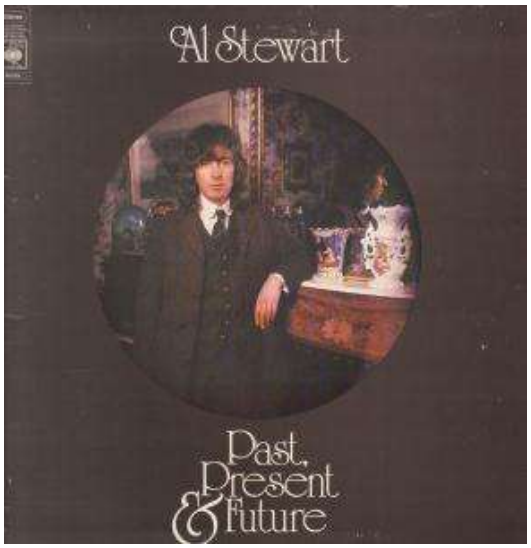
Cyber Security: Past, Present and Future

Chris Mitchell
www.chrismitchell.net



3

Agenda

- What is cyber security?
- The past
- The present
- The future …

4

Agenda

- What is cyber security?
- The past
- The present
- The future …

Defining cyber security

- There is no generally agreed definition for the term **cyber security**.
- Not so surprising since security itself is a very difficult word to define!
- I see cyber security as a simple extension of the existing notions of **information security** and **computer security** recognising the pervasive nature of modern ICT.
- Hence we are now dealing with a pervasive threat and one that government cannot ignore since it has impacts on almost every aspect of daily life.

CIA

- Long-standing definition of scope of *computer security* is as:
  - *Confidentiality* (preventing unauthorised disclosure of information);
  - *Integrity* (preventing unauthorised modification of information);
  - *Availability* (preventing denial of access by authorised parties to resources, including processing, communications, and information).
- Not such a bad definition for cyber security, although it omits a few issues.

Similar terms

- There are many widely used terms with similar (or more specialised) meanings, e.g.:
  - *Communications security*: protecting information sent via networks;
  - *IT (or ICT) security*: protecting information handled by, and resources associated with, IT (ICT) infrastructures;
  - *Critical National Infrastructure (CNI) security*: protecting countrywide infrastructures, such as electricity, gas and water supplies, road and rail networks, etc.
- Cyber security subsumes all this …

9

9

Why a new term?

- Why is yet another term needed?
- The
  - pervasiveness of ICT, and
  - ever-growing interdependence and complexity of systems,

  means that security is a government and public policy issue, rather than just an issue for individual citizens or corporate entities.
- I see emergence of cyber security as an indication of government recognising its responsibility for protecting the citizen (and not just in protecting its own infrastructure).

10

10

Public policy

- Security is no longer a private matter.
- Poor decisions made by all manufacturers and service providers could seriously affect safety of citizens (not just CNI – or perhaps everything is now a CNI).
- Public policy makers are a long way from being in a position to address this issue satisfactorily.
- We all hope that initiatives like the two new CDTs in cyber security will, in the long run, help to redress this imbalance.

Agenda

- What is cyber security?
- The past
- The present
- The future …

The academic subject

- Academic interest in cyber security has developed in independent strands since the 1970s, including:
  - cryptography;
  - computer security; and
  - network/protocol security.
- Of course, other topics have also grown up independently since then, including malware studies, intrusion detection, etc.
- Also, much of the work has been done jointly by academia and industry (and, to some extent, government agencies).
- Look at some of these strands (noting strong UK influence).

13

13

Cryptography

- Cryptography emerged from the shadows to become an academic subject in the 1970s.
- Number of important developments in 70s:
  - development of DES (public) standard block cipher;
  - invention of public key cryptography, RSA and Diffie-Hellman key agreement;
  - start of public discussion of design and analysis of ciphers, including stream ciphers.

14

14

DES

- DES arose as a result of a competition by NBS in the US for a block cipher.
- This has become a model for development of new international crypto standards
- NIST (successor to NBS) has led two competitions giving us AES (DES successor) & SHA-3 (hash-function successor to SHA-1/2).
- Other bodies now launching similar competitions (e.g. recent competition for an authenticated encryption scheme).

15

15

Public key crypto and RSA

- Diffie and Hellman (at Stanford) wrote *New directions in cryptography* in 1976, describing:
  - notion of public key cryptography (PKC), and
  - the Diffie-Hellman (DH) key agreement method.
- This stimulated Rivest, Shamir and Adleman (at MIT) to develop the first practical public key encryption scheme, RSA.
- Interestingly, PKC, RSA and DH were independently developed in early 1970s by Ellis, Cocks and Williamson at GCHQ here in the UK.

16

16

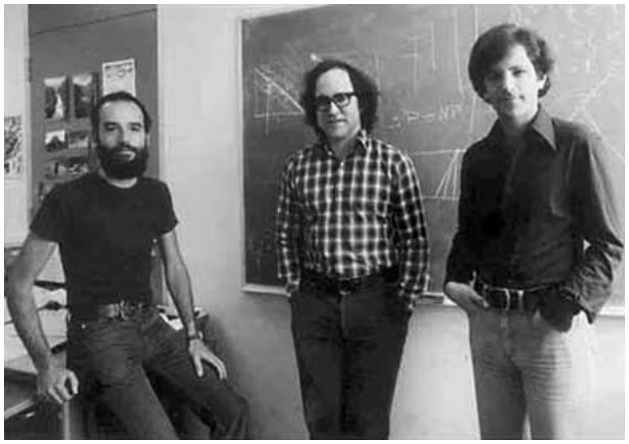
Merkle, Hellman and Diffie

17

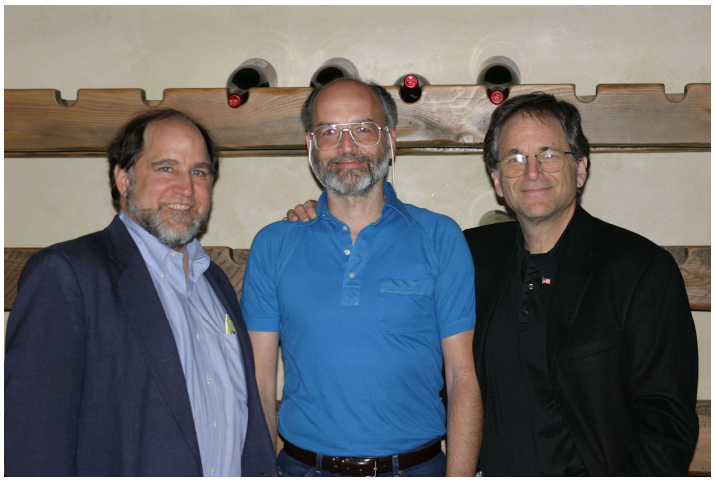
Diffie and Hellman

18

Shamir, Rivest & Adleman – then …



… and more recently (in the right order)



James Ellis, Clifford Cocks and Malcolm Williamson



21

21

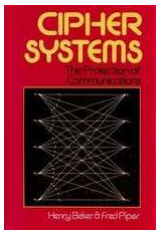
Development of academic subject

- Three books published in the early 1980s played a major role in the development of academic crypto, by:
  - Alan Konheim (*Cryptography: A primer*),
  - Carl Mayer and Stephen Matyas (*Cryptography: A New Dimension in Computer Data Security*), and
  - Henry Beker and Fred Piper (*Cipher Systems*), here in the UK.

22

22

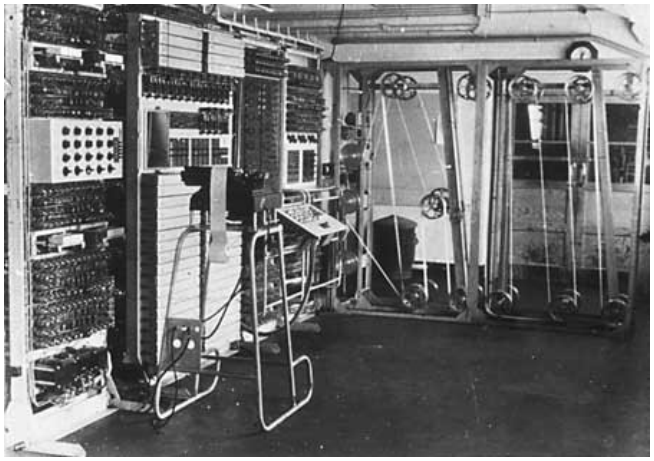
Beker and Piper: Cipher Systems



History of computing

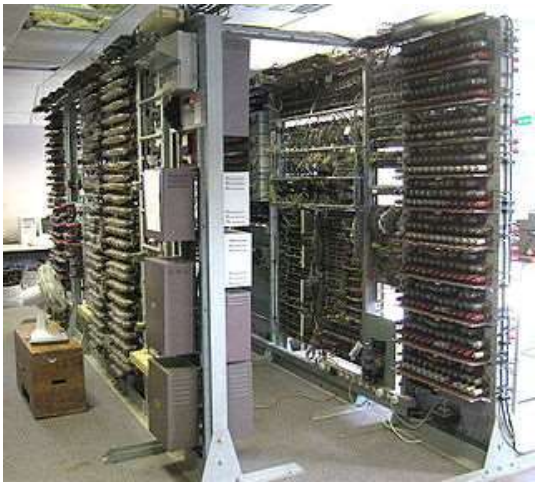
- The development of computing as we know it today was presaged by the development of Colossus in the UK during the 2nd World War.
- Colossus, a fully programmable computer, was developed in 1943 to break the Lorenz SZ40/42 stream cipher.
- Alan Turing and Tommy Flowers played a major role in its development.

Colossus



25

Colossus rebuilt (at Bletchley)



26

Computer security

- In parallel with development of cryptography, modern day computer security emerged in the 1960s and 70s, including:
  - access control models (including fundamental work by Lampson)
  - notion of process isolation (key to modern models of computer security);
  - virtualisation (notable work by Paul Karger at DEC, ideas resuscitated more recently)
  - multilevel security (to meet government requirements);
  - Orange Book certification (US DoD).

27

27

Butler Lampson

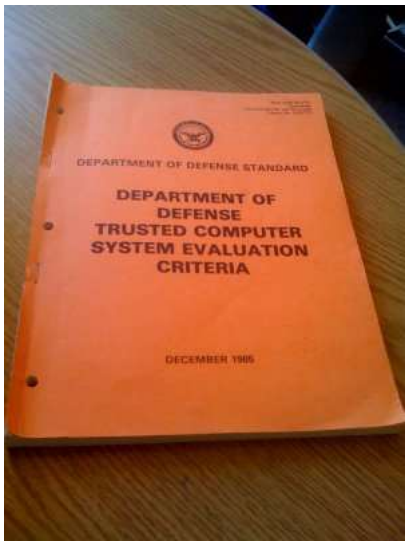
28

28

Paul Karger

29

Orange Book



30

Software verification

- Techniques to enable mathematical proofs to be formulated regarding properties of software have been developed in parallel with other security technologies.
- University of Oxford has played a leading role in this area over several decades – I'm sure there are many here today infinitely better qualified than me to explain this history.
- These techniques are likely to prove invaluable in helping to developing everyday 'utility' user software provably free of vulnerabilities.

31

31

Applications of cryptography

- A further strand has been the development of ways of using cryptography in computers and networks.
- The UK's Roger Needham played a key role in two of these:
  - using one-way functions to protect stored passwords (1966);
  - the Needham-Schroeder authentication protocols (1978).

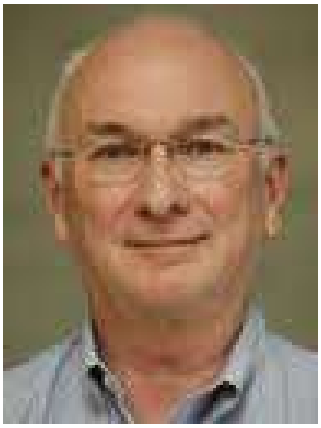
32

32

Roger Needham

33

Michael Schroeder

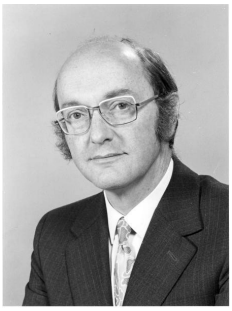


34

Another key book

- A key book for the development of the applications of cryptography was published in the early 1980s.
- Donald Davies and Wyn Price (at the UK's NPL) published *Security for computer networks* in 1984.

Donald Davies (and Wyn Price)



Some links

- Donald Davies (who played a major role in developing packet switched networks) worked with Alan Turing at NPL in the late 1940s, helping to develop the ACE computer.
- Donald Davies also played a key role in setting up the standards committee which evolved into ISO/IEC JTC 1/SC 27 (more on this later).

Interesting observations

- There has been a very strong UK influence on the development of all aspects of cyber security.
- The key technological ideas date back at least 30-40 years.
- We are still struggling to properly deploy some of the well-established technologies developed many years ago.

Education

- Before 1992 (when RHUL launched its MSc in Info Sec) security barely had an impact on university taught courses
- A handful of PhDs in cryptography and computer security were being produced.
- Now, nearly 30 years later, there are plethora of masters-level taught courses in the area, and many PhD students are graduating in security topics every year.

39

39

Royal Holloway

40

40

In the real world – crypto

- 'Early adopters' of cryptography were:
  - the banks (DES rapidly became a de facto international standard),
  - mobile telecommunications (GSM).
- For example, crypto has been widely deployed to protect PINs transferred between ATMs and banks for decades.
- Similarly, from the beginning GSM SIMs incorporated secret keys and crypto-based authentication.

41

41

42

42

43

In the real world – secure computing

- Multilevel secure computing has remained primarily the realm of government.
- DOS and Windows pre XP had no security model – assumed single user – no internal protection for OS against applications.
- Unix always had a simple security model.
- Both Windows and Unix had major user authentication flaws.

44

Emergence of cyber security

- We have seen an evolution of security:
  - from being a concern only of government and military for their own secrets (**for ever**),
  - to a matter of huge importance for corporations, e.g. banks, telecoms, and owners of IT infrastructure (**from 1970s**),
  - to a matter of concern for domestic users, threats of phishing, ID theft, etc. (**from 1990s**),
  - to being a matter of public policy: cyber security (**from around ,mid 2000s**).

Agenda

- What is cyber security?
- The past
- The present
- The future …

Managing security

- The compliance approach to security management appears to dominate.
- Most prominent amongst the compliance approaches is specified in the ISO/IEC 27000 series (ISO/IEC 27002 was previously BS 7799 and ISO/IEC 17799).
- Sector-specific compliance documents also exist, e.g. for payments industry (PCI) and for government.
- Compliance standards try to capture and encourage use of current understanding about best practice.
- However, serious danger of reducing security management to a 'box ticking' exercise.

47

47

Designing security

- We have developed heuristics for designing secure systems, building requirements on detailed risk analyses.
- These have been successful to some extent, e.g. in developing 3G mobile security system.
- In most cases they fall some way short of the 'ideal' of provable security.
- In practice many problems remain, e.g. sub-optimal uses of cryptography, incomplete risk analyses, poor implementation, …
- Perhaps most serious problems arise where system designers do not take security sufficiently seriously, e.g. when they do not understand the risks.

48

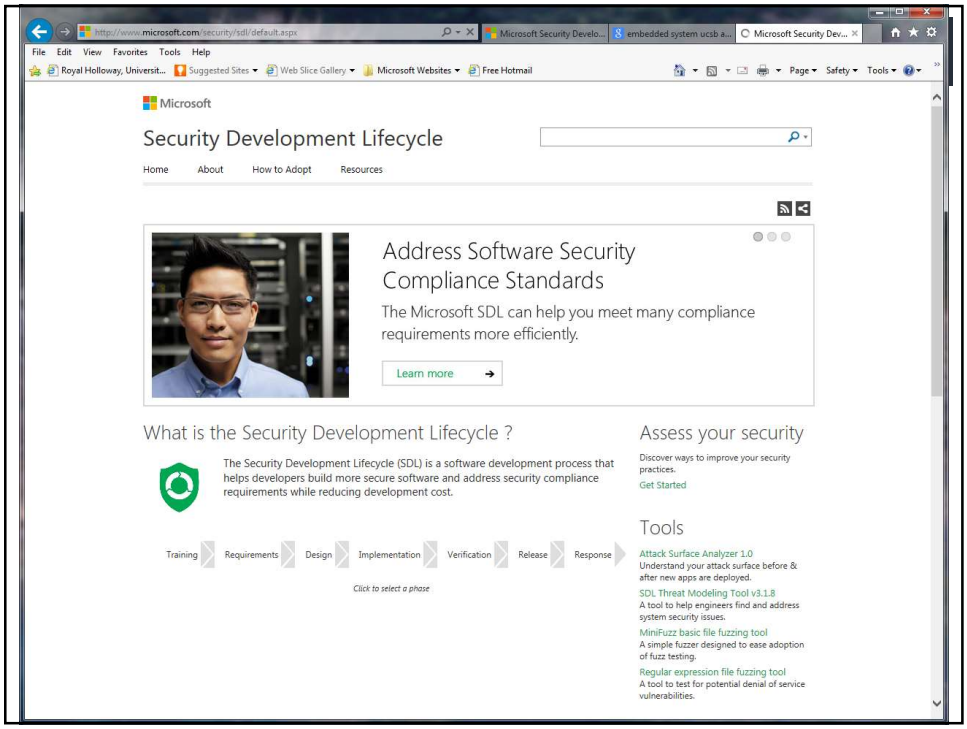
48

Implementing security

- Many problems arise in going from designs to implementations.
- Manufacturers of major pieces of software are constantly issuing patches to fix vulnerabilities arising from flawed design or implementation.
- Recent research has shown that many widely deployed embedded systems are hopelessly insecure
- Even widely deployed protocols like SSL/TLS and IPsec have been shown to have security flaws.

Building secure systems

- Major software manufacturers have developed methodologies to try to improve design and implementation with respect to security.
- Notable example is Microsoft's Security Development Lifecycle (SDL).
- Has been widely adopted across the industry.
- Yes, it is all heuristic in nature (although some of the freely available tools do use formal techniques).



51

Information Security Group

ROYAL HOLLOWAY UNIVERSITY OF LONDON

Security standards

- Today we have a very broad-ranging set of international standards for security, covering:
  - security management (27000 series);
  - cryptographic techniques;
  - security evaluation (common criteria);
  - network and system security;
  - privacy and identity management.
- Not always adopted, not least because of lack of awareness.

52

52

Hidden dangers

- Often systems are used in situations, or are subject to interconnectivity, of which the original designers had no idea.
- 'Black box' security components are used, which may not be secure.
- There is a widespread lack of understanding of security, how vulnerabilities can arise, and how pervasive the threats are.
- This applies in particular to products not thought of as needing security, e.g. a wide range of embedded systems.

53

53

Security education today

- Information security has become a widely offered masters degree topic – good supply of specialists.
- Also has become a core part of a Computer Science undergraduate curriculum.
- However, it appears there are still issues with software developers not understanding threats to software
- Security needs to be fully integrated into undergraduate education.

54

54

Rise of privacy concerns

- Over the last decade the need to enforce privacy for IT systems has become a major concern, in parallel with need for security.
- Providing privacy requires security (to prevent leakage and corruption of personal data).
- However, the goals of privacy and security may be very different, e.g. accountability can be seen as 'anti-privacy'.

Agenda

- What is cyber security?
- The past
- The present
- The future …

Major challenges

- Many huge challenges remain for security:
  - in security management we need to go beyond a rigid compliance approach.
  - need to understand security implications of ever-greater connectivity and pervasiveness of computing;
  - must address threats arising from ever-increasing complexity, and the growing criticality of systems;
  - widespread use of cloud introduces new range of privacy and security concerns.

Managing security

- Managing security in organisations large and small is today a major challenge.
- We need to find ways of addressing the large gap that often exists between:
  - organisational threat analyses, procedures and processes (perhaps developed using ISO/IEC 27000), and
  - the actual practice of (in)security by employees.
- If security rules prevent employee doing his/her job properly, then they will be broken.

Building secure systems

- We need better tools to design everyday systems that will be secure (as opposed to security systems).
- Current methodologies do not prevent all vulnerabilities.
- Moreover, they simply don't work for some types of software, e.g. software for providing cloud services which is constantly being modified.

Proving systems secure

- Ultimately we need ways of developing systems which we can prove have no vulnerabilities.
- This is extremely challenging since systems are so complex, systems often need to be developed quickly, and vulnerabilities can arise in so many ways, e.g. through:
  - imperfect risk analysis, or emergence of new classes of threat, e.g. through deployment of new technology;
  - flawed design;
  - flawed implementation;
  - use of poor security components (e.g. flawed crypto).

Vulnerabilities and disclosure I

- We have a developing crisis relating to vulnerabilities and disclosure.
- Security vulnerabilities in products are being found at a huge rate.
- Despite efforts by manufacturers (including a standard – ISO/IEC 29147) there is a lack of consensus on the morality/best practice of disclosing vulnerabilities.
- Highlighted by the famous Megamos car immobiliser security case, in which three academics were prevented by a UK court from presenting full details of a system they had broken.

61

62

Vulnerabilities and disclosure II

- This is just the tip of the iceberg …
- Established 'best practice' for 'responsible disclosure' were developed piecemeal through practices in finding and revealing crypto and software vulnerabilities.
- Researchers believe they have a right to publish vulnerabilities (perhaps after giving manufacturers a few months to fix things), arguing that manufacturers deserve to be punished for poor security practice.
- However, in many cases it is the poor old users who suffer the most.
- Who is right and what should be done?
- This touches strongly on public policy …

63

63

Public policy

- Some degree of regulation of pervasive/consumer IT probably inevitable.
- Need to get it right.
- In principle, existing regulations might well be sufficient – e.g. covering safety.
- However, new classes of vulnerability caused by interconnectivity and computing everywhere probably elude existing regulatory regimes.

64

64

Future of security education

- The last 20-30 years has seen a growth in masters level cybersecurity education from nothing to a very significant level.
- Security education at the undergraduate level, particularly for Computer Science and Electrical Engineering, is still developing.
- An appreciation of security risks needs to be built into broad range of curricula.

65

65

Address growing privacy concerns

- The Snowden and other revelations (e.g. relating to Facebook) have drawn attention to the huge potential for monitoring and processing of personal data.
- This is not going to go away.
- Somehow, we need to reconcile desire for privacy with use of 'free' services depending on targeted advertising, and needs of government security services.

66

66

Concluding remarks

- Cybersecurity has emerged as a major academic discipline in its own right, paralleling developments in industry, commerce and government.
- A wide range of major challenges remain.
- With criminal organisations and governments increasingly targeting all aspects of our information infrastructure, which is itself growing more complex daily, **there are no shortages of security issues to be addressed for the foreseeable future**.

67