Curso: (62612) Diseño de aplicaciones seguras

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 II: Seleccionando tecnologías

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

Seleccionando tecnologías

- Comparar y contrastar, para seleccionar lo mas adecuado a los requerimientos
- Normalmente seleccionamos con cuidado, pero no teniendo en cuenta odos los factores
- Vamos a dar algunas ideas

Departamento de Informática e Ingeniería de Sistemas
Universidad Zaragoza

El lenguaje

- Un fallo frecuente es elegir un lenguaje sin tener en cuenta su impacto en la seguridad
- En general, cuantas más comprobaciones estáticas haga el compilador, más fiables serán los programas

Departamento de Informática e Ingeniería de Sistemas
Universidad Zaragoza

Algunas características interesantes

- Java y su 'security manager' (*sandboxing*)
- Perl y su 'taint mode' (seguimiento de las variables para controlar las entradas de usuario)
- PHP y sus 'magic quotes' (pero ...)
- Casi todos los lenguajes modernos y sus comprobaciones de límites (*bound checking*)
- Casi todos los lenguajes proporcionan mecanismos para evitar que los datos pasen al sistema de ficheros (*swapping*, **mlock()** en C, por ejemplo)

Departamento de Informática e Ingeniería de Sistemas
Universidad Zaragoza

Objetos distribuidos

- La arquitectura cliente/servidor cada vez más predominante
- Basada en objetos distribuidos (CORBA, DCOM, RMI, EJB, servicios web, . . .)
- Disponibilidad remota de recursos, redundancia, paralelismo
- Contenedores: invocación de programas basados en componentes y conjuntos de componentes distribuidos diferentes que pueden interactuar

Departamento de Informática e Ingeniería de Sistemas
Universidad Zaragoza

¿Qué mirar?

- Identificación
- Autentificación
- Cifrado
- Delegación
- Representación
- Interacciones
- ...

Departamento de Informática e Ingeniería de Sistemas
Universidad Zaragoza

El sistema operativo

- Los sistemas modernos están divididos en código del núcleo y código de usuario.
- Los programas de usuario corren en 'modo usuario' y, ocasionalmente, requieren servicios del núcleo.
- Muchos servicios críticos se ejecutan en el espacio del núcleo.
- Habitualmente el núcleo tiene algún modelo de seguridad que gestiona el acceso a los dispositivos, ficheros, procesos y objetos.

Sistema operativo: los procesos

- El mecanismo subyacente al modelo de seguridad y la interfaz con ese mecanismo cambia notablemente entre sistemas.
- Independientemente de eso, la idea siempre es la misma: un proceso de usuario no puede acceder a la memoria de otro proceso directamente.
- La comunicación entre procesos siempre se hace a través del sistema operativo.

Departamento de Informática e Ingeniería de Sistemas
Universidad Zaragoza

Algunos sistemas operativos

Tienen modelo de seguridad

- Windows NT/2000/XP/Vista/7
- Todos los sistemas tipo Unix

No lo tienen

- Ningún Windows inferior a Me
- PalmOS (Cuidado con la Palm e Internet!)
- En general, aquellos en los que todos los programas compraten espacio de direcciones

Algunos sistemas operativos

- Normalmente los diferentes módulos 'confían' en los otros.
- Esto es especialmente grave: en muchos casos, utilizamos 'drivers' proporcionados por terceros (sin poder auditarlos)
- Los núcleos no suelen incluir protección contra el propio núcleo: si hay un fallo, puede dar acceso a todo el sistema.
- Hay excepciones, (algunos Unix, *Trusted Match*, por ejemplo). En Windows no.

Tecnologías de autentificación

- Los problemas más frecuentes tienen que ver con la autentificación (si excluimos los fallos de los programas)
- Es importante elegir una tecnología adecuada
- Incluso sistemas bien diseñados tienen problemas por la mala elección de claves

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)

Departamento de Informática e Ingeniería de Sistemas
Universidad Zaragoza

Identificadores físicos

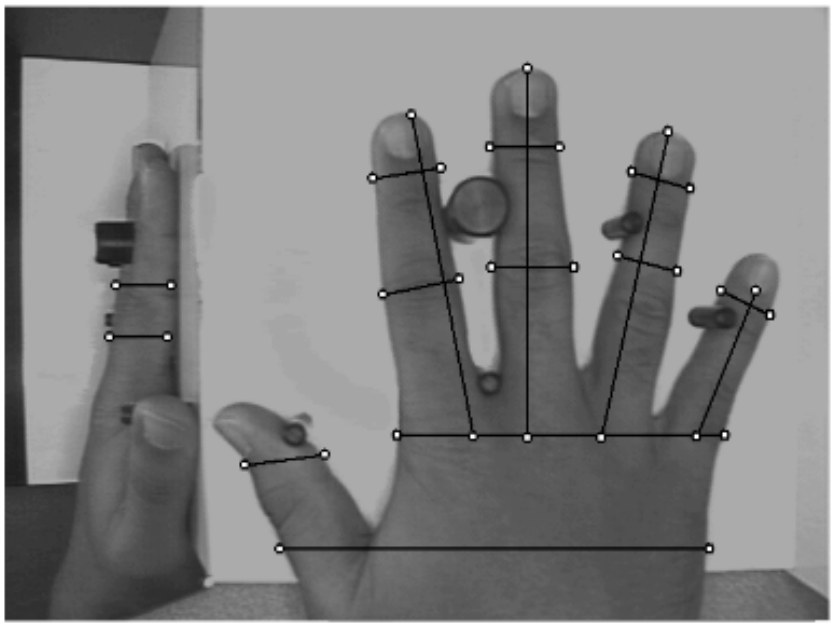
Basados en algo que el usuario tiene

- 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

Basadas en la medición de características físicas o de comportamiento

- Huellas dactilares, venas, ...



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,*

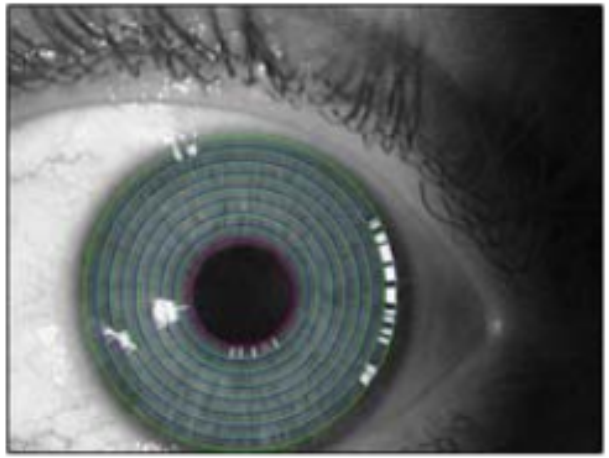
12:6 *lo* **obligaban a pronunciar** *la palabra* **"Shibólet"**. *Pero él decía* **"Sibólet"**, *porque no podía pronunciar correctamente. Entonces lo tomaban y lo degollaban junto a los vados del Jordán. En aquella ocasión, murieron cuarenta y dos mil hombres de Efraím.*

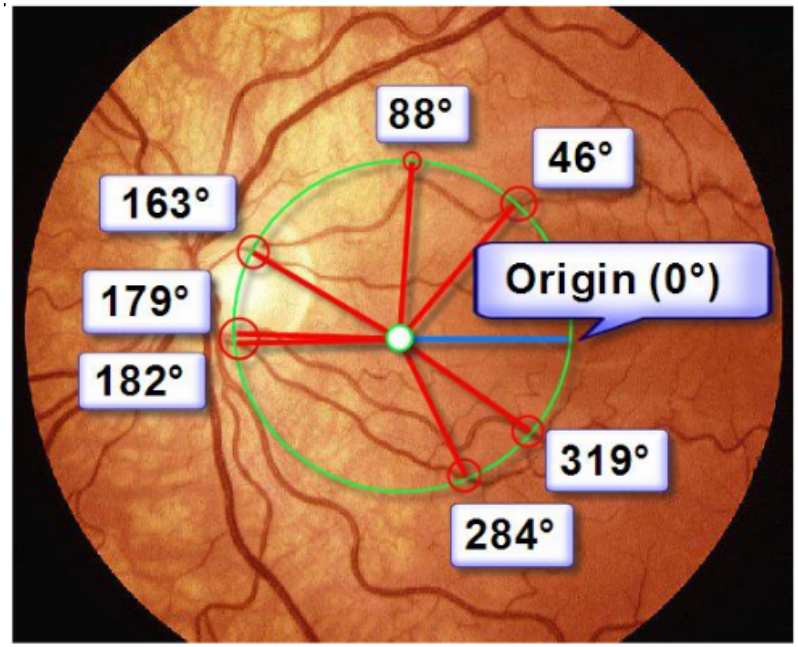
Libro de los Jueces

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

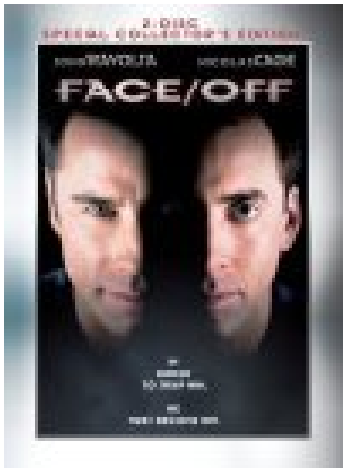
- 'Robar' huellas

`http://www.heise.de/ct/english/02/11/114/`
Lisa Thalheim, Jan Krissler, Peter-Michael Ziegler. Body Check

`http://news.bbc.co.uk/2/hi/science/nature/1991517.stm`
Doubt cast on fingerprint security
Tsutomu Matsumoto

Biometría. Problemas

- ‘Robar’ partes del cuerpo de uno!!



- ¿Y la intimidad?

Departamento de Informática e Ingeniería de Sistemas
Universidad Zaragoza

Biometría. A veces las cosas fallan

'HP computers are racist'

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

Departamento de Informática e Ingeniería de Sistemas
Universidad Zaragoza

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)