PENN
SAS Computing

SSC

Social Sciences Computing
a division of SAS Computing

File Security

John Marcotte
Director of SSC

February 2008

PENN
SAS Computing

SSC

File Security

- Review security issues
- Overview of encryption
- Software
- Data Security Plan
- Questions

PENN
SAS Computing

SSC

Reasons for Security

- **Sensitive information**
  - SSN
  - Date of birth
  - Health information
- **Privacy**
- **NIH mandate**
- **Computer theft**

PENN
SAS Computing
SSC

Purpose of Security

- **Protect files on disk**
  - Single file
  - Multiple files
  - Add and remove files routinely
  - Flash drives, CDs and DVDs
- **Send and receive files securely**
  - Ad-hoc basis
  - On-going correspondence

PENN
SAS Computing

SSC

File Security

- **Physical Security**
  - Doors and locks
  - Safes and cabinets

PENN
SAS Computing

SSC

File Security

- **Logical Security**
  - Strong Passwords
  - Network restrictions
  - Encryption

PENN
SAS Computing
SSC

Strong Passwords

- At least 8 characters, 14 characters or longer is better
- Not in the dictionary
- Mix of letters, numbers, special characters (e.g. #,*,&,$)

PENN
SAS Computing
SSC

Permissions

- Non-sensitive information
- Keep out intruders without physical access
- Default permissions are usually not restrictive

PENN
SAS Computing
SSC

File Security

- **Permissions**
  - File system rights
  - Administrator failsafe
  - Physical security important
- **Encryption**
  - Encryption key required even with physical access
  - Lost key could make file contents inaccessible

PENN
SAS Computing

SSC

Encryption

- Protect information even if physical access
- Risk of information loss if encryption keys lost or corrupted
- Special recovery plan needed
- Hard to share files on network

PENN
SAS Computing

SSC

Encryption Methods

- **Advanced Encryption System (AES) (128, 192, 256 bit)**
- **Data Encryption System (DES) (64 bit)***
- **Triple-DES (3DES) (128 bit)***

Other methods: Archfour (128 bit), **BlowFish (128 bit), TwoFish (256 bit),** IDEA (128 bit), Cast-128 (128 bit)

A key should be a minimum of 64 bits. With sufficient resources (14,000 computers in 1997!) , a 64 bit key can be cracked.

PENN
SAS Computing

SSC

Encryption Methods

- **Symmetric**
  Shared secret
  Encrypt and decrypt with same key
  Never send key via e-mail

- **Asymmetric**
  Public key-Private key pair
  Encrypt with shared public key
  Decrypt with private key

PENN
SAS Computing
SSC

Encryption Methods

- **Password-protected key**
  Change password without changing encryption key; best for file system
- **Password as key**
  Decrypt and re-encrypt to change password; good for single file

PENN
SAS Computing
SSC

Encryption Issues

- Recovery
- Network traffic
- Export and Import restrictions
- Secure deletion of files
- Temp files
- Clipboard

PENN
SAS Computing

SSC

Encryption Recovery

- Copy of non-encrypted version of file in safe
- Copy of encryption key in safe
- *Key escrow system*
- Recovery software in safe

PENN
SAS Computing

SSC

Network Traffic

- Network traffic is not usually encrypted
- Use SSH (Secure Shell) to create encrypted tunnel
  - Software: *PuTTY, SecureCRT, WinSCP, FileZilla*
- On the web, use https:// that uses SSL (Secure Sockets Layer) if sending and receiving private information

❖ *Are all network paths encrypted?*

PENN
SAS Computing

SSC

International Issues

Export and Import Restrictions

- The United States has restrictions on exporting encryption software; AES and 3DES are restricted.
- Some countries have import restrictions
- 64-bit encryption is allowed
- Blowfish is also allowed

PENN
SAS Computing

SSC

Secure Deletion

- Deleted files can be undeleted if not overwritten
- Special software is required

PENN
SAS Computing

SSC

Software

- TrueCrypt
- AxCrypt
- GNU Privacy Guard (GPG) & Pretty Good Privacy (PGP)
- Eraser
- SFTPdrive

PENN
SAS Computing

SSC

TrueCrypt

- Open Source and Freeware
- Cross-platform: Windows, Linux, Mac
- Mounts virtual encrypted disk
- Password protected key
- Ability to backup encryption key

PENN
SAS Computing

SSC

TrueCrypt

- Can work with encrypted files without having to decrypt them
- Files saved on the encrypted disk are automatically encrypted
- Erased files on encrypted disk are still protected
- Copying files off the encrypted disk decrypts them

PENN
SAS Computing

SSC

TrueCrypt

- Works on USB flash drive
- Must be installed
  - Symmetric: shared secret or key file
  - Limited simultaneous user capability
  - *No automatic key escrow*

PENN
SAS Computing

SSC

TrueCrypt

Web-site: http://www.truecrypt.org/

Beginner's Tutorial:
http://www.truecrypt.org/docs/?s=tutorial

PENN
SAS Computing

SSC

TrueCrypt and SAS

- SAS creates temporary files in the "work" directory. By default the work directory is not on the encrypted drive.
- To run SAS on the encrypted drive, modify the Windows shortcut for SAS to put work files on the encrypted drive.
- Add *–work X:\SAS-work* at the end of the command to invoke the SAS program.
  - *X:* is the letter for the encrypted drive
  - *SAS-work* is a directory that you created on the encrypted drive for your SAS work files
- Full shortcut: SAS 9.1 (English).lnk

  "C:\Program Files\SAS\SAS 9.1\sas.exe"
  -CONFIG "C:\Program Files\SAS\SAS 9.1\nls\en\SASV9.CFG"
  -work x:\sas-work

PENN
SAS Computing

SSC

AxCrypt

- Open Source and Freeware
- Encrypt single file
- Decrypt file to use it
- Password as key
- Small (< 75K) decryption program that can be included with file

Web-site: http://axcrypt.sourceforge.net/

PENN
SAS Computing

SSC

GPG and PGP

- **GPG** : *Gnu Privacy Guard*
- **PGP** : *Pretty Good Privacy*
- GPG is an open source, freeware version of PGP.
- Asymmetric encryption:
  Public Key-Private Key (no shared secret)
- Cross-platform: Windows, Linux
- Decrypt file to use it
- Ideal for sending information securely on an on-going basis.
- Can be integrated into many e-mail clients
- Everyone must have set up GPG keys in advance

Web-site: http://www.gnupg.org/

PENN
SAS Computing

SSC

Eraser

- Open Source and Freeware
- Overwrites deleted file so it cannot be recovered
- Overwrite all deleted files on a disk so that they cannot be recovered.

Web-site: http://www.heidi.ie/eraser/

PENN
SAS Computing

SSC

SFTPdrive

- Commercial software
- Map drive through SSH encrypted tunnel
- Works through gateway or proxy server
- No good freeware alternative

Web-site: http://www.sftpdrive.com/

PENN
SAS Computing
SSC

Encrypted Tunnels

- Port forwarding using SSH client: *PuTTY* or *SecureCRT*
- Open file share through tunnel

o Can make a secure connection to only one server at a time

- Alternative: use *SFTPdrive*

- Copy files via SSH with WinSCP or FileZilla

PENN
SAS Computing
SSC

Wireless

- Wireless may not be encrypted
- AirSAS uses the SecureW2 client which does encrypt
- Home wireless is not usually encrypted; Use WPA (Wi-Fi Protected Access)
- *WEP (Wireless Encryption Protocol) can be hacked*

PENN
SAS Computing

SSC

Laptops

- Laptops are often stolen or lost
- Encrypt entire disk; system will not start without password
- Software to track location
- Software to erase disk remotely

❖ *Penn is considering what to recommend*

PENN
SAS Computing

SSC

Flash Drives

- TrueCrypt can create an encrypted section of a flash drive
- TrueCrypt must be pre-installed, or you must be the administrator on any computers where you want to use the flash drive
- TrueCrypt is installed in labs

PENN
SAS Computing

SSC

Sensitive Data Plan

- ***Data provider must approve plan to protect data.***
- One possibility is a stand alone non-networked PC in a locked office
- Original data media locked in safe or cabinet

PENN
SAS Computing

SSC

Stand Alone PC

- Stand alone, non-networked PC in locked office
- Use encryption to protect data even if physical access is compromised
- Second computer for e-mail and network access.
- KVM (Keyboard-Video-Mouse) switch to share keyboard, video and mouse between networked and non-networked PCs

PENN
SAS Computing

SSC

More Information

- **A (Very) Brief Introduction to Cryptography**

http://www.int.gu.edu.au/courses/2010int/crypto.html

- **Encryption Algorithms**

http://www.cescomm.co.nz/about/algorithms.html

- **Security Dictionary**

http://www.cryptomathic.com/labs/techdict.html

PENN
SAS Computing

SSC

File Security and Encryption

Questions