



# ¿Es Internet un lugar seguro para vivir?

---



**José M. Piquer**  
**DCC - U. de Chile**

# Seguridad

## Los Temas Principales

- Red Interna
- Red Externa
- Autenticación (vendedor/comprador)
- Privacidad
- Alteración
- No Repudiación
- Negación de Servicio/Virus





# Seguridad

---

## Los Ataques más Famosos

- **El gusano de Morris (1988)**
- **Berferd en AT&T (1991)**
- **Robo de passwords de proveedores de Internet (1993)**
- **Direcciones IP falsas (1994)**
- **Giros desde el Citibank (1995)**
- **Robo Base de Datos Falabella (1995)**
- **Defacing sitio cumbre presidencial (1996)**
- **Mails confidenciales desde el Banco Central (2002)**
- **Denegación de Servicio a los servidores raíz de nombres (2003)**
- **Denegación de servicio a los servidores en Estonia (2007)**
- ➔ **los ataques no paran de aumentar (Viruses, Hackers, etc)?**

## ¿Podemos Evitarlos?

- **El 90% de los ataques de acceso externo provienen de passwords triviales**
- **La seguridad no viene provista en IP, debe manejarse en la instalación**
- **La denegación de servicio es el ataque más peligroso y sin defensa clara (basado en la debilidad de terceros)**

# Seguridad

## ¿Y podemos hacer negocios en estas condiciones?

- Conocemos bien la tecnología para hacerlo
- No viene nativa en TCP/IP
- Debemos configurar redes y servicios para hacerlo
- Debe existir un acuerdo de confianza
- Hoy se hace mucho comercio sobre la red
- Es más seguro que el uso de tarjetas en el mundo real

## ¿Podemos estar tranquilos en nuestra red interna?

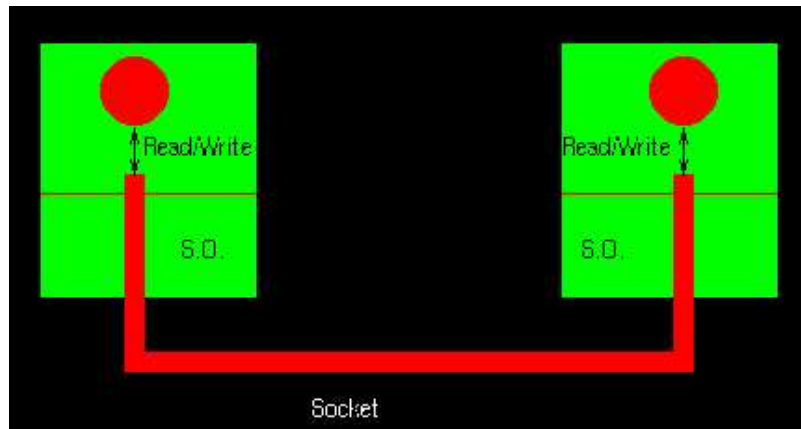
- Instalando paquetes de cortafuegos/IDS
- Definiendo claras políticas de seguridad
- Entendiendo bien la tecnología
- Manteniéndose permanentemente al día, grupo experto





## Arquitectura de TCP/IP en el S.O.

- TCP/IP viene incluido en el S.O.
- End-to-end argument
- Los clientes y servidores son procesos normales
- La parte S.O. no la cambiaremos, pero el resto es configurable
- Todo TCP/IP es software, por lo que nunca podemos confiar en nuestro "interlocutor"
- La idea es simular un canal de comunicación entre cliente y servidor





# Arquitectura de TCP/IP en el S.O.



## Demonios buenos y malos

- **Cliente:** pide conectarse con una máquina y un port
- **Servidor:** acepta conexiones en un port
- El número de port discrimina qué servicio quiero
- Si no hay un servidor aceptando conexiones en el port, el cliente recibe *connection refused*
- Hay ports "privilegiados", y solo el super usuario puede correr servidores en ellos.
- Cualquier usuario puede instalar un servidor



Todo servidor activo es un potencial hoyo de seguridad



# Ataques Clásicos

---

## Acceso a Cuentas no Autorizados

- ¿Cómo adivinar una password?
- Caballo de Troya
- Crack de Passwords
- Espionaje de Red: Snoop (hubs, switches, wireless)
- ¿Cómo ser dueño de una máquina?
- Obtener Password de administrador
- Bugs en Servidores (código conocido: buffer overflow)
- Propagarse por la red



La mayoría de los ataques de seres humanos en Internet provienen de passwords triviales (cada vez menos "triviales")



Muchos servidores son penetrables con ataques disponibles en la red



# Ataques Clásicos

---

## Captura de Datos Confidenciales

- Snoop: hoy en wireless es un problema
- Caballo de Troya
- Impostura de Servidores
- Descriptación



Una llave RSA de 700 bits toma algunos meses en romperse (uso actual: 1024).

## Falsificación de Documentos

- Mail anónimo

## Falsificación de Clientes

- Acceso no autorizado a servicios



Los ataques importantes (giro de dinero) siempre son *internos* (el que escribió el programa, el que conocía el procedimiento)



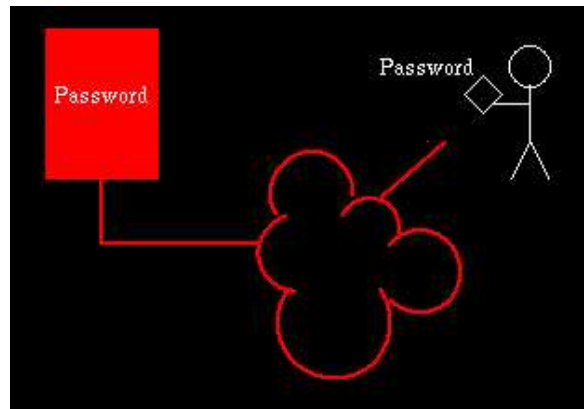
La mayoría de los ataques hoy son automatizados (desde programas)



## Soluciones Existentes

### Acceso a Cuentas no Autorizados

- Forzar passwords no triviales
- Password *aging*
- Impedir login desde fuera de la red
- Impedir que passwords transiten por la red (llave pública)
- Passwords de un sólo uso (ojo con phishing en línea)
- biometría/smartcards





## Soluciones Existentes

---

### Bugs en Servidores

- **Aplicar últimos parches de seguridad (automatizar?)**
- **Revisar boletines del CERT**
- **Usar la menor cantidad de servicios estándares**
- **Separar red de servicios externos de red interna**
- **IDS: detección de ataques automatizada**



# Soluciones Existentes

---

## Manejo de Bitácoras

- Usar syslog para bitácoras intensivas
- Concentrar en una máquina
- Salvar en un archivo histórico
- Usar tcpwrapper o equivalente para controlar
- Externalizar: centro de monitoreo remoto



# Soluciones Existentes

## Captura de Datos Confidenciales

- **Encriptación: SSL, secure http**
- **RSA para además certificar a los servidores**
- **+128 bits son obligatorios**
- ➔ **¡NUNCA inventar su propia criptografía!**



## Soluciones Existentes

---

### Falsificación de Documentos

- e-mail normal es inseguro
- Usar mail firmado (Certificados, PGP u otro)
- Al firmar un mail, no se puede alterar
- Se puede demostrar que ese mail fue enviado por su origen
- Todos pueden leerlo



## Soluciones Existentes

---

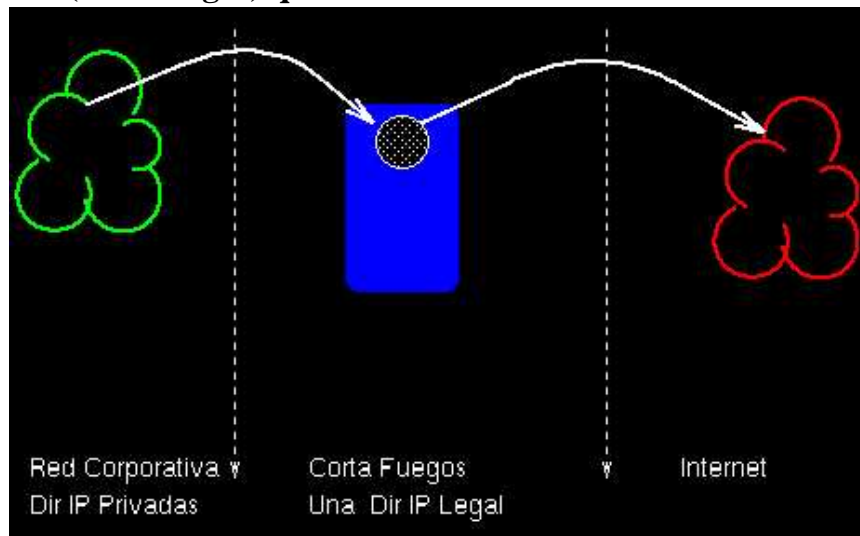
### Falsificación de Clientes

- Máquina y usuario dicen ser quienes no son
- Filtrar por dirección IP cliente (tcpwrapper)
- Pero puede ser alterada
- Verificar nombre de máquina == dir IP
- ➔ Sólo queda validar usuario fuertemente (en el servidor)



# Seguridad en Internet

- Conectar red interna a Internet
- Definir política de servicios
- Qué accesa la red interna
- Qué accesa la red externa
- Mantener una clara distinción entre ambas
- Usar un *firewall* (cortafuegos) que aisle el tráfico IP entre ambas redes (no rutea)





# Seguridad en Internet

## Firewalls y Seguridad

- **Access List por interfaz (sin ports)**
- **No rutear en el Firewall**
- **Único punto débil es el Firewall mismo**
- **Si no hay logins es más seguro**
- **Pero perdemos funcionalidad!**



**La gente está dispuesta a correr riesgos increíbles para hacer la vida más fácil**



# Seguridad en Internet

---

## Conexión a Internet

- Hoy no se puede conectar la red interna directamente
- El Firewall puede ser simplemente un servidor configurado para no rutear
- Existen productos comerciales (caros) que ayudan
- Linux como Firewall es una buena alternativa gratis
- Sin una política clara de seguridad, nada sirve



Un Firewall mal configurado puede ser más peligroso que una red abierta



# Virus

- 
- Ya no mucho diskette/CD
  - Mucho por mail (usuarios, ejecutables, Outlook)
  - Cada vez mas por servidores (gusanos)
  - ➔ Los virus son probablemente el principal problema actual de seguridad (en dinero perdido)
  - ➔ En dos días he recibido 300 mails con virus
  - ➔ Imposible educar a los usuarios
  - ➔ Indispensable un antivirus central (servidor de correo) y por equipo usuario

## Ejemplo



## Conclusiones

- 
- **Aislar las redes internas/externas**
  - **Usar proxies y firewall con servidor seguro**
  - **Login externo es el principal enemigo**
  - **Mayor peligro: DDoS**
  - **La verdadera seguridad es interna**
  - **Implica una política clara**
  - **Bitácoras históricas de todo lo que ocurre**
  - **AntiVirus corporativo Y en los equipos finales, actualizado en línea**
  - ➔ **Toda medida de seguridad sacrifica funcionalidad**



## Situación en Chile

---

- Internet ha crecido **enormemente**
- Los crackers crecen al mismo ritmo que los usuarios
- Chile figura en rankings de proveniencia de ataques demasiado arriba
- 20% de los dominios de .CL tienen servidores de nombres "abiertos" (utilizables para ataques)
- Es seguro en cuanto a sitios donde navegar, pero el RUT es un talón de aquiles
- Phishing en aumento en/para servidores chilenos
- Falta responsabilidad de los ISP para controlar los abusos de sus clientes (SPAM, Virus, BotNets)
- Falta apoyo profesional en seguridad (expertos, conocimiento, inteligencia)
- Las empresas no saben lo que necesitan y no quieren comprar cajitas con software que no saben lo que hace.
- ➔ Equilibrio seguridad/funcionalidad/costo difícil