Seguridad en Sistemas Informáticos

Introducción

Área de Ingeniería Telemática
Dpto. Automática y Computación
http://www.tlm.unavarra.es/

Hoy

- Introducción a la asignatura

Seguridad en Sistemas Informáticos

- Objetivos
  - obtener el conocimiento suficiente para asegurar una red telemática de modo que sólo esté abierta a quien nosotros deseemos.
    - estudiando los tipos de ataques que se pueden realizar
    - diferentes partes qué hay que proteger en una red (la cadena de seguridad)
    - métodos de protección técnico (cortafuegos, IDSs, ACLs, blindaje de dispositivos...) como organizativo (auditorías, definición de políticas de seguridad, metodología adaptativa...).
  - cuando sea el **responsable de una red** pueda elaborar una política de seguridad en la que se identifiquen las vulnerabilidades de la misma para que posteriormente pueda adoptar las contramedidas más adecuadas a cada caso.

Seguridad en Sistemas Informáticos

- Optativa de 3º de Ing. Técnica en Informática de Gestión
  Área de Ingeniería Telemática
- 6 Creditos (3T + 3P)

- Teoría: Mikel Izal (mikel.izal@unavarra.es)
- Prácticas: Raul Cruz
- Página de la asignatura en:
  http://www.tlm.unavarra.es
  - La contraseña para matricularse es: s2011
  - Apúntese y elija grupo de prácticas

Organización

- Sesiones teóricas
- Practicas guiadas probando herramientas/ataques
- Trabajos en grupo
  - Trabajo 1 atacar un escenario vulnerable (penetration testing)
  - Trabajo 2 proteger un escenario vulnerable

    Análisis y presentación de debilidades en un escenario e implementación de soluciones
  - Demostración con ejemplos
- Composición de la nota final
  - 40% - Prácticas de laboratorio
  - 25% - Trabajo en grupo 1
  - 25% - Trabajo en grupo 2
  - 10% - Participación y critica de trabajo

Planning teoría

clase	Tema/trabajos
7 sep	Introducción
14 sep	Amenazas 1: intrusion y reconocimiento
21 sep	Amenazas 2: Intrusión y ataques a sistemas
28 sep	Amenazas 3: Ataques a la red
5 oct	Seguridad en la web
12 oct	
19 oct	Seguridad perimetral y cortafuegos
26 oct	**Presentaciones del trabajo 1**
2 nov	Criptografía
9 nov	Criptografia + **Trabajo 2 presentación y sesión trabajo en grupo**
16 nov	Monitorización y detectores de intrusion
23 nov	Redes privadas virtuales
30 nov	**Trabajo 2 propuestas**
7 dic	Seguridad en wifi
14 dic	Politicas de seguridad + ingeniería social
21 dic	**Presentaciones del trabajo 2**

Planning prácticas

clase	Tema/trabajos
6y8 sep	
13y15 sep	
20y22 sep	Intrusion: reconocimiento
27y29 sep	Intrusion: vulnerabilidades
4y6 oct	Ataques a la red
11y13 oct	Seguridad en web
18y20 oct	Laboratorio para el trabajo 1
25y27 oct	Firewalls
[1]y3 nov	
8y10 nov	Herramientas criptográficas
15y17 nov	
22y24 nov	Sistemas de monitorización y detección de intrusiones
[29n]y1dic	VPN
6y8 dic	Wifi Laboratorio para el trabajo 2
13y15 dic	Seguridad en wifi
20y22 dic	

Seguridad en Sistemas Informáticos

- Objetivos
  - obtener el conocimiento suficiente para asegurar una red telemática de modo que sólo esté abierta a quien nosotros deseemos.
    - estudiando los tipos de ataques que se pueden realizar
    - diferentes partes qué hay que proteger en una red (la cadena de seguridad)
    - métodos de protección técnico (cortafuegos, IDSs, ACLs, blindaje de dispositivos...) como organizativo (auditorías, definición de políticas de seguridad, metodología adaptativa...).
  - cuando sea el **responsable de una red** pueda elaborar una política de seguridad en la que se identifiquen las vulnerabilidades de la misma para que posteriormente pueda adoptar las contramedidas más adecuadas a cada caso.

¿Pero de que va la asignatura?

"It is easy to run a secure computer system. You merely have to disconnect all dial-up connections and permit only direct-wired terminals, put the machine and its terminals in a shielded room, and post a guard at the door"

F.T.Grampp y R.H.Morris

- Era una buena solución en los primeros tiempos de ordenadores centralizados pero hoy dependemos demasiado de la conectividad de los ordenadores

Por que?

- La sociedad de la información
  - La información es un bien valioso.
  - Se puede comprar y vender, hacer negocio con la comunicación, hay información sensible que hay que proteger...
  - El valor de la información sólo tiene sentido si se puede comunicar, enviar sólo a quien la ha comprado, hacer disponible a alguien pero proteger del resto...
- Problemas contra los que protegerse
  - Robo de información
  - Suplantación/robo de identidad
  - Destrucción de información o de servicio
  - Control de los recursos
  - ...

Seguridad en Sistemas Informáticos

- Queremos que nuestros ordenadores, redes y servicios sean usados remotamente pero sólo por quien tenga derecho
  - No es una cuestión de ética es una cuestión de propiedad
- Hace falta AAA : Authentication, Autorization and Acounting
  - **Authentication**: probar la identidad o el derecho a usar algo
  - **Autorization**: ser capaz de garantizar el uso a quien haya sido capaz de probar su identidad y negarlo a quien no
  - **Acounting**: apuntar quien y cuando se hace uso de un recurso
- El recurso puede ser el uso de un ordenador, de una red, de acceso a una base de datos... Comercio con la información

Seguridad en Sistemas Informáticos

- Para ello tendremos que conseguir garantizar diferentes propiedades y utilizarlas para conseguir los objetivos anteriores
  - **Confidencialidad**, ser capaces de comunicarnos sin que terceras partes puedan saber lo que decimos
  - **Integridad**, ser capaz de garantizar que lo que enviamos no sea modificado
  - **Disponibilidad**, ser capaz de garantizar que a los que tienen derecho a usar al recurso no puedan serles negado por usuarios no autorizados (Denegacion de Servicio)
  - ...

Inseguridad

- Al igual que sucede en la vida real, en las telecomunicaciones y en la informática la seguridad absoluta no existe.

- En el caso del mundo telemático las causas de la inseguridad son muy claras:

Causas de la inseguridad (I)

- Internet TCP/IP
  - Pensado en los años 60, desarrollado en los años 70, fines militares y de investigación
  - Militares: El enemigo está fuera e intenta destruir la red
  - Investigación: Red de colaboradores
- Internet se diseño para ser muy flexible y fiable

  (es decir, para no fallar nunca por avería de un nodo de comunicaciones)

  pero no para ser seguro

  No se pensó que Internet se emplearía más allá de unos pocos ordenadores muy controlados y a los que muy poca gente tuviera acceso en todo el mundo.
- Resistente a fallos y seguro son opuestos?
- **Protocolos no pensados para ser seguros**

Causas de la inseguridad (II)

- Las aplicaciones y programas informáticos son realizados por personas. Las personas tienen un pensamiento brillante pero imperfecto
- Un principio básico de la Ingeniería del software

  "**todo programa informático contiene imperfecciones y errores**"
- Reducir al máximo mediante técnicas de validación o corrección de errores que se realizan previamente a la distribución de un programa informático.
- Pero...
  - falta de tiempo
  - escasez de recursos
  - conocimientos insuficientes
  - ... No siempre se realiza correctamente
- **Gran parte del software informático que empleamos contiene agujeros de seguridad muy importantes.**

  ¿Falta de cultura de seguridad? ¿Si no se detecta un juego oculto en una aplicación como me voy a creer que se han eliminado los errores?
- **Errores del software**

Causas de la inseguridad (III)

- "*La paradoja de las redes informáticas*"

  Se construyen para facilitar el intercambio de información pero luego resulta que no deseamos compartir nuestra información con todo el mundo.

- La diferencia entre que nuestra información esté accesible para todo el mundo o sólo para quien nosotros queramos es solo **configuración**
  - Errores humanos de configuración
  - Configuración poco segura por defecto

    facilidad de uso contra seguridad
  - Preguntar al usuario no es la solución

    Ingeniería social
- "*Los errores humanos faciliten el 93 % de ataques informáticos*" (Fuente: Computer Security Institute).
- **Errores de configuración + errores humanos**

Causas de la inseguridad (IV)

- A pesar de todas las medidas de seguridad de un programa... a pesar de todos los cortafuegos y alarmas que queramos instalar... a pesar de revisar la configuración y asegurarnos de que nada puede pasar

  La operación del día a día de un sistema incluye humanos que tendrán el poder sobre el sistema

  - que pueden desactivar selectivamente medidas de seguridad (apuntar o elegir mal la contraseña, desactivar cortafuegos para solucionar un problema y olvidarse)
  - o ser engañados para ello
  - Se puede hackear al administrador en lugar del sistema?
  - Ingeniería social (seguro que todos habéis sido atacados con esto)

- **El factor humano**

¿Quien es el enemigo?

- Internet es una red cada vez mas extendida
  - Originalmente funcionaba más como una comunidad de colegas... más confianza
  - Al hacerse comercial y extenderse hay cada vez mas poblacion... y siempre hay alguien dispuesto a hacer el mal (y a pagar por que se haga)
  - Con el crecimiento también hay mas anonimato
  - La legislación no es global por lo que se puede atacar desde donde no sea ilegal
- **Evolución**
  - Hacking romantico
  - Ataques por encargo y espionaje industrial
  - SPAM, Phising y demas timos por internet
  - Troyanos, gusanos, botnets... secuestrando ordenadores
  - Hacking profesional, malware as a service

El enemigo (I)

- Qué es eso de los Hackers? (wikipedia)

  Hacker (del inglés *hack*, recortar) es el neologismo utilizado para referirse a un experto (véase Gurú) en varias o alguna rama técnica relacionada con las Tecnologías de la Información y las Telecomunicaciones: programación, redes de computadoras, sistemas operativos, hardware de red/voz, etc. Su entendimiento es más sofisticado y profundo respecto a los sistemas informáticos, ya sea de tipo hardware o software. Se suele llamar *hackeo* y *hackear* a las obras propias de un hacker.

- Experto informatico
  - connotaciones positivas o negativas según el ambiente. En sus origenes llamara alguien hacker es un halago
  - pero ha trascendido a la opinión publica como sinónimo de pirata informático (también llamado cracker)

    http://biblioweb.sindominio.net/telematica/historia-cultura-hacker.html

El enemigo (II)

- **Wannabe**: alguien que desea iniciarse.
- **Newbie**: novato en el Hacking.
- **Hacker**: persona que se dedica a hacer hacking (cualquier acción encaminada a conseguir la intrusión en un sistema. No conlleva la destrucción de datos ni la instalación de virus).
- **Lammer ó Script kiddie** : Principiante en el mundo del hacking que se las da de listo o que copia, descaradamente, el trabajo de otros hackers. Cuando se les descubre se les desprecia y se les expulsa del circulo en el que se han introducido.
- **Cracker ó Pirata**: Persona dedicada a la copia y distribución de software ilegal, tanto software comercial crackeado, como shareware, etc. No confundir este termino con el de hacker.
- **Phreaker**: persona que usa comunicaciones sin pagarlas o pagando menos de lo que corresponde (es una especie de Hacker telefónico).
- **Virii**: especialista en virus.

Manifiesto del hacker

.....Exploramos... y nos llamáis delincuentes. Buscamos ampliar nuestros conocimientos... y nos llamáis delincuentes. No diferenciamos el color de la piel, ni la nacionalidad, ni la religión... y vosotros nos llamáis delincuentes. Construís bombas atómicas, hacéis la guerra, asesináis, estafáis al país y nos mentís tratando de hacernos creer que sois buenos, y aún nos tratáis de delincuentes. Sí, soy un delincuente. Mi delito es la curiosidad. Mi delito es juzgar a la gente por lo que dice y por lo que piensa, no por lo que parece. Mi delito es ser más inteligente que vosotros, algo que nunca me perdonaréis. Soy un hacker, y éste es mi manifiesto. Podéis eliminar a algunos de nosotros, pero no a todos... después de todo, somos todos iguales.

- Suena muy bien...

  pero aun así si el ordenador lo he pagado yo y no quiero que nadie mas lo utilice...

Historias de Hackers

- En un principio Internet era más una comunidad de colegas, sus usuarios eran científicos de universidades.
  - Los protocolos eran simples y su objetivo es hacer que los ordenadores se entiendan entre si. (Recuerde RC y el funcionamiento del SMTP por ejemplo)
  - Es fácil que un usuario con conocimientos de los sistemas operativos pueda conseguir engañarlos para hacer cosas que se suponía que no debían hacer
- La red fue creciendo , muchas universidades y centros de investigación se conectaron, incluso aparecen empresas con la finalidad de ofrecer modems para que los científicos llamen desde su casa y usen los ordenadores de sus centros... empieza la Internet comercial poco a poco... los militares empiezan a ver que no controlan la red y se separa la red ARPANET y la red MILNET... Estamos en 1986...

Historias de Hackers

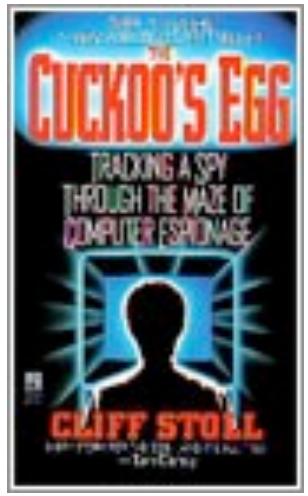
- En el LBL en Berkeley, Clifford Stoll es administrador del sistema UNIX
  - Un error en la contabilidad del uso del sistema (de $0.75) le hace descubrir que alguien usa el sistema como superusuario
  - En lugar de echarlo del sistema lo observa para ver como se conecta (instalando impresoras que imprimen lo que llega por los modems)
    - El intruso utiliza un fallo en el programa Emacs para ejecutar un fichero como root y convertirse en superusuario
  - La localización del intruso se prolonga durante meses, a través de redes telefónicas e Internet
    - Durante este periodo observa las tácticas del intruso para infiltrarse en ordenadores de militares y de universidades

Historias de Hackers

- El intruso del LBL se conecta a traves de los protocolos de Internet desde el sistema Unix del LBL en ordenadores conectados a Internet
- El intruso no sigue tácticas sofisticadas sino que se basa en la paciencia:
  - prueba contraseñas fáciles repetidamente en muchos ordenadores
  - En realidad ese método da muy buen resultado y encuentra muchos sistemas poco protegidos
- Todo esto se cuenta en una novela

  “El huevo del cuco” de Clifford Stoll

  De como Stoll paso de astronomo administrador de UNIX a experto en seguridad informática



Historias de Hackers

- La historia concluye en 1988 cuando el famoso Morris worm se convierte en el primer gusano en paralizar casi completamente Internet.
  - Explotaba por primera vez vulnerabilidades de buffer overflow
  - también buscaba contraseñas fáciles de forma automática (lo mismo que el intruso de LBL pero hecho por un programa)

- Empieza a parecer que en Internet no te puedes fiar de todo el mundo.
  - Es relativamente fácil engañar a algunos programas/maquinas si eres un experto
- La situación actual no es tan diferente

Enseñanzas

- No es tan difícil infiltrarse en ordenadores o engañar a los protocolos
  - A veces la paciencia importa mas que la habilidad
  - Los atacantes pueden ser pacientes pero los programas lo son aun más
  - El defensor tiene que defender todos los accesos pero al atacante le basta con encontrar uno sin proteger
  - Es fácil para un atacante experto contra un defensor inexperto
- Pero...
  - Los defensores pueden usar las mismas técnicas y ser pacientes
  - Si el defensor es un experto tiene ventajas claras: observar sin ser visto, acceso local a la maquina... puede apagar la maquina o la red

Despues...

- Internet comercial
- Aparecen los virus y luego los gusanos y similares
- Cada vez hay mas cosas robables en Internet
  - Identidad y demás datos personales
  - Credenciales bancarias
  - Cuentas de voz sobre IP
  - Cualquier otra cuenta que te permita comprar
  - Cualquier otra cuenta que te permita suplantar la identidad
  - Robo sin mas de recursos de CPU, para almacenar información peligrosa o para romper contraseñas o enviar spam
  - Y eso solo a nivel del usuario normal... espionaje Industrial...
- Aparecen defensas: antivirus, cortafuegos, IDSs, auditorias

Enumerando lo innumerable

- Herramientas de seguridad se basan en buscar o evitar patrones de ataques conocidos
- **Badness enumeration**

  (permitir por defecto)
  - Necesitamos una lista de lo que no se puede hacer.
  - Buscamos o filtramos ataques conocidos
  - Esto es lo que hacen los antivirus
  - Problema, no detiene a los ataques nuevos, es puramente reactivo
  - Hay quien ha puesto esto en "10 peores ideas de seguridad"
- **Goodness enumeration**

  (denegar por defecto)
  - Es mas fácil hacer la lista de las cosas que se pueden hacer (los usuarios las pedirán)
  - No esta exento de problemas (también las cosas que se deben permitir son innumerables)
  - Aun así se considera mejor filosofía para un sitio que necesite mucha seguridad

Historias de hackers (y 2)

- 9 marzo de 2005: Suicidio de Costas Tsalikidis, Ingeniero de 38 años al cargo de la planificación de red de Vodafone-Grecia
- 10 marzo de 2005: Se comunica al presidente de Grecia que su teléfono móvil ha sido pinchado, al igual que el del alcalde de Atenas y al menos otros 100 altos cargos, incluido personal de la embajada de EEUU

  Durante casi un año

  No se han encontrado grabaciones pero dado la facilidad con que podían hacerse se supone que se han grabado conversaciones
- Es el cybercrimen (conocido) con más potencial de haber captado secretos de estado

Historias de hackers (y 2)

- Se descubren modificaciones en el software de los conmutadores que conmutan llamadas entre terminales moviles del operador o entre terminales móviles y otros operadores
- Las modificaciones afectan a las capacidades que tienen los conmutadores de redirigir llamadas para permitir a la policía pinchar llamadas bajo orden judicial

  Aunque Vodafone-Grecia no tiene el interfaz gráfico para utilizar esas capacidades los conmutadores tienen software para copiar una llamada en una linea telefónica para que la escuche la policia. Aunque se supone que sin el interfaz gráfico no se puede activar
- El software encontrado redirige automaticamente las llamadas de ciertos números que tiene en una lista a otros números de una segunda lista (shadow)
- Aparte de modificar funciones del conmutador (listado de procesos, ocultar las listas de numeros, impedir detección de que los bloques donde esta el programa han sido modificados...)

Historias de hackers (y 2)

- La lista de números que se redirigen revela a quién estaban escuchando
- La lista de números shadow permite localizar a donde se enviaban las llamadas pero son móviles (el operador puede averiguar que los primeros se activaron en junio de 2004, 1 año antes)
- El programa permite a quien lo instalo acceso remoto para cambiar las listas de números
- Fue descubierto por casualidad porque al actualizar a la siguiente versión de soft del conmutador interfería con el envío de SMS lo que dio un fallo que fue detectado. A partir de ahí los logs y backups del sistema permitieron estudiar lo que había pasado
- Se desconoce como fue instalado el programa si fue una intrusión remota o si contaron con ayuda dentro del operador...

- La historia aqui: http://www.spectrum.ieee.org/print/5280

Enseñanzas

- Aunque sea un caso de escuchas en moviles en esencia es una infiltración a un sistema informático
- Al contrario que en ciertas películas en la realidad no hay ninguna ventana que te diga que tu sistema ha sido infiltrado

  Descubrirás los ataques mucho después cuando los daños sean importantes... si los descubres
- Los logs y backups periodicos son muy importantes para el análisis a posteriori
- Las funcionalidades que no usas pero aun asi están instaladas son muy peligrosas
- ...

Mas enseñanzas

- La seguridad es un tema muy difícil de esquematizar
  - No hay reglas que te digan lo que tienes que hacer
- En está asignatura aprenderemos técnicas y herramientas útiles para proteger un sistema/ red
  - Pero nada sustituye al experto que analice los resultados
  - Las herramientas harán sonar alarmas e informaran de situaciones anormales pero es el experto en seguridad el que tendrá que explicar lo que pasa y reaccionar

La situacion actual...

- La seguridad informática tiene cada vez más importancia
  - Incidentes, ataques a infraestructuras críticas y prevención de terrorismo digital
  - Mayor sensibilidad por la privacidad y protección de datos
- Insecurity as a service
  - Profesionalización de los atacantes y mafias
- La seguridad también genera negocio

Riesgo informático

- ***Riesgo = Vulnerabilidad x Amenaza***
  - Vulnerabilidad como consecuencia de las propias debilidades del sistema
    - qué software usamos y que debilidades tiene
    - cómo está configurado
    - qué protocolos utilizamos
  - Amenaza como consecuencia de factores externos
    - tipo de negocio: somos un banco o una universidad?
    - visibilidad
- Podemos actuar sobre lo primero
- Sobre lo segundo sólo podemos dedicar mas recursos

Contenidos de la teoría

- Protegiendo nuestras redes
  - Firewalls y otros filtros
  - Detección de Intrusos, sistemas de integridad
  - Criptografía y herramientas
  - Sistemas de AAA y VPNs
  - Redes inalámbricas
- Amenazas
  - Intrusión y ataques a sistemas
  - Ataques a la red
  - Programas maliciosos: virus, troyanos, gusanos, backdoors, rootkits...
  - Inseguridad en Web

Evolución de las amenazas

- De los hackers solitarios a la mafias organizadas
- Hacking romantico
- Gusanos
- Botnets
- Malware as a service
- Ataques dirigidos y ataques genericos
- Hacktivismo

Evolución de las amenazas

Ha oido hablar de... ?

- Virus
- Troyanos
- Gusanos (Worms)
- Botnets
- Keyloggers
- Backdoors
- Rootkits
- Denegacion de servicio
- ...

Conclusiones

- El peligro existe
  - **Internet no se concibió como algo seguro**
    - Robusto si, pero seguro no
    - Resistente a no funcionamiento accidental pero no frente a ataques del usuario
  - Los **programas informáticos** son **imperfectos**
  - Los **errores humanos** facilitan aun más el ataque
- Las herramientas ayudan a un administrador experto pero no lo sustituyen
- Como podemos protegernos?
- Próxima clase: Analicemos primero las amenazas...