"La banca virtual e interactiva: Seguridad en los servicios actuales y proyectos futuros"

Ing. Giovanni B. Pichling Zolezzi

Guatemala, Agosto 2005

Contenido

I.- Banca Virtual e Interactiva.

- A.- Que es la banca virtual e interactiva.
- B.- Que productos y servicios se ofrecen.
- C.- Diseño operativo.
- D.- Equipos y medios de comunicación empleados.

II.- Riesgos informáticos.

- A.- Virus, gusanos, troyanos, ingeniería social, anonimato ....
- B.- Perfil del autor de delitos informáticos.
- C.- Proceso de identificación y verificación de clientes.
- D.- Debilidades explotadas por los delincuentes cibernéticos.

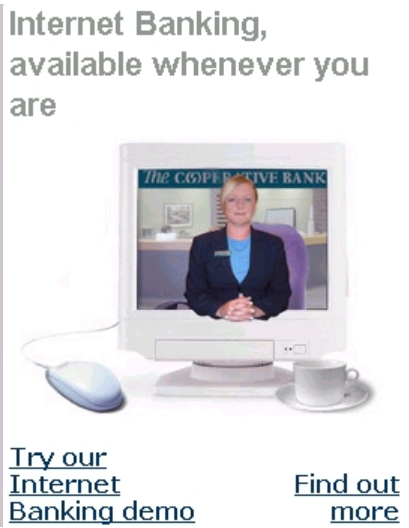
III.- Proyectos Futuros.

- A.- Tarjetas inteligentes.
- B.- Procesos de identificación.

IV.- Recomendaciones.

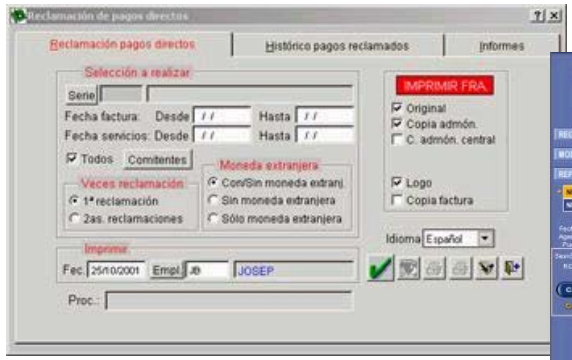
I.- A.- Que es la banca virtual e interactiva

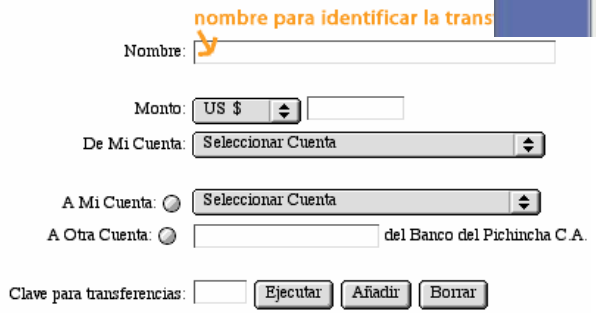
La banca virtual e interactiva es un servicio ofrecido por los bancos a sus clientes y usuarios, para luego de ser identificados, y mediante el empleo de determinados equipos o artefactos previamente homologados, puedan interactuar directamente con sus cuentas en cualquier lugar y a cualquier hora, implementando para ello programas de cómputo que ponen a su disposición a través de la red Internacional de datos, red interna de los bancos, red de cajeros automáticos o del servicio de telefonía pública (fijo, celular o satelital), y sin que para el desarrollo de esta actividad se requiera la intervención directa de ningún funcionario o empleado del banco.

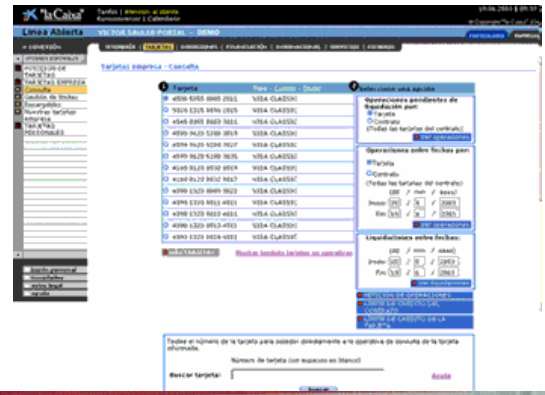


I.- B.- Que productos y servicios se ofrecen

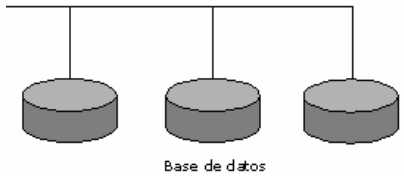
Consulta de saldos.
Consulta de movimientos.
Consulta de documentos.
Consulta de cheques.
Estados de cuenta.
Transferencias.
Transferencias a terceros.
Transferencias a otros bancos.
Pago a proveedores.
Pago de remuneraciones.
Otros pagos masivos.
Pago de servicios.
Pagos varios.
Transferencias al exterior.







I.- C.- Diseño operativo

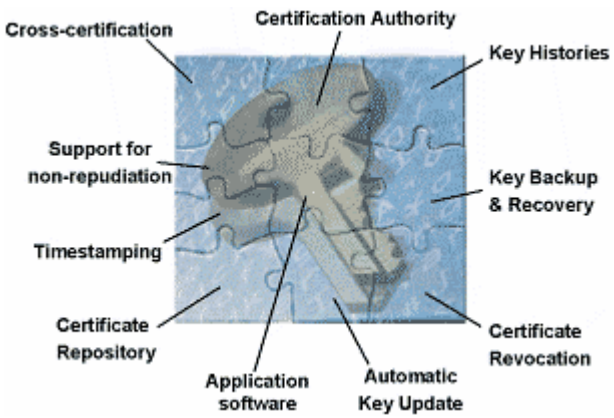


Aplicaciones y productos

Proveedor de servicios Internet

Banco

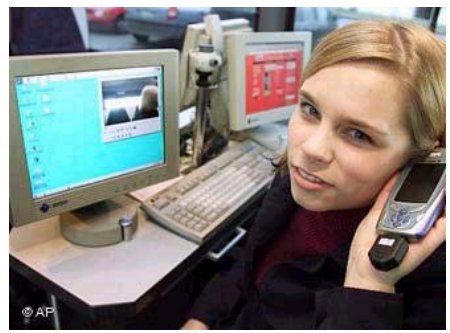
Identifica banco
entrega certificado



Entidad certificadora

INTERNET

Cliente PC y Celular

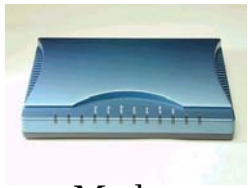


Cliente computadora

Cliente ATM

I.- D.- Equipos y medios de comunicación empleados

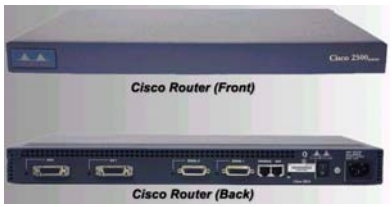
Bases de datos



Modem

Palm

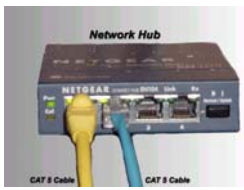
Celular



Router

INTERNET

Cajeros automáticos



Hubs

Transmisor inalámbrico

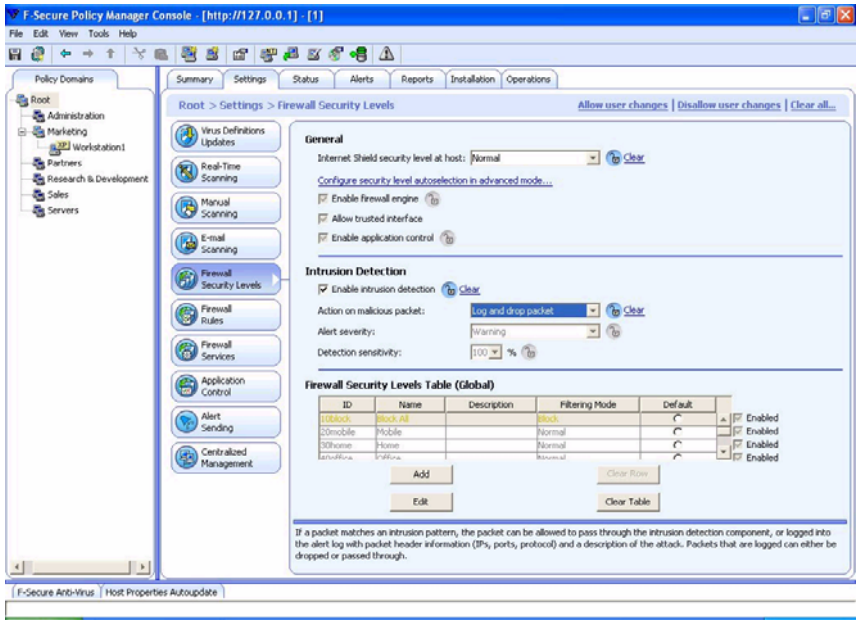
Switch

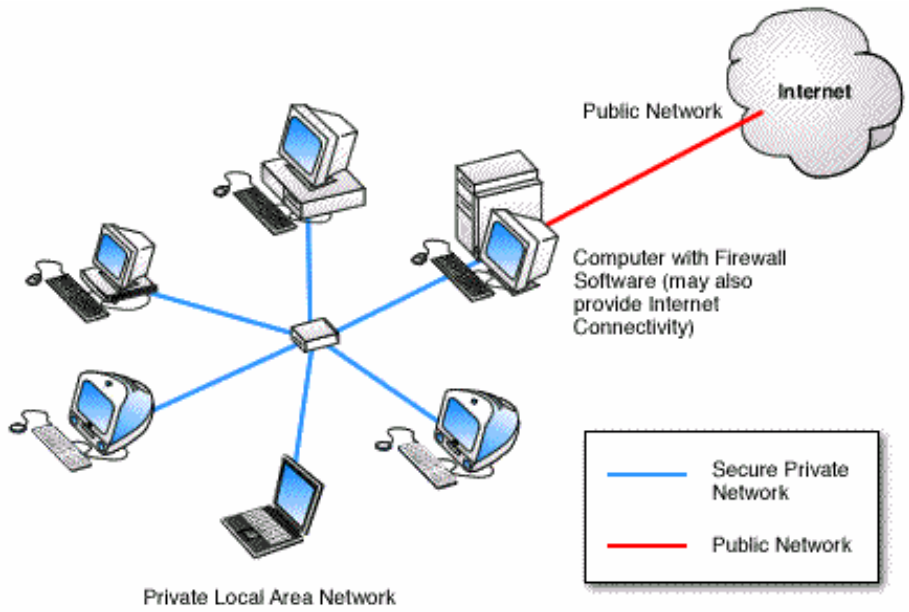
Firewall

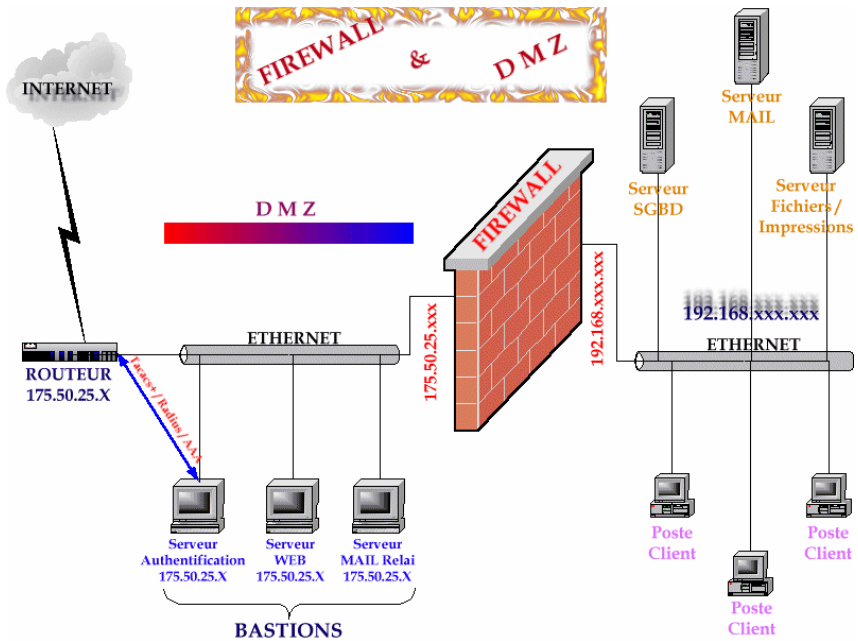
Laptop

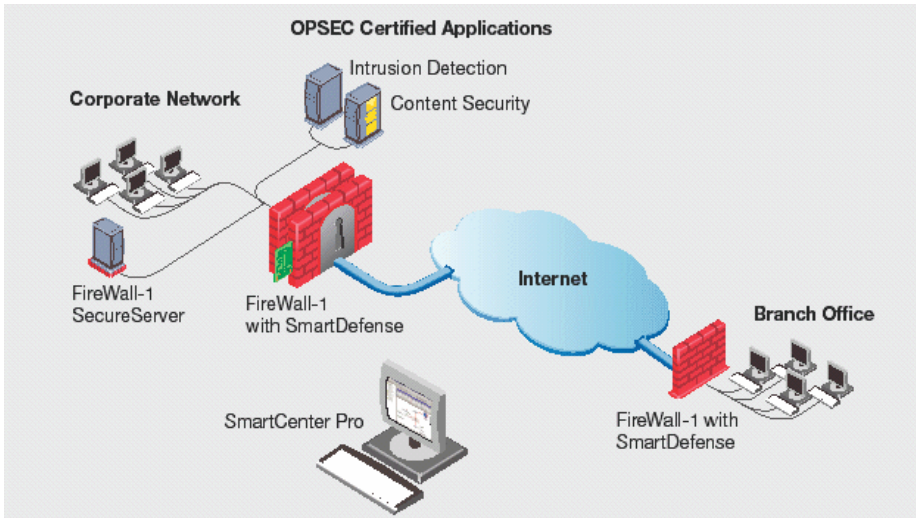
Satélite

I.- D.- Equipos y medios de comunicación empleados









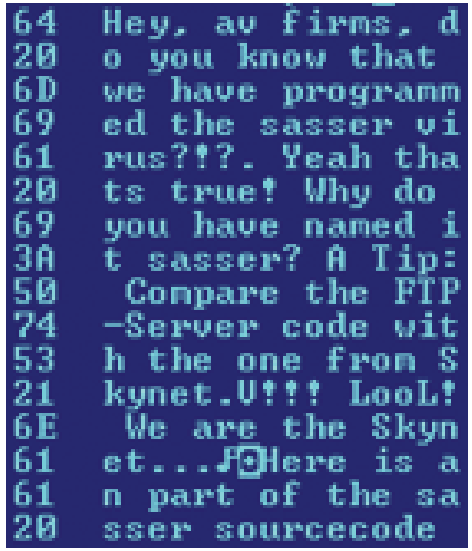
II.- Riesgos informáticos

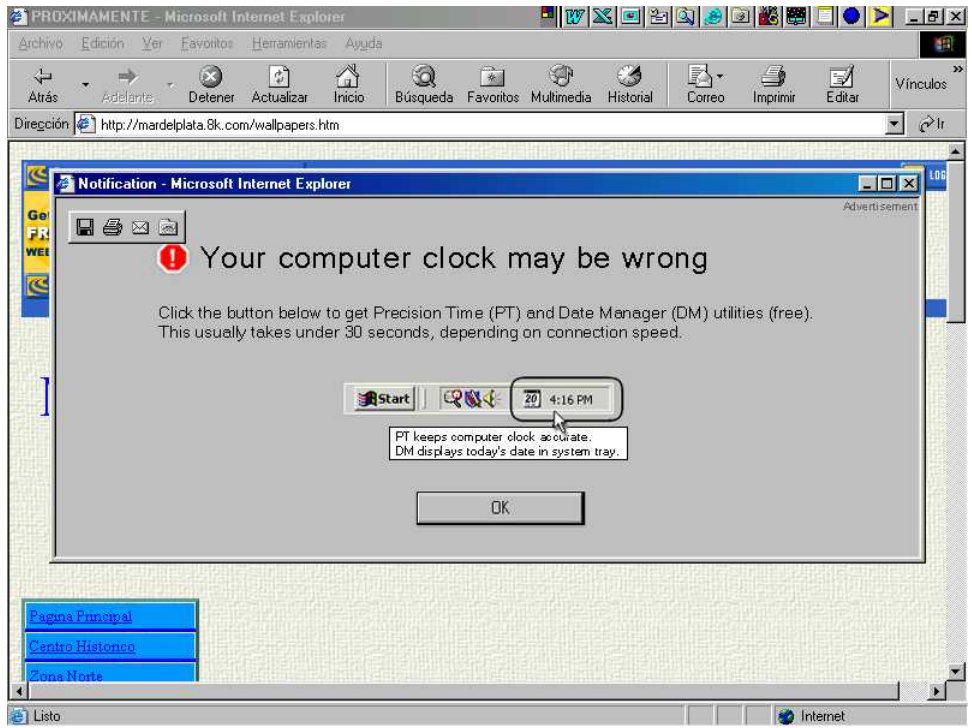
Virus, gusanos, troyanos :

Es un conjunto de instrucciones escritas en un lenguaje de cómputo, contenidas en un tipo determinado de archivo, con capacidad de insertar una copia de su código en otros archivos de similares características, y que al ser activado, logra su expansión a otros equipos y desarrollar sus actividades programadas.

Tipos de virus por sus características:
Uniformes
Encriptados
- fijo
- variables

Oligomórficos
Polimórficos
Metamórficos
Sobre escritura
Stealth o silenciosos





II.- Riesgos informáticos

Algunos virus de interés :

- Sevalcabor al revés se lee robaclaves
- Troyano Bancos.FC -> Ftpex.exe
- Gusano Wootbot.bj

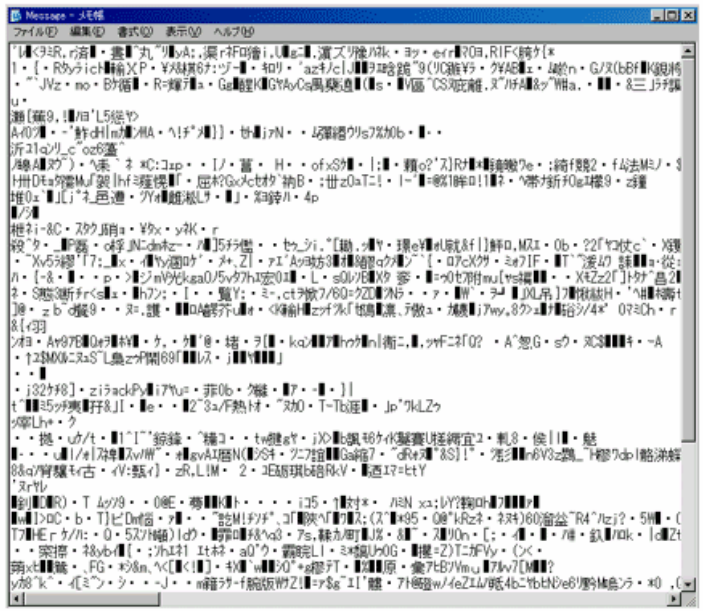
...un pirata informático ha estado tratando de llevarse por delante Internet. Hasta ahora, lo ha intentado en seis ocasiones. Su última tentativa comenzó el lunes de la semana pasada, cuando el virus SoBig F (Así de grande F) entró en la Red a través de un foro de intercambio de pornografía... una semana después, **el 6% de los correos electrónicos que circulan por el mundo está infectado con este programa**, que se ha introducido en unos 100.000 ordenadores de todo el planeta. Según la empresa de seguridad informática Messagelabs, el SoBig F ha sido detectado en nada menos que 168 de los 192 países que hay en el mundo.

SoBig ha aparecido apenas dos días después de que se lograra desactivar otro virus, el **Blaster**, que no se transmitía a través del correo electrónico, sino simplemente al entrar en Internet. El Blaster infectó a medio millón de ordenadores en todo el mundo.

Durante 2002, las empresas y particulares invirtieron 7.000 millones de dólares -unos 6.450 millones de euros- para defenderse de los virus informáticos. En 2005, esa cifra superará los 12.000 millones de dólares...

When W32.Mydoom.BI@mm is executed, it performs the following actions:

1. Copies itself as %System%\WINLOG0N.EXE.
2. May open a text file using NOTEPAD.EXE. The file contains garbage data and may look similar to the following:

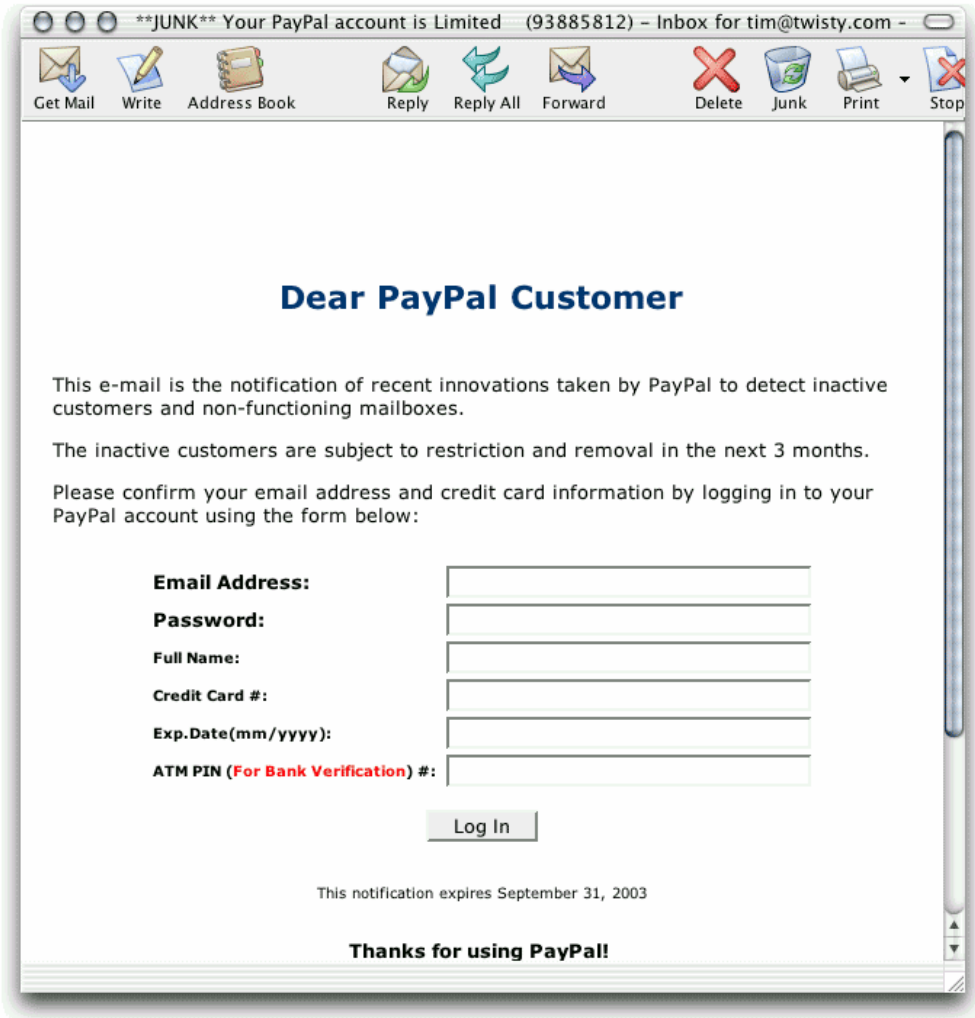


3. Creates the following files, which may steal account information from a predetermined Chinese bank:
   - %System%\wxapi.dll
   - %System%\svch0st.exe

II.- Riesgos informáticos

Ingeniería social:

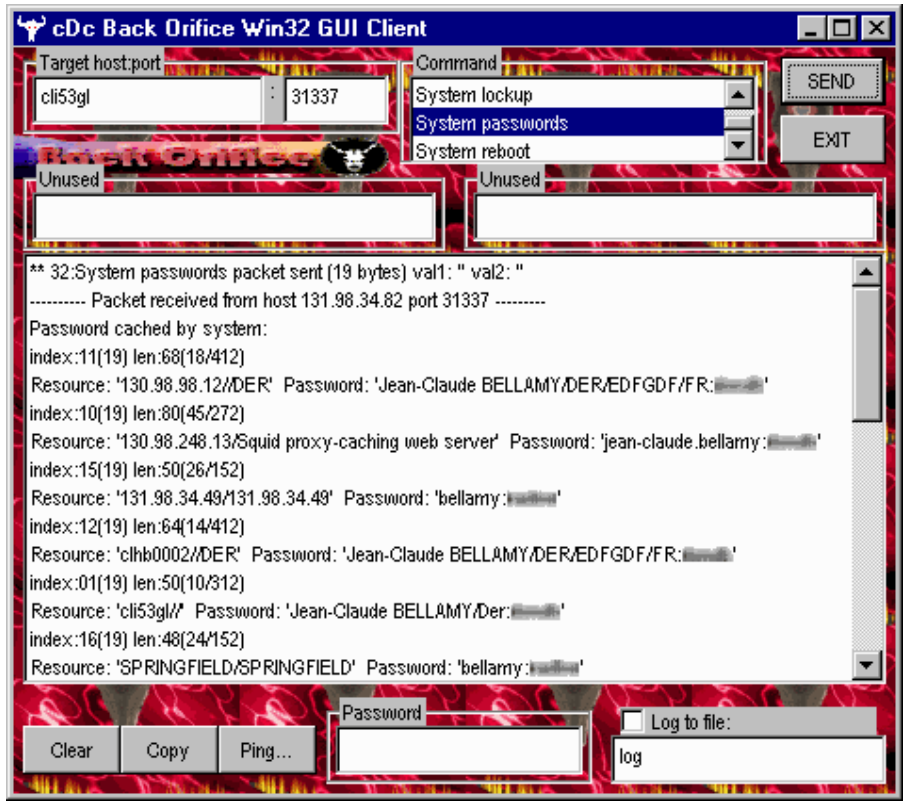
Técnica utilizada por la delincuencia cibernética que consiste en engañar a la persona elegida, ofreciéndole beneficios económicos, premios, oportunidades únicas de negocio, necesidad de actualizar datos o amenazas, a fin de conseguir información personal que le permita suplantar a la víctima u obtener beneficios económicos de la misma.



II.- Riesgos informáticos

Puertas falsas:

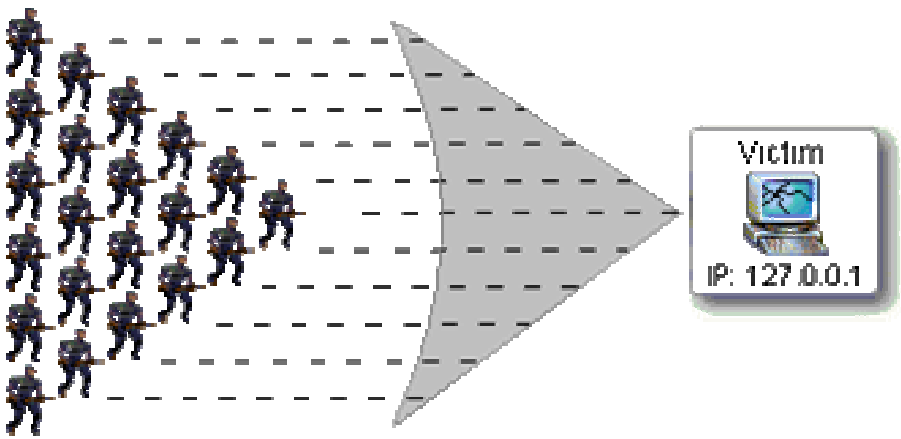
Es una técnica utilizada en el tiempo de desarrollo de aplicaciones informáticas en las que el programador inserta instrucciones que facilitan la prueba de las mismas, superando la etapa de verificación de identidad del usuario. También es utilizado para abrir puertos de comunicación que le permitan a un atacante operar con la computadora comprometida.

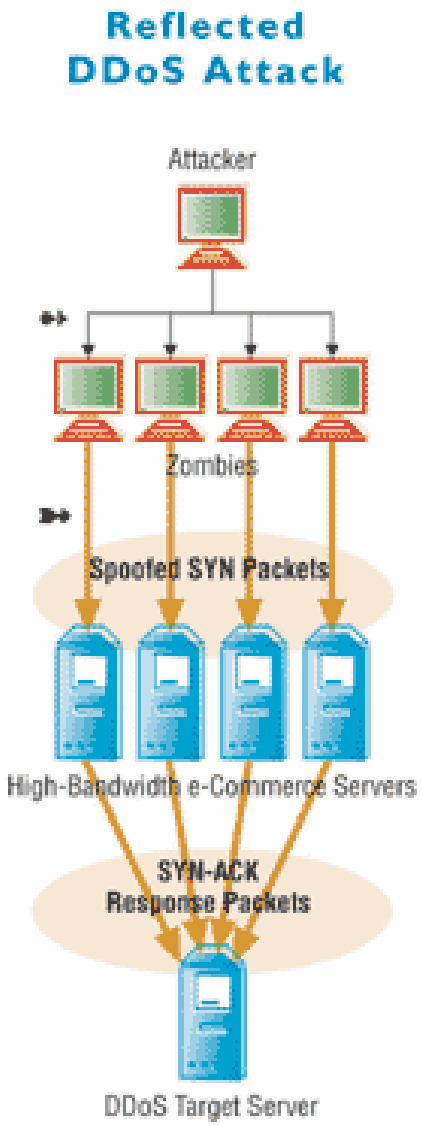


II.- Riesgos informáticos

Ataques de negación de servicio:

Es una modalidad realizada por personas cuyo objetivo es el de bloquear los canales de comunicación mediante el envío masivo de información o mediante la solicitud de requerimientos múltiples de operaciones en los servidores que administran los sistemas de las entidades bancarias.





II.- Riesgos informáticos

Anonimato:

Consiste en la habilidad de ocultar la identidad de las personas durante el uso de la red internacional de datos y las páginas que se visitan, valiéndose para este efecto de servidores especializados o programas de cómputo que muestran una dirección IP que no corresponde con el equipo utilizado para la navegación.

II.- Riesgos informáticos

Skimming:

Es la lectura no autorizada de bandas magnéticas con la finalidad de reproducir la información en otro medio, concretando el robo de identidad asociado a la clave secreta de la tarjeta.

Before
An untampered-with cash machine. This is what an ATM should look like.

Step one
A fraudster fits the skimming device to the ATM's card slot. The device will scan and store personal card details.

Step two
Next, a strip of metal containing a hidden pinhole camera is affixed to the top of the ATM. Apacs admits these miniature cameras are often very well hidden from view.

Step three
The rigged ATM is now ready to roll. All that's needed is an unsuspecting customer.

Step four
While a customer is keying in their pin number, the fraudster is round the corner waiting for the wireless skimming device to transmit the card data to a laptop. This data is used to create a cloned card which can be used immediately with the filmed pin number.

II.- Riesgos informáticos

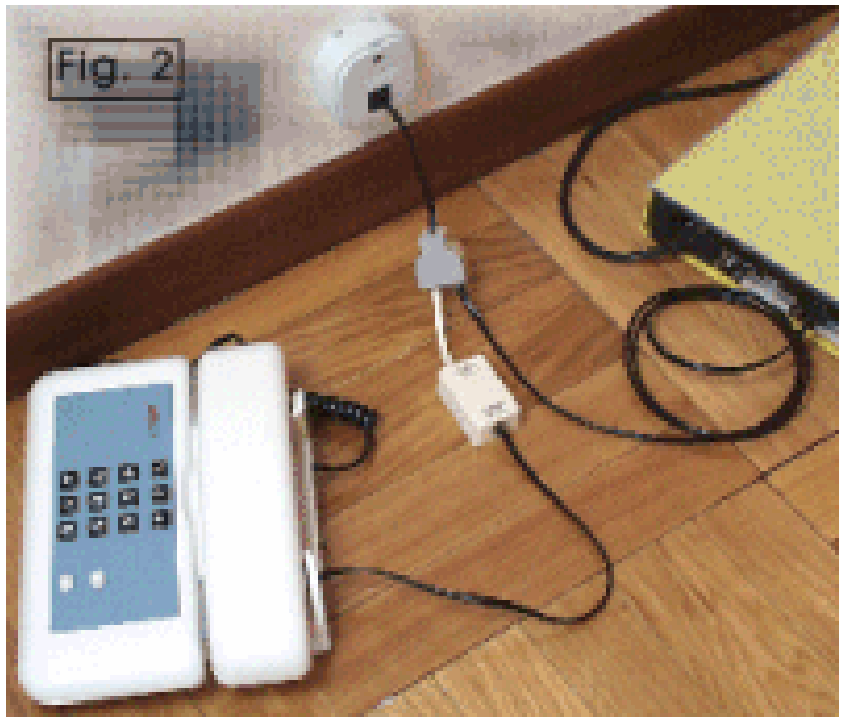
Reemplazo de máscaras de cajeros automáticos:

Consiste en la colocación de una máscara con las mismas características del cajero de la entidad afectada, cubriendo la pantalla, teclado y lectora de tarjeta del mismo con la finalidad de obtener información confidencial de los clientes y usuarios del sistema bancario.

II.- Riesgos informáticos

Interceptación de líneas telefónicas:

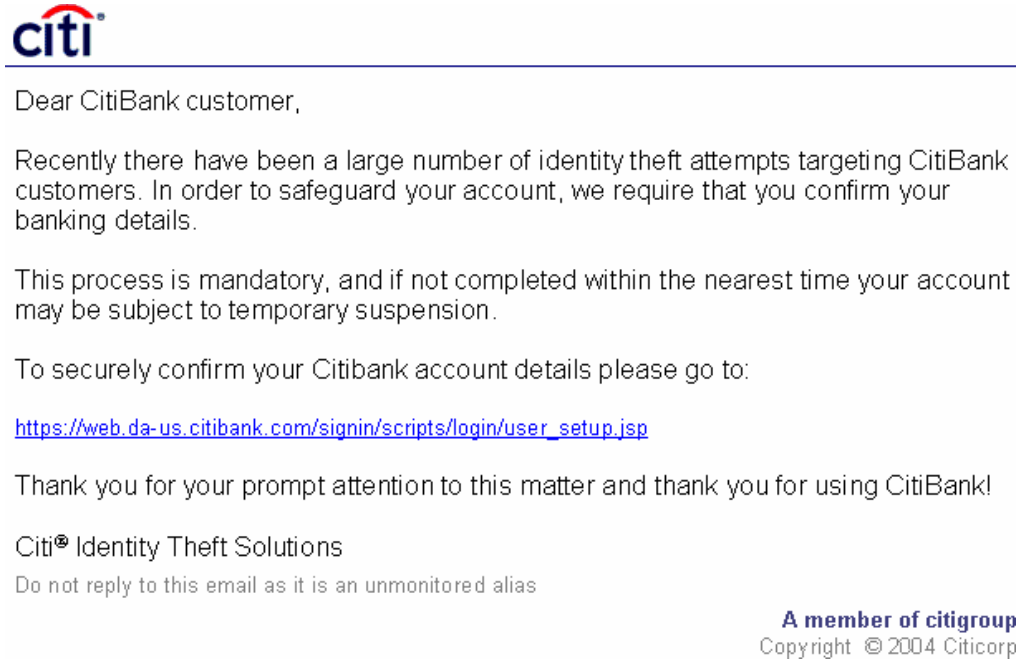
Consiste en la colocación de un dispositivo en la línea telefónica elegida a fin de “escuchar” la información transmitida por ese medio, a partir de dicha información pueden obtenerse el número de cuenta y código secreto de las tarjetas bancarias.



II.- Riesgos informáticos

Spam:

Modalidad de envío masivo de correo, que pretende engañar a los clientes de un banco para motivarlo a seguir el enlace incorporado en el mensaje. Inicialmente eran enviados en formato de texto, ahora el mensaje viene en forma de archivo gráfico para evitar el bloqueo de los mismos.


citi

Dear CitiBank customer,

Recently there have been a large number of identity theft attempts targeting CitiBank customers. In order to safeguard your account, we require that you confirm your banking details.

This process is mandatory, and if not completed within the nearest time your account may be subject to temporary suspension.

To securely confirm your Citibank account details please go to:

https://web.da-us.citibank.com/signin/scripts/login/user_setup.jsp

Thank you for your prompt attention to this matter and thank you for using CitiBank!

Citi® Identity Theft Solutions

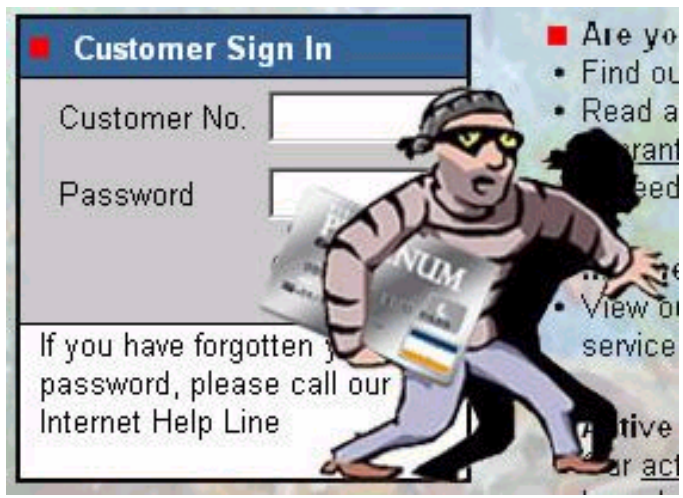
Do not reply to this email as it is an unmonitored alias

A member of citigroup

Copyright © 2004 Citicorp

Phishing:

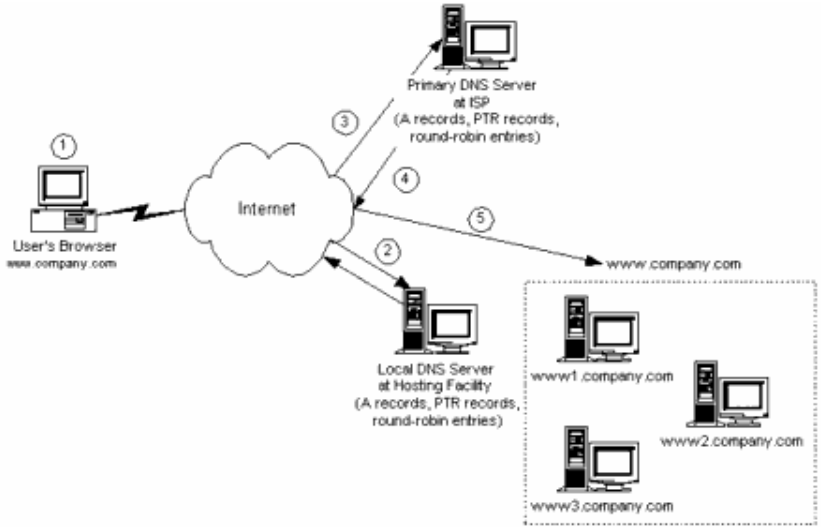
Es una modalidad empleada por la delincuencia cibernética en la que colocan en la red de datos internacional, una copia similar a la página de la entidad afectada con la finalidad de obtener información confidencial.



II.- Riesgos informáticos

Pharming:

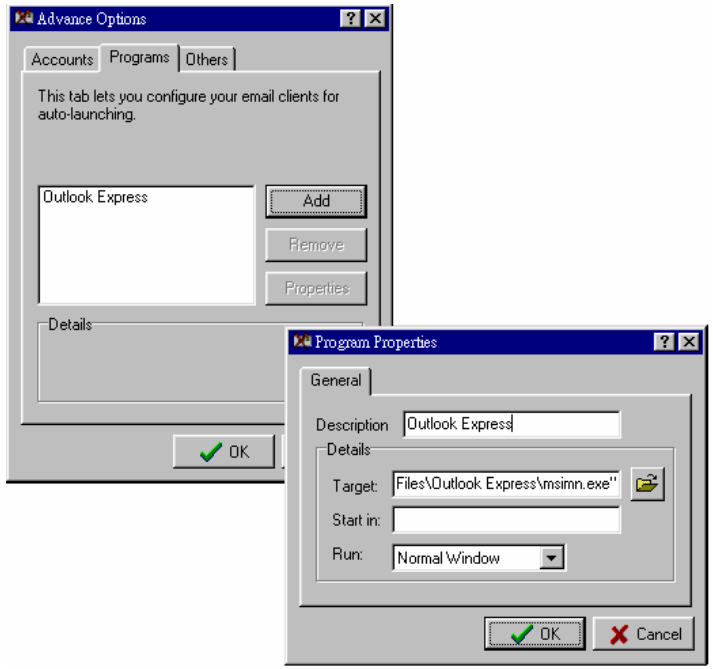
Es una modalidad que consiste en el ataque a los servidores de resolución de nombres en la red de datos internacional con la finalidad de lograr el desvío de la navegación de las víctimas a servidores administrados por los delincuentes cibernéticos.

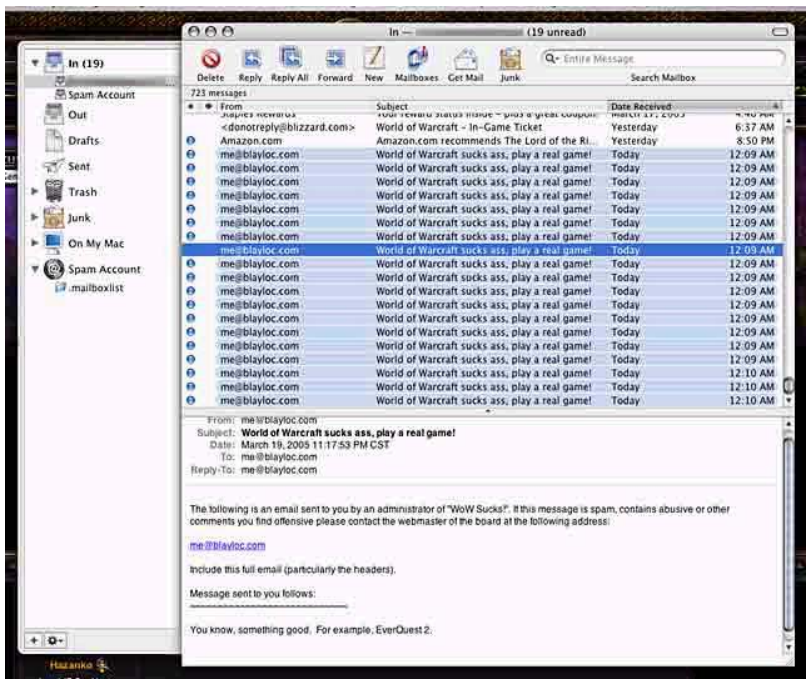


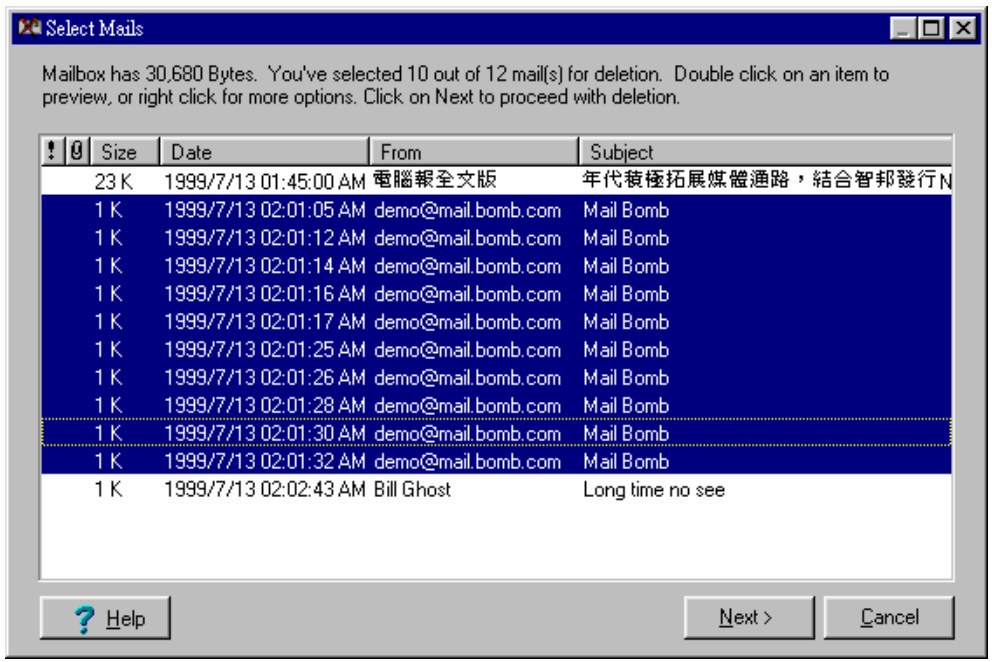
II.- Riesgos informáticos

Interceptación de correos electrónicos:

Consiste en el seguimiento y obtención de información de determinadas cuentas de correo electrónico en los servidores de Internet de correo electrónico, durante el traslado del correo o modificando la configuración de su cuenta de correo electrónico mediante un programa troyano.



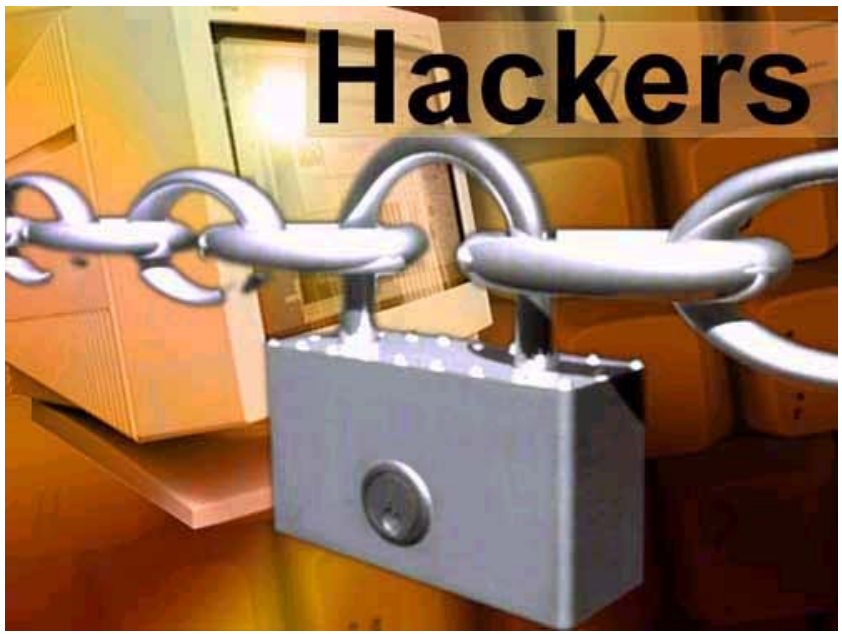




II.- Riesgos informáticos

Legislación:

En muchos países no se encuentra adecuadamente tipificado el delito informático, lo que es aprovechado por los delincuentes cibernéticos para migrar a aquellos lugares y continuar operando debido a las facilidades de comunicación que les ofrece la tecnología.

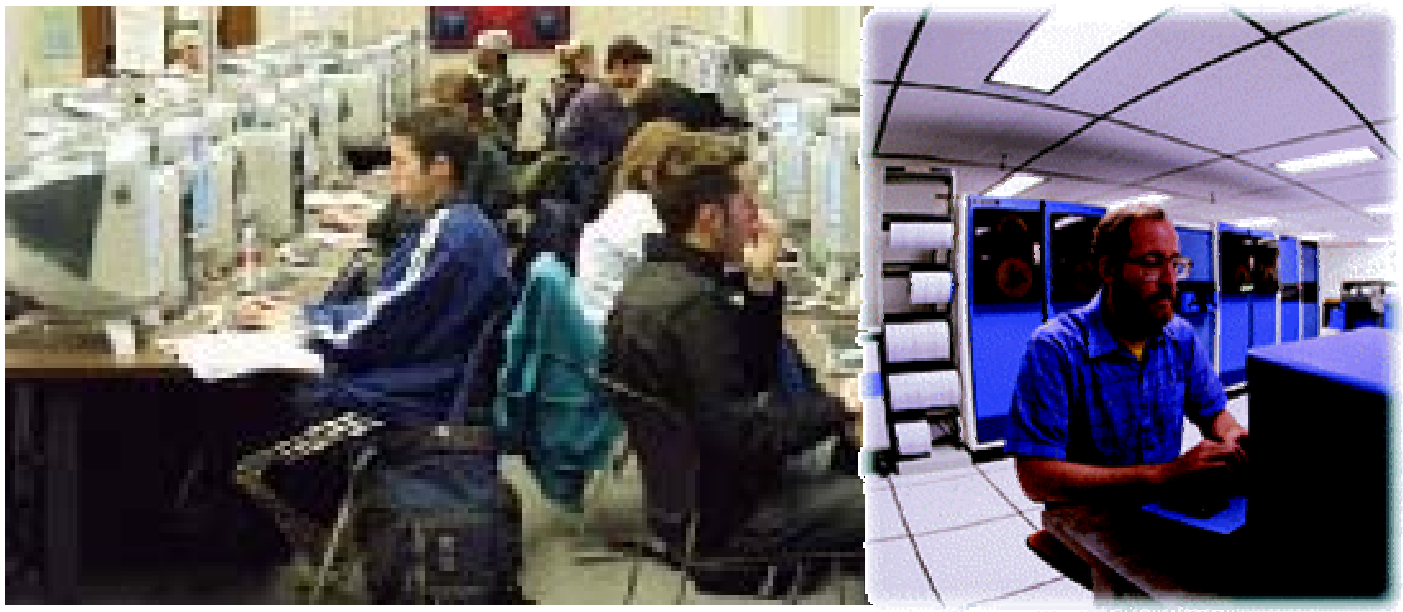


II.- B.- Perfil del autor de delitos cibernéticos

- Jóvenes expertos con estudios avanzados en informática
- Adultos con tiempo suficiente para dedicarse a la investigación

II.- B.- Perfil del autor de delitos cibernéticos

- Personas con necesidad de información o curiosos
- Personas con necesidades económicas u obtener una revancha personal
- Personas con necesidad de información específica o espionaje industrial



II.- C.- Proceso de identificación y verificación del cliente

Los bancos han implementado diversos métodos y procedimientos para la identificación de personas que hacen uso de los sistemas disponibles tanto en Internet, como en la red de cajeros y la banca telefónica.

En algunos casos estos métodos son simples y reproducen el mismo esquema utilizado en cajeros automáticos, en otros, se han implementado medidas adicionales con la finalidad de evitar el robo de identidad.

Como elementos de identificación y verificación se utilizan, números de tarjeta bancaria, código de identificación de usuario, código de identificación personal de tarjeta bancaria, claves de acceso a Internet, segunda clave de verificación o clave de desafío, claves dinámicas entre otras alternativas propuestas.

	B	I	N	G	O
1	4	21	35	47	63
2	1	19	37	50	72
3	10	24	46	51	61
4	6	23	40	55	69
5	3	21	41	49	74

II.- D.- Debilidades explotadas por los delincuentes cibernéticos

Los delincuentes cibernéticos dirigen sus ataques a usuarios domésticos debido a que no actualizan las fallas detectadas en sistemas operativos o programas con la misma prontitud que lo hacen las empresas.

Los usuarios de un navegador de Internet puede verse comprometido en un robo de información personal solo con visitar un sitio Internet malicioso.

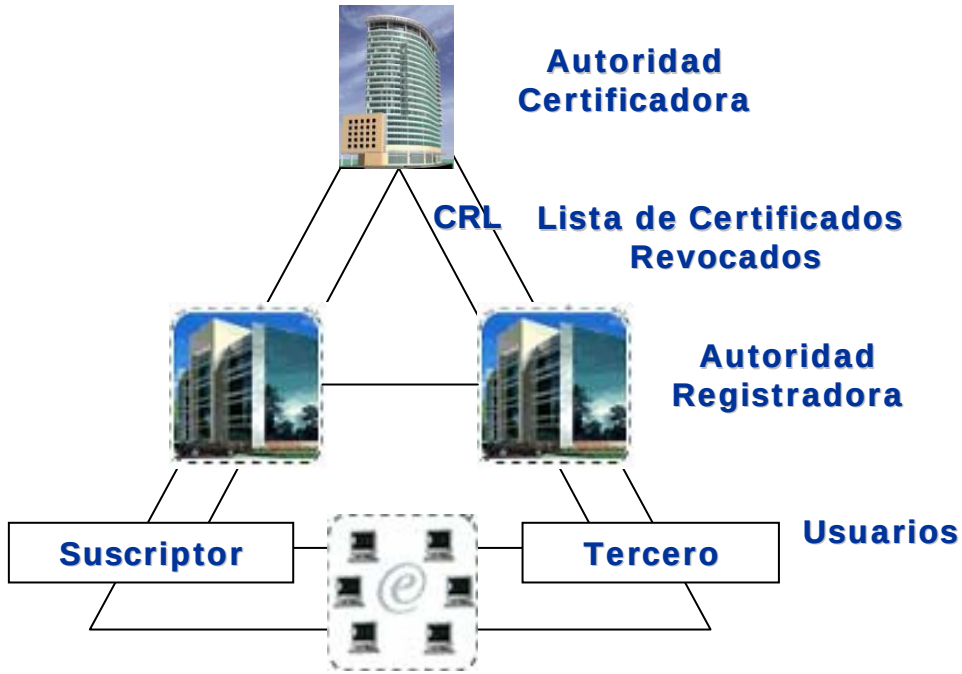
Las debilidades de aplicaciones de reproducción de medios puede facilitar a un hacker el control de la computadora de un usuario a través de un archivo mp3.

El acceso inalámbrico a Internet presenta debilidades que pueden permitir el acceso a información personal.

III.- Proyectos futuros

El eBusiness utiliza un esquema de confianza basado en la infraestructura conocida como PKI (Public Key Infraestructure)que utiliza conceptos y técnicas de llave pública y llave privada, encriptación y otros elementos de seguridad para proveer sus servicios.

El que se reconozca PKI como infraestructura es por el hecho que en sí misma no es una aplicación final de una Organización, sino que es una base formada por diversos elementos que permiten proveer seguridad a las aplicaciones de negocios existentes y a las que se desarrollen a futuro.



III.- A.- Tarjetas inteligentes

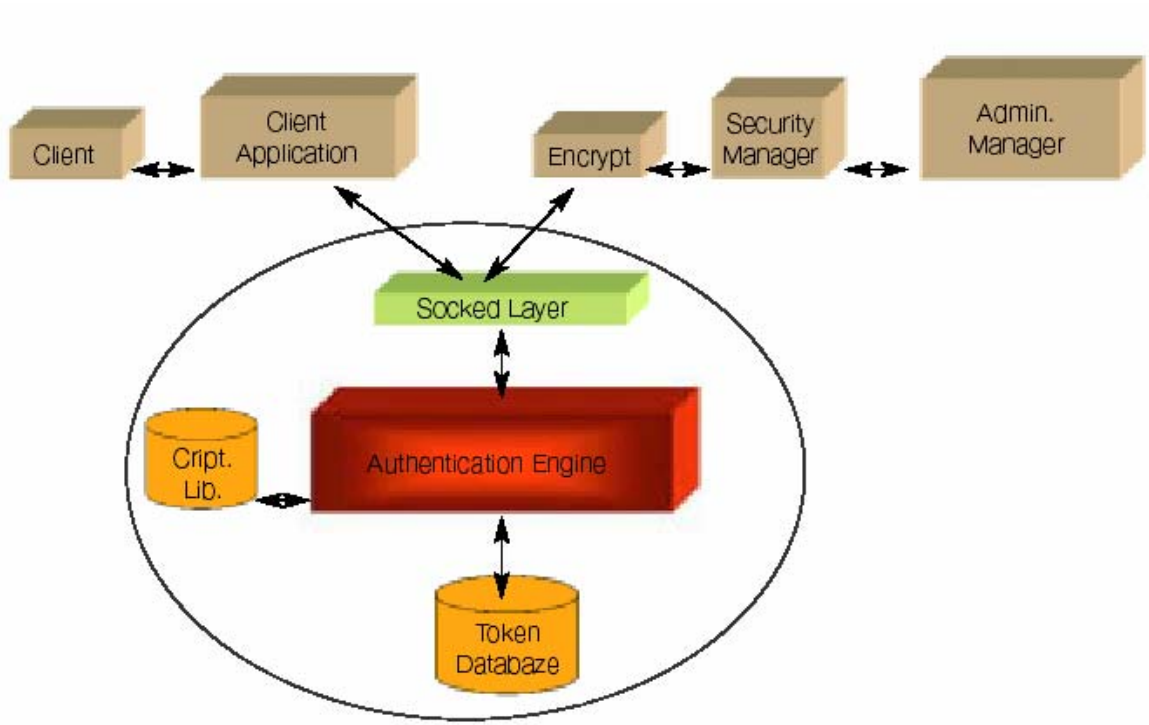
Existen tres tipos de tarjetas inteligentes:

con CHIP que tiene solo memoria de lectura
con CHIP de circuito integrado y microprocesador
con conexión electromagnética a microprocesador externo

III.- B.- Proceso de identificación

Claves dinámicas:

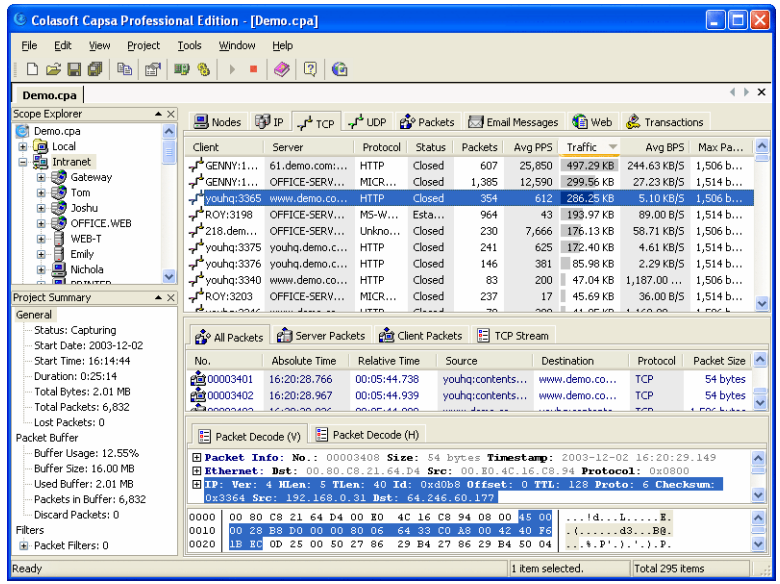
Son códigos de identificación únicos, los mismos que son generados aleatoriamente utilizado un algoritmo predeterminado y reconocido por la aplicación que la utiliza. Los dispositivos que generan dichas claves se conocen con el nombre de Token.



IV.- Recomendaciones

Para los bancos:

- Adecuar los sistemas de control utilizando la misma tecnología empleada por los delincuentes cibernéticos.
- Implementar nuevos sistemas de monitoreo especializados para observar el tráfico de la información, de las operaciones en línea y que permitan la detección temprana de actividades sospechosas u operaciones inusuales.
- Implementar nuevos sistemas de identificación de usuario, un nombre de usuario y una password no son suficientes.
- Realizar pruebas de acceso periódicas y en profundidad, de esta forma se detectarán vulnerabilidades inherentes a la aplicación y no solo en la red o canal de información utilizado ethical hacking.
- Revisar la política e infraestructura de seguridad de forma periódica y contínua.
- Someter a control todas las propuesta de inversiónes en seguridad y replantearlas en base a un cálculo de retorno de inversión usando los datos obtenidos en la fase de análisis de riesgos.



- Security testing methodologies including the OSSTMM
- Stealthy network recon
- Multi-OS banner grabbing
- Remote root vulnerability exploitation
- Privilege escalation hacker
- Unauthorized data extraction
- Remote access trojan hacking
- Offensive sniffing
- Wireless insecurity
- Breaking IP-based ACLs via spoofing
- Evidence removal and anti-forensics
- Attacking network infrastructure devices
- Brute forcing remotely
- Web Applications
- Breaking into databases with SQL Injection
- Cross Site Scripting hacking

IV.- Recomendaciones

Para los clientes:

- Abstenerse de utilizar equipos de acceso público (cibercafés, cabinas, universidades) para efectuar operaciones bancarias.
- Informarse con su banco acerca de las medidas de seguridad implementadas para usar con seguridad los productos y servicios ofrecidos.
- Mantener actualizados los sistemas operativos, navegadores de Internet y programas para evitar virus informáticos, programas troyanos o software espía.
- Verifique la autenticidad de la página utilizada.
- No proporcione su información confidencial a ninguna persona y digite usted mismo la página web de su banco, no deje guiar su navegación por direcciones contenidas en e-mails.
- Cambie continuamente sus clave de acceso, o si sospecha que alguien más puede conocerla.
- Al finalizar sus operaciones en la página web del banco, presione el control “terminar sesión”.
- Si tiene cualquier duda consulte con su banco.