Professional Development Topic 3: Risks and Threats

Prof Nick Taylor
Department of Computer Science
Heriot-Watt University

Content

- Computer Crime
  - Theft
  - Piracy
  - Espionage
  - Fraud
  - Sabotage
- Malicious Software
  - Viruses
  - Trojans
  - Worms
- Security
  - Verification
  - Authentication
  - Encryption

Computer Crime

- Theft
  - Stealing plain and simple
    - Taking away another's property
- Piracy
  - Stealing potential revenue
    - Copyright or patent violation
- Espionage
  - Stealing secrets
    - Acquisition of confidential information
- Fraud
  - Deceitfully gaining advantage
    - Financial or other personal advantage
- Sabotage
  - Reducing effectiveness of a system
    - Deliberate destruction or damage

Breaches of System Integrity

- Physical
  - Computer Failure
  - Power Failure
  - Network Failure
  - Equipment Theft
  - Lightning
  - Flood
  - Sabotage
  - Fire
- Logical
  - Viruses
  - Untested Software
  - User Error
  - Operator Error
  - Staff Misuse
  - Internal Access
  - Computer Fraud
  - Hacking
  - Tapping Lines

Source: IT Security Breaches Survey (NCC, DTI, ICL) covering period 1992-4 with 832 respondents. [Lists ranked by % of respondents reporting named breach]

Estimated Cost of Breaches

	Max Cost of Single Incidents (£1000s)	Number of Breaches	% of Total Cost of All Breaches
All Breaches	1,200	444	100
Computer Fraud	1,200	7	33
Computer Failure	200	67	13
Equipment Theft	60	69	13
Viruses	100	93	9
Flood	200	17	7
Fire	50	5	3
Sabotage	75	5	2
Lightning	20	12	2
Network Failure	20	26	2
User Error	50	9	1
Operator Error	20	13	1
Untested Software	20	19	1
Hacking	8	4	0.3
Staff Misuse	2	10	0.2
Internal Access	2	4	0.07
Tapping Lines	0.2	1	0.006
Other	20	11	1

Theft

- Depriving somebody of physical property
  - Taking something away physically
- Depriving somebody of an exclusivity right
  - Taking a copy of something
  - Not necessarily infringing their intellectual property rights
  - Violating their right to privacy perhaps
- Piracy as Theft
  - Violating intellectual property rights
- Espionage as Theft
  - Violating right to privacy/secrecy

Piracy

- Depriving somebody of an intellectual property right
  - Infringing copyright, patent, design right, trademark, etc.
  - Right to be acknowledged as author/owner
  - Right to not have one's work tampered with
  - Right to license for financial gain
  - Right to sell-on for financial gain
- Stealing revenue
  - *Copying programs*
  - *Copying Data*
    - *Words, art, music*
  - *Unscrambling/Decrypting protection mechanisms*
    - *DeCSS example*

Espionage

- *Sniffers*
  - Computer networks share comms channels so any node on a network can receive transmissions intended for other nodes
  - Normally a node would discard any packets not addressed to it but it is possible to configure nodes to be "promiscuous" and receive all packets
  - Sniffing is using a promiscuous node to inspect all packets on a network particularly start of session packets which convey username and password details
  - Encryption can prevent sniffers from making sense of the information sniffed
- *TEMPEST*
  - Data can be captured from screens, keyboards, even disk accesses using TEMPEST - the Transient Electro-Magnetic Pulse Emission Standard
  - Encryption can't be used for display screens

Fraud

- Gaining any advantage through deceit
  - Not just financial advantage
  - Some form of deceit must be involved
- Impossible to estimate how much financial fraud occurs, with or without computer assistance
  - The only guarantee is that fraud will always be grossly under-reported by the victims
- The scandal of large scale fraud can bring companies to their knees
  - Barings bank
- Rule of thumb for estimating cost of fraud
  - Multiply reported figures by 10!

Sabotage

- *Feb 2000 saw denial of service attacks on Amazon, Buy.com, CNN.com, eBay, Excite, E*Trade, Yahoo and ZDNet*
- *Estimated £9 billion of damage worldwide in 2001 as a result of lost productivity and intellectual property* [McAfee]
- *Estimated 51,000 viruses currently in circulation* [GROUP Technologies]
- *3.2 million spam attacks in Feb 2002 cf 300,000 in Aug 2000*
  [Brightmail Probe Network]

Malicious Software

- Virus
  - Self-replicating code segment
  - Embedded in larger host program
  - Activated when host executed
  - Copies itself into other programs
  - Modifies new hosts to call it
- Trojan Horse
  - Program which performs a useful function but which includes HIDDEN destructive code
- Worm
  - Self-replicating program
  - No carrier program needed
  - Spreads via LANs or WANs
  - Copies itself to connected hosts

A Word About Bombs

- Malicious code can be triggered by execution of the host program in which it is carried or by a “bomb”
- Logic bomb
  - Monitors system activity and detonates when a particular event occurs or when an event occurs for the nth time
- Time bomb
  - Monitors the system clock and detonates at a particular time or date

Basic Virus Types

- Boot Sector or Partition Record
  - Infect disks, diskettes, etc.
- Application, Link or Macro
  - Infect executable files
- Transient
  - Execute briefly each time host started
- Resident
  - Execute when host started but remain active in memory
- Direct
  - Infectious only when programs are executed or files are accessed
- Indirect
  - Actively search for files to infect

Virus Signatures

- Virus scanners look for tell-tale signatures –
  - Storage signatures
    - The attached virus code is always located in the same position in the infected file and can be searched for by virus scanners
  - Execution signatures
    - The sequence of modifications performed by the virus can be detected by monitoring software
  - Transmission signatures
    - Apart from the standard network monitoring undertaken by firewalls, etc. e-mail viruses, for instance, can be detected when they access address books, etc.

Advanced Virus Types

- Stealth viruses
  - Hide their existence in one of three ways –
    - Intercept attempts to determine file sizes by virus scanners and send the original, uninfected, file size back to the scanner
    - Take a copy of the original, uninfected, boot sector and redirect attempts to check the boot sector to the copy
    - Disable a virus scanner and simply stop it working
- Polymorphic viruses
  - Camouflage themselves
    - Make each copy of themselves slightly different by scrambling their code or adding bits of decoy code

Virus Examples I

- **Brain (1986)**
  - Type: Boot sector
  - Effects: Reduces RAM by 7K
Traps BIOS interrupts
Infects disks in A: or B: drives
  - Damage: Volume label modified
- **Jerusalem/Israeli (1987)**
  - Type: Link, Resident, Direct
  - Effects: Appends code to .COM & .EXE files (1813 byte extension)
  - Damage: Slows system after 30 mins
Deletes files executed on Friday 13th
- **Yale/Alameda (1987)**
  - Type: Boot sector
  - Effects: Reduces RAM by 1K
Traps BIOS interrupts
Infects any diskettes used to re-boot
  - Damage: Destroys a diskette sector

Virus Examples II

- **Cascade (1988)**
  - Type: Link, Resident, Direct
  - Effects: Appends code to .COM files (1701/4 byte extension)
  - Damage: Display of falling letters
- **4096 (1990)**
  - Type: Link, Resident, Stealth
  - Effects: Traps DOS interrupts
Traps BIOS interrupts
Infects .COM & .EXE files
  - Damage: File dates incremented by 100 years
- **Michelangelo (1992)**
  - Type: Boot sector
  - Effects: Master boot record moved
  - Damage: On 6th March destroys data on boot device when booted

Virus Examples III

- Melissa (1999)
  - Spreads incredibly rapidly via e-mail
  - Sent itself to 50 addresses in address book
  - MS Word macro virus spawned variants
    E.g. “Papa” MS Excel macro virus
  - Infected PCs initially; Apple Macs later
  - 100,000 systems infected [FBI estimate]
  - Cost £50 million of damage
  - David Smith sentenced to 20 months and £1,500 fine (light due to “co-operation”)
- Whether by design or not, Melissa gave viruses a new weapon – psychology
  - By using personal address books, Melissa encouraged recipients to open the attached document because they knew the person who appeared to have sent it
  - Viruses could now employ psychological tricks to fool otherwise sensible people into ignoring the precautions which they knew they ought to be taking

Virus Examples IV

- The Love Bug (2000)
  - "Psychological" virus (*cf Melissa)*
    - E-mail purporting to come from somebody known and headed "ILOVEYOU" is clearly designed to tempt the recipient into opening it
  - Spread by e-mail using MS Outlook address book and also via IRC
  - Hid MP3 and JPEG files
  - 45 million people received it
  - Cost £1.7 billion in damage
  - Perpetrator was a 27 year old computer analyst at a bank in the Philippines
- Code Red (2001)
  - Memory resident (not file resident)
  - Infected 360,000 servers in 14 hours
  - 800,000 infected in total (plus modems)
  - Cost £1.8 billion in downtime & cleanup
- Nimda (2001)
  - Runs in preview mode of MS Internet Explorer e-mail system

AIDS Trojan Horse

- Originator: Dr Joseph Popp on behalf of PC Cyborg Corp. Panama 1989
  - Purported to offer advice on AIDS
  - On installation printed an invoice
  - Also copied other files onto hard disk
  - Licence agreement refers to adversely affecting other programs if fee not paid
  - After a certain number of reboots the hard disk was wiped - even if the software was never run
- Popp charged with blackmail but not extradited from USA on mental grounds

M.O.s of Worms

- Cracking Passwords
  - Dictionary attacks
  - Obvious choice attacks
- Exploiting Distributed Trust
  - This is what allows us to log on to remote machines without identifying ourselves each time
- Monitoring and Intercepting Signals
  - Eavesdropping on broadcast networks
  - Passwords often sent in plaintext
- Impersonating Trusted Parties
  - Manipulating transmission protocols enables a user/machine to pretend that they are another
- Exploiting Bugs and Security Holes
  - Debugging modes
  - Buffer overflows (UNIX favourite)

The Internet Worm

- Originator: Robert Morris
  Cornell University student 1988
  - Targeted at Suns and Decs
  - Utilised
    - Password cracking
    - Distributed trust
    - Debugging mode in sendmail
    - Fingerd stack overflow bug
  - 10% of the 60,000 hosts on DARPA estimated to have been infected
  - Estimated cost of damage £70 million
- Morris was suspended from Cornell, investigated for 6 months by the FBI and sentenced to 400 hours community service and fined £6,000 under the Computer Fraud and Abuse Act 1986

Worm Examples I

- The Blaster Worm (2003)
  - Exploits a buffer overflow in MS Windows NT, 2000, Server and XP
  - Malformed messages sent as Remote Procedure Calls (RPCs) affect the Distributed Component Object Model (DCOM) interface
  - This allows an executable, msblast.exe, to be downloaded and run on the infected PC
  - Blaster tries to connect to “random” (actually random within certain subsets of) IP addresses
  - The malicious code will either contribute to a denial of service attack on the MS Windows Update website or crash the local PC

Worm Examples 2

- The Sasser Worm (2004)
  - Exploits a buffer overflow in MS Windows NT, 2000, Server and XP
  - Can run on, but not infect, MS Windows 95 & 98
  - Similar to Blaster worm but causes the buffer overflow in the Local Security Authority Subsystem Service (LSASS)
  - This allows an executable, avserve2.exe, to be downloaded and run on the infected PC
  - Sasser tries to connect to “random” (actually random within certain subsets of) IP addresses
  - The malicious code causes a significant deterioration in performance of the local PC

Preventative Measures

- Authenticated Execution Management Systems (AEMS)
  - Reverse usual virus black-list idea
  - Employ a white-list of safe executables and only execute white-listed runfiles
- Sandboxes
  - Monitor the behaviour of all programs received from the internet
- Blocks
  - Prevent certain file types from being accessed in specific ways
- Heuristics
  - Initially developed to detect malicious MS Office macros
  - Can be used to analyse any code with a view to blocking suspect commands

Computer Security

- British Standard for Information Security Management Systems
  - Part 1 Code of Practice
  - Part 2 Management Standard
- BS 7799 Certification components
  - Security policy
  - Security organisation
  - Assets classification and control
  - Personnel security
  - Physical and environmental security
  - Computer and network management
  - System access control
  - System development and maintenance
  - Business continuity planning
  - Compliance
- ITSEC
  - DTI scheme for independently assuring security products

Hardware Security

- Physical access
  - Locks
- Electromagnetic emissions
  - Data can be captured from screens, keyboards, disk accesses
  - TEMPEST - Transient Electro-Magnetic Pulse Emission Standard
  - Metallic shielding (Faraday Cages)
  - Tempest fonts (designed to be of acceptable quality to viewers but invisible to eavesdroppers)
- Magnetic resonance
  - Data can be recovered from disks even after over-writing
- Line tapping
  - Wireless LANs
    - “Warchalkers”, ESSIDs, WEP

Software Security

- Verification of identities
- Authentication of messages
- Encryption of data
- Access controls
- Audit trails
- Risk analyses

Security Techniques

- Verification Mechanisms
  - Something possessed
  - Something known
  - Personal characteristics
- Authentication Systems
  - Certificates
  - Digests
  - Digital signatures
- Encryption Algorithms
  - Codes and Ciphers
    - Caesar, Vernam, ...
  - Data Encryption Standard
    - Possibly susceptible to known plaintext attack
  - Public Key Cryptography
    - RSA - Rivest, Shamir and Adleman

Verification I Something Possessed

- Can be lost, stolen or forged!
- Magnetic strip cards
  - 3 tracks of data
  - Anti-forgery techniques
    - Watermark tape
      - Underlying non-erasable pattern
      - Uses an extra track to check this
    - Sandwich tape
      - Two layers of differing intensity
      - Uses high-intensity recording
- Smart cards
  - Greater storage capacity
    - Kbytes as opposed to 250 bytes
  - On-card processing possible
    - Card can be challenged to produce correct response to many requests

Verification II Something Known

- Group Passwords
  - Known to many people
- Non-unique Passwords
  - Confirm a claimed identity
- Unique Passwords
  - Claim an identity
- Variable Passwords
  - Each derived from a previous one
- Single-use Passwords
  - Changed after each access

Password Selection and Reselection

- Free user choice
  - Susceptible to guessing/cracking
    - People do not choose sensible passwords
    - It only takes one poor choice to undermine a system
  - May not be changed very often
    - It only takes one lazy person to undermine a system
- Automatic system allocation
  - Password Generators
    - Unmemorable passwords are bound to be written down
    - Smarter generators try to produce pronounceable words

Verification III Personal Characteristics

- Physiological Biometrics
  - Physical characteristics
    - DNA
    - Face
    - Fingerprint
    - Geometry – Hand
    - Geometry - Two fingers
    - Iris
    - Retina
    - Vascular
- • Behavioural Biometrics
  - Result of an involuntary action
    - Signature
    - Voice
- BioAPI Consortium
  - Open industry standard for biometrics

DNA

- Human genome consists of 3 billion base pairs
  - Adenine-Thymine; Cytosine-Guanine
- Over 99% of our DNA is identical
  - DNA tests use the “junk DNA”
- DNA is not unique
  - 1 in 83 births in the USA is a twin
  - 28% of twins share the same DNA
  - 1 million people in USA are non-unique
- DNA tests consist of
  - Cutting a DNA sample into different sized fragments with an enzyme
  - Placing the fragments on a gel and sorting them by size in an electric field
  - Treating with a probe which adheres to unique patterns of DNA and creates a black line where it “sticks”

Face Recognition

- Two types of system
- Facial Metrics
  - Measure specific features
    - Distance between inside corners of eye
    - Distance between outside corners of eyes and mouth
  - Store these measures for comparison
- Eigenfaces
  - 150 eigenfaces (stereotypes)
  - Score a presented face with a “degree of fit” against each of these 150
  - The top 40 eigenfaces (the 40 with the highest scores) can reproduce a face with 99% accuracy

Fingerprints

- Not even identical twins have the same fingerprints
- Computer checking does not use the loops, whorls, etc. that we do
  - Minutiae
    - Where a ridge starts, stops or forks
    - (x,y) position and direction recorded
    - 90 minutiae obtained from one print
  - AFIS
    - Automated Fingerprint Identification Systems
    - 10 digits => 900 minutiae per person
  - Matcher
    - Does the comparisons
    - Can process 5,000 - 6,000 people/sec
    - Parallel processing also used (and scales really well of course)

Geometry

- Geometric techniques produce small data sets and do not discriminate well
- Geometry can be ascertained in two ways -
  - Mechanical
  - Edge detection from an image
- Hand Geometry
  - Estimates of key measurements are made
    - Finger lengths
    - Thumb widths
- Two Finger Geometry
  - A reduced form of Hand Geometry

Iris Patterns

- Iris scanning seems to be the most robust and most accurate biometric discovered to date
- Standard video cameras are sufficient to capture the images
- The probability of two irises having the same biometric value is 1 in 10^{78}
  - Even identical twins have different patterns
  - Are your eyes both the same?
- Just 256 bytes per person
- It is claimed that BT has a scanner that can capture the iris print of the driver of a car moving at 50mph!?

Retinal Patterns

- Blood vessel patterns in the retina are unique
- User looks through an aperture and aligns eye with the aid of target circles which should be made to appear concentric
- Infra-red light illuminates the retina
- This enhances the image of the blood vessels
- Camera captures the image
- Comparison can then be performed against previously captured images

Vascular Patterns

- Infra-red light used to illuminate blood vessels (cf retinal scans)
- Camera used to capture image
- Can be used on readily accessible parts of the body
  - Face
  - Back of hand
  - Wrist

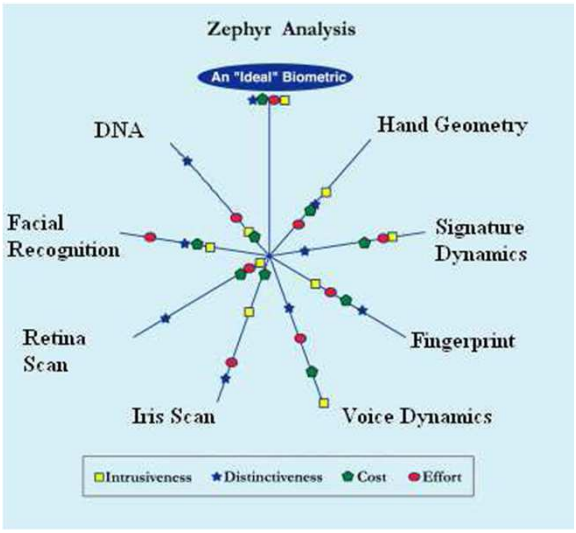
Signature Recognition

- Best systems do not treat this as a pattern recognition task because signature repeatability is poor
- The dynamics of the pen motions are the key properties used
  - Accelerations
  - Directions
  - Pressures
  - Stroke lengths
- Capturing these features is not easy and consistency is difficult to achieve

Voice Recognition

- A pattern recognition task
  - A set phrase is used to create a template
  - The phrase needs to be repeated several times during the creation of the template
- Subsequent entry of the phrase can then be compared against a number of templates
- This technique attempts to be invariant to physical characteristics of a voice and can become dangerously dependent on the behavioural characteristics of speech

Comparison of Biometric Technology I



Comparison if Biometric Technology II

Biometric	Matching		Variation		Max Samples Per Person	Sensor Cost	Sensor Size
	1 to 1	1 to M	Lifetime	Day to Day			
Fingerprint	√	√	None	Little	10	$10\text{-}10^{-2}$	Very Small
Iris Scan	√	√	None	Very Little	2	$10^{-2}\text{-}10^{-3}$	Med
Hand Geometry	√	X	Much	Very Little	2	10^{2}	Med
Facial Recognition	√	X	Much	Med	1	10^{2}	Small
Voice Dynamics	√	X	Much	Med	1	$0\text{-}10^{2}$	Very Small
DNA	√	X	None	None	1	N/A	N/A
Signature Dynamics	√	X	Much	Med	1	10^{2}	Med

Comparison if Biometric Technology III

Biometric	FAR (%)	FRR (%)	Time (secs)	Cost (£)	Size (bytes)
Fingerprint	0.001	2.0-3.0	<4	<100	200-512
Iris Scan	0.00008	0.1-0.2	5	21000	512
Hand Geometry	0.01	4.0	<5	800-1200	9
Facial Recognition	<1.0	10.0	12		88-1024
Voice Dynamics	8	<1.0	5	1000	1-2K
DNA	No Data	No Data	12 hrs	No Data	No Data
Signature Dynamics	<1.0	<1.0	5	1000	100

Authentication I Certificates

- Web sites can present digital certificates to browsers
- The certificate is proof of identity of the site
- It will have been issued to the site by a Certificate Authority (E.g. RSA, Verisign)
- Most browsers are pre-configured to accept certificates issued by the major Certificate Authorities
- If the certificate being offered has not been issued by a known Certificate Authority the user is given the option of accepting it anyway - after checking it!

Authentication II Digests

- Digests summarise a message in a succinct form
  - They range from simple Check Sums through to Authenticators based on cryptographic Hash Functions
- Cyclic Redundancy Check (CRC)
  - Simply an error check mechanism
  - Blocks of data are divided by a pre-selected polynomial; remainders used as check fields
- Decimal Shift and Add (DSA)
  - Repeated shifting and adding of blocks using two secret keys (of 10 decimal digits each)
- Message Authenticator Algorithm (MAA)
  - Binary version of DSA developed at NPL
  - Keys are 32 bit binary numbers
  - ISO approved under the name MAA

Authentication II Digital Signatures

- Digital signatures provide a recipient of a message with proof of the authenticity of the sender
- Public key cryptography is used
- A private key is used to encrypt a compressed string derived from the message and the result is the digital signature (cf hash functions)
- The digital signature is sent with the message
- The public key can be used by anybody to decrypt the digital signature and thus verify the authenticity of the sender in a nonrepudiatable form

Encryption I Codes and Ciphers

- Plaintext
  - The unencoded text which is to be transformed for protection
- Ciphertext
  - The encoded text which needs decoding before it can be read
- Codes
  - Transform whole words or phrases from plaintext to ciphertext
- Ciphers
  - Transform single characters or groups of characters from plaintext to ciphertext
  - Block Ciphers
    - Transform single-sized blocks of characters from plaintext to ciphertext

Encryption II Public Key Cryptography

- In the following –
  E() = Encryption Algorithm
  D() = Decryption Algorithm
  P = Plaintext
  C = Ciphertext
  ki = Keys
- Basic Cryptography
  E(P) => C $E^{-1}(C) => P$
  E() must be kept secret
- Private Key Cryptography (DES)
  E(P,k) => C $E^{-1}(C,k) => P$
  E() can be published but k must be secret
- Public Key Cryptography (RSA)
  E(P,k1) => C D(C,k2) => P
  E(), D() and k1can be published
  k2 must be kept secret [D() =/= $E^{-1}()$]