

The logo features a large, stylized letter 'A' in blue with a black outline. A horizontal blue bar with rounded ends is positioned across the middle of the 'A'. The words 'ABSOLUTE ID' are written in a bold, black, sans-serif font across this bar.

ABSOLUTE ID

**When You Absolutely
Need to Know!**

A circular badge with a dark blue background and a white border, containing the word 'WHITEPAPER' in white, uppercase, sans-serif font.

WHITEPAPER

RemoteSafe™ Product Overview
Secure Solutions to Top Threats in Data Protection

Introduction

In the 21st Century, we have a global climate, where users are highly mobile and more technologically savvy than at any other time in history. Individuals and institutions take for granted the ability to instantly communicate anytime, anyplace with anyone over a worldwide heterogeneous technological environment into which more data is transmitted in a single hour than the sum total of the entire Library of Congress and then some. The Internet is a severely under protected network and storage environment where people are lulled into the misplaced belief that their information is safe and secure.

With the rising incidence of threats to sensitive data, and increasing requirements to protect that data, organizations must focus squarely on their security infrastructure. Protecting sensitive and critical data, no matter where it resides, and ensuring that only the appropriate persons have access to that data, must be a core requirement of every company's security strategy.

Ad-ware, spy-ware, mal-ware, etc., are now all more correctly named crime-ware, giving them a more appropriate descriptor. Crime-ware is any computer program or set of programs designed expressly to facilitate illegal activity online. There are many types of attacks including the more pervasive attacks listed below and described in more detail in Appendix of Risks:

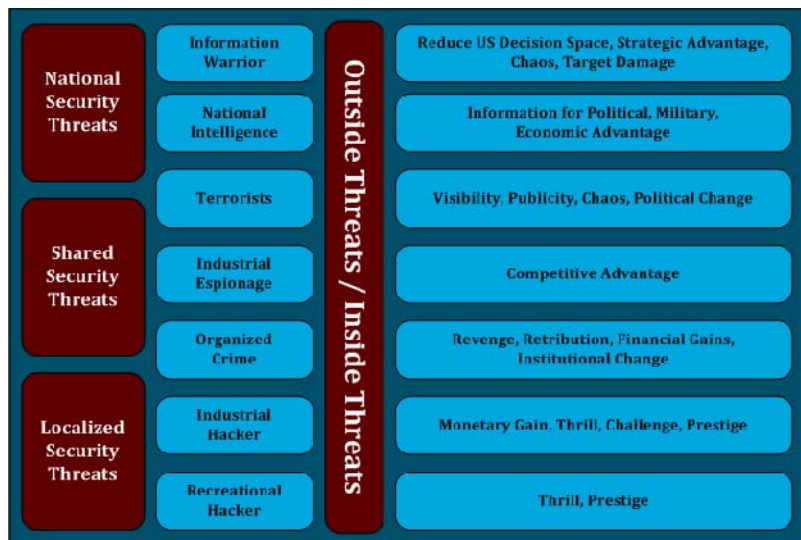
- *Phishing*
- *Password Database Theft*
- *Password Stealing and Identity Theft*
- *Man-in-the-Middle (MitM) Attacks*
- *Man-in-the-Browser (MitB) Attacks*
- *Identity Theft*
- *StuxNet Worm Derivations*

Even today, with all of the public information about how unsafe the Internet has become, individuals and financial institutions alike routinely put their highly cherished "Financial Family Jewels" of information out for the cyber-thief to steal. Whether it's the cost to build the necessary protective environments or the poor deployment of security technology, the result is the same – everyday cyber-thieves add another notch in their data theft belts.

The "REAL" Threat

Crime and technology are getting ever closer. Today's reports on security risks mostly cover amateur frontal attacks that exploit poor system administration or the latest hole that is not yet patched and are relatively inexpensive to mount.

Builders of viruses take a little less direct approach by planting malicious code, but even this can be done nowadays by amateurs with limited means and unserious motives.



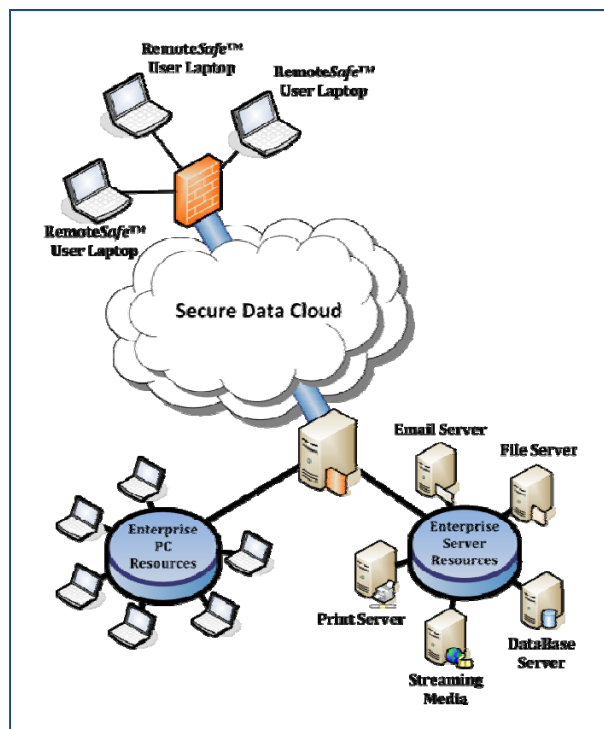
Serious hackers are less interested in hacking for fun and more interested in attacking for profit. Organized crime from diverse geographies is devoting extraordinary amounts of energy and resources to online fraud and theft. Technology has created a new super-empowered criminal.

Information warfare professionals are distinguished from the amateurs by objectives, resources, access, and time. A professional is well funded and has adequate resources to research and test the attack in a closed environment – to make its execution flawless and therefore less likely to attract attention. The resulting attacks do not get press coverage because they are not mounted against low value assets; however, in one unguarded instant, you might be facing lost revenues, lost reputation, and even regulatory exposure.

Absolute ID's RocITSafe™ family of products are designed and developed from the core with the highest level of security in mind. Every RocITSafe solution contains a fully integrated and highly secure operating environment that dramatically enhances protection against Cyber-theft.

RemoteSafe™ Product Overview

RemoteSafe is a member of the RocITSafe product family and is a highly secure mobile computing platform, delivered on a FIPS certified hardware encrypted flash drive or spinning hard drive.



RemoteSafe allows mobile users to securely log onto one or more remote desktop computers. RemoteSafe can run in three modes; 1) Bare-Metal-Boot mode – the most secure of the three operating modes – turns off the client platforms hard drive preventing all forms of cyber-attacks from penetrating the system; 2) Dual Bootable/Pluggable which uses the client system's Windows OS but loads a secure middleware application on the client system creating a secure buffer between the client hardware and the RemoteSafe software system; 3) Pluggable only which uses the entire underlying client system Windows OS and creates a secure communication channel between RemoteSafe and the host system.

RemoteSafe leverages existing IT infrastructure within an enterprise, such as the enterprise's existing VPN services, intranet network security, and workstation security deployed within the enterprises Windows computer workstations.

RemoteSafe is deployed onto RocITSafe drives and provides the end-user with the ability to securely access their office desktop, and/or a pool of shared desktops that maintains their Windows applications and services. Utilizing a RocITSafe Drive eliminates the need to purchase and secure new mobile computers, such as laptops, and provides a much higher level of information security and assurance.

The VRE contains a module – CredentialSafe™ – which enables an enterprise to securely provision, manage, and store X.509 certificates, and RocITCrypt credentials on RemoteSafe, hidden and protected from end-user access. After the user authenticates to their drive, it launches the secure Virtual Runtime Environment (VRE) installed on the drive. RemoteSafe then automatically launches

an application that allows the user to set up a secure VPN connection with the enterprise. This secure channel leverages the X.509 Certificates stored in the CredentialSafe secure storage area on the drive.

After opening a secure VPN communication channel, RemoteSafe automatically starts a remote desktop client application that provides the user a remote log on to a Windows computer, over the secure VPN communication channel. The user is then able to select one or more workstations, if enabled by the RemoteSafe Administrator.

RemoteSafe also allows users to run a remote desktop that is defined within a shared computer resource pool. In this configuration, the end user selects a resource pool DNS name that utilizes either hardware and/or software load balancers to a pool of enterprise workstations that have been configured for a set of users credentials. When the user selects the resource pool DNS, they are automatically routed to one of the computer workstations running in the pool.

Additionally, RemoteSafe can be configured with a Secure Internet Browser that can be centrally configured and managed by the systems administrator to provide highly secure browsing of white listed internet or intranet sites.

RemoteSafe™ Platform

The RemoteSafe Platform is a hardware agnostic solution which is a highly configurable and manageable runtime environment and set of applications, deployed on a secure bootable USB flash or spinning drive that provides a FIPS certified AES256 encrypted partition. The drive can be configured with either password or biometric authentication enabling access to the encrypted partition.

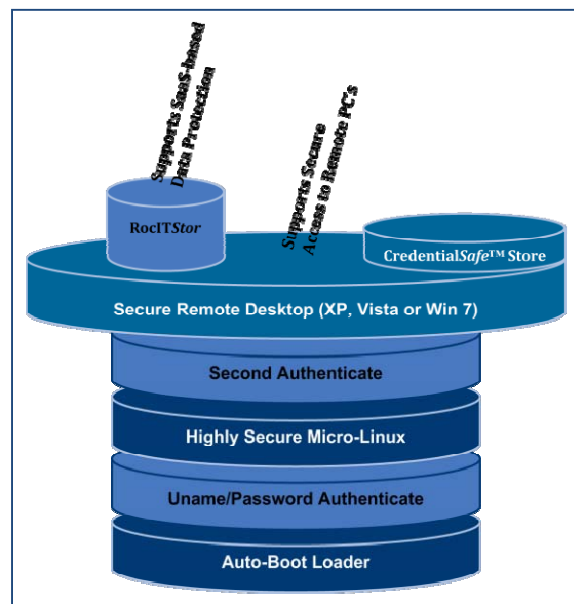
RemoteSafe is designed hierarchically where each layer of the solution provides additional levels of security and user control.

The architecture has three major elements in the hierarchy starting from the core and moving up the secure stack – VRE™ » ViSoS™ » RemoteSafe Solution.

At the core of every RemoteSafe solution lays the VRE™. The VRE includes: 1) Auto Boot Loader; 2) Secure Kernel; 3) Micro-Linux.

Just above the VRE is the ViSoS layer which includes: 1) Secure Remote Desktop; 2) CredentialSafe.

Finally, at the user layer, RemoteSafe includes: 1) Secure access to RocITCrypt and RocITStor services; 2) Access to Proprietary & Standard User Application Software; and 2) Access to Proprietary & Standard User-specific Hardware.



RemoteSafe drives are configured with a Secure area and two physical partitions that create a layered security approach to data protection, including:

- *Secure Drive Area*
- *Public Read-Only Boot Partition*
- *Secure Encrypted Partition*

Once the user authenticates to *RemoteSafe*, the solution launches *ViSoS™* Runtime Environment (VRE) – a secure runtime environment that provides a highly secure container in which the user can run applications.

ViSoS™ Runtime Environment (VRE)

The VRE is a highly secure, Linux-based operating environment that has been DoD hardened and locked-down from end-user access providing the following capabilities:

- Configuration of network management and protocols
- Automated Drive Management and Control including updating the drive software, services, applications, and configuration settings, and remotely locking and disabling access to the drive.
- Running secure channel communication solutions such as setting up many enterprises VPN client solutions.

The VRE also contains a certificate/credential management service – *CredentialSafe* – and supports secure access to smart card readers that are attached to the remote host computer system, enables CAC/PIV authentication and utilization of certificates on smart cards with the applications and services on the system.

CredentialSafe™ – Secure Credential and Certificate Storage

CredentialSafe is an Absolute ID proprietary service that provides secure storage, management, and utilization of enterprise and user credentials and X.509 certificates to secure (encrypt/decrypt) data, and/or set up secure communication channels with other systems.

This service is integrated with the underlying drive hardware and provides the option to store credentials in a secure area of the drive that is not exposed or accessible to end users. It also supports administrative interaction with the pre-configured *RocITCrypt* service to centrally manage credentials on a server.

The credentials and X.509 certificates are exposed to the applications and services running within the VRE through a PKCS11 library, so that applications such as VPN clients, remote desktop clients (RDC), or browsers can utilize the certificates to perform authentication, or secure remote communication channels.

The credentials are also utilized by Absolute ID's *RocITStor* application to securely authenticate with the *RocITStor* storage service, and encrypt/decrypt file objects for secure data-in-flight and data-at-rest user requirements.

RocITCrypt™: Credential-based Data Protection Service

RocITCrypt is a centrally managed security service that allows the enterprise to provision and manage a variety of different credentials for their organization and end users. Through the use of sophisticated key management technologies, administrators are able to define and set up individual security keys (credentials) that can be granted to different users and groups within the organization. These credentials are then used to encrypt different data within the organization; including simple data blocks, database records, full files or folders, or individual documents. Once encrypted the data becomes “opaque” and packaged into a secure data object that can be securely passed around the network, or within enterprise applications.

Each opaque data object has an associated metadata record that defines the credential algorithm (keys) that was utilized to encrypt the object. Only users that have the necessary credentials may gain access (either read-only or read/write) to the object to be able to decrypt and utilize the

object. Absolute ID provides utilities that can be integrated into enterprise applications and infrastructure, such that encryption and decryption occurs on the “edge” utilizing end user credentials that are securely stored within user tokens or secure credentials storage locations.

Each integrated end-user application, enterprise service, or web site leverages these credentials to ensure that unsecure data is no longer available “in the clear” at rest, on the wire, or within the specified application itself. Information such as user’s on-line e-identity and credit card information (two key targets for cyber-thieves), on-line banking statements, stock portfolio information, etc.

The RocITCrypt service is a highly fault tolerant, scalable, and redundant service that virtually eliminates the need for key bunkering, and dramatically minimizes the cost of “server encryption farms”, since it decentralizes the highly processor intensive operations of encryption and decryption to the edge within the end-user’s secure RemoteSafe environment.

Secure Channel Communication / Virtual Private Network (VPN)

The VRE can be configured to work with many existing enterprise Virtual Private Network (VPN) services, using a secured communication channel. The VRE will be configured to auto-connect to the corporate VPN using IPSEC cryptographic tunneling protocols leveraging X-509 certificates or RocITCrypt credentials stored in CredentialSafe to provide security, confidentiality, sender authentication, and message integrity within the VPN.

When the user boots up the secure VRE environment, they are prompted to authenticate to the VPN, by providing their password and/or certificate or credential stored within the secure area of RemoteSafe, or certificate stored on their CAC/PIV card. Additionally, the VPN gateway can be configured to white list the MAC addresses of the RocITSafe Drives to reduce the risk of access to the VPN from un-trusted systems or users.

Once the user has authenticated to the VPN server, they are able to access resources available to them within the enterprise network infrastructure, including: servers, workstations, or peripheral devices such as printers.

At this point, the VRE launches a secure remote desktop client (SeRDC) that is used to remotely access intranet resources, such as the user’s office workstation or workstation pool over the secure VPN communication channel.

Secure Remote Desktop Client (SeRDC)

The Secure Remote Desktop Client (SeRDC) is the RemoteSafe secure client for Windows Terminal Services, capable of natively speaking Remote Desktop Protocol (RDP) in order to present a user’s Windows desktop. The RDC is configured by the administrator to utilize 128-bit encryption and password protected sessions.

The Remote Desktop Protocol (RDP) is the presentation-layer protocol that allows a terminal or client to communicate with a Windows XP Professional-based computer. RDP works across any TCP/IP connection, including local area network (LAN), wide area network (WAN), dial-up, Integrated Services Digital Network (ISDN), digital subscriber line (DSL), or virtual private network (VPN) connections. RDP delivers to the client computer the display and input capabilities for applications running on a Windows XP Professional-based computer.

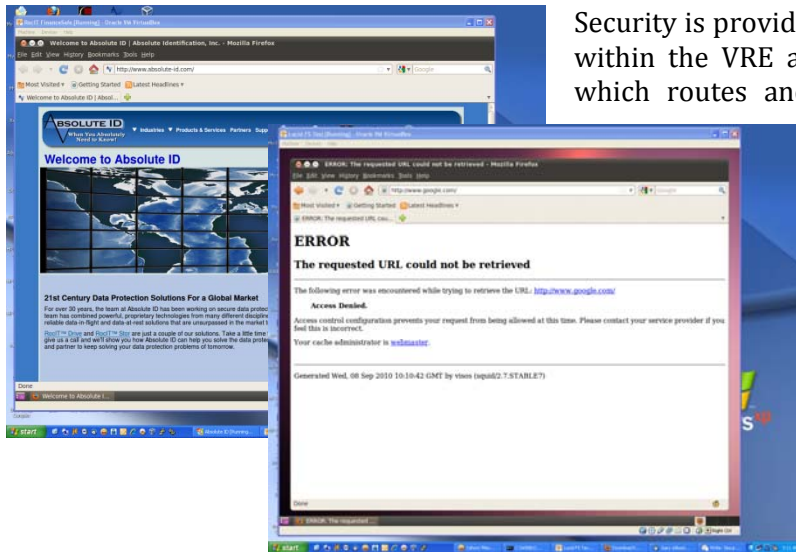
When using Remote Desktop Protocol, many of the client resources are available within the session, including the client drives, audio sources, serial and parallel ports, printers, and smart card readers.

Data encryption protects your data by encrypting it on the communications link between the client and the Windows XP Professional-based computer. Encryption protects against the risk of unauthorized interception of transmitted data. The RDC sessions are configured utilizing 128-bit encryption.

Note: Administrator must configure the Remote Desktop services on the host workstation(s) to which RemoteSafe Drive will be connected to ensure the necessary security protocols are evoked.

Secure Internet Browser

A Secure FireFox browser is installed – optionally – within the VRE and configured by the administrator defining white (available) and/or black (unavailable) IP addresses, URL's, and domains. The Secure Browser can be configured with a user-defined home page.



Security is provided by configuring the network stack within the VRE and setting up a transparent proxy which routes and filters all network traffic to an administrator defined set of trusted sites. The administrator has the flexibility to set up white (trusted) and black (un-trusted) URL's and IP addresses, such that the browser will not have access to any unwanted sites.

Additionally, the browser runs within a virtual runtime environment and filesystem that is refreshed whenever it is started (sandbox); thereby eliminating the ability for the

browser to inadvertently infect the VRE filesystem with viruses or malware.

The secure browser is configurable by an enterprise administrator with the following customizable list of features:

- Anonymous proxy that ensures the end user can only browse to either available sites (white list), or is blocked from other sites (black list).
- All browser executables, settings, temporary files, and downloaded files are stored in a secure encrypted partition on the thumb drive. i.e. There is NEVER any data left behind on the host computer hard drive.
- The browser runs in a jailed “sandbox” environment that is refreshed every time that the drive is restarted. Thus, there is *never* any data left behind and it always starts from a clean instance as configured by the Administrator.
- Browser key-logging defense mechanisms are supported to enable users to enter critical form data such as user names and passwords without worry about potential hardware or software key logger threats.
- The browser has automatic access to the end-user drive client certificate stored inside of the drive's secure certificate store.
- When running in bootable mode, the VRE can be configured to optionally mount and expose Shared Partitions. If a Shared Partition is exposed to the Browser and is not configured as a

read-only drive, then the user may download and store files via the browser to the shared partition.

- The browser supports the storage, management, and use of user names and passwords located within a secure password locker inside of the VRE.

RocITStor™: Secure Storage Service

To augment the highly secure operating environment which RemoteSafe provides every user, RocITStor can be added and is the newest generation of SaaS (Software as a Service), or enterprise data protection solution that provides users with the power of RocITCrypt to crypto-protect their data while also offering a secure way to collaborate with workflow partners and/or communities of common interest. RocITStor is a small footprint data protection application targeted to any individual who needs to lock down data on a laptop or desktop computer. RocITStor is loaded directly onto a user's desktop and provides a secure encrypted mapped drive as an additional resource from within the windows explorer.

RocITStor is available as either a SaaS service or as an enterprise solution for corporate customers desiring the ability to control their own servers, or leverage existing storage infrastructure including NAS (Network-Attached-Storage) and SAN (Storage-Area-Network) solutions.

RemoteSafe™ Hardware Platforms

The RemoteSafe secure software stack is hardware agnostic and supports several best-of-breed USB hardware platforms, including:

- *Kanguru Defender Elite (Preferred Choice)*
- *MXI Security (Biometric Choice)*

All RemoteSafe drives support both a secure bootable USB flash drive that is partitioned with a public accessible, or CD-ROM boot partition, and a secure AES256 encrypted partition that is unlocked upon authentication to the drive with a password, or through biometric authentication.

The drives are password protected and fully manageable from a central management server that supports many management capabilities including the ability to disable drives in the field if lost or stolen.

Kanguru Defender Elite

Defender Elite is a FIPS 140-2 certified USB Flash Drive. The drive has an onboard cryptographic processor which handles all data encryption/decryption. The chip also handles the authentication component of the password login process (on-chip matching). Defender Elite holds the following hardware security certifications:

- *FIPS 140-2 Certificate # 1270 (Device)*
- *FIPS 197 Certificate # 1066 (AES with 256-bit key in CBC mode)*
- *SHA-1, SHA-256 Certificate # 1099*
- *RSA Certificate # 506*
- *ANSI X9.31 DRNG w/ AES 256-bit Certificate # 603*

The AES key (which is generated onboard through a FIPS approved random number generator) is used to encrypt / decrypt data on the secure partition and is obfuscated and stored in a hardened secure location on the device. This location is inaccessible to the users of the device. The device is filled with a tamperproof hardened epoxy which completely covers all chipset components and pin

connections. Brute force attack countermeasures are built into the firmware of the device which will trigger an AES key deletion to prevent unauthorized access to the data set.

Remote Disable for Virtual Environment

Defender Elite provides an administrator with the ability to remotely disable a lost/stolen device. In the RemoteSafe configuration, there is a service initiated upon boot-up of the virtual Linux environment (which runs in the background – completely transparent to the user). This service calls out to the central server (hosted by the enterprise) over a TLS encrypted tunnel to alert the server that the particular device has just authenticated. The server checks against any pending actions for the specific device and provides the corresponding command back to the service running on the device. If the device has no pending action (ideal), then the user's virtual environment opens and allows access to the device. If there is a pending action such as a disable command, access to the virtual environment is terminated and a flag is set to disable access unless an administrator allows access again.

Kanguru Defender Elite Management Features

The Kanguru Defender Elite provides the following additional management features and capabilities:

Device Configuration

- Enable & Disable Devices
- Master Password Configuration
- User Password Configuration
- Define Password Security Policies
- Reset Devices to Default Configuration
- Customize Auto Unmount Settings
- Save / Load Settings for Quick Provisioning
- Store Contact Info on Devices
- IP Domain Control (Whitelist / Blacklist)
- Set Offline Access Settings
- Network / Remote Mgmt Configuration
- Dormant Device Mode

Remote Actions

- Wipe Device Data
- Disable Device
- Wipe Device Data & Disable Device
- Change User Password
- Change Security Policies

- Update Device Version
- Send Message to Device
- Set or Update IP and Domain Permissions (Whitelist/Blacklist)

Control

- Export Audit Logs to XLS
- Graphical Reports
- Advanced Users and Roles
- Device Groups
- Advanced Auditing, Filtering and Logging
- Active Directory Support

Device Control

- Computer, User and Device Management
- System Wide Policies
- Computer Policies
- Policy Templates
- Email Alerts
- Advanced Filtering

Appendix of Risks

Phishing

Although passwords can also be obtained through less sophisticated means such as eavesdropping, guessing, dumpster diving, and shoulder-surfing, phishing is a common form of cybercrime typically carried out through e-mail or instant messaging, providing links or instructions that direct the recipient to a fraudulent Web site masquerading as a legitimate one. The unsuspecting user enters personal information (such as user names, passwords, Social Security Numbers, and credit card/account numbers), which is then collected by the hacker. Of particular attraction to phishing scams are online banking, payment services, and social networking sites.

According to the Gartner survey referenced previously, phishing attacks continue to exact financial damage on consumers and financial institutions, with a trend toward higher-volume and lower-value attacks. The survey found that more than five million U.S. consumers lost money to phishing attacks in the 12 months between September 2007 and 2008, a 39.8% increase over the number of victims a year earlier.

Password Database Theft

Stolen user credentials are a valuable commodity and often times, cybercrime rings operate solely to obtain this information and sell it to the highest bidder or use it themselves to access user accounts. Hackers steal user data and passwords from one web site operator to hack other sites. Since many people use the same user ID and password combination for multiple sites, the attacker can hack additional accounts that the user has.

The Sinowal Trojan is a well-known attack developed by a cybercrime group several years ago that is responsible for the theft of login credentials of approximately 300,000 online bank accounts and almost as many credit card accounts. In late 2009, Microsoft Hotmail⁷, Google Gmail, Yahoo, and AOL were victims of phishing attacks that exposed thousands of e-mail account user IDs and passwords.

Password Stealing and Identity Theft

These types of attacks rely on the ability of the attacker to fool users into giving up their personal information and credentials. Since users are typically vulnerable to these types of attacks, any method that relies on a credential that can be disclosed is vulnerable to social engineering attacks. Note, however, that this does not include a physical transfer because users can be rather easily fooled over the phone or via e-mail and the Internet to disclose personal information, but just like the keys to their house or their ATM card, people are less likely to hand someone they don't know their physical smart card or token device.

In contrast, hardware-based secure storage and smart cards are non-transferable and, resist cloning therefore, are less vulnerable to social engineering. The status of software-based secure storage and software-based smart cards is very dependent on the implementation. Many popular implementations enable a user to copy and paste the credential, making it transferable and, therefore, vulnerable. However, it is possible to prevent the user from doing this (without expert hacking skills), in which case, the solution does provide some degree of protection.

Man-in-the-Middle (MitM) Attacks

In this type of threat, the attacker can actively inject messages of its own into the traffic between the user's machine and the authenticating server. One approach for MitM attacks involves pharming, which involves using malicious network infrastructures, such as malicious wireless access points or compromised DNS servers, to redirect users from the legitimate site they are trying to access to a malicious fraudulent Website that accesses the user credentials and acts on behalf of the user to perform malicious activities.

This type of attack is only successful when the hacker can impersonate each endpoint to the satisfaction of the other. The use of SSL authentication using a mutually trusted certification authority provides strong protection against MitM threats. When the certificate validation relies on the user, the user may fail to correctly validate server certificates and will click through the warning messages. Therefore, when using a certificate-based authentication solution, the onus is usually on the bank itself to ascertain whether the user's

certificate is valid and will not allow a session to be created when the certificate does not match the one in its system.

Although SSL with server authentication makes man-in-the-middle attacks harder to carry out, they are still possible by using phishing or other methods. We do remark that one-time passwords have the advantage that stealing the credential provides the attacker with a single access only (in contrast to stealing a regular password or a credential in secure storage, which provides the attacker with long-term, repeated access). Damage is limited but the vulnerability still exists.

The most effective implementation to defend against these attacks is through the use of smart cards/tokens that utilize the device along with a user ID and password for secure two-factor authentication.

Man-in-the-Browser (MitB) Attacks

MitB is a Trojan horse program, a variant of a MitM attack that infects the user internet browser and inserts itself between the user and the Web browser, modifying and intercepting data sent by the user before it reaches the browser's security mechanism. A MitB attack has the ability to modify Web pages and transaction content in a method that is undetectable by the user and host application. It operates in a stealth manner with no detectable signs to the user or the host application. Silent-banker is a well-known example of a MitB attack targeted at bank transactions. It uses a Trojan program to intercept and modify the transaction, and then redirect it into the attacker's account.

A MitB attack is carried out by infecting a user browser with a browser add-on, or plug-in that performs malicious actions. In principle, as soon as a user's machine is infected with malware, the attacker can do anything the user can, and can act on their behalf. If a user logs into their bank account while infected, the attacker can make any bank transfer that the user can. By the virtue of being invoked by the browser during Web surfing, that code can take over the session and perform malicious actions without the user's knowledge.

An effective defense against MitB attacks is through transaction verification utilizing either out-of-band (OOB) technology, in which a user's identity is verified through a separate channel, such as a telephone. Using a separate channel reduces the risk that both the internet and the additional channel have been compromised. In large financial environments, for example, when a user initiates a transaction, such as a funds transfer, the details of the transaction can be captured and sent back to the user via an automated phone call or SMS message for verification before the transaction is processed. User input is performed either through Interactive Voice Response (IVR) or the keypad. Both of these approaches assume that the user has mobile phone connectivity during the transaction.

Another approach involves the use of a secure portable Web browser that is launched from a bank-issued USB token after the user inserts the device and enters their password. After successful login, the user is taken directly to the issuing bank's Web site. Utilizing a clean, non-infected browser helps ensure that there is no malware in the browser.

Fraud detection also helps limit the damage an MITB attack can wreak. Although fraud monitoring works after the fact, once a threat has been detected, it can provide useful information to the financial organization as to the types of threats being perpetrated against their infrastructure. User behavior analysis and trend reporting that most fraud detection programs provide can help FSPs determine the risk associated with certain types of transactions. However, fraud detection alone provides little comfort without a formidable defense strategy. When working together with strong user authentication, threats can be captured and contained, while authorized users are allowed secure access to their accounts.

Identity Theft

Identity theft refers to all types of crime in which someone illicitly obtains and uses another person's personal data through deception or fraud, typically for monetary gain. With enough personal information about an individual, a criminal can assume that individual's identity to carry out a wide range of crimes. Identity theft occurs through a wide range of methods—from very low-tech means, such as check forgery and mail theft to more high-tech schemes, such as computer spyware and social network data mining.

StuxNet Worm Derivations

Targets Scada Systems: Thumbdrive-based: Exploits Zero-Day vulnerability in MS Windows Systems: specially crafted link file and just by viewing the link file vulnerability icon you launch the worm. Digitally signed from RealTech or J-Micron in Taiwan.

About ABID

Absolute Identification, Inc. is an innovative provider of data protection products and services that protect critical data throughout its entire lifecycle. Every Absolute ID solution employs technologies which create sophisticated, highly secure data that cannot be broken, dramatically enhancing data availability, confidentiality, and integrity and prevents unauthorized access or theft of digital data while providing a new total cost of ownership (TCO) for key management. Absolute Identification, Inc., is headquartered in Scotts Valley, CA.

Contacts

For further information about the company, visit www.absolute-id.com or contact Absolute Identification, Inc. at one of the locations listed below:

.....

Headquarters

5353 Scotts Valley Dr.
Suite D
Scotts Valley, CA 95066
Phone: (831)459-8199
Toll Free: (888)459-8199
Fax: (831)480-5886
Info@absolute-id.com

ABID International

114 France St.
DDO, Quebec
Canada, H9A 1K1
Phone: (831)278-0957
Fax: (831)515-5256
Canada@absolute-id.com

ABID Federal Group

22 East 35th Place
Steger, IL 60475
Phone: (708)755-1583
Phone: (831)278-0952
Fax: (831)515-5215
Federal@absolute-id.com