GRUPO DE SEGURIDAD INFORMÁTICA

Fundamentos de la Seguridad Informática

Introducción

Plan

- Qué es la Ingeniería de la Seguridad?
- Areas de aplicación
- Conceptos y Propiedades básicas
- Algunas conclusiones sobre Seguridad Informática

Ingeniería de la Seguridad

- Construcción de sistemas de los que se pueda depender ante actos maliciosos y/o errores
- Como disciplina se focaliza en las herramientas, procesos, y métodos necesarios para diseñar, implementar y testear sistemas, así como adaptarlos a medida que sus ambientes evolucionan

Ingeniería de la Seguridad

- Requiere expertise interdisciplinaria:
  - Criptografía
  - Seguridad Computacional (Computer Security)
  - *Hardware tamper-resistance*
  - Métodos formales
  - Psicología aplicada
  - Métodos organizacionales y de auditoría
  - ...

Ingeniería de la Seguridad

- La mayoría de los sistemas de seguridad tienen requerimientos críticos de aseguramiento. Su falla puede:
  - Poner en peligro vidas y el medio ambiente (sistemas de seguridad y control de plantas nucleares)
  - Dañar seriamente una valiosa infraestructura económica (ATM y otros sistemas bancarios)
  - Poner en peligro la privacidad de las personas (sistemas de registro médicos)

Ingeniería de la Seguridad

  - Cuestionar la viabilidad de sectores de negocio (pay-TV)
  - Facilitar actos criminales (sistemas de alarmas)
- Aún la percepción de que un sistema es más vulnerable de lo que realmente es puede significar una traba a un desarrollo económico (e-commerce con tarjetas de crédito)

Ingeniería de la Seguridad

- Los requerimientos de seguridad difieren mucho de un sistema a otro
- Usualmente se necesita una combinación de
  - Autenticación de usuario
  - Integridad y trazabilidad de transacciones
  - Tolerancia a fallas
  - Mensajería secreta
- ...pero la mayoría de los sistemas fallan porque no se protegen los activos correctos, o se los protege mal

Areas de Aplicación

- Para entender el tipo de requerimientos de seguridad que los sistemas deben implementar se analizarán tres áreas de aplicación:
  - Bancos
  - Hospitales
  - Hogares

Aplicación 1: Un Banco

- El sistema de *bookkeeping* es el sistema core de un banco
  - Master files de los clientes y Registro de las transacciones diarias
  - Mayor amenaza: el personal del banco
  - Defensa: antiguos procedimientos de *bookkeeping* (el dinero puede ser solamente movido, nunca creado ni destruído)
  - Detección: sistemas de alarmas ante transacciones inusuales

Aplicación 1: Un Banco

- Una de las caras públicas del banco son sus ATMs
  - Autenticación de transacciones basadas en tarjetas de crédito y PINs, con defensas ante ataques externos e internos, es complicado de implementar
  - ATMs fueron el primer uso comercial a gran escala de la criptografía
- Sistemas de mensajes de alto nivel
  - Usados para mover grandes sumas de dinero
  - Ataques exitosos a esos sistemas son enormemente redituables

Aplicación 1: Un Banco

  - Defensa: mezcla de procedimientos de bookkeeping, control de acceso y criptografía
- Mayoría de bancos tiene una caja fuerte cuya alarma está en constante comunicación con una compañia de seguridad
  - Se usa criptografía para prevenir la manipulación de esta comunicación
- Presencia en Internet, con sitio Web y facilidades de e-banking
  - Mecanismos de protección: SSL/TLS, firewalls,...

Aplicación 2: Un Hospital

- La adopción de tecnologías informáticas genera requerimientos de seguridad particulares
  - Corrección de la información provista (como dosis de suministro de medicamentos) debe ser asegurada contra manipulación
  - Acceso (por parte de médicos por ejemplo) a información privada de los pacientes requiere el uso de herramientas de autenticación y cifrado

Aplicación 2: Un Hospital

- Se deben definir políticas de control de acceso para sistemas de registro de pacientes
  - Estos sistemas deben definir reglas de acceso que involucren roles
  - Estas aplicaciones han motivado la investigación en Role-Based Access Control (RBAC)
- El uso de registros “anónimos” de pacientes es difícil de implementar
  - La simple encriptación de nombres no es suficiente

Aplicación 2: Un Hospital

- Nuevas tecnologías pueden introducir riesgos que no son entendidos
  - Uso de bases de datos on-line de medicamentos, interrumpiendo el uso de formularios impresos de los mismos
  - Ataques que provoquen la degradación del servicio de la red (virus y DoS) pueden tener consecuencias graves para la práctica médica

Aplicación 3: el Hogar

- Mucha gente usa en sus hogares algunos de los sistemas descritos anteriormente
  - Sistema de e-banking para pagar facturas
  - Acceso encriptado a los datos médicos
  - Alarma de robos comunicada con sistema de seguridad
- Inmovilizador eléctronico en el auto, que envía un challenge encriptado a la llave
  - Evita robos de autos
  - Incentiva secuestros?

Aplicación 3: el Hogar

- Antiguos teléfonos celulares eran fácilmente clonables
  - GSM cuenta con un sistema de autenticación basado en un protocolo criptográfico *challenge-response*
- *TV set-top boxes* descifran películas si una suscripción es abonada; reproductores DVD usan mecanismos de control de copias basados en criptografía y *copyright marking*

Aplicación 3: el Hogar

- Contadores de electricidad y gas recargables usando tarjetas inteligentes
- Tecnologías similares usadas en universidades para el pago de fotocopias, lavaderos y dispensadores de bebidas
- *Internet of Things*

Definiciones y Conceptos Básicos

Sistema

- Un producto o componente, como un protocolo criptográfico, una tarjeta inteligente, o el hardware de una PC
- Un conjunto de componentes como los arriba descriptos, mas un OS, comunicaciones y otras cosas que conforman una infraestructura de una organización
- ...más un conjunto de aplicaciones
- Cualquiera o todas las de arriba más staff TI

Seguridad

- Protección de los activos (éstos deben ser conocidos)
- Tipos de protección:
  - Prevención: tomar medidas que prevengan el daño de los activos
  - Detección: detectar cuándo, cómo y por quién un activo ha sido dañado
  - Reacción: medidas que permitan recuperar el activo o remediar el daño causado al mismo

Seguridad Informática

- Propiedades de seguridad de los activos (ITSEC)
  - Confidencialidad: prevención de difusión no autorizada de la información
  - Integridad; prevención de modificación no autorizada de la información
  - Disponibilidad: prevención de apropiación no autorizada de información o recursos
- Completando la lista: Autenticidad, Trazabilidad y No repudio

Confidencialidad

- Prevenir acceso no autorizado a la información
- Quién tiene derecho a acceder a qué
- Modelo Bell-LaPadula
- Privacidad (información personal)
- Secreto (información de una organización)
- Propiedad de la información: clasificación de la información debería ser independiente del uso y contexto

Confidencialidad

- Ocultar el contenido de un objeto y también su existencia? (Análisis de tráfico):
  - *Unlinkability*
  - Anonimato

Integridad

- El significado de esta propiedad ha variado en el tiempo
- Originalmente: integridad de transacciones (atomicidad)
- Actualmente
  - Origen
  - Corrección e invarianza de la información
  - Prevención de escritura no autorizada

Integridad

- Visión *user-oriented*
  - *No user of the system, even if authorized, may be permitted to modify data items in such a way that assets or accounting records of the company are lost or corrupted* (Clark & Wilson)
- Visión *state-oriented*
  - *Data Integrity: The state that exists when computarized data is the same as that in the source documents and has not been exposed to accidental or malicious alteration or destruction* (The Orange Book)

Integridad

- Visión *communications-oriented:*
  - Detección y Corrección de modificación, inserción, borrado o replay de información transmitida
  - Manipulación intencional o error de transmisión
- Integridad es a menudo un pre-requisito para otras propiedades de seguridad:
  - ataque a la confidencialidad de la información modificando las tablas de control de acceso referenciadas por el OS

Disponibilidad

- *The property of being accessible and usable upon demand by an authorized entity* (ISO 7498-2)
- Asegurar que un atacante no pueda impedir un uso razonable de recursos de un sistema a usuarios legítimos del mismo
- Prevenir *Denial of Service (DoS)*:
  - *The prevention of authorized access to resources or the delaying of time-critical operations* (ISO 7498-2)

Trazabilidad (*Accountability*)

- Propiedades de seguridad tradicionales ponen el énfasis en prevenir, pero es imposible prevenir todas las acciones impropias
  - Acciones autorizadas pueden violar la seguridad
  - Errores de diseño del sistema
- Un nuevo requerimiento de seguridad: los usuarios de un sistema deben hacerse responsables de sus acciones sobre el mismo
  - *Accountability: Audit information must be selectively kept and protected so that actions affecting security can be traced to the responsible party* (The Orange Book)

Trazabilidad (*Accountability*)

- Esto es posible si el sistema permite identificar y autenticar al usuario
- También debe mantener una traza de auditoría de eventos relevantes para la seguridad
- Si un ataque es perpetrado, esta traza puede ayudar a identificar el atacante y los pasos seguidos para comprometer al sistema

No Repudio

- Servicios de no repudio proveen evidencia de que un evento específico ha ocurrido
- Firmas digitales es uno de estos servicios: son evidencia que puede ser verificada por un tercero
- Servicios típicos:
  - No repudio de origen (del envío de un documento, por ejemplo)
  - No repudio de entrega (proveyendo evidencia que un mensaje ha sido entregado a un cierto destinatario)

Políticas y Modelos de Seguridad

- Una política de seguridad tiene que establecer cuáles son los activos que deben ser protegidos y además podría tambíen indicar cómo hacerlo
- *Security Policy Objective (Sterne):*
  - *A statement of intent to protect an identified resource from unauthorized use*
- Cómo alcanzar los objetivos: dos niveles
  - Organizacional
  - Automatización

Políticas y Modelos de Seguridad

- Política de Seguridad Organizacional
  - Un conjunto de leyes, reglas y prácticas que regulan cómo una organización gestiona, protege y distribuye recursos para alcanzar los objetivos de un política de seguridad
- Política de Seguridad Automatizada
  - El conjunto de restricciones y propiedades que especifican cómo un sistema informático previene que tanto información como recursos sean utilizados violando una política de seguridad

Políticas y Modelos de Seguridad

- Formalización de estas nociones (Goguen & Meseguer)
- Distinción precisa entre
  - política de seguridad (requerimientos de seguridad sobre un sistema) y
  - el sistema en sí (especificación de alto nivel del comportamiento del sistema mediante una máquina abstracta de estados)
- Lenguaje para la definición de políticas de seguridad basado en el concepto de *non-interference*

Algunas Conclusiones

Seguridad Informática: Una Definición

- *Computer Security* (Qué se hace):
  - *Deals with the prevention and detection of unauthorized actions by users of a computer system* (Gollman)
  - Esta definición implica que autorización apropiada y control de acceso son esenciales. La primera implícitamente asume la existencia de una *política de seguridad.*
- *Computer Security* (Causas):
  - *Concerned with the measures we can take to deal with intentional actions by parties behaving in some* unwelcome fashion

Seguridad Informática: Algunas conclusiones

- No existe una única definición de seguridad
- Uno debe ser cuidadoso cuando lee un documento en no confundir su propia definición con aquella usada en el documento
- Se invierte (y gasta) una gran cantidad de tiempo en tratar de definir notaciones no ambiguas para la seguridad

Seguridad Informática: Un Dilema

- Debido a que el número de usuarios que dependen de la seguridad informática es equivalente al de los conectados a la Internet, los requerimientos han cambiado radicalmente, y dan lugar al siguiente dilema:
  - *Security-unaware users have specific security requirements but usually no security expertise* (Gollman)
- Este dilema es visible en las estrategias actuales usadas para evaluación de la seguridad: las funciones de seguridad provistas por un sistema deben ser explicitadas y aseguradas

Bibliografía y Referencias

- **R. Anderson**, *Security Engineering – A Guide to Building Dependable Distributed Systems,* Wiley, 2001.
- **D. Gollman**, *Computer Security*, Wiley, 2006.
- **D.R Clark, D.R. Wilson**, *A comparison of comercial and military computer security policies*, Proc. 1987 IEEE Symposium on Security and Privacy, 1987.

Bibliografía y Referencias

- **US Department of Defense**, *DoD Trusted Computer System Evaluation Criteria (The Orange Book)*, 1985.
- **D. Sterne**, *On the buzzword "Security Policy"*, Proc. 1991 IEEE Symposium on Security and Privacy, 1991.
- **J.A. Goguen, J. Meseguer**, *Security Policies and Security Models*, Proc. 1982 IEEE Symposium on Security and Privacy, 1982.