Computer Science Tripos part 2 – Security

Ross J. Anderson

This course builds on the 1b 'Introduction to Security' course to give you a solid foundation in contemporary computer security and cryptology. We look at a number of applications which need various combinations of confidentiality, availability, integrity and covertness properties; at the mechanisms which we can use to incorporate these properties in systems; at how such systems fail, and how they can be made robust against various kinds of failure; and at the various policy and legal issues.

The course consists of twelve lectures on the following topics:

Lecture 1: Multilevel security policy models. The Bell-LaPadula model; system Z; the lattice model; the Biba model; composability, noninterference and nondeducibility; polyinstantiation; the effect of viruses; covert channels.

Lecture 2: Further security policy topics. The Clark-Wilson model; the Chinese Wall; privacy and compartmented mode models; inference control.

Lecture 3: Advanced access control topics: Unix and Internet security including sendmail problems, the Internet worm, password sniffing attacks and firewalls.

Lecture 4: Malicious code, intrusion detection, application level controls, denial of service.

Lecture 5: Copyright marking; steganography; unobtrusive communications; Tempest; tamper resistance

Lecture 6: Stream ciphers. Monoalphabetics, Vigenère ciphers, the one-time pad. Linear feedback shift registers; the nonlinear filter generator; A5; the multiplexer generator; divide and conquer attacks; fast correlation attacks.

Lecture 7: Block ciphers. Feistel ciphers including DES. Differential and linear cryptanalysis. Other styles of block cipher, including SAFER, Skipjack and IDEA. Modes of operation. Hash functions and their applications.

Lecture 8: Elementary cryptographic protocols, including Needham-Schroder, Otway-Rees, Kerberos and Kryptoknight. Key management in banking systems. Protocol failures and the BAN logic.

Lecture 9: Guest lecture on number theory and factoring algorithms. The Pollard rho method and the quadratic sieve.

Lecture 10: Public key cryptography: Diffie-Hellman, ElGamal, DSA, RSA, digital cash, threshold signatures.

Lecture 11: Public key protocols and failures: Denning-Sacco, Needham Schroder, Tatebayashi-Matsuzaki-Newmann. Chosen protocol attacks. The BAN logic for public key protocols.

Lecture 12: Security engineering: what actually goes wrong with real systems. Threat trees and risk models. Evaluation and accreditation. Policy and legal issues: civil and criminal evidence rules, the Data Protection Acts the Computer Misuse Act, export control and key escrow. Organisational issues; due diligence and the role of insurance.

Books and other sources

System security is an extremely wide subject, drawing on a great range of disciplines. Although computer secience is now the central one, we draw on mathematics, electrical engineering, semiconductor physics, applied psychology, financial accounting, the criminal law ... there's never a dull moment.

The best way for you to acquire a feel for what's going on is by wide reading. The history is fun: for the period up to world war 2, see Kahn's *'The Codebreakers'*, while details of how codebreakers at Bletchley Park cracked the Enigma during the war are in Welchman's *'The Hut Six Story'* and Hinsley and Stripp's *'Codebreakers'*.

Textbooks: Ed Amoroso's *'Fundamentals of Computer Security Technology'* is a good general introduction, while Dieter Gollmann's *'Computer Security'* is very good on the military side of things. For more specific information on Unix and Internet security, see Cheswick and Bellovin's *'Firewalls and Internet Security'* and Garfinkel and Spafford's *'Practical Unix and Internet Security'*. None of the above goes into cryptology in much depth. For that, try Schneier's *'Applied Cryptography'* which is quite broad and includes 'C' source code for a lot of algorithms (be sure to get the second edition). More specialised books are referred to in the *further reading* notes at the end of each lecture.

If you are thinking of a career (research or otherwise) which touches on this subject, I'd encourage you to come to the security seminars, which are held on most Tuesday afternoons during term, and the lab's security group meetings at 4pm on Fridays (both in TP4).

Finally, there are many relevant and interesting resources on the web, from newsgroups such as `sci.crypt.research` and `comp.risks` through hacker and CERT sites to researchers' home pages and organisations involved in crypto policy.

Ross Anderson
January 1999