You Can’t Get There From Here!

Prof. Neil Barrett

BCS Oxford – 29th Nov. 2005

Introduction

- Information Security
- Identification, Authentication, Authorisation and Non-repudiation
- Crimes committed on or with computers
- Evidential issues
- The limitations of information security
  - Practical
  - Theoretical
- Conclusions

Information Security

- A collection of measures to establish
  - Confidentiality
  - Integrity
  - Availability
- Only authorised users should be able to access information
  - To create, delete, read, change…
- But crucially, how do we establish who is and is not ‘authorised’?

Identification, Authentication, Authorisation and Non-Repudiation

- Identification – Who is this user and do we recognise them?
- Authentication – Can we prove that this is indeed the person?
- Authorisation – If it is the right person, what information should they be able to access and in what fashion?
- Non-Repudiation – Can we ensure that the person cannot deny responsibility for any access that they carry out?

Identification

- User name
- Some way of allowing the computer system to recognise the person

Authentication

- Type 1 – Something they know – a password
- Type 2 – Something they have – a token
- Type 3 – Something they are – a fingerprint
- One or Two factor
- Determines trust level of the computer

Authorisation

- Access to data by means of some controlling data structure
  - An Access Control List or similar structure
- Based on reliable identification and successful authentication
- Ensures that users can only access what they are meant to access

Non-Repudiation

- Arises from clean, reliable and unalterable records of “who did what to what piece of data”?
- Records can be digitally signed, reliably stored etc

Crimes on Computers

- Raising permission levels
- Accessing information
- Altering or preventing access to information
- Manipulating records
- All involve, to some extent, exceeding ‘authorised access’
  - Presuming always, of course, that the authorised access has been suitably well-defined.

Evidential Issues

- Computers record the actions of authenticated users
  - In terms of the access granted to processes based on the authorisation data structure
- But a process cannot be prosecuted
  - Only a person can stand in the dock
- So, the data collected for non-repudiation purposes must be capable of presenting in court

Evidential Issues (2)

- This means that the auditing data must be
  - Comprehensive
  - Complete
  - Clear
  - Capable of preservation
- Reliable copies of original data is fine
  - But the process of that copying must itself be capable of analysis
- Data can be put in front of the court
  - It forms ‘documentary’ evidence

Limitations

- Of course, this depends on the reliability and integrity of the information security
  - Can we reliably restrict access to information based upon some rules
  - The rules relate to the authentication and authorisation controls
- We need to be able to analyse the operation of the program elements to achieve this

Limitations (2)

- Unfortunately, this analysis is not rigorously possible
- Turing proved elements of the ‘Halting Problem’
  - That determining in advance whether a given program would or would not halt is in fact undecidable
- That is, it is mathematically impossible to determine a program’s actions in advance
  - The only way to determine the actions is to run it

Implications

- Anti-virus is impossible!
  - Requires you to know in advance what a given program will do
- Program monitoring is impossible
  - Requires you to wrap a program inside another program
    - But then, what happens to that program?
      - It too needs to be wrapped
        - » Etc…

Implications (2)

- Because information security cannot be algorithmically determined
  - Authorisation cannot be
  - So, the task of determining whether or not a given user is responsible for a given action is impossible
- We are left only with heuristics

Implications (3)

- Heuristics provide technical solutions
  - In which the task of exceeding authorised access is made as difficult as possible
- Information security should Protect, Detect and Deter
  - Detection and Deterrence therefore must be seen as important elements
    - Can we determine what a user has done?
    - Can we persuade them therefore not to do it because we will be able to detect it?

Conclusions

- Information security is useful, important… but mathematically impossible
- The best we can do is a form of ‘best endeavours’
- But this will give us problems in the courts as evidence is presented!

Thank You!

- Prof. Neil Barrett FBCS