Secure Storage and Encryption of Data

Dr Scott Summers
UK Data Service
University of Essex

Managing and Sharing Research Data: Best Practice for Data Protection – Lift, London
28th and 29th November 2018

UK Data Service

Overview

- Looking after research data for the longer-term and protecting them from unwanted loss requires having good strategies in place for:
  - securely storing
  - backing-up
  - transmitting / encrypting
  - and disposing of data


BBC Mobile News | Sport | Weather

NEWS TECHNOLOGY

Home | World | UK | England | N. Ireland | Scotland | Wales | Business | Politics | Health | Educ

8 December 2010 Last updated at 11:43

Nasa sells shuttle PCs without wiping secret data

US space agency Nasa has been left red-faced after selling off computers without ensuring that highly sensitive data had been removed.

An internal investigation found 10 cases where PCs were sold despite failing data removal procedures.

Another four PCs - which were about to be sold - were found to contain data restricted under arms control rules.

Nasa is selling of hundreds of PCs used Space Shuttle programme

- Collaborative research brings additional challenges for the shared storage of, and access to, data

UK Data Service

Stuff happens!

Stuff happens: data loss

- What would happen if you lost your data?
- Imagine if you left your bag on a train, containing your laptop (with all your digital research notes on) and your paper based notes too – this situation happened to Andrew Penson

- Source: https://twitter.com/ADPenson/status/883637257323896832

UK Data Service

Stuff happens: data theft

- What would happen if you data was stolen?
- Imagine if you lost four years worth of research data – this situation happened to Billy Hinchen

https://www.youtube.com/watch?v=3xlax_Iin0Y

- Source:

  https://figshare.com/blog/The_stuff_of_nightmares_imagine_losing_all_your_research_data/121

UK Data Service

Stuff happens: data theft

- What would happen if your data was stolen?
- Imagine if seven years worth of your Ebola research was stolen – this situation happened to Dr Fitzgerald

- Source:

  https://www.standard.co.uk/news/crime/burglar-stole-laptop-with-seven-years-of-ebola-research-from-doctor-s-house-a3689406.html

UK Data Service

Storing data

Data storage

- Local storage
- University and collaborative storage
- Cloud storage
- Data archives or repositories

zipcloud box justcloud.com bitcasa OneDrive IDrive Dropbox Google Drive MediaFire iCloud

UK • DATA ARCHIVE

UK Data Service

Data storage: How to decide

- How much storage space do I need?
- Who needs access?
- What precautions should I take to protect my data against loss?
- Which storage solutions are suitable for personal data?

Local data storage

- Internal hard drive / flash drive
- Note that all digital media are fallible
- Optical (CD, DVD & Blu-ray) and magnetic media (hard drives, tape) degrade over time
- Physical storage media become obsolete e.g. floppy disks

- Data files should be copied to new media every two-to-five years after they are first created

UK Data Service

University and collaborative storage

- Your university or department may have options available. For example:
  - Network attached drives
  - Secure backed up storage space
  - VPN giving access to external researchers
  - Locally managed Dropbox-like services such as OneDrive and Essex ZendTo
  - Secure file transfer protocol (FTP) server

Sharing data between researchers

- Too often sent as insecure email attachments
- Physical media?
- Virtual Research Environments
  - MS SharePoint
  - Clinked
  - Huddle
  - Basecamp

UK Data Service

Cloud storage services

By David Fletcher
http://www.cloudtweaks.com/2011/05/the-lighter-side-of-the-cloud-data-transfer/

- Online or ‘cloud’ services are becoming increasingly popular
- Google Drive, DropBox, Microsoft OneDrive and iCloud

Google Drive Dropbox OneDrive

- Benefits:
  - Very convenient
  - Accessible anywhere
  - Good protection if working in the field?
  - Background file syncing
  - Mirrors files
  - Mobile apps available

But,

  - These are not necessarily secure
  - Potential GDPR issues
  - Limited control over where data is stored
  - Not necessarily permanent
  - Intellectual property right concerns?
  - Limited storage?

UK Data Service

Cloud storage services

- Perhaps more secure options?

Mega.nz

SpiderOak

Tresorit

- Cloud data storage should be avoided for high-risk information such as files that contain personal or sensitive information, or information that has a high intellectual property value

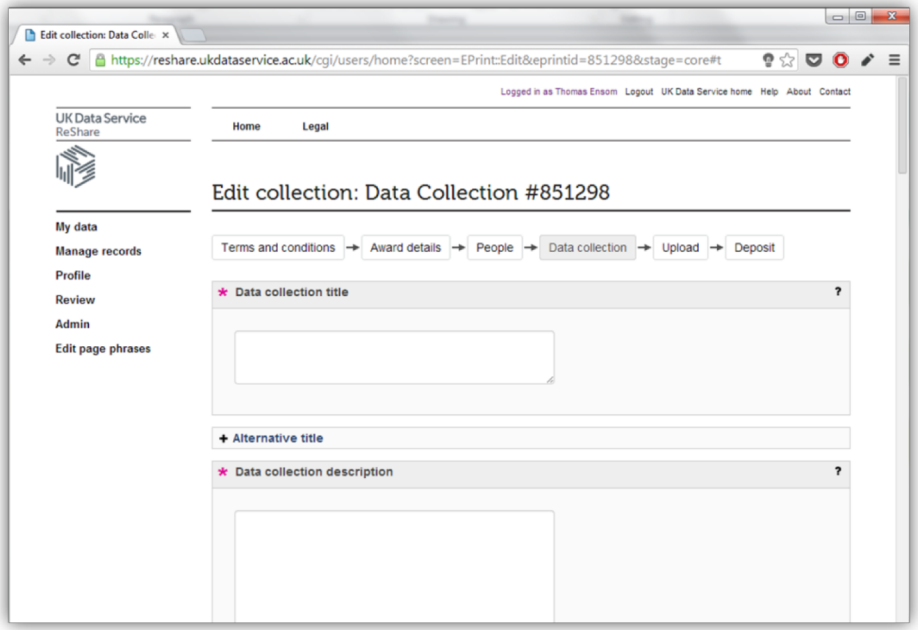
‘Personal data’ storage and transfers outside the EU

- 3 Routes

1. European Commission has decide that the country has an **adequate level** of protection
2. In absence of ‘adequacy decision’ personal data can be transferred to a third country where the controller or processor has provided **appropriate safeguards** and data subjects have **enforceable rights** and **legal remedies**
3. In absence of the above, there are derogations for specific situations including ‘**expressly consented**’

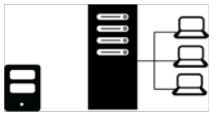
File sharing – data archive or repository

- A repository acts as more of a ‘final destination’ for data
- Many universities have data repositories now catering to its researchers, e.g. Research Data Essex
- UK Data Service has its own service called ‘ReShare’, for social science data of any kind
- http://reshare.ukdataservice.ac.uk/



UK Data Service

Data Storage: Comparison



	Portable	Cloud	Local	Networked drive
Advantage	Easy transport No internet needed Low cost	Easy access and sharing Automatic backup Automatic version control	Full control Easy to protect from unauthorised access	Central storage Shared and remote access Central backup
Disadvantage	Easily lost and damaged Not for long-term storage	Not always secure No control over storage location (breach data protection) Free service may claim right to use content	No sharing	Higher security needed Higher cost
Sensitive data	Encrypt files Password protect	Should not be stored in the cloud	Password protect PC Encrypt hard drive	Protect from unauthorised access

UK Data Service

Backing-up data

Backing-up data

- It is not a case of *if* you will lose data, but *when* you will lose data!
- Keep additional backup copies and protect against: software failure, hardware failure, malicious attacks and natural disasters
- **Would your data survive a disaster?**

UK Data Service

Common causes of data loss / damage

- Hardware failure
- Software malfunction
- Malware or hacking
- Human error (research data accidentally gets deleted or overwritten or is lost in transport)
- Theft, natural disaster or fire
- Degradation of storage media

Backups will permit you to restore data in the case of loss or damage

UK Data Service

Digital back-up strategy

Consider:

- **What's backed-up?** - all, some or just the bits you change?
- **Where?** - original copy, external local and remote copies
- **What media?** - DVD, external hard drive, USB, Cloud?
- **How often?** - hourly, daily, weekly? Automate the process?
- **How many copies?** - minimum of three copies!
- **What method/software?** - duplicating, syncing or mirroring?
- **For how long is it kept?** - data retention policies that might apply?
- **Verify and recover** - never assume, regularly test and restore

Backing-up need not be expensive

- 2Tb external drives are around £70, with back-up software

"We back up our data on sticky notes because sticky notes never crash."

Also consider non-digital storage options too!

UK Data Service

Verification and integrity checks

- Ensure that your backup method is working as intended
- Automated services - check
- Be wary when using sync tools in particular
  - Mirror in the wrong direction or using the wrong method, and you could lose new files completely

- You can use checksums to verify the integrity of a backup
- Also useful when transferring files
- Checksum somewhat like a files' fingerprint
- …but changes when the file changes

UK Data Service

Checksums

- Each time you run a checksum a number string is created for each file
- Even if one byte of data has been altered or corrupted that string will change
- Therefore, if the checksums before and after backing up a data file match, then you can be sure that the data have not altered during this process
- A free software tool for computing MD5 checksums is MD5summer for windows
- OS X has this functionality built into Terminal
- We will run through a demonstration of this later

UK Data Service

Data storage strategy

1. Use two types of storage media
   - At least two different types of storage media should be used, e.g. Solid State Disk (SSD) and CD-ROM or Hard Disk Drive (HDD) and SDD

2. Replace storage media
   - Replace storage media after 2-5 years

3. Carry out integrity checks
   - Frequently carry out integrity checks to ensure that the stored data has not been corrupted. This can be done with checksum tools. These allow you to detect if a file was changed in any way, intentionally or unintentionally

Data security

Data security

Protect data from unauthorised:

- Access
- Use
- Change
- Disclosure
- Destruction

Who knows who is watching, listening or attempting to access your data…

UK Data Service

The GDPR considerations

- Personal data should be sought to be **minimised**, **anonymised** and/or **pseudonymisation** – where appropriate – and ensure that **technical and organisational measures** are in place to ensure respect for the principle of **data minimisation**

Data security strategy

- Control access to computers:
  - use passwords and lock your machine when away from it
  - run up-to-date anti-virus and firewall protection
  - power surge protection
  - UPS power supplies
  - utilise encryption
    - on all devices: desktops, laptops, memory sticks, mobile devices
    - at all locations: work, home, travel
  - restrict access to sensitive materials e.g. consent forms and patient records
  - personal data need more protection – always keep them separate and secure
- Control physical access to buildings, rooms and filing cabinets
- Properly dispose of data and equipment once your project is finished

UK Data Service

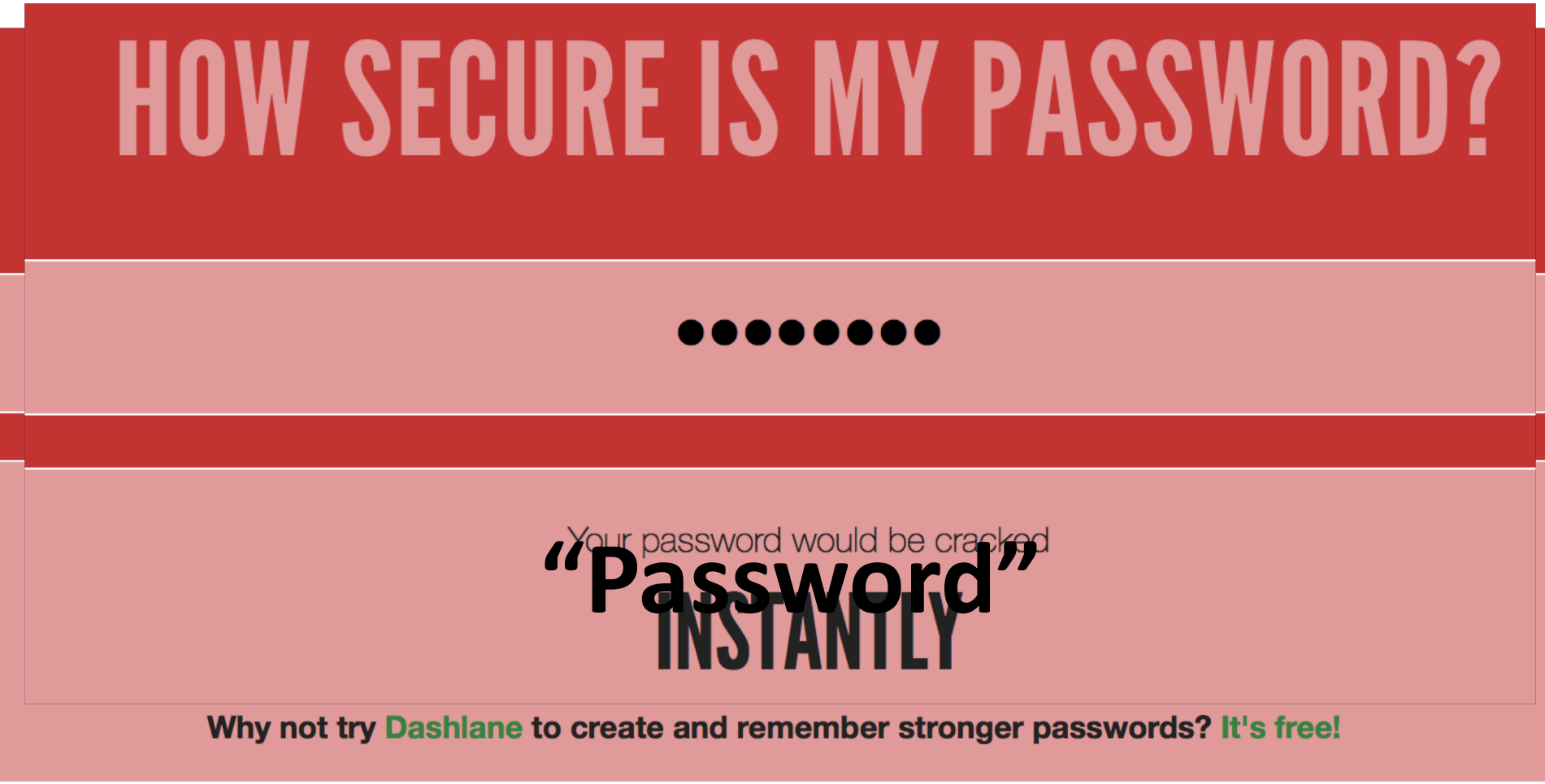
Passwords

- Strong passwords are crucial
- Avoid using weak or easy to guess passwords and reusing passwords
- Consider password managers, complex passwords or **stringing words together** to create stronger passwords
- But, remember that you need to be able to remember the passwords!
- **Why does this matter?**
- No matter how good the encryption is that you use if you use a weak password the encryption will offer little protection

https://howsecureismypassword.net (*Never use real passwords)

UK Data Service

Password security



"Password"

UK Data Service

Password security

UK Data Service

Password security

Edward Snowden on passwords

https://www.youtube.com/watch?v=yzGzB-yYKcc

UK Data Service

Encryption

- Encryption is the process of encoding digital information in such a way that only authorised parties can view it

- Basic principles
  - Applies an algorithm that makes a file unreadable
  - Needs a ‘key’ of some kind (passphrase or / and file) to decrypt

- Some types of encryption provide greater protection than others, the type and level of encryption used should correspond to the sensitivity of the data being protected

- As a general rule, more bits equals stronger encryption, therefore, 256-bit encryption is stronger than 128-bit encryption

Encryption

- When using encryption 128-bit encryption should be the minimum level used

- **Always** encrypt personal or sensitive data
  - = anything you would not send on a postcard
  - e.g. moving files, such as interview transcripts
  - e.g. storing files to shared areas or insecure devices

- The UK Data Service recommends Pretty Good Privacy (PGP)
  - More complicated than just a password, but much more secure
  - Involves use of multiple public and private keys

UK Data Service

Encryption software

Encryption software can be easy to use and enables users to:

- encrypt hard drives, partitions, files and folders
- encrypt portable storage devices such as USB flash drives

VeraCrypt

BitLocker

Axcrypt

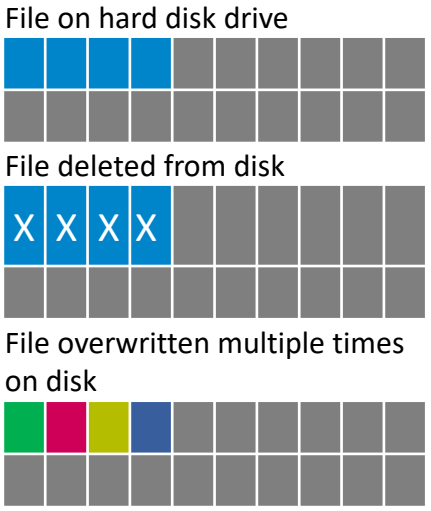
FileVault2

We will run through a demonstration of VeraCrypt later

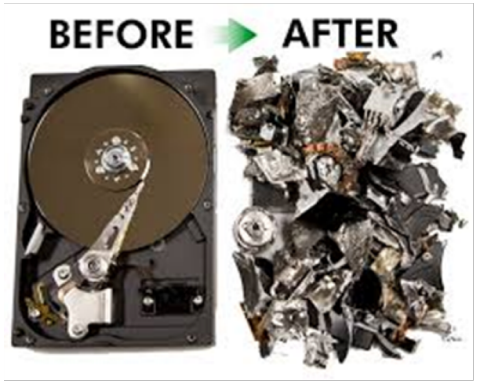
UK Data Service

Data disposal

- When you delete a file from a hard drive, it is likely to still be retrievable (even after emptying the recycle bin)



- Even reformatting a hard drive is ***not*** sufficient
- Files need to be overwritten multiple times with random data for best chances of removal
- The **only** sure way to ensure data is irretrievable is to physically destroy the drive (using an approved secure destruction facility)



UK Data Service

Data disposal software

BCWipe - uses ‘military-grade procedures to surgically remove all traces of any file’

- Can be applied to entire disk drives

AxCrypt - free open source file and folder shredding

- Integrates into Windows well, useful for single files

- Physically destroy portable media, as you would shred paper

UK Data Service

Summary of best practices in data storage and security

- Have a personal backup and storage strategy: (a) store an original local copy; (b) external local copy and (c) external remote copy
- Copy data files to new media every two-to-five years after first created
- Know your institutional back-up strategy
- Check data integrity of stored data files regularly (using checksums)
- Create new versions of files using a consistent and transparent system structure
- Encrypt data – especially when sensitive or transmitting and sharing
- Know data retention policies that apply: funder, publisher, home institution
- Archive data
- Securely destroy data at the end of the project

Resources

Video Tutorials

- VeraCrypt - https://www.youtube.com/watch?v=Ogm9QHQpFqU
- AxCrypt - https://www.youtube.com/watch?v=ACcRlnsoYZg
- FileVault 2 - https://www.youtube.com/watch?v=JIZ9EFMS0ic
- BitLocker - https://www.youtube.com/watch?v=y4Iosu-Yfsw
- Time Machine - https://www.youtube.com/watch?v=hlsQaVj7WtA
- MD5summer - https://www.youtube.com/watch?v=VcBfkB6N7-k

Questions

Contact Details:

Scott Summers
UK Data Service
University of Essex
ukdataservice.ac.uk/help/get-in-touch