



O-ISC '07
Ohio Information Security Conference

Securing Data Using PC Encryption

Adam C. Bacon
NCR Corporation



Speaker Biography

- Employed with NCR over 7 years
- Currently employed as Information Security Engineer with NCR Global Information Security Team
- Previously held UNIX and Windows systems administration positions; most recently served as ClearCase Administrator at NCR supporting development teams and Sun Solaris servers running IBM Rational ClearCase, an enterprise software configuration management tool

- What is encryption?
- Why use PC Encryption?
- Things to consider
- NCR's Evaluation
- NCR's Implementation
- Questions & Answers

What is encryption?

What is encryption?

- Encryption is a security feature that scrambles stored or transmitted data using a key and an encryption algorithm
- If the secret pass phrase or key is not known, the data cannot be decrypted
- There are many algorithms and key lengths that are available, but the focus of this presentation is not to discuss which types of encryption algorithms are best

What is encryption?

■ What is PC Encryption?

- Software that encrypts data on hard drives
- Can be whole-disk or file/folder-based
- Can require a higher level of authentication, such as...
 - a certificate
 - a smart card
 - a hard token
 - an extra password
- Can include encryption of data written to removable media
- Can include encryption of data on PDAs/Smartphones



Why use PC Encryption?

Why use PC Encryption?

- Laptops in an organization contain sensitive information
 - employee information
 - customer information
 - contract information
 - sales information
 - intellectual property
- What type of information do you want to protect?
- What type of information is the highest risk (most critical) within your organization?

Why use PC Encryption?

■ Information is everywhere

- Obvious locations
 - files
 - e-mail messages
 - databases and extracts
- Not so obvious locations
 - temporary files
 - cached files
 - log files
 - Microsoft Outlook OST files
 - Windows page file
 - Windows hibernation file

Why use PC Encryption?

- Loss of sensitive information would...
 - be reported in newspapers
 - involve lawsuits and fines
 - invoke California privacy law (as an example)
 - start internal and external investigations
 - increase stakeholder scrutiny
 - potentially involve a loss of business

Why use PC Encryption

- Having a laptop's data encrypted...
 - protects...
 - the employee
 - the organization
 - the customers
 - others whose personally identifiable information is stored on the laptop or removable media
 - mitigates the risk of someone stealing a laptop that is *powered off*
 - does **not** provide a significant level of protection of data on a laptop that is *powered on* and running

Things to consider

- Conduct a risk assessment
 - Given my organization, what type of information do I want to protect?
 - Why implement or consider implementing PC encryption?
 - Are any information assets under regulatory requirements?

Things to consider

- What technical features are desired?
 - What type of encryption, whole-disk or file/folder-based?
 - Will data written to removable media be encrypted? If so, how will this impact...
 - sharing data with individuals who do not have the encryption software?
 - sharing data with individuals outside of the organization?
 - backup and recovery of laptop data?
 - What type of authentication?
 - passwords
 - smart cards
 - tokens
 - single or multiple logins
 - synchronized passwords
 - What is the organization's culture?



NCR's Evaluation

■ Background

- Management approved a PC encryption pilot project to protect sensitive content on laptop hard disk drives

■ Business requirements

- Minimize NCR's risk
- Protect NCR's customers, employees, stockholders, brand, and reputation

■ Technology requirements

- Encrypt the entire hard drive (whole-disk encryption)
- Encrypt data on removable media and allow secure access to that data on PCs without installed encryption software
- Leverage NCR's existing IT infrastructure
- Be as transparent to the user as possible
- Require minimal Help Desk / administration / support cost

- Why use whole-disk encryption?
 - Once deployed it is transparent to the user
 - It runs beneath the operating system, so it does not impact applications and network drivers are not loaded at login
 - If drive is “slaved,” data cannot be accessed

- Why not use file/folder-based encryption?
 - It only provides a protected/encrypted area (folder) on the laptop that users may or may not use
 - Users would need to be trained to use the protected/encrypted area (folder), and they often forget
 - To be effective, this approach requires significant training
 - Even with training, can it ever be known that all of a user’s sensitive data was in the protected/encrypted area (folder), if the laptop is stolen?
 - Existing processes may exist that have users place files in a location other than the protected/encrypted area (folder)
 - Files containing sensitive data may exist outside of the protected/encrypted area (folder)

- Upon further evaluation of various PC encryption solutions, NCR realized that the encryption solution needed to...
 - not require an additional login for the user
 - have the ability to synchronize the user's encryption password with his/her Windows logon
 - include the ability to automatically encrypt data written to removable media (but not mandate it)
 - be supported by NCR's global help desk

NCR's Implementation

NCR's Implementation

- NCR chose an enterprise whole-disk PC encryption product
- The encryption product provides pre-boot (pre-Windows) authentication
 - Single sign-on feature (i.e. only one login is required)
 - Pre-boot password synchronized with Windows password
- Data is encrypted as it is written to disk and decrypted as it is read from disk (on the fly)
 - Estimated performance degradation is only 3-5%
- Data written to removable media can be encrypted automatically or manually

NCR's Implementation

- Pre-boot architecture integrates most transparently with the operating system and makes vulnerability to hacking low
 - Single sign-on & Windows password synchronization – one logon
 - Ability to automatically encrypt files written to USB drive / floppy disk
 - Ability to easily and completely burn encrypted CDs and DVDs
- Sharing of data with computers not running encryption software is possible, while maintaining data encryption
 - Files attached to e-mail messages and copied to network drives are not encrypted by default, but can be encrypted if packaged in a self-extracting/decrypting archive
 - Encrypted files on USB drives / floppy disks can be accessed on a PC not running encryption software by supplying a password unique to that media
- Administration
 - No dedicated server required, only share space
 - Centralized and secure recovery of user passwords
 - Ability to boot and access data, in cases of hard disk corruption
 - Application and updates able to be deployed via NCR's software distribution tool

- Worked with management to identify the “Top 100” NCR candidates based on highest priority
- “Phased approach” deployment
 - Proof of concept
 - Verify that the product’s settings and configuration are correct
 - Pilot
 - Verify that users are able to install the product
 - Verify that support is handled properly
 - Phase I
 - Deploy to the “Top 100” candidates
 - Additional phases
 - Deploy to the remaining candidates

- Occasional installation issues
- Post-installation issues encountered
 - Offline password resets
 - Image backups
 - Encryption of data written to removable media
 - Perception that PC is running slower

■ Support

- NCR's global help desk provides
 - Password resets
 - One-time logins
- PC Encryption (Level 3) team facilitates
 - Decryption of an encrypted hard drive
 - Troubleshooting of new issues

■ Conclusion

- While very beneficial for an organization, PC encryption involves significant time to configure and support during an initial installation

Questions & Answers

