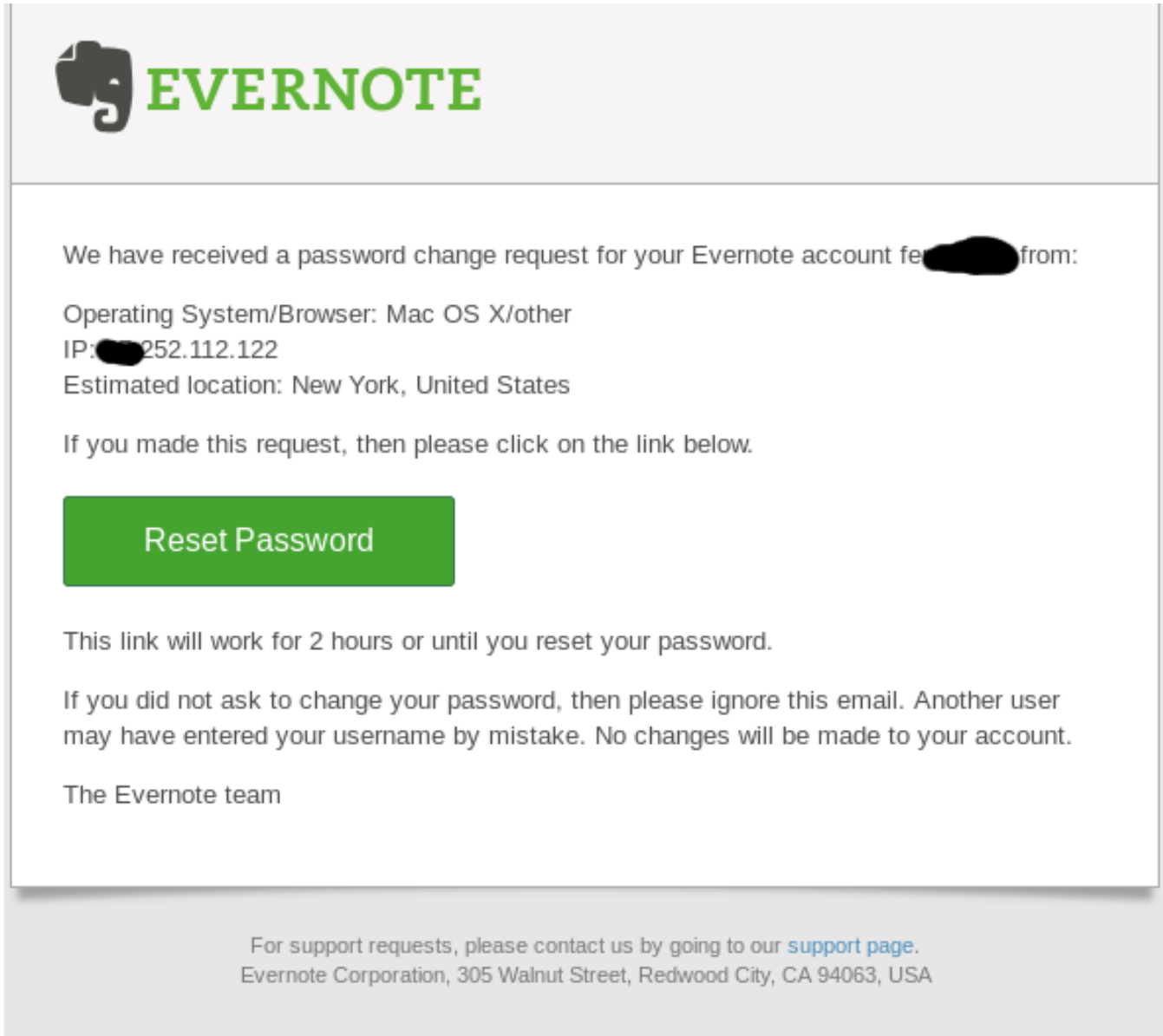


Sistemas de recuperación de la clave

- Las preguntas secretas sólo son claves más débiles
  Aunque...

  `https://www.owasp.org/index.php/Choosing_and_Using_Security_Questions_Cheat_Sheet`
- Las pistas 'hints', parecido
- Enviar la clave (al correo de registro, correo físico, SMS, ...).
  Preferiblemente sistemas 'fuera de banda'.
- Enviar un enlace para reinicializarla:
  - expiración del enlace,
  - url o identificador no predecible,
  - posibilidad de re-enviarlo
  - puede haber filtros anti-spam
  - ...
- O una clave temporal

El caso de Evernote



EVERNOTE

We have received a password change request for your Evernote account fe[redacted] from:

Operating System/Browser: Mac OS X/other
IP:[redacted]252.112.122
Estimated location: New York, United States

If you made this request, then please click on the link below.

Reset Password

This link will work for 2 hours or until you reset your password.

If you did not ask to change your password, then please ignore this email. Another user may have entered your username by mistake. No changes will be made to your account.

The Evernote team

For support requests, please contact us by going to our support page.
Evernote Corporation, 305 Walnut Street, Redwood City, CA 94063, USA

Mas consejos

- La autentificación es tan segura como el sistema de gestión de usuarios
- Utilizar la forma mas apropiada de autentificación de acuerdo al bien que se protege (claves, SMS, ...)
- Re-autentificar al usuario para transacciones de valor alto y áreas protegidas
  - Autentificar la transacción, no el usuario.
- Las claves son fáciles de romper, no son válidas para sistemas de valor alto.

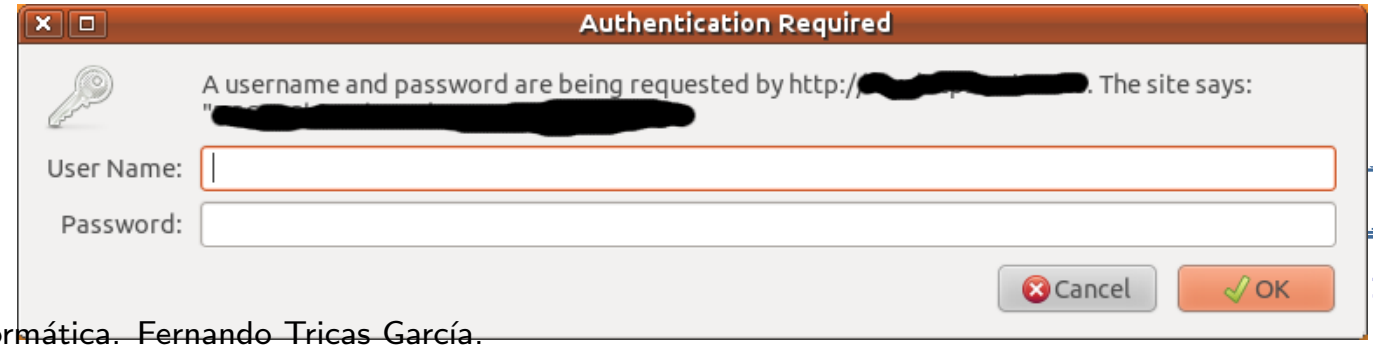
En la web

Autentificación básica ('basic') y basada en resumen ('Digest')

- La básica lo manda todo en texto claro. No debería usarse mas que con SSL (toda la comunicación, las credenciales se envían en cada paso).
- HTTP 1.0 Digest: información 'ofuscada' en Base64
- HTTP 1.1 Digest: reto y respuesta. Adecuada para cosas de poco valor.

Los problemas:

- Transmisión insegura
- Pueden ser atacadas mediante repetición y 'man in the middle'
- Necesitan SSL para tener confidencialidad e integridad
- Interfaz inconsistente
- No proporciona mucho control a la aplicación



En la web. Autentificación basada en formularios

Utilización amplia, mucha gente acostumbrada a usarla:

- Si es posible, reutilizar algún componente confiable
- Y pensar bien los casos de uso (todo va bien, algo va mal, ...)

Los problemas:

- Ataques de repetición y de interposición
- Va en texto claro si no se usa HTTPS
- Posibilidad de elevación de privilegios (si conseguimos que se ejecute otra cosa ...)
- Poco control sobre las claves
- Reutilización de sesiones si no se hace con cuidado

En la web. Autentificación basada en certificados

¿Quién no tiene alguno?

- Se emite un certificado (o se usa uno que alguien emitió)
- Su calidad se basa en la infraestructura de clave pública (depende de quién lo haga)

Problemas:

- Compartir PCs. Cambiar de PC.
- Gestión de certificados en el navegador.
- Revocación de certificados no controlados por nosotros
- No todas las certificadoras están aceptadas en todos los navegadores. usabilidad.
- Coste

En la web. Autentificación integrada

- Microsoft IIS + ASP.NET
- Similar a la existencia de certificados (se usa Kerberos)

Autentificación fuerte

En general, algo que tienes + algo que sabes.

- Claves de un solo uso (sistemas baratos).
  - Problemas de interposición
- Certificados 'soft'
  - Mismos problemas que cualquier sistema con credenciales automatizadas
- Certificados 'hard'
  - Soluciona algunos problemas
  - Pero, al final, es información digital
- Pregunta-respuesta. Se toma un valor, se procesa criptográficamente y se pregunta al usuario.
- SMS: se envía algún código al usuario que debe teclearlo
  - No enviar información sensible
  - Alguien puede enviarlos por nosotros (y el usuario no se dará cuenta)

Atención

- La validación se hace en el servidor
- Autentificación en negativo: un usuario es anónimo hasta que prueba que no lo es (y no al revés).
- Preguntas con varios campos
  Mal:

  select $*$ **from table where** username=username **and** password=password
  - La clave se debería usar para determinar si se da o no, no en la consulta
  - Comprobar que sólo se devuelve 0 o 1 resultado
- No dejar cuentas por defecto
- No usar nombres de usuarios predecibles (mejor dejar que los usuarios elijan)
- No permitir claves cortas, vacías, palabras del diccionario, ...

Atención a ...

- Claves por defecto
- Escalada de privilegios
- Acceso físico a los recursos
- Adivinar las claves: diccionarios, fuerza bruta, valores precalculados, ...
- 'Escuchar' las claves en la transmisión
- Repetición de la transimisión
- Degradar la fortaleza de la autentificación
- Servidores 'impostores'
- Ataques 'Man-in-the-Middle'
- Secuestro de sesiones
- 'Grabadores' del teclado, troyanos, virus
- Ataques 'desconectados' (si se consigue información 'sensible', explorarla 'en casa')
- Ingeniería social
- Explorar la basura, robo de identidad, ...

En todo caso...

- Cormac Herley, Dinei Florencio, 'Where Do Security Policies Come From?', Junio 2010.

  `http://research.microsoft.com/apps/pubs/?id=132623`

- Joseph Bonneau, Sören Preisbusch, 'The password thicket: technical and market failures in human authentication on the web' (The Ninth Workshop on the Economics of Information Security, WEIS 2010).

  `http://weis2010.econinfosec.org/papers/session3/weis2010_bonneau.pdf`

- Bill Cheswick, resumido en 'Password and Account Lockout Better Practices'

  `http://www.owasp.org/download/jmanico/owasp_podcast_76.mp3`

  `http://www.clerkendweller.com/2010/11/2/Password-and-Account-Lockout-Better-Practices`

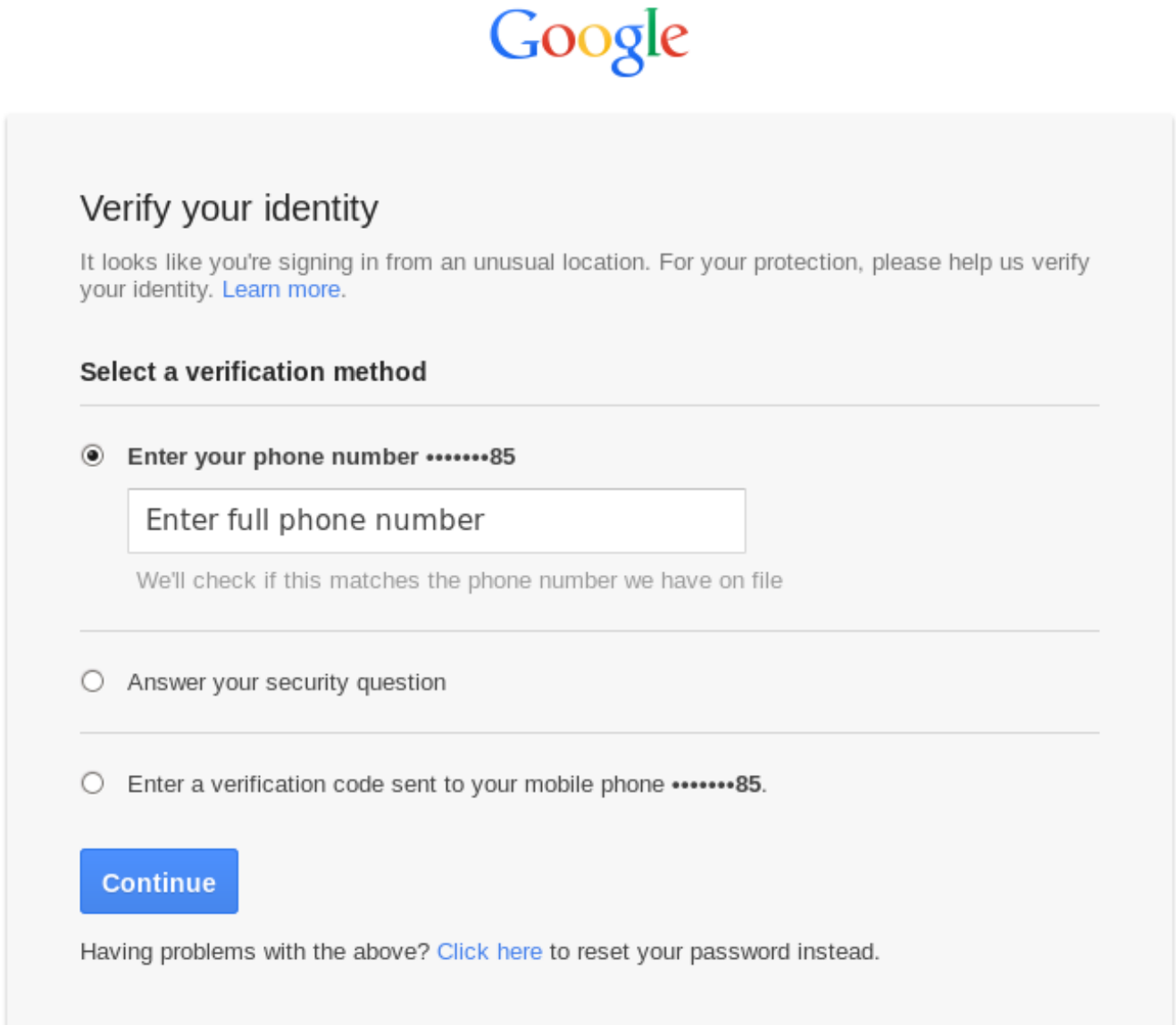
Algunas listas de consejos

- Autentificación:

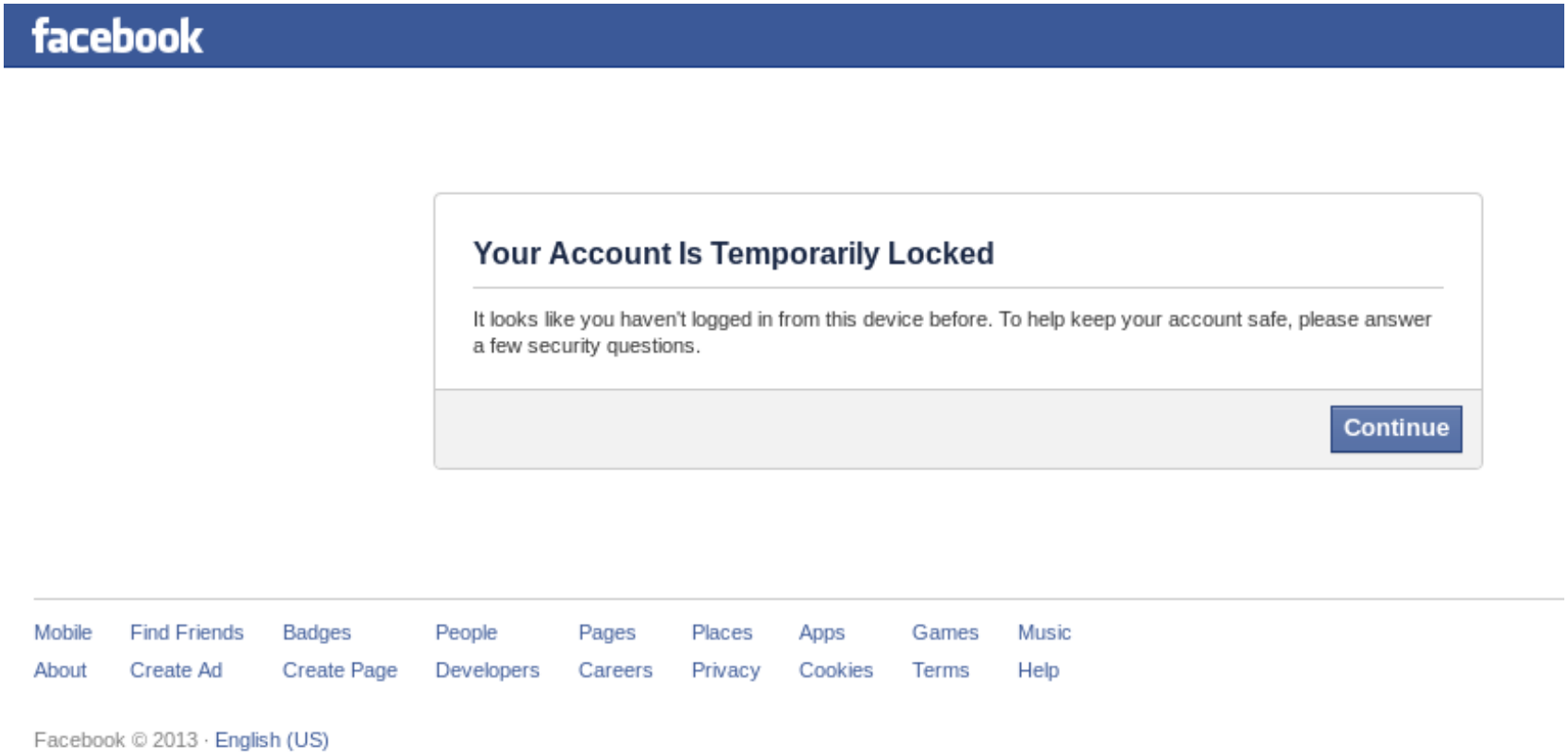
  `https://www.owasp.org/index.php/Authentication_Cheat_Sheet`
- Recordatorio de claves:

  `https://www.owasp.org/index.php/Forgot_Password_Cheat_Sheet`

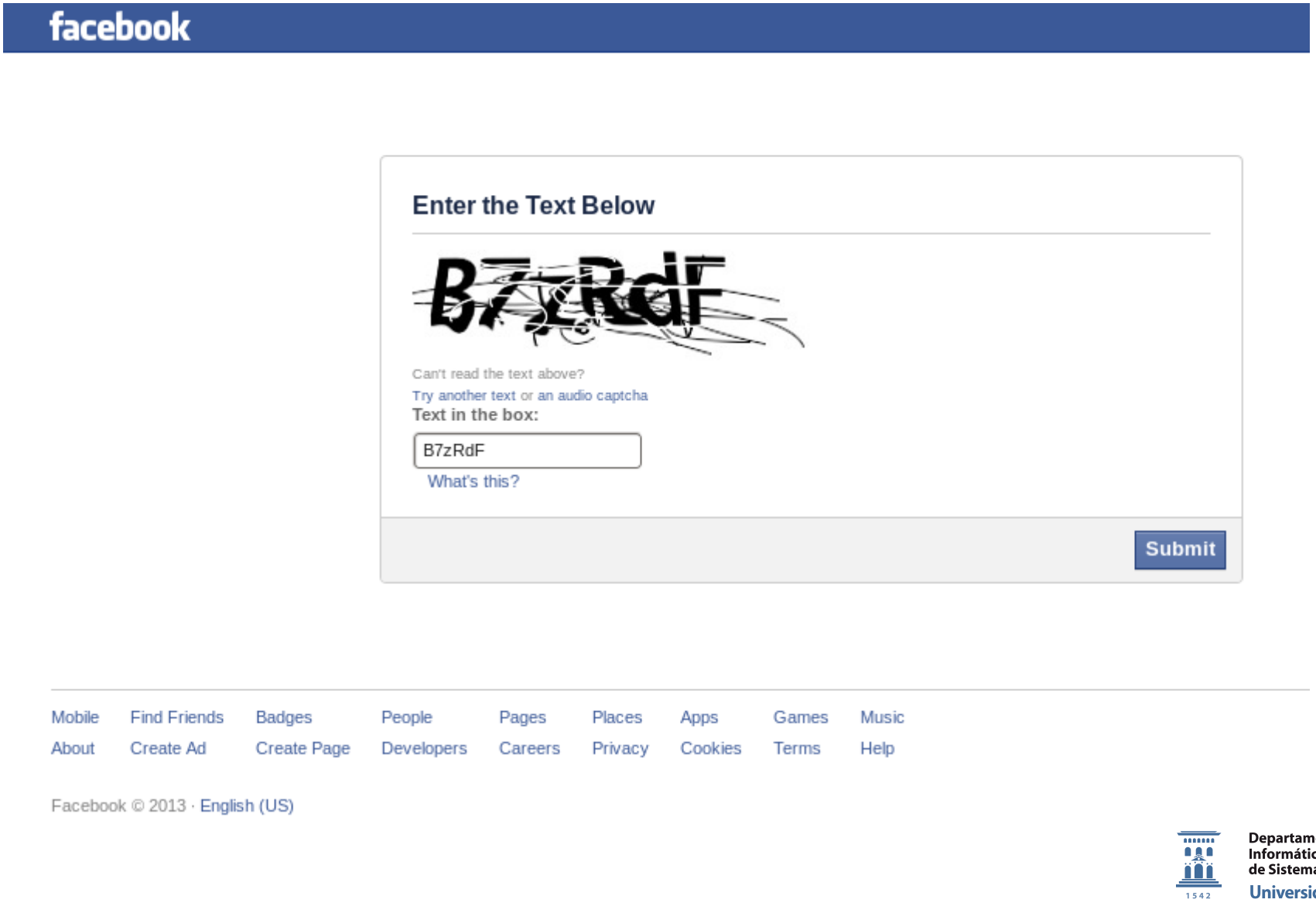
El caso de GMail



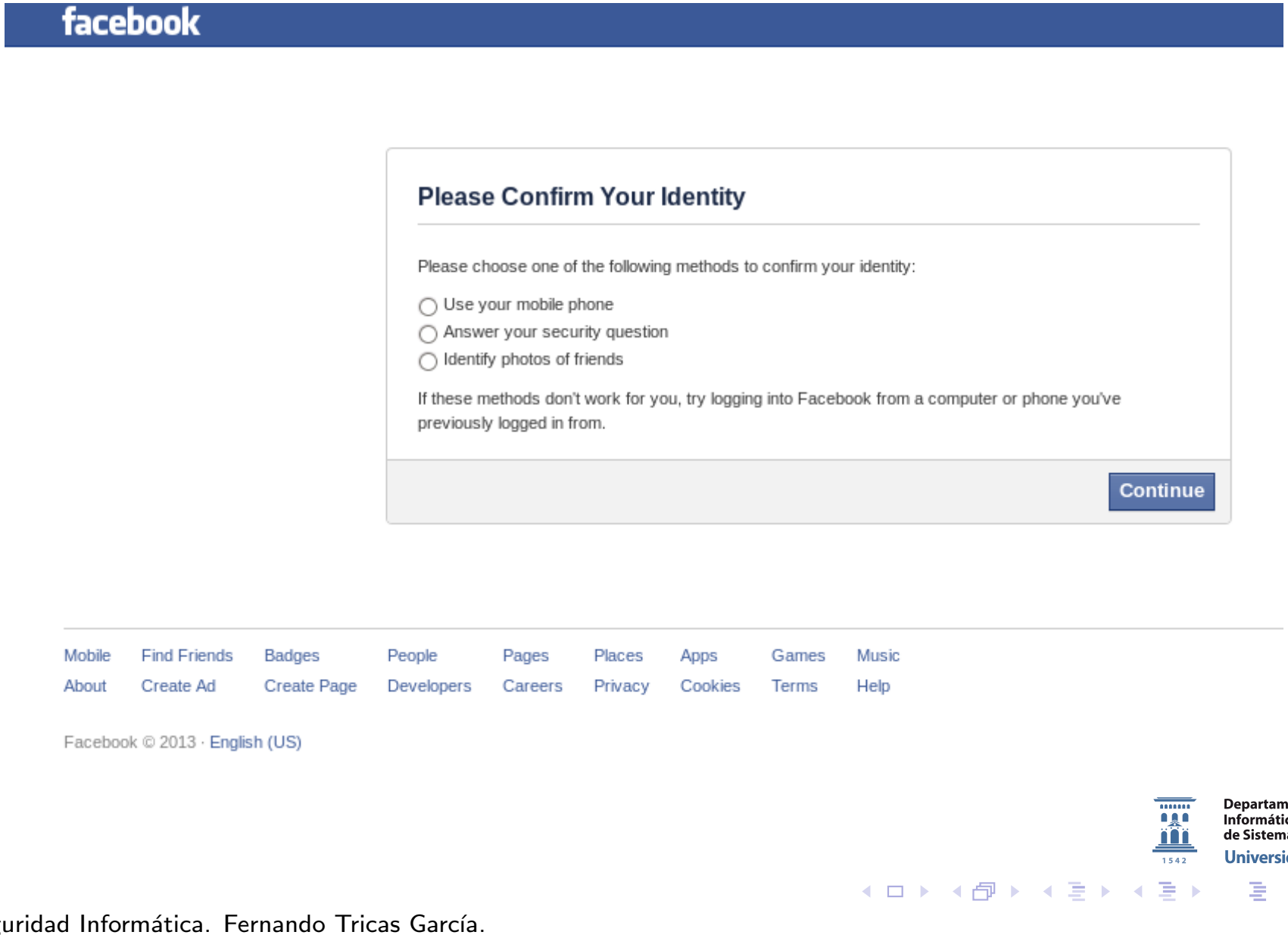
El caso de Facebook (I)



El caso de Facebook (II)

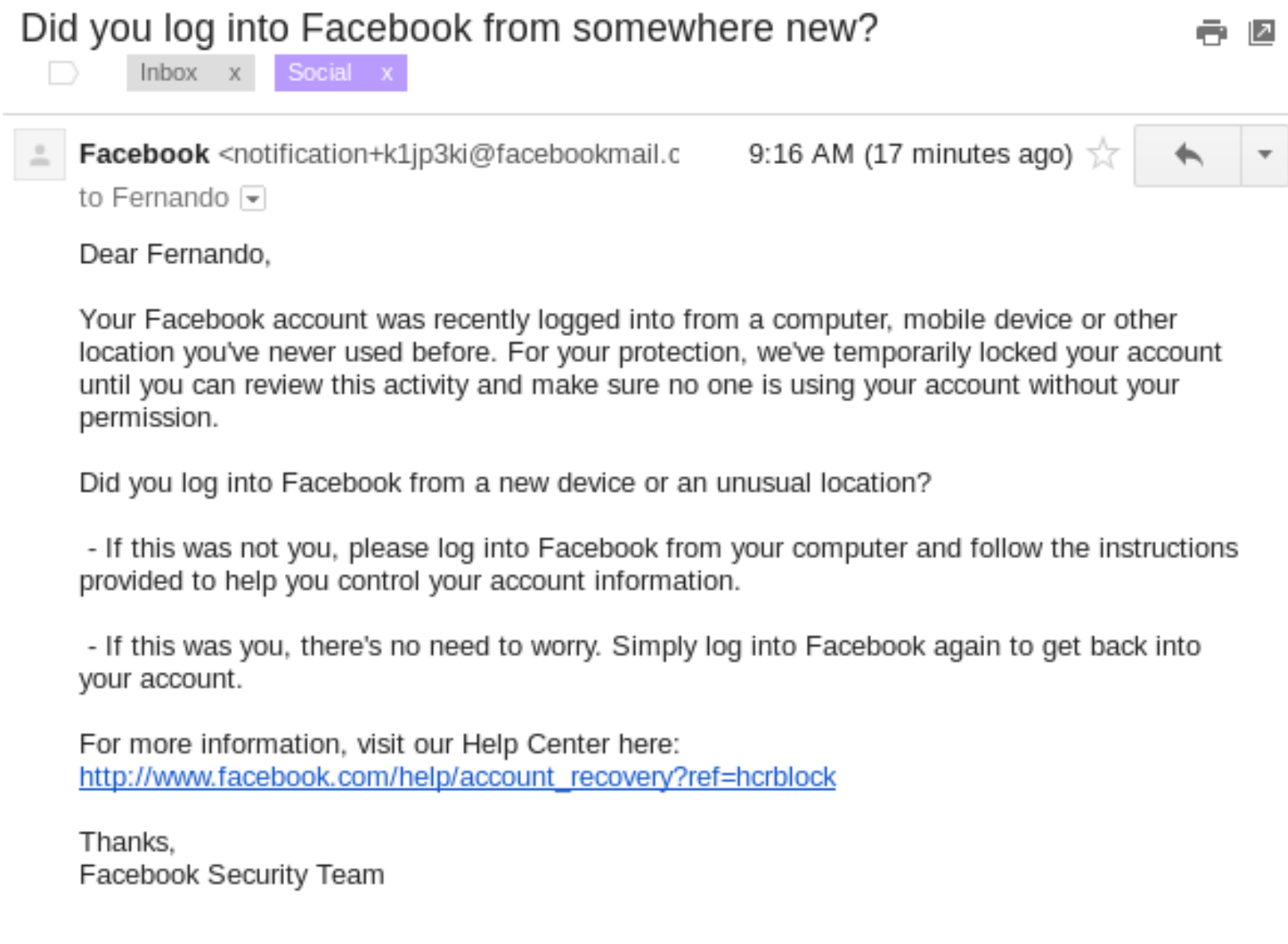


El caso de Facebook (III)



El caso de Facebook (V)

(Me salto el IV, son fotos reales de amigos)



Did you log into Facebook from somewhere new?

Inbox x Social x

Facebook <notification+k1jp3ki@facebookmail.c 9:16 AM (17 minutes ago)

to Fernando

Dear Fernando,

Your Facebook account was recently logged into from a computer, mobile device or other location you've never used before. For your protection, we've temporarily locked your account until you can review this activity and make sure no one is using your account without your permission.

Did you log into Facebook from a new device or an unusual location?

- If this was not you, please log into Facebook from your computer and follow the instructions provided to help you control your account information.

- If this was you, there's no need to worry. Simply log into Facebook again to get back into your account.

For more information, visit our Help Center here:
http://www.facebook.com/help/account_recovery?ref=hcrblock

Thanks,
Facebook Security Team

Autentificación basada en la máquina

- A veces se utiliza la IP (cortafuegos)
- DNS (junto con la IP)
- MAC (*Medium Access Control*)
- Otros identificadores (identificador del procesador en Pentium III)

Se trata de identificadores aportados por una fuente no confiable!! Un atacante puede hacer que el cliente proporcione los datos que le resulten más convenientes.

Algunos identificadores . . .

- IP y DNS son más fiables en cierto sentido: aunque consiga falsearlas (*IP spoofing*)
  - Necesita hacerlas llegar al objetivo
  - Necesita ser capaz de leer la respuesta
    Habitualmente, estando en el mismo segmento de red
  - No son fáciles de realizar (aunque cada vez más)

Algunos identificadores . . .

- Los ataques basados en DNS también se pueden realizar falseando la IP
- Otra forma es falseando las memorias intermedias (*cache poisoning attack*)
- Más sencillos de realizar (incluso por errores del administrador)

Identificadores físicos

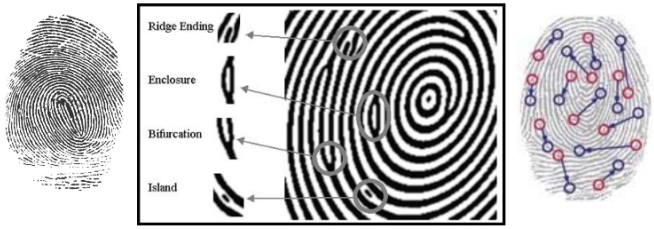
Basados en algo que el usuario tiene

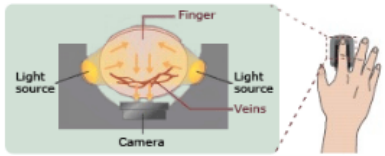
- Llaves, tarjetas magnéticas, tarjetas con chip
- Difusión amplia, pero con problemas
  - Hacen falta dispositivos adicionales
  - Teclear el número de la tarjeta no es lo mismo que tenerla
  - Pérdidas, robos, ...
  - Fáciles de replicar (bandas magnéticas), en algunos casos sin tener el original (algunas llaves, y cerrajeros hábiles)

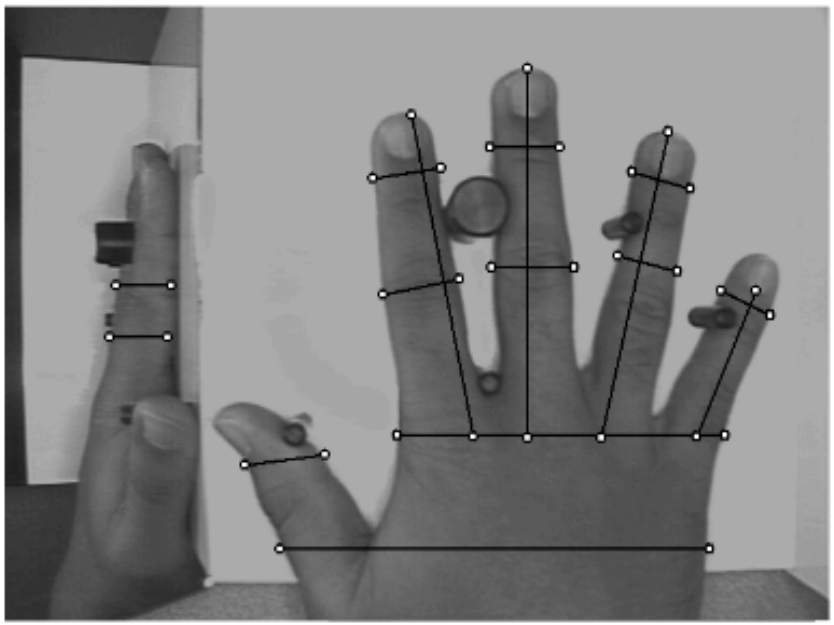
Biometría ¿Identificación o Autentificación?

Basadas en la medición de características físicas o de comportamiento

- Huellas dactilares, venas, ...







Departamento de Informática e Ingeniería de Sistemas
Universidad Zaragoza

Hace muuucho tiempo...

12:4 *Jefté reunió a todos los hombres de Galaad y atacó a Efraím. Y los de Galaad derrotaron a los efraimitas, que decían despectivamente: "Ustedes, los de Galaad, son fugitivos de Efraím, en medio de Manasés".*

12:5 *Galaad ocupó los vados del Jordán para cortarle el paso a los efraimitas. Y cuando un* **fugitivo de Efraím intentaba pasar**, *los hombres de Galaad* **le preguntaban**: *"¿Tú eres de Efraím?". Si* **él respondía** *que no,*

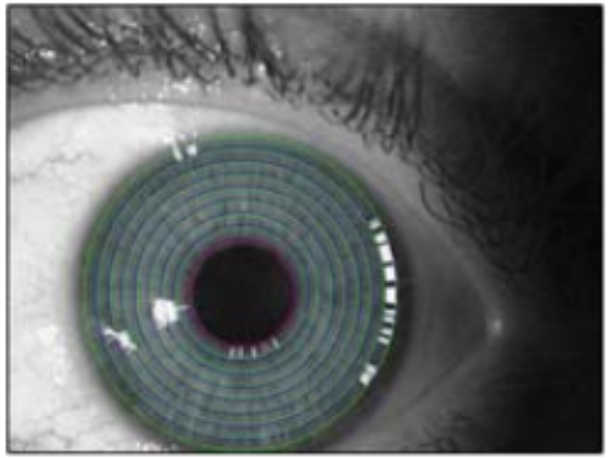
12:6 *lo* **obligaban a pronunciar** *la palabra* **"Shibólet"**. *Pero él decía* **"Sibólet"**, *porque no podía pronunciar correctamente. Entonces lo tomaban y lo degollaban junto a los vados del Jordán. En aquella ocasión, murieron cuarenta y dos mil hombres de Efraím.*

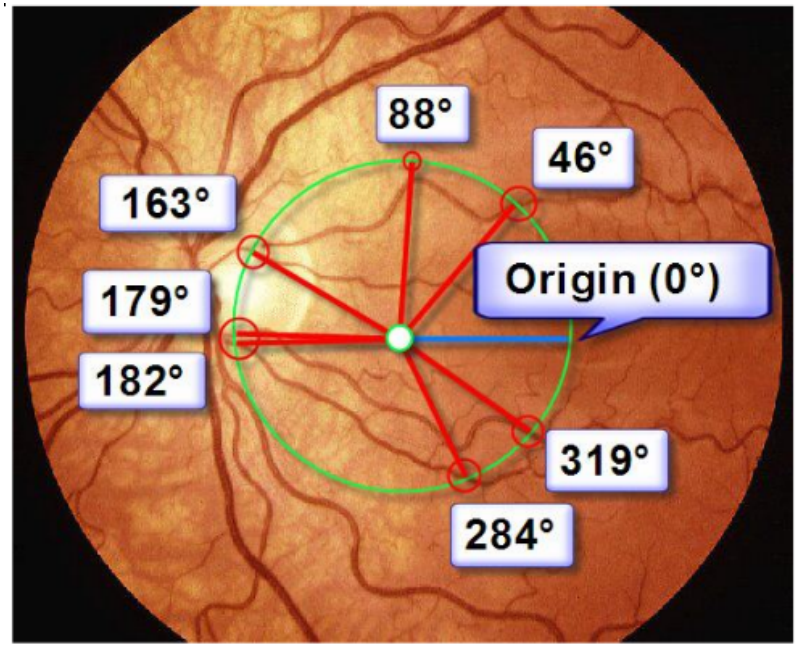
Libro de los Jueces

Departamento de Informática e Ingeniería de Sistemas
Universidad Zaragoza

Biometría

- Iris, retina, ...





http://www.blackhat.com/presentations/bh-dc-08/Franken/Presentation/bh-dc-08-franken.pdf

Zac Franken, Black Hat DC Briefings 2008

Biometría

- Firma, firmas de voz, ...
- Conveniente, porque no se olvida, ni se pierde
- También hay problemas ...

Departamento de Informática e Ingeniería de Sistemas
Universidad Zaragoza

Biometría

Problemas:

- Dispositivos específicos (y caros)
- ¿Y la seguridad del dispositivo de entrada?
- Una vez comprometido, no es posible cambiar!
  Mejor complementarlos con guardias 'de verdad'
- ¿Y si estamos enfermos, nerviosos?
- Son únicos, pero no son secretos
- ¿Misma 'clave' en muchos sitios?

Biometría

Más problemas

- 'Robar' huellas

`http://www.cse.chalmers.se/edu/year/2013/course/EDA263/oh10/L03_DL2_Biometricaccessprotectiondevices.pdf` (Copia del original)

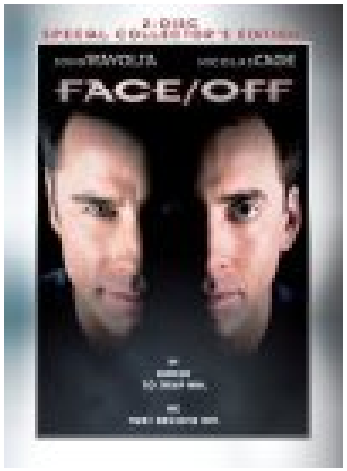
Lisa Thalheim, Jan Krissler, Peter-Michael Ziegler. 'Body Check'

`http://news.bbc.co.uk/2/hi/science/nature/1991517.stm`

Tsutomu Matsumoto. 'Doubt cast on fingerprint security'

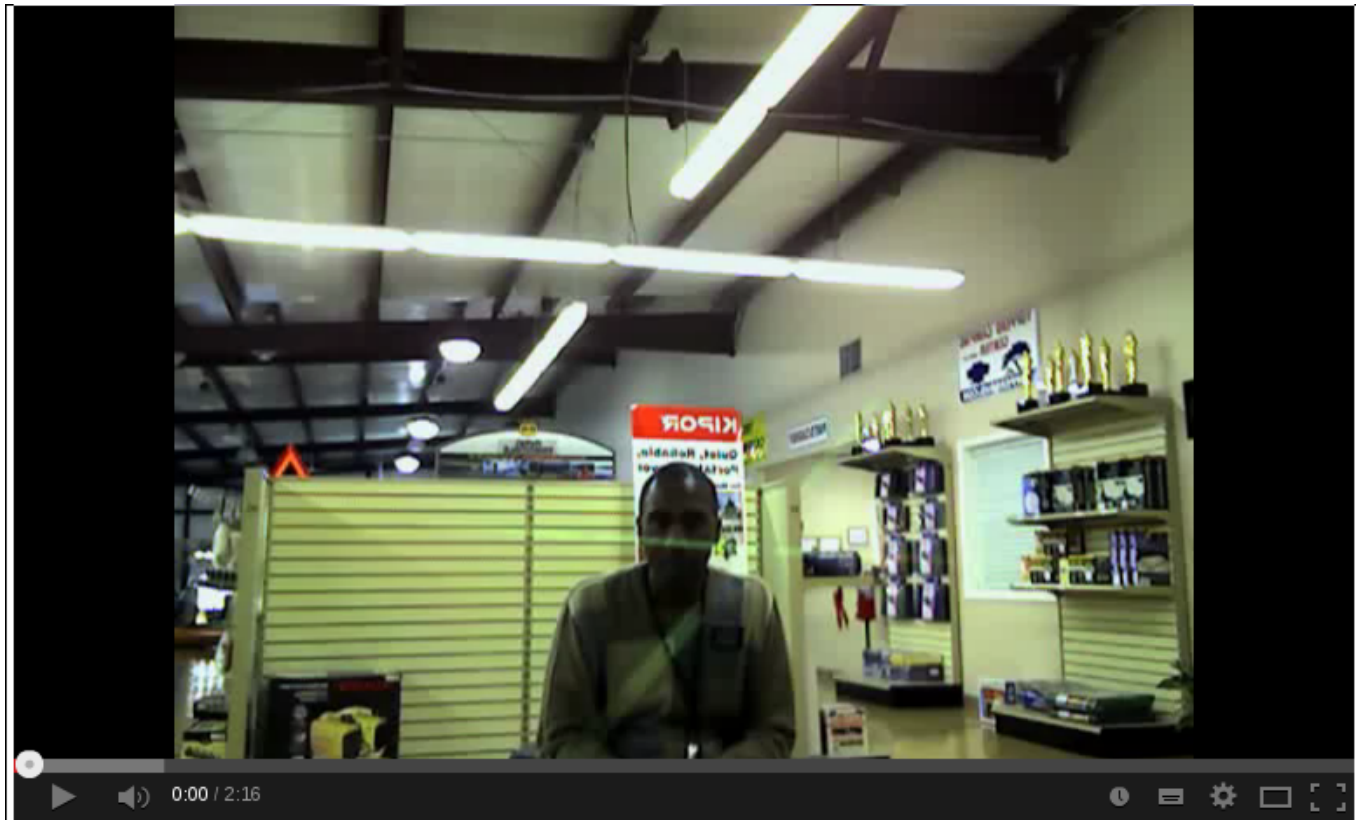
Biometría. Problemas

- ‘Robar’ partes del cuerpo de uno!!



- ¿Y la intimidad?

Biometría. A veces las cosas fallan



'HP computers are racist'

`http://www.youtube.com/watch?v=t4DT3tQqgRM`

Criptografía

- Se utiliza un secreto (digital) y las matemáticas
- Análogo digital a tener un objeto físico
- Ya no hacen falta dispositivos especiales, pero todos los problemas persisten
- Es fácil de robar

Autentificación y defensa en profundidad

- Mezclar técnicas
  Algunos ejemplos:
  - Objeto + clave (Cajeros automáticos)
    O clave + objeto (banca electrónica)

  - Claves cifradas (cada vez que vamos a usar una clave, necesitamos otra para descifrarla)