15: Seguridad

Sistemas Operativos 2

Ing. Alejandro León Liu

- **Seguridad**
- Principios
- Amenazas de programas
- Amenazas de red
- Criptografía
- Autenticación de usuarios
- Defensas de seguridad

SEGURIDAD

- Protección: problema interno
  - Permisos
  - Privilegios
- Seguridad
  - Ambiente externo
  - Resguardar un sistema de acceso, uso, modificación y eliminación de información por usuarios no autorizados.

- Un sistema seguro garantiza
  - Confidencialidad
    - Asegurar que únicamente usuarios autorizados tengan acceso a la información
  - Integridad
    - Asegurar que la información sea modificada únicamente por usuarios autorizados
  - Disponibilidad
    - Asegurar que la información está disponible a usuarios autorizados cuando lo necesiten
    - Proteger contra un Denial of service

- El gran problema de seguridad

- “A chain is only as strong as its weakest link”
- Proveer seguridad en varios niveles
  - Nivel de aplicaciones
  - Nivel de red y comunicaciones
  - Nivel de Sistema Operativo
  - Nivel físico
    - Data centers seguros
  - Nivel humano
    - “Social engineering”
    - Phishing

- ¿De quién nos debemos proteger?
  - Virus, trojans, otros programas
  - Crimen organizado
  - Corporaciones: competencia
  - Desastres naturales
  - Humanos
    - Intensionalmente
    - Accidentalmente
  - Ex empleados
- Más difícil que seguridad física
  - Automatizar ataques
  - Ataques remotos
  - Copia de información

- Seguridad
- **Principios**
- Amenazas de programas
- Amenazas de red
- Criptografía
- Autenticación de usuarios
- Defensas de seguridad

PRINCIPIOS

- Principio de menos privilegios
  - Ejecución con el mínimo número de privilegios y recursos
  - Separación de responsabilidades
  - Evitar uso de usuarios administradores
  - Minimizar consecuencias
- Minimizar la superficie de ataque
  - Cada “feature” en un sistema aumenta el riesgo de un ataque
  - Reducir riesgo, reduciendo superficie de ataque
  - Agregar un “feature”
    - Funcionalidad vrs. Riesgo

- Mantener la seguridad simple
  - Menos errores
  - Ejecución más rápida
  - Evitar errores en
    - Código de manejo de errores
    - Escribir a logs
- Detección de intrusos
  - Registrar accesos (o intentos)
    - Protección de bitácoras y logs
  - Auditar accesos
  - Procedimiento para responder a un intruso

- Defensa en profundidad
  - Diversidad de mecanismos de seguridad
  - Si un mecanismo falla, los otros mecanismos pueden proteger el sitema
  - No confiar en un firewall para la seguridad de un sistema
    - Usuarios y permisos
    - Seguridad física a data center
    - Cifrado de datos en la comunicación
  - “No poner todos los huevos en un mismo cesto”

- Modelo de seguridad Positivo
  - Default deny
  - Secure defaults
  - Regresar a un estado seguro después de una falla
  - Whitelist vrs. Blacklist
    - Whitelist: define lo válido. Lo demás es inválido
    - Blacklist: define lo inválido. Lo demás es válido.

```
isAdmin = true;
try {
  codeWhichMayFail();
  isAdmin = isUserInRole( "Administrator" );
}
catch (Exception ex) {
  log.write(ex.toString());
}
```

```
While (true)
{
   transaction = getNextTransaction();
   transaction.process();
   transaction.markAsProcessed();
}
```

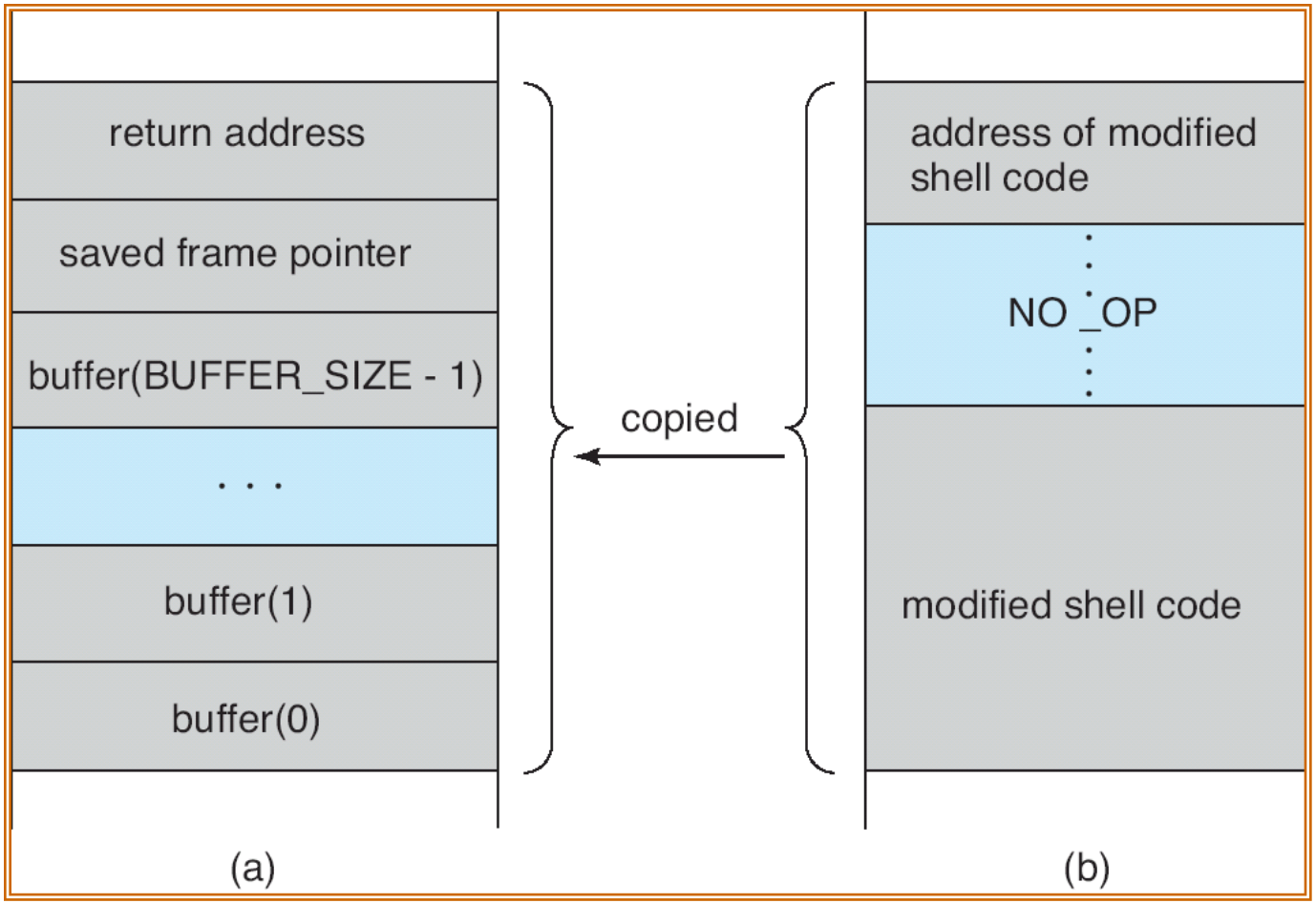
- Evitar seguridad por obscuridad
  - Secreto es bueno, pero no lo suficiente
  - Cambiar el puerto default de algún servicio
  - En aplicaciones:
    - Permisos: Únicamente ocultar opciones en menú
  - Spiders
    - Brute force
    - Port scans

- Seguridad
- Principios
- **Amenazas de programas**
- Amenazas de red
- Criptografía
- Autenticación de usuarios
- Defensas de seguridad

AMENAZAS DE PROGRAMAS

- Trojans
  - Abuso de su ambiente de trabajo
  - Programa malicioso, se esconde detrás de una aplicación confiable
- Trap door
  - Desarrollador deja un acceso al sistema que solo él puede usar
  - “Salami technique”
  - Difícil detectar: analizar código fuente

- Logic Bomb
  - Programa que inicia una vez se de cierto escenario
  - Difícil detectar previo a que se active
- Stack y buffer overflow
  - Explotar bug en programa
  - Overflow de un campo de entrada
    - Escribe en memoria hasta llegar a la pila
  - Sobreescribir la dirección de retorno en la pila con el código escrito (input)
  - Escribir el código de un programa malicioso
    - Ejecutar un shell


return address
saved frame pointer
buffer(BUFFER_SIZE - 1)
. . .
buffer(1)
buffer(0)
copied
address of modified shell code
NO _OP
modified shell code
(a)
(b)

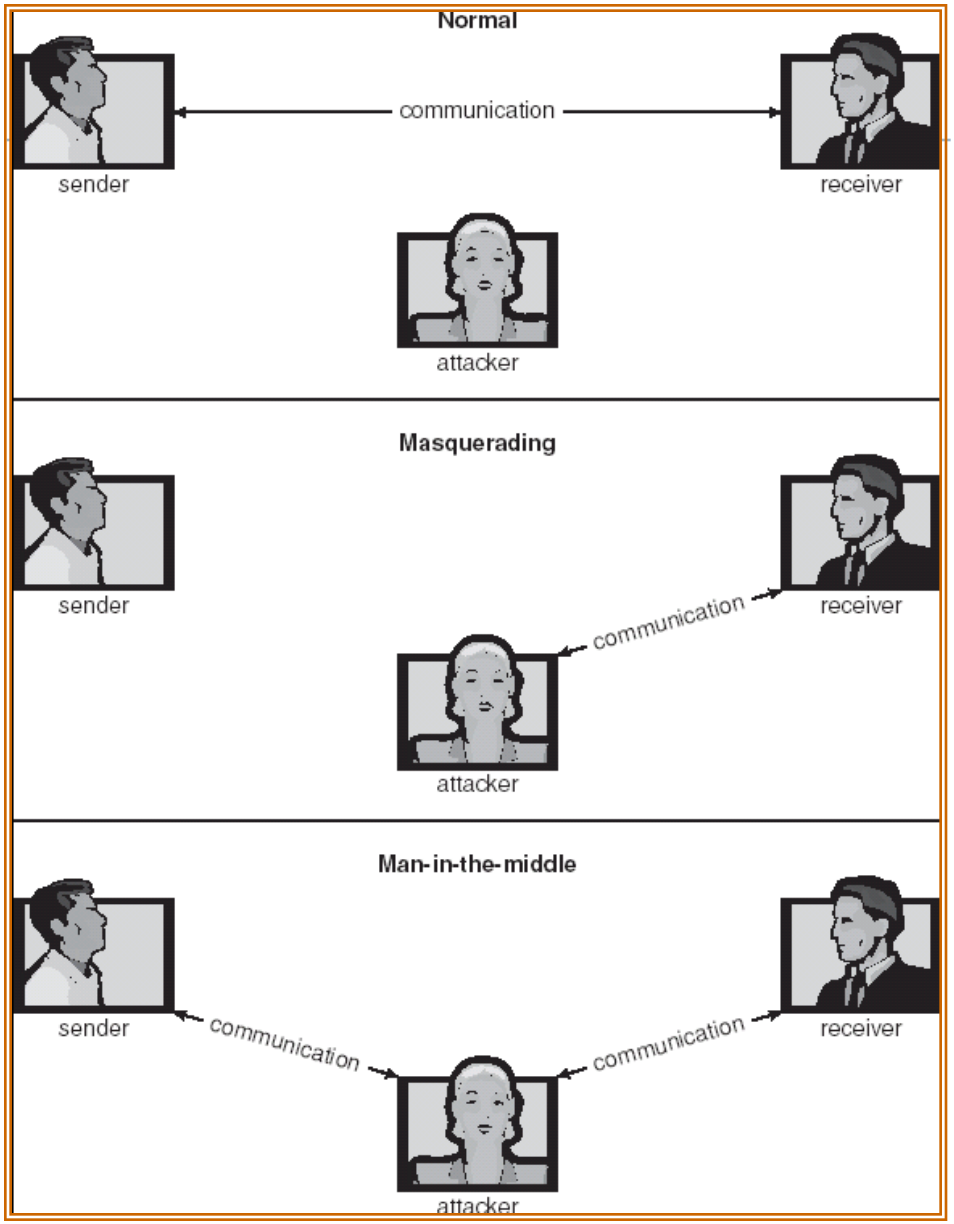
- Virus
  - Segmento de código en algún programa
  - Replica e infecta otros programas
  - Algún programa, como un trojan instala el virus en el sistema
  - Varios tipos
    - En programas
    - En boot
    - En macros (office por ejemplo)
    - Ocultos
      - Modificar el sistema para evitar ser detectados
  - Windows: más vulnerable
    - Uso de usuarios administrativos
  - Rootkits

- Worms
  - Replicarse
  - Consumir recursos del sistema
  - Impedir que otros procesos se ejecuten

- Seguridad
- Principios
- Amenazas de programas
- **Amenazas de red**
- Criptografía
- Autenticación de usuarios
- Defensas de seguridad

AMENAZAS DE RED

- Port scan
  - Detectar vulnerabilidades de un sistema
  - Automatizado
- Denial of service
  - Robar recursos
  - Imposible prevenir
- Masquerading
  - Pretender ser alguien más
- Man in the middle

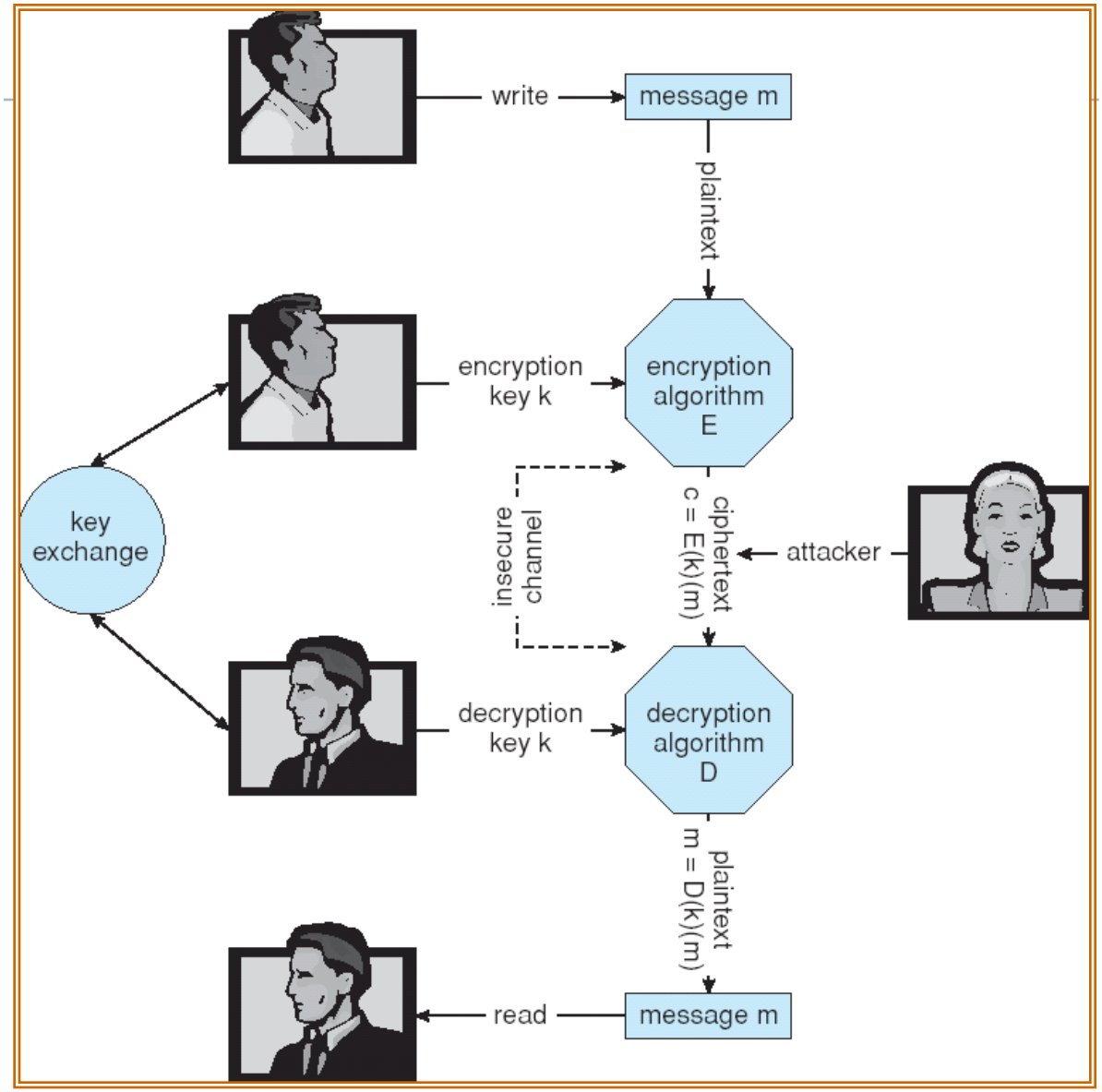

Normal
communication
sender
receiver
attacker
Masquerading
sender
communication
receiver
attacker
Man-in-the-middle
sender
communication
communication
receiver
attacker

- Seguridad
- Principios
- Amenazas de programas
- Amenazas de red
- **Criptografía**
- Autenticación de usuarios
- Defensas de seguridad

CRIPTOGRAFÍA

- Paquetes de red
  - Contienen dirección fuente falsificable
  - No solo el destinatario recibe un paquete
- Routers: reciben y transmiten paquetes
- Criptografía: “Hiding information”
  - Basado en llaves secretadas, distribuidas previamente
  - Identificar quién envía un mensaje
  - Cifrar el mensaje de forma que únicamente el destinatario lo pueda leer
  - Limitar el número de receptores de un mensaje

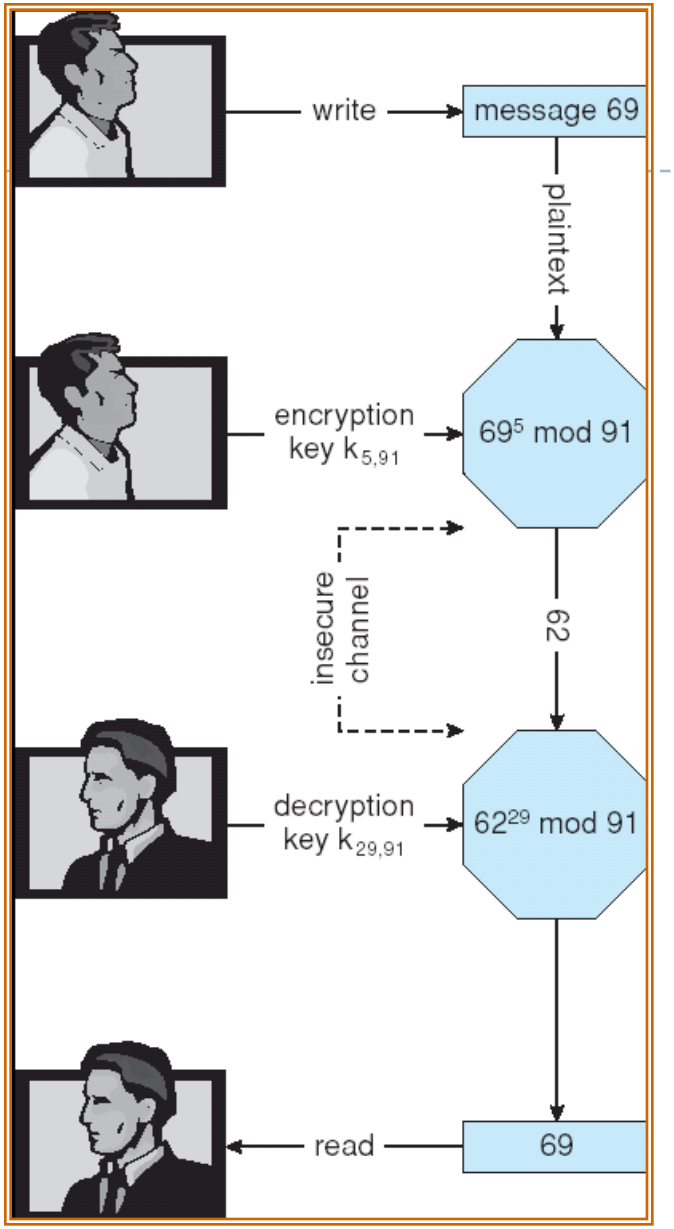
- Algoritmo de cifrado:
  - Conjunto K de llaves
  - Conjunto M de mensajes
  - Conjunto C de cifrados (mensajes cifrados)
  - Función E (cifrar): $K \rightarrow (M \rightarrow C)$
  - Función D (descifrar): $K \rightarrow (C \rightarrow M)$
  - m se puede calcular de E(k)(m) = c si y solo si, se posee D(k)


write
message m
plaintext
encryption key k
encryption algorithm E
key exchange
insecure channel
ciphertext c = E(k)(m)
attacker
decryption key k
decryption algorithm D
plaintext m = D(k)(m)
read
message m

- Cifrado simétrico
  - Misma llave para cifrar y descifrar
  - DES
  - 3DES
  - AES
  - Transformaciones: eficiente

- Cifrado asimétrico
  - Llave privada
  - Llave pública
  - Cálculo matemático: más costoso que cifrado simétrico
    - Mensajes cortos
    - Intercambio de llaves de algoritmos simétricos
  - RSA
    - Llave pública: $E(k_e , N)$
    - Llave privada: $D(k_d , N)$
    - N: producto de q y p primos
    - Algoritmo cifrar: $E(k_e , N)(m) = m^{k_e} \bmod N$,
      - k_e *tal que* $k_e k_d \bmod (p-1)(q-1) = 1$
    - Algoritmo descifrar: $D(k_d , N)(c) = c^{k_d} \bmod N$

- $p = 7$, $q = 13$
- $N = 7 * 13 = 91$
- $(p-1)(q-1) = 72$
- Llave pública: k_e, $N = 5, 91$
- Llave privada: k_d , $N = 29, 91$



- Autenticación
  - Verificar que el emisor es quién dice ser
  - Verificar que mensaje no sea modificado
  - Limitar el número de emisores de un mensaje
  - No repudio: prueba de que el emisor emitió el mensaje
  - Algoritmo de autenticación:
    - Conjunto K de llaves
    - Conjunto M de mensajes
    - Conjunto A de autenticadores
    - Función Firmar: $S : K \rightarrow (M \rightarrow A)$
    - Función Validar: $V : K \rightarrow (M \times A \rightarrow \{\text{true, false}\})$

- Funciones Hash
  - Crea un hash (digest) de tamaño n bits a partir de un mensaje.
  - Si $H(m) = H(m')$, then $m = m'$, el mensaje no ha sido modificado
  - MD5
  - SHA-1
- Message Authentication Code (MAC)
  - Cifrado simétrico
  - $S(k)(m) = f(k, H(m))$
    - Hash de un mensaje especificado
  - $V(k)(m, a) \equiv (f(k, H(m)) = a)$
    - Comparar el autenticador (recibido) con el hash del mensaje especificado

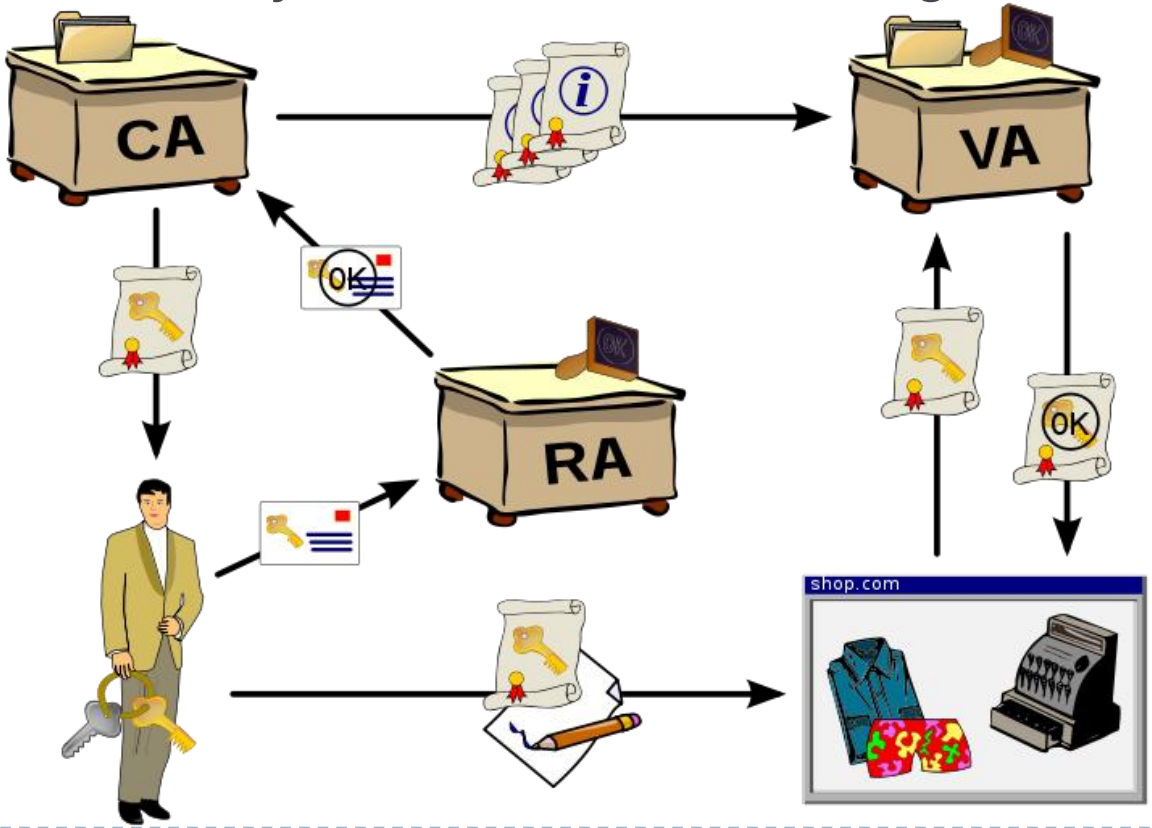
- Firmas digitales
  - Cifrado asimétrico
  - Autenticadores son firmas digitales
  - RSA
    - Usando llaves al revez
    - $S(k_s)(m) = H(m)^{k_s} \bmod N$
    - $V(k_v)(m, a) \equiv (a^{k_v} \bmod N = H(m))$
- En ocasiones no es necesario la confidencialidad
  - Empresas firman parches
  - Usuarios pueden garantizar que parches provienen de la empresa

- Distribución de llaves
  - Usar cifrado asimétrico para compartir llaves de algoritmos simétricos
  - Certificados digitales
    - Llave pública firmada por un tercero de confianza (trusted party)
    - Tercero de confianza recibe pruebas para otorgar llave pública
    - ¿Cómo confiar en tercero en confianza?
      - Las autoridades certificadoras incluyen sus llaves públicas en browsers, etc..

- SSL
  - Estándar para comunicación segura entre web browsers y web servers
  - http: texto claro
  - Cliente se conecta a servidor web por medio de https (puerto 443)
  - Servidor se identifica (envía llave pública)
    - Cliente valida que llave pertenezca a servidor
    - Cliente valida que la llave no esté expirada
    - Cliente valida llave con tercero en confianza

- Cliente envía su llave pública
- Servidor cifra un mensaje (llave de sesión) con su llave privada y la llave pública del cliente
- Cliente descifra mensaje con su llave privada y la llave pública del servidor
- Comunicación entre cliente y servidor cifrada con una llave de sesión

- PKI
  - Software, hardware y políticas para crear, manejar, distribuir, usar y revocar certificados digitales



- Declaración Única Aduanera (DUA-GT)
  - PKI
  - SAT: Autoridad certificadora
  - Ebclosion: Autoridad de registro
  - Autoridad validadora
  - Certificado digital: smartcard
  - Beneficios
    - Autenticación de agentes aduaneros
    - Cifrado de mensajes
    - No repudio

- Seguridad
- Principios
- Amenazas de programas
- Amenazas de red
- Criptografía
- **Autenticación de usuarios**
- Defensas de seguridad

AUTENTICACIÓN DE USUARIOS

- Contraseñas
  - Modelo sencillo
  - Adivinados o divulgados
    - Ingeniería social
    - Brute force (programa que adivina contraseñas usando diccionarios)
    - Sniffing: ver cuando se digitan
      - Key logger
      - Cámaras
  - Almacenadas cifradas
  - Función compleja de invertir, fácil de calcular

- One time passwords
  - Eliminar problema de snifffing
  - Challenge & response
  - La contraseña es una función
    - F(challenge) = response
- Two factor authentication
  - Smartcards & pin
- Biométricos

- Seguridad
- Principios
- Amenazas de programas
- Amenazas de red
- Criptografía
- Autenticación de usuarios
- **Defensas de seguridad**

DEFENSAS DE SEGURIDAD

- Defensa en profundidad
- Políticas de seguridad
  - Usuarios
    - Contratos, Non disclosure Agreement (NDA)
    - Políticas de contraseñas
    - Política de baja de empleados
    - Política de instalación de programas
    - Políticas de navegación
  - Desarrollo
    - Estándares de desarrollo
    - Quality Assurance (QA). Pruebas
    - Configuraciones de servidores aceptadas
  - Infraestructura
    - Análisis de riesgos

- Análisis de Vulnerabilidades
  - Contraseñas fáciles
  - Programas no autorizados
  - Procesos de larga ejecución (demonios sospechosos)
  - Cambios en programas del sistema
  - Port scan (puertos escuchando)
- Firewalls
  - Permitir (prohibir) tráfico de una red a otra
  - Permitir (prohibir) tráfico de cierto protocolo
  - Inspección de paquetes
    - Revisa estado (paquetes anteriores)
    - Denial of service
    - Virus, ataques de red

- Intrusion detection
  - IDS (Intrusion detection systems)
  - Detectar intrusos
    - Comandos de usuarios sospechosos
    - Llamadas al sistema sospechosas
    - Encabezados de paquetes de red
  - Alarmas
    - Correos / Mensajes
    - Bloquear
- Protección anti-virus