



Ethical Hacking and Countermeasures

Version 6



Module XLVI

Securing Laptop Computers

Laptop Stolen With Personal Data On 300,000 Health Insurance Clients

Horizon Blue Cross Blue Shield of New Jersey is offering its members free credit monitoring for one year as a result of the security breach.

By Marianne Kolbasuk McGee, [InformationWeek](#)

Jan. 30, 2008

URL: <http://www.informationweek.com/story/showArticle.jhtml?articleID=206100526>

Horizon Blue Cross Blue Shield of New Jersey has notified its members that an employee laptop computer containing personal information -- including Social Security numbers -- for about 300,000 individuals was stolen in early January.

The health care insurer has sent letters to thousands of its members alerting them about the theft, which occurred in Newark, N.J., on Jan. 5. On its Web site, the company says a "security feature was initiated" on Jan. 28 that "destroys all the data on the stolen computer."

Horizon Blue Cross Blue Shield of New Jersey says the personal information contained on the computer also included names and addresses of members, but no medical data.

The company says it "believes" it is "highly unlikely" that any personal data stored on the stolen computer has been accessed and that the computer was "password protected."

Nonetheless, the insurer is offering affected members free credit monitoring for one year.

Horizon Blue Cross Blue Shield of New Jersey is the latest company to report a security breach related to a stolen laptop.

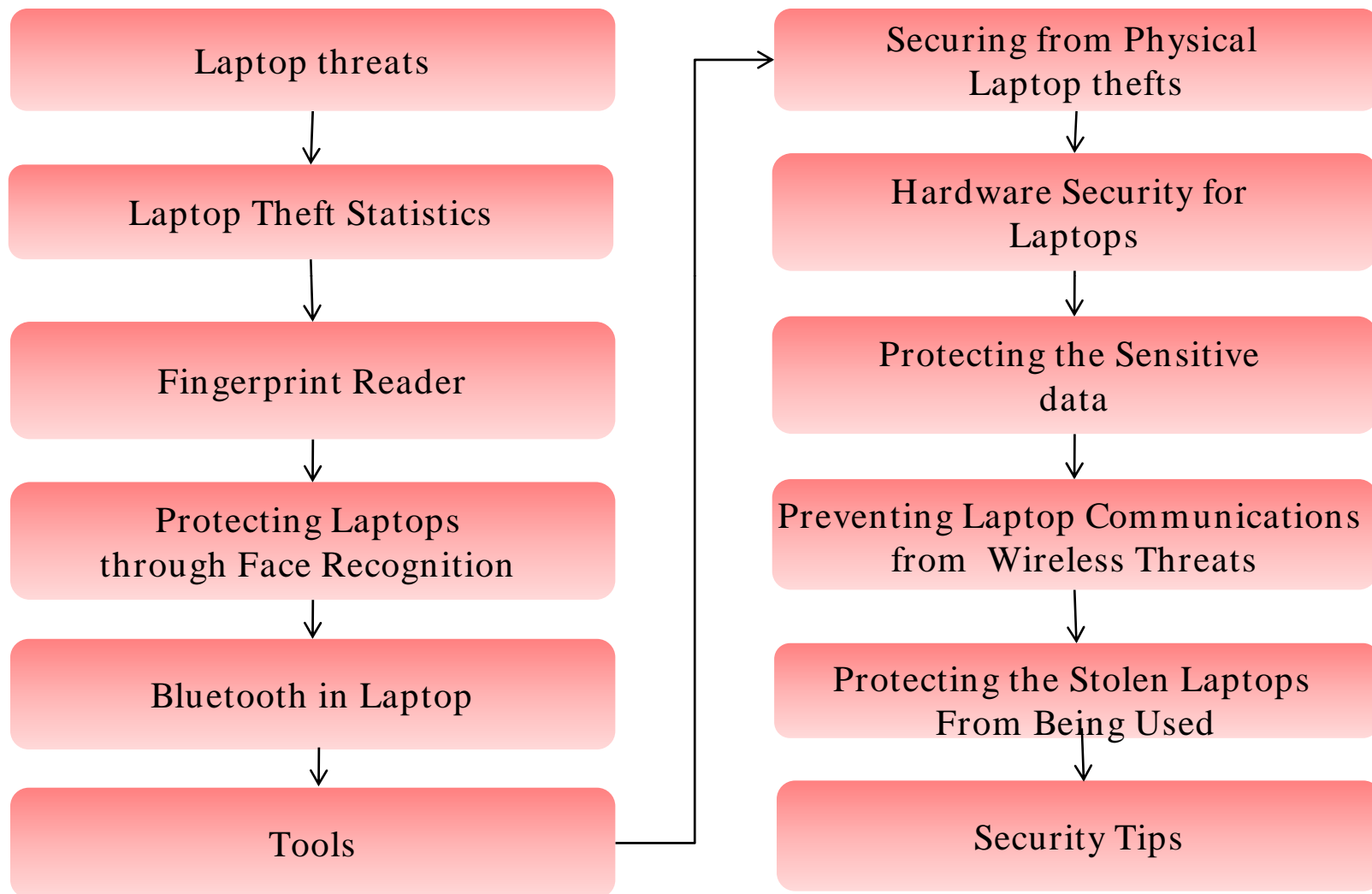
Source: <http://www.informationweek.com/>

Module Objective

This module will familiarize you with:

- Laptop threats
- Laptop Theft Statistics
- Fingerprint Reader
- Protecting Laptops through Face Recognition
- Bluetooth in Laptops
- Tools
- Securing from Physical Laptop thefts
- Hardware Security for Laptops
- Protecting the Sensitive data
- Preventing Laptop Communications from Wireless Threats
- Protecting the Stolen Laptops From Being Used
- Security Tips

Module Flow





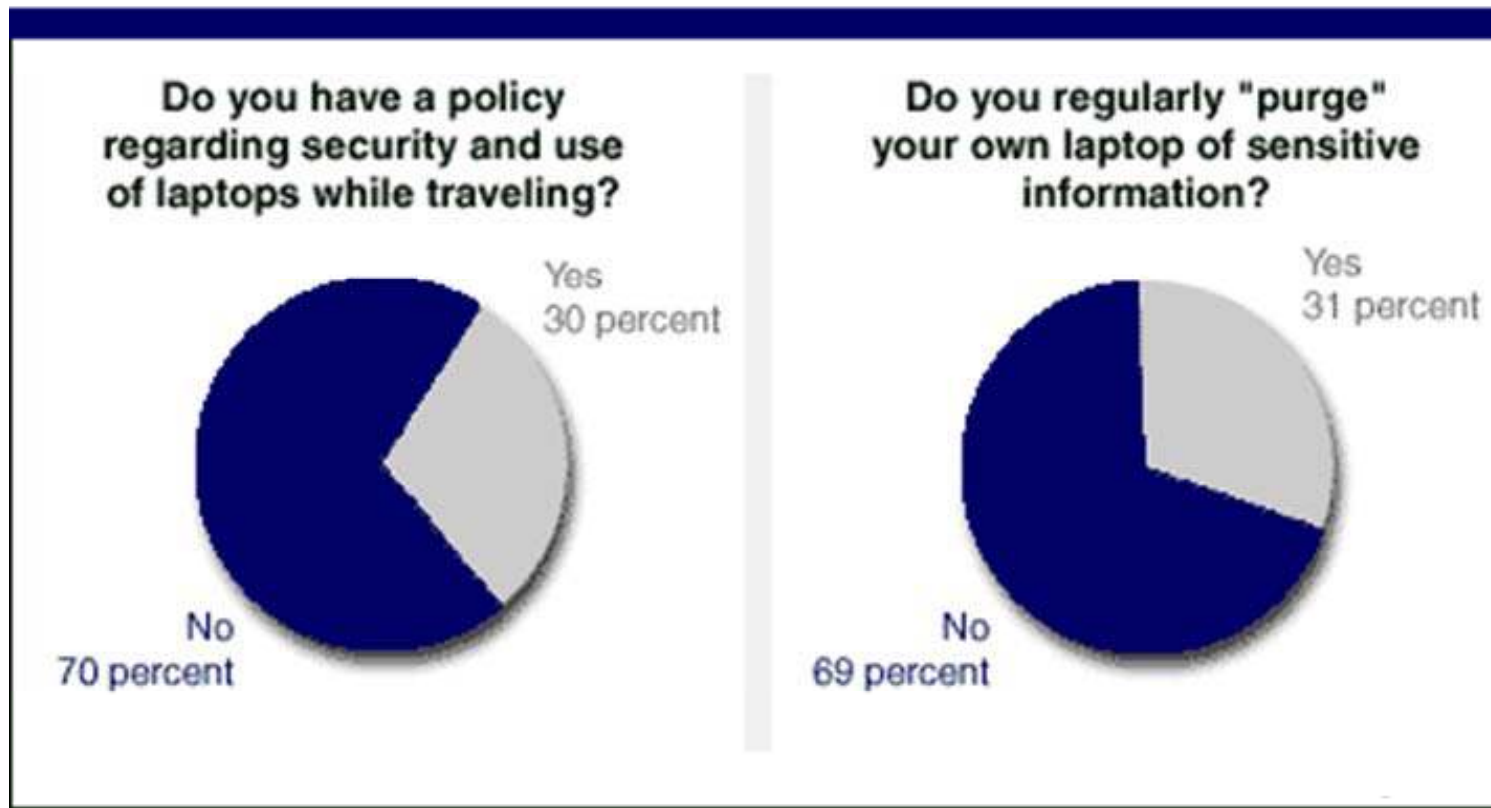
Source: <http://www.popularmechanics.com/>

Statistics for Stolen and Recovered Laptops



Source: <http://articles.techrepublic.com/>

Statistics on Security



Source: <http://articles.techrepublic.com/>

Percentage of Organizations Following the Security Measures

	Number of Organizations	Percentage of Organizations
Passwords	35	97
Encryption of data	20	56
Employee certification/signoff	20	56
Awareness training	16	44
Locking cables	13	36
Data restriction on laptop	13	36
Automatic encryption of data	12	33
Internet tracking/locator software	9	25
Smart cards	7	19
Key cards	7	19
Deletion programs	4	11
Biometric access controls	4	11
Kensington locks	2	6
Motion sensors and alarms	1	3
Travel prohibitions	1	3
Unknown	1	3
Others	0	0

Source: <http://www.iacis.org/>

Copyright © by **EC-Council**

Laptop Threats

Physical Security

- Criminals target laptops for quick profits and misuse of the confidential data
- Laptops containing personal and corporate information can be hacked by the attackers and used for their profits



Information Security

- Corrupting, destroying, or gaining access to a Laptop through hacking, malicious programs, or social engineering
- Accessing the data through weak passwords and open access
- Application security and vulnerabilities to attack the vulnerable application
- Attacking the laptops with unencrypted data and unprotected file systems
- Copying the data through removable drives, storage mediums, and unnecessary ports which are not disabled



Wireless Security

- Intercepting and monitoring wireless traffic through various sniffer tools and interception software
- Packet insertion and hijacking attacks into the sniffed wireless traffic
- Jamming is used where the attacker uses different wireless devices at different frequencies which creates radio frequency interferences for any wireless network in vicinity
- Peer to peer attacks is performed by using Ad Hoc mode
- Man in the middle attack
- Wi-phishing is used by hijackers to setup an access point with SSID that is used by default on most access points



If a laptop were lost...

- What information of a strategic nature would be disclosed? Real examples of this type of information include pending mergers, new product intellectual property, strategies and launch plans, and previously undisclosed financial operating results
- What information of a tactical nature would be disclosed? Examples include private compensation information, plans for organizational changes, proposals to clients, and the myriad of similar information that can be gained from reading a person's email, calendar, contacts, or collection of documents and spreadsheets

If a laptop were lost...

- What information about the company's network or computing infrastructure would be revealed that would facilitate an electronic attack?
Examples of this type of information include usernames and passwords, dial in numbers, IP addressing schemes, DNS naming conventions, ISPs used, primary mail servers, and other networking details related to connecting the laptop to the corporate or Internet environment.
- What personal information about the laptop owner can be obtained?

Fingerprint Reader

Fingerprint Reader enables the user to access the laptop in a more secured and easy way

It provides higher level of security while accessing the data or network

BioNet 2 laptop fingerprint reader designed from Biometric fingerprint reader is specially used for portable storage devices such as laptops and PDAs

It offers secured access to the applications like, valuable logons, web links, documents, image files, and more



Protecting Laptops Through Face Recognition

Face Recognition technology is used to access authentication on the laptop by recognizing the face as the password

It takes the snapshot of the user and creates digital shots which serve as the password

It supports multiple users to allow trusted ones to access the laptop

Features:

- Advanced Face recognition software via Integrated Camera for authenticating user
- One-key recovery helps to recover operating system in case of system crash or system effected by virus



Bluetooth in Laptops

Bluetooth enables two laptop devices to connect with each other negating the usage of cables and wires

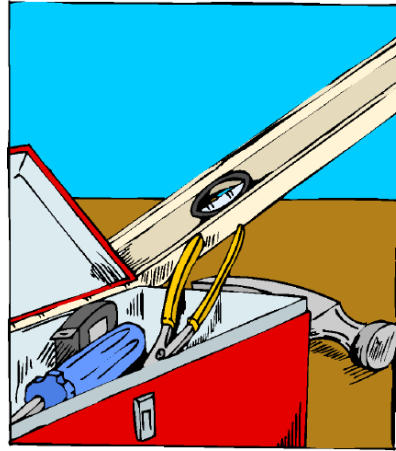
A Bluetooth enabled laptop tries to pair with another intended laptop but not with an unknown device

The Bluetooth laptop devices create an initialization key PIN code or passkey used for authentication

Attacker can sniff this session to access the data

The information passed between the two laptop devices should be encrypted which is upto 128 bits





Tools

Laptop Security

Laptops can be secured physically from being stolen or lost by using security tools

The tools will let the laptop to be fixed at one place, lock it to an immovable device or use secured laptop trolleys



Laptop Security Tools

Steel Cable Locks



Laptop Tie-down Brackets



LapSafe laptop trolley



Portable Laptop Carts



Laptop Locker



Laptop Alarm

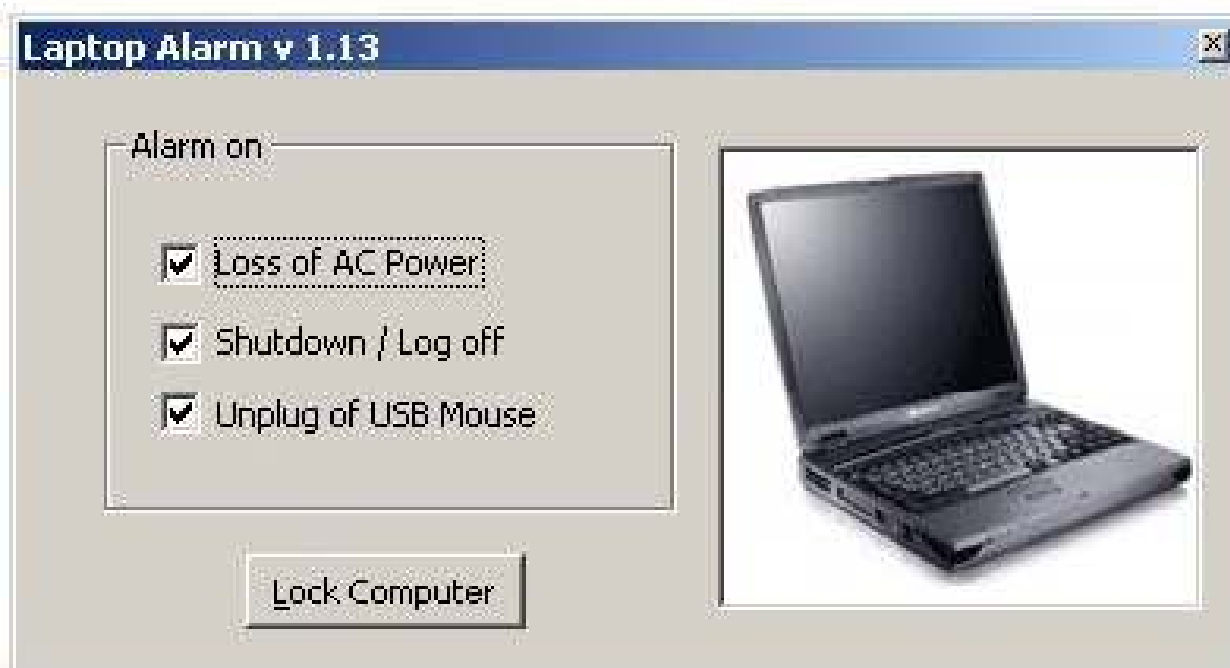
Laptop Alarm will emit a loud alarm whenever someone tries to steal your laptop

It emits the loud sound on

- A/C Power Removal
- Mouse Removal
- Mouse Movement
- Shutdown / Suspend



Laptop Alarm: Screenshot



Flexysafe is the laptops safe security case

Flexysafe Digital, the safe that is designed for people who take their laptop computers home from work



Master Lock patented lock and cable system

Features

- Locks notebook computer to prevent theft and protect data
- Galvanized steel cable provides strong security and peace of mind



eToken represents the most effective combination for protecting data on your laptops

It is a strong authentication, with disk encryption and boot-protection solution

A smart card-based strong authentication solution ensures PC and laptop security with two key components

- Physical protection of the encryption keys
- User authentication prior to encryption key access



STOP-Lock

STOP-Lock combines tracking system with a locking mechanism to help deter thieves

It is a highly-visible small metal plate that attaches securely to the cover of the laptop

The plate is stamped with unique barcode information that registers the computer with a national database



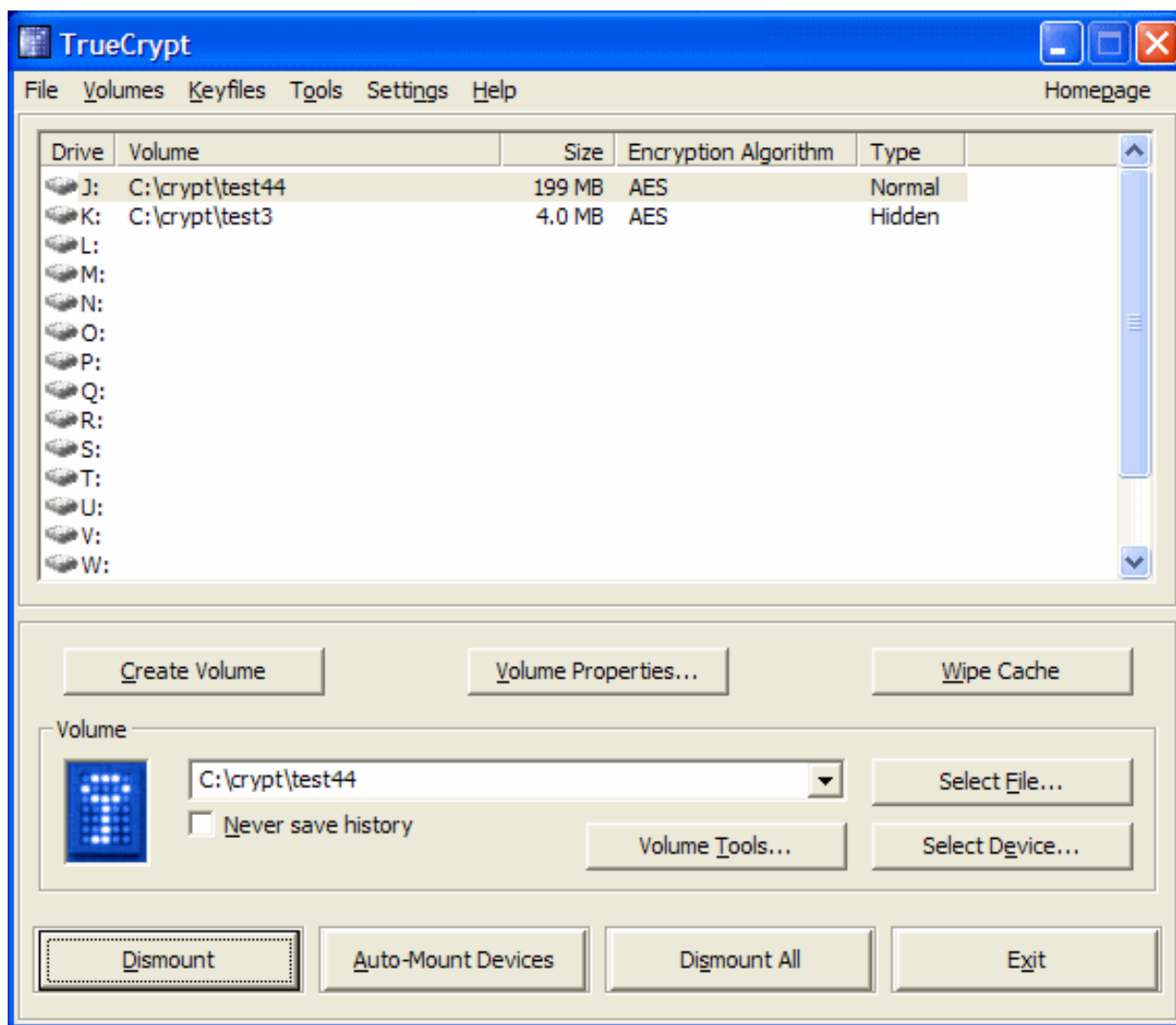
Free open-source disk encryption software

Features

- Creates a virtual encrypted disk within a file and mounts it as a real disk
- Encrypts an entire partition or storage device such as USB flash drive or hard drive
- Provides two levels of plausible deniability, in case an adversary forces you to reveal the password
 - No TrueCrypt volume can be identified
 - Hidden volume (steganography)



True Crypt: Screenshot



PAL PC tracker will track and locate the lost or stolen computer

It sends stealth signal which include the user's computer tracing details

When the user connects to the Internet, it will send a stealth email message to the user and server which contains exact location of the pre-defined email address set by the user



PAL PC Tracker: Screenshot



Cryptex

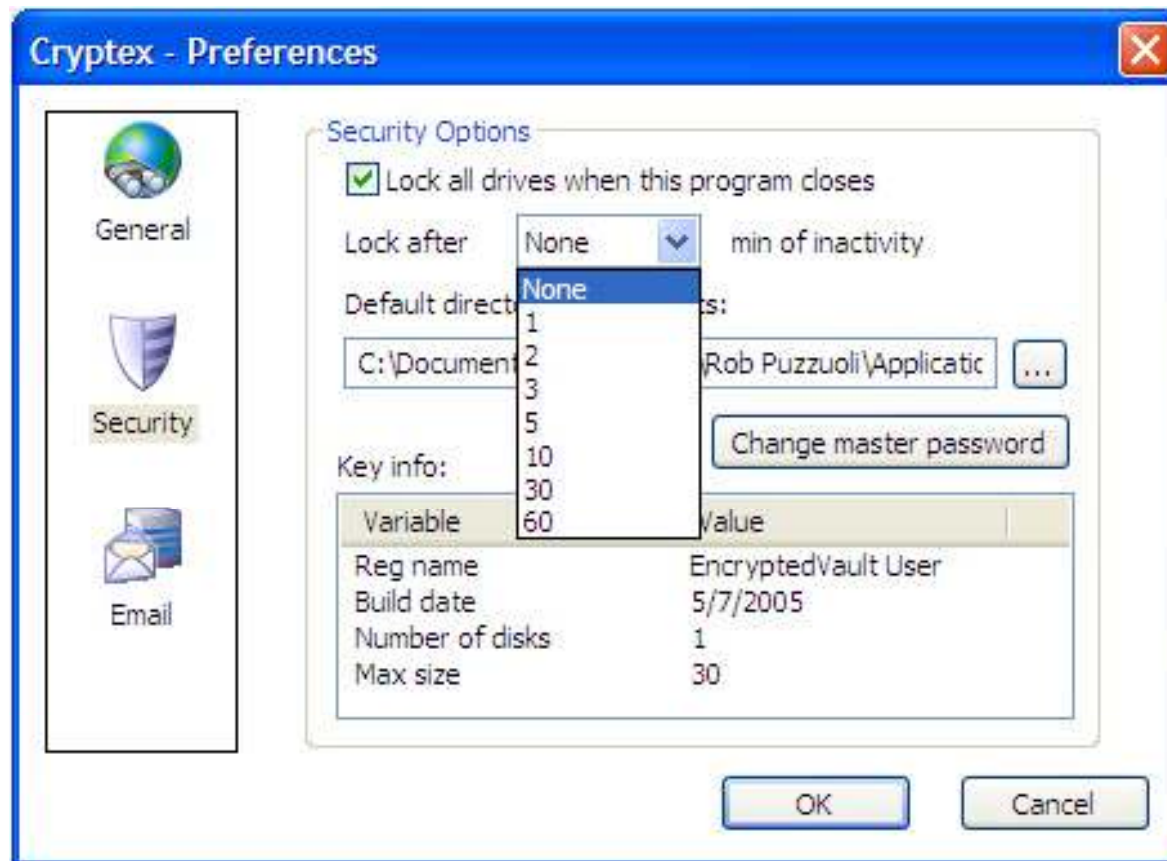
Cryptex provides an unbreakable, 448-bit encryption data storage on laptops

It keeps the data safe by creating an encrypting vault on the hard drive

It will disappear from the view when the vault is locked



Cryptex: Screenshot

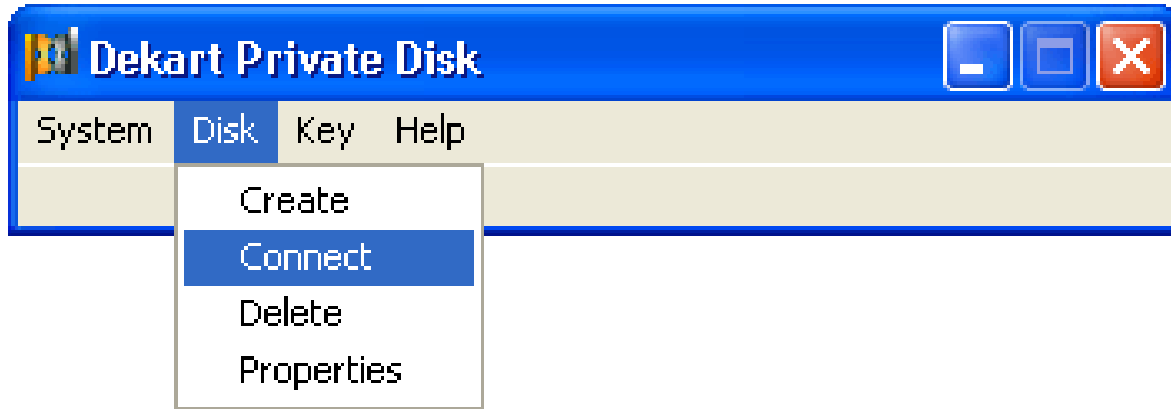


Dekart Private Disk Multifactor

Private Disk Multifactor is a disk encryption program that secures confidential data on laptops

It provides proactive protection against viruses, Trojans, adware, spyware, and unauthorized network access

Sensitive data is not only encrypted, but are protected with Dekart's innovative Disk Firewall mechanism



Laptop Anti-Theft

Laptop Anti-Theft recognizes and traces through both internal and external networks for LAN/WAN configurations to pin point actual location of the lost or stolen laptop

Once installed invisibly on your laptop system, Laptop Anti-Theft sends a stealth e-mail message containing it's exact location to a pre-determined e-mail address set by the owner

Each signal contains all the required information on the status and physical location of your laptop



Inspice Trace

Inspice Trace is a location tracking program that emails you the precise location of your stolen or lost laptop

It lets you unrecoverably destroy sensitive data in your laptop in case of theft



ZTRACE GOLD is an invisible software security application that traces the location of missing laptops for recovery

It is undetectable and unerasable on a laptop's hard drive

If the laptop is reported missing, a patent pending process occurs for the ZTRACE Recovery Team to identify the computer's exact physical location

The ZTRACE Recovery Team coordinates with local law enforcement for a completely outsourced recovery solution



ZTRACE GOLD: Screenshot



SecureTrieve Pro is a software tool that encrypts, protects and retrieves critical files from a lost or stolen laptop

It automatically retrieves critical files remotely from your missing laptop

It offers very powerful encryption capabilities

It goes through firewalls to find the exact location of your stolen laptop



XTool Laptop Tracker

XTool Laptop Tracker supports all the recovery methods: Internet, Caller ID, WiFi, WebCam, GPS, Remote Forensic Tools

It cannot be detected by anti-virus programs and can bypass 90% of all corporate and personal firewalls

XTool Laptop Tracker Agent is small and uses encryption to transmit the collected data to the XTool Monitoring Center

It utilizes worldwide Internet monitoring and unique dial-up monitoring coverage



XTool Laptop Tracker: Screenshot

XTool Agent Computer Tracker XTool Asset Auditor XTool Data Protector

Activity Log Report Theft/Loss

Computer Tracker

Show: From: To:

[Export Excel](#)

Date Log	Organizational Unit	XTSN	Computer Name	User Name	OS	OS Edition	IP Trace	Phone
09/10/06 10:19:21 AM	Stealth Signal, Inc	67645	LAPTOPDELL4	PEDROC	Win XP	Professional	216.74.243.97	
09/10/06 10:21:58 AM	Stealth Signal, Inc	67645	LAPTOPDELL4	PEDROC	Win XP	Professional	216.74.243.97	
09/10/06 1:11:35 PM	Stealth Signal, Inc	67645	LAPTOPDELL4	PEDROC	Win XP	Professional	216.74.243.97	
09/11/06 10:18:02 AM	Stealth Signal, Inc	67645	LAPTOPDELL4	PEDROC	Win XP	Professional	216.74.243.97	
09/11/06 10:18:47 AM	Stealth Signal, Inc	67645	LAPTOPDELL4	PEDROC	Win XP	Professional	216.74.243.97	
09/11/06 10:50:27 AM	Stealth Signal, Inc	67645	LAPTOPDELL4	PEDROC	Win XP	Professional	216.74.243.97	
09/11/06 1:19:50 PM	Stealth Signal, Inc	67645	LAPTOPDELL4	PEDROC	Win XP	Professional	216.74.243.97	
09/11/06 2:37:25 PM	Stealth Signal, Inc	67645	LAPTOPDELL4	PEDROC	Win XP	Professional	216.74.243.97	
09/11/06 4:06:36 PM	Stealth Signal, Inc	67645	LAPTOPDELL4	PEDROC	Win XP	Professional	216.74.243.97	
09/11/06 8:06:51 PM	Stealth Signal, Inc	67645	LAPTOPDELL4	PEDROC	Win XP	Professional	216.74.243.97	
09/12/06 9:50:24 AM	Stealth Signal, Inc	67645	LAPTOPDELL4	PEDROC	Win XP	Professional	71.2.112.168	
09/12/06 9:51:37 AM	Stealth Signal, Inc	67645	LAPTOPDELL4	PEDROC	Win XP	Professional	71.2.112.168	
09/12/06 11:29:51 AM	Stealth Signal, Inc	67645	LAPTOPDELL4	PEDROC	Win XP	Professional	71.2.112.168	
09/13/06 12:05:46 AM	Stealth Signal, Inc	67645	LAPTOPDELL4	PEDROC	Win XP	Professional	71.2.112.168	
09/13/06 11:31:00 AM	Stealth Signal, Inc	67645	LAPTOPDELL4	PEDROC	Win XP	Professional	71.2.112.168	
09/13/06 1:07:10 PM	Stealth Signal, Inc	67645	LAPTOPDELL4	PEDROC	Win XP	Professional	71.2.112.168	
09/13/06 4:33:10 PM	Stealth Signal, Inc	67645	LAPTOPDELL4	PEDROC	Win XP	Professional	71.2.112.168	
09/14/06 12:04:23 AM	Stealth Signal, Inc	67645	LAPTOPDELL4	PEDROC	Win XP	Professional	71.2.112.168	
09/14/06 4:34:21 PM	Stealth Signal, Inc	67645	LAPTOPDELL4	PEDROC	Win XP	Professional	71.2.112.168	
09/15/06 12:05:59 AM	Stealth Signal, Inc	67645	LAPTOPDELL4	PEDROC	Win XP	Professional	71.2.112.168	
09/15/06 9:16:47 AM	Stealth Signal, Inc	67645	LAPTOPDELL4	PEDROC	Win XP	Professional	216.74.243.97	
09/15/06 1:57:28 PM	Stealth Signal, Inc	67645	LAPTOPDELL4	PEDROC	Win XP	Professional	71.2.112.132	
09/15/06 2:06:07 PM	Stealth Signal, Inc	67645	LAPTOPDELL4	PEDROC	Win XP	Professional	62.77.77.101	
09/15/06 2:11:30 PM	Stealth Signal, Inc	67645	LAPTOPDELL4	PEDROC	Win XP	Professional	71.2.112.168	

First Prev 1 2 3 4 5 6 7 8 9 10 11 12 13 14 Next Last

XTool Encrypted Disk

XTool Encrypted Disk is a centrally managed proactive remote laptop security solution

It ensures the intellectual property, important information and confidential data stored on your remote laptops is secure

Protect remote users from data security threats by encrypting sensitive information and preventing unauthorized access to important and confidential files

Define alerts to enforce data security policies

XTool Encrypted Disk: Screenshot



XTool Asset Auditor is a centrally managed auditing service

It uses a low bandwidth agent to remotely collect information about hardware components, software installed and application usage

The zero-touch auditing solution makes keeping track of your mobile computer's hardware and software contents effortless and available no matter where they travel

XTool Asset Auditor: Screenshot

Customer Control Center Ver 7.1 User Administrator (Admin
Organizational Unit: All)

XTool

- Main
- Browser
- Map View
- XTool Computer Tracker**
- XTool Asset Auditor**
 - Hardware
 - Hardware List
 - Leases & Warranties
 - Reports**
 - Software
 - Application and Files
 - Applications Activity
 - Audited Files Activity
 - Audited Files Current
 - Audit Settings
 - Reports
- XTool Data Protector**
- XTool Management**
 - Downloads
- Documentation
- Logout

XTool Asset Manager - Hardware Reports

Report Name	Description
Installed Computers	List of the computers where the XTool Asset Manager service is active
Recommended Windows XP Upgrade	Computers that meet the minimal requirements. (CPU speed > 30Mhz / Memory > 128 MB / Free Disk > 1.50 GB)
Not Recommended for Windows XP Upgrade	Computers that do not meet the minimal requirements. (CPU speed > 30Mhz / Memory > 128 MB / Free Disk > 1.50 GB)
Recommended Windows 2000 Upgrade	Computers that meet the minimal requirements. (CPU speed > 133 Mhz / Memory > 64 MB / Free Disk > 2.0 GB)
Not Recommended for Windows 2000 Upgrade	Computers that do not meet the minimal requirements. (CPU speed > 133 Mhz / Memory > 64 MB / Free Disk > 2.0 GB)
Recommended OS X Upgrade	Computers that meet the minimal requirements. (Free Disk > 3.0GB / Memory > 128 MB)
Not Recommended for OS X upgrade	Computers that do not meet the minimal requirements. (Free Disk > 3.0 GB / Memory > 128 MB)
Recommended for Office XP Upgrade	Computers that meet the minimal requirements. (CPU speed > 133 Mhz / Memory > 88 MB / Free Disk > 360 MB)
Not Recommended for Office XP Upgrade	Computers that do not meet the minimal requirements. (CPU speed > 133 Mhz / Memory > 88 MB / Free Disk > 360 MB)
Recommended for Office 2000 Upgrade	Computers that meet the minimal requirements. (CPU speed > 75 Mhz / Memory > 64 MB / Free Disk > 252 MB)
Not Recommended for Office 2000 Upgrade	Computers that do not meet the minimal requirements. (CPU speed > 75 Mhz / Memory > 64 MB / Free Disk > 252 MB)
Recommended for Office 2003 Upgrade	Computers that meet the minimal requirements. (CPU speed > 233 Mhz / Memory > 128 MB / Free Disk > 400 MB)
Not Recommended for Office 2003 Upgrade	Computers that do not meet the minimal requirements. (CPU speed > 233 Mhz / Memory > 128 MB / Free Disk > 400 MB)
Recommended Office w. X Upgrade	Computers that meet the minimal requirements. (Free Disk > 160 MB / Memory > 128 MB / MAC OS X 11Installed)
Not Recommended for Office w. X upgrade	Computers that do not meet the minimal requirements. (Free Disk > 160 MB / Memory > 128 MB / MAC OS X 11Installed)
Free Disk Space Warning	List of the computers that have less than 10 percent of Free Disk space
OS Mismatch for Windows XP	Computers that do not meet any of the minimal requirements. (CPU speed > 300 Mhz / Memory > 128 MB / Free Disk > 1.5GB)
OS Mismatch for Windows 2000	Computers that do not meet any of the minimal requirements. (CPU speed > 133 Mhz / Memory > 128 MB / Free Disk > 2.0 GB)
OS Mismatch for OS X	Computers that do not meet any of the minimal requirements. (Free Disk > 3.0GB / Memory > 128 MB)
Computers by BIOS	List of computers by BIOS
Computers by CPU	List of computers by CPU
Machines by OS	List of machines by OS
Machines by Physical Hard Disk Drivers	List of machines by Physical Hard Disk Drivers
Machines by Logical Hard Disk Drivers	List of machines by Logical Hard Disk Drivers
Machines by RAM	List of machines by RAM
Computers by Ports	List of computers by Ports
Computers by Printers	List of computers by Printers
Shared Printers	List of Shared Printers
Computers by Network Communication	List of computers by Network Communication
Computers by Video & Sound Card	List of computers by Video & Sound Card
Computers by CD Rom	List of computers by CD Rom

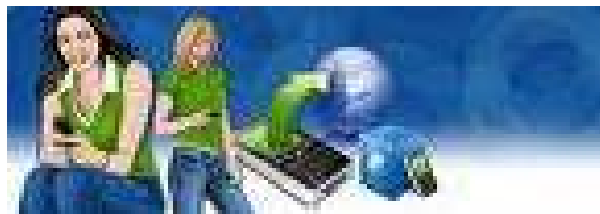
1 of 1

XTool Remote Delete

The XTool Remote Delete enables users to remotely and securely delete sensitive data to prevent unauthorized access to important and confidential files

It minimizes data security breaches

It provides a feedback that confirms what files were found and deleted from the target computer



XTool Remote Delete: Screenshot

Customer Control Center Ver 7.1 User: Administrator (Admin)
 Organizational Unit: All

XTool Agent Computer Tracker XTool Asset Auditor

Properties Remote Delete Request

Remote Delete Unit

Remote Delete Unit		Unit Description
XTSN	67645	
Computer Name	LAPTOPDELL4	
User Name	PEDROC	
Processor	Genuine Intel(R) CPU T2400 @ 1.83GHz - 1831	
OS	Win XP	
Unit Information		Unit Information
Serial	1MFFZ91-1MFFZ91-CN1296164A3212	
Tag		
Type	LAPTOP	
Manufacturer	DELL INC.	
Depto	NO INFO	
Assigned To		
Remote Delete		Remote Delete
XTSN	67645	
Request Date	09/28/06 11:44 AM	
Path	Starts with: <input type="text" value="C:\My Documents\"/> <input type="button" value="v"/>	
File Name	Starts with: <input type="text" value="filename"/> <input type="button" value="v"/>	
Deletion Type	Secure Delete Adequate Security (3-pass random overwrite meth	<input type="button" value="v"/>
		<input type="button" value="Add"/>



Countermeasures and Security

Securing from Physical Laptop Thefts

Use Remote Laptop Security to prevent access to the secured data

Use a docking station

- Docking station permanently affixes the laptop to the desktop and also locks the laptop securely at one place

Eject the PCMCIA NIC cards when the laptop is not in use

Use a personal firewall to the laptop

Use security gadgets like motion detection and alarms to alert you when the laptop is moved by a third party

Use tracking software to trace the laptop using traceable signals when the laptop is lost or stolen



Hardware Security for Laptops

Security cable locking devices fix the laptop to an immovable object

Cable alarms alert the user at the time of malicious activities

Key lock locks down the laptop to the surface where it is most used

A remote control storage case is used for the laptops to protect from thefts



Protecting the Sensitive Data

Use the NTFS file system which provides file level security and protects from laptop thieves

Disable the Guest Account

Rename the Administrator Account

Consider creating a dummy Administrator account

Prevent the last logged-in user name from being displayed

Enable EFS (Encrypting File System)

Disable the Infrared Port on the laptop

Backup the data before leaving

Consider using offline storage for transporting sensitive documents



Preventing Laptop Communications from Wireless Threats

Enabling Wired Equivalent Privacy (WEP) / Wi-Fi Protected Access (WPA) on the wireless network

MAC address control allows the wireless connections from MAC card whose MAC address is stored in the filter

End to end encryption where the conversation is in the encrypted mode

VPN (Virtual Private Network) protects the information transmitted over wireless links

Access points evaluation checks for any rogue access points in wireless networks



Protecting the Stolen Laptops from Being Used

Set the BIOS password which prevents the machine from continuing with the operations when the password is incorrect for three consecutive attempts

Set Login password to successfully login to the computer

Encrypting the file system

Use Biometric authentication mechanism (such as, fingerprint reader, face reader, retinal pattern reader etc.)

Use of tracing and tracking software's



Install anti-virus software and firewalls

Use cable locks on laptops as visual deterrents

Use asset tracking and recovery software

Invest in advanced data protection

Back-up valuable data on a scheduled basis

Keep laptops unnoticeable

Avoid leaving unsecured notebooks unattended

Encrypt your data

Never leave access numbers or passwords in your carrying case

Use alarm bells

Lock unwanted ports

Summary

Criminals target laptops for quick profits and misuse of the confidential data

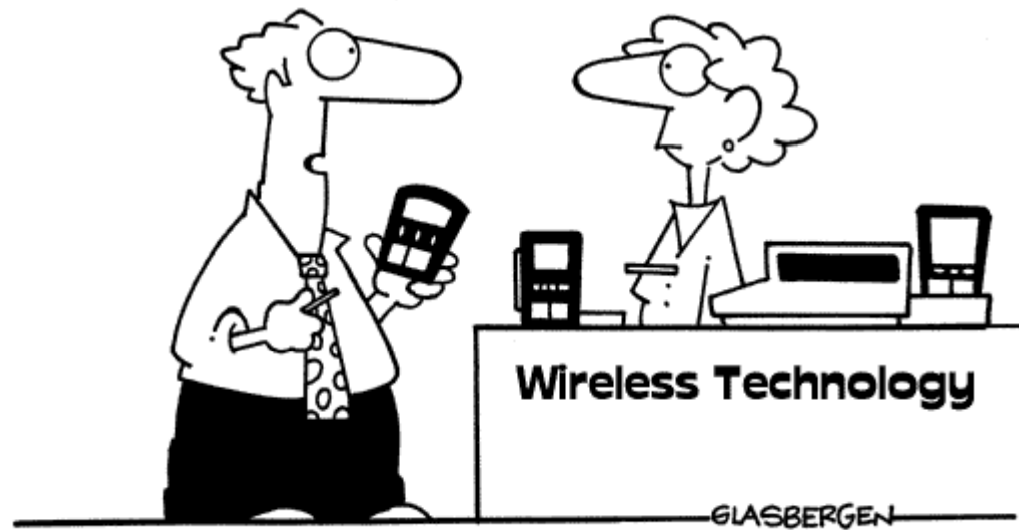
Interception and monitoring wireless traffic through various sniffer tools and interception software

MAC address control allows the wireless connections from MAC card whose MAC address is stored in the filter

WPA is used as an extensive level of security for wireless LAN's

Face Recognition technology is used to access the laptop by recognizing the face as the password

Copyright © 2001 Randy Glasbergen. www.glasbergen.com



"While I'm sending e-mail, trading stocks, and communicating with clients, my feet are just wasting time. What have you got to make my feet more productive?"

Copyright 2003 by Randy Glasbergen.
www.glasbergen.com



**“Watch where you’re going, Larry — you walked
right through my wireless data stream!”**