



The Royal Academy
of Engineering

The Security of Personal Information

19 July 2007



The Royal Academy
of Engineering

Can Personal Information be Held Securely?

Martyn Thomas CBE FREng



The Royal Academy
of Engineering

What do we mean by *securely*?

Integrity: accidental or malicious changes to data

Availability: allowable downtime per year

Reliability: returning the wrong data or failing to return any data, or crashing ...

Confidentiality: preventing unauthorised access to data



The Royal Academy
of Engineering

How secure is *secure enough*?

Confidentiality

How often is it tolerable to leak personal data?

What maximum number of records may be leaked each year?

If the system fails to meet these requirements, what action must be taken?

Without clear requirements, we cannot know how to design the systems.

If the requirement is for zero leakage, the systems will be very expensive, and may be unusable.



High Confidentiality v Usability

- Physically secure environment, no internet access?
- Multiple levels of authentication: what you possess/what you know.
- Automatic disconnection on very short idle time-outs
- Stringent vetting of personnel who have access

Most systems that use private data would be unusable if these requirements were introduced



Software Engineering Issues

1. You *cannot* show high dependability by testing alone
2. Most existing software cannot be analysed in depth
3. Many programming languages have serious defects
4. Existing software contains large numbers of vulnerabilities
5. Developing secure software and **showing the absence of security vulnerabilities** needs special expertise and software tools



Systems Engineering Issues

1. Consider the **whole lifecycle** of the data, from collection to complete destruction
2. Pay particular attention to systems maintenance, archiving and auditing
3. Many security breaches result from human error or corrupt insiders
4. Encryption can be a powerful tool for protecting confidentiality



The Royal Academy
of Engineering

Recommendations

Be explicit about the security requirements

Assume commercial software is insecure

Encrypt all data as collected; decrypt it at the last minute

Hold the minimum data that is personally identifiable, for the minimum period; separate identity from data

Avoid linking data from different roles unless essential – encourage multiple identities

Assume that data leaks are inevitable and plan accordingly