

The nature of the beast

- Win Schwartz, Information Warfare, Thunder's Mouth Press 1996
 - "Your company will become a designated target of information warfare. If not yesterday or today then definitely tomorrow."

- Sunday Times, Computer Security, 1991
 - "95% of organisations that loose their corporate data fail within 18 months"

An introduction to Network security

- we will cover
 - the CIA security model
 - the DDPRR (detect, deter, protect, react, and recover) security model

- examine
 - current state of legislation with respect to
 - security
 - encryption

The nature of the beast

| Source of threat | Validated existence | Likely by 2005 | Beyond 2005 |
|----------------------|---------------------|----------------|-------------|
| Criminal hacker | Widespread | | |
| Organised crime | Limited | Widespread | |
| Political dissidents | Widespread | | |
| Terrorists | Limited | Widespread | |
| Spies | Limited | | Widespread |
| Tactical disruption | | | Widespread |
| Strategic disruption | | | Limited |

Why is security important?

- for businesses:
 - IT is core to virtually all business processes within most organisations
 - many organisations could go out of business if IT was disrupted in a serious way

- legally, the Data Protection Act 1988 says:
 - "Appropriate security measures shall be taken against unauthorised access to, or alteration, disclosure or destruction of, personal data and against accidental loss or destruction or personal data"

Three concepts of CIA security model

- confidentiality
 - information must not be disclosed to any unauthorised person

- integrity
 - system must not corrupt data
 - system must disallow unauthorised, malicious or accidental data changes
 - three aspects of integrity
 - authorised actions
 - separation and protection of resources
 - error detection and correction

Security and the IS manager

- what does security mean to the IS manager?
 - understanding how a system can be misused and protect against it

- protect and manage technical and social aspects of a system

Three concepts of CIA security model

- availability
 - presence of objects or service in a usable form
 - capacity to meet service needs
 - adequate timeliness of a service

IS Manager uses

- security management
 - risk, threat and vulnerability assessment
 - BS7799
 - ITSEC (Information Technology Security Evaluation Criteria)
 - Orange Book

- security policies
 - real world security policy
 - security models
 - access control models
 - information flow models

- technical security
 - cryptography, penetration testing, backup of data

Mobile computing

- mobile phones can be scanned
- wireless networks can be scanned by laptops
 - see Pringle amplifier in the news

High profile cracking

- see www.2600.org

Definition of security

- deter
 - to create and implement policies that allow us to generate a feasible and believable deterrence
- detect
 - to create and implement policies that allow us to detect how, when and where intrusion has taken place
- protect
 - to create and implement policies and procedures that allow us to manage people and the IS in an effective manner so as to protect against unauthorised usage

Definition of security

- react
 - to create and implement policies and procedures which define how we react to an intrusion
 - need to ensure that penetration does not happen again
 - vulnerability is eliminated
- recover
 - recover all data and programs from a breach in security

Wide area networks - the early days

- UNIX-UNIX system mail (UUCP); mail trapdoors (1975)
 - UUCP allowed users on one machine to execute commands on another
 - used to transfer email and files automatically between systems
 - early versions of sendmail (an implementation of UUCP) under UNIX had a trapdoor
 - the **debug** option gave you a root shell!

Cracking history

- Trojan horse
 - in 1972 Dan Edwards of the NSA coined this term for a macro utility which had an undocumented side effect that violated security
- trap door
 - during 1973 and 1974 David Stryker, John Shore and Stanley Wilson of Navel research labs USA, subverted the EXEC VIII operating system of a UNIVAC 1108 by using a Trojan horse
 - 1972..1975 as a series of experiments for the US air force, Steven Lipner and Roger Schell used trapdoors and Trojan horses to subvert MULTICS into giving confidential information without leaving a trace

Public key cryptography - the early days

- Public-key cryptography discovered by W. Diffie, M. Hellman, “New directions in cryptography”, IEEE Transactions on Information Theory, Vol. 22(6), 1976
 - provides the mechanism whereby people and commerce to trade via an untrusted Internet
 - D.C. Lynch, L.Lundquist, “Digital money: the new era of Internet commerce”, Wiley, 1996

Wide area networks - the early days

- ARPANET 1969..1989, Internet 1977..present
 - ARPANET was the first WAN, started in 1969 with four nodes and became the model for todays Internet
 - TCP/IP (Transmission control protocol and Internet Protocol) designed in 1977 by Vinson Cerf and Robert Khan
 - ARPANET disbanded in 1989

Cracking - the early years

- Internet worm
 - the first large scale attack against computers on the Internet
 - within hours it had invaded 3000..6000 hosts
 - 5..10% of the Internet at the time
 - it used well known and documented bugs and trapdoors to gain remote access to machines
 - E. Spafford, “Crisis and aftermath”, CACM, 32(6), 1989

Public key cryptography - the early days

- RSA Public-Key Cryptographic system
 - RSA algorithm is the oldest (so far unknown) to be unbroken. It provides:
 - confidentiality and authentication
 - security based on finding some very large prime numbers
 - R. Rivest, A. Shamir, L. Adleman, “A method for Obtaining Digital Signatures and Public-Key Crypto-systems”, CACM, 21(2), 1978

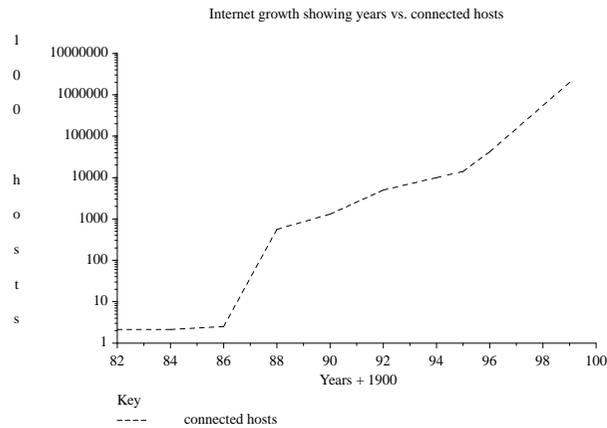
Email privacy - the early years

- PGP and PEM (1989)
 - email is vulnerable to forgery, spoofing, alteration and interception
 - Privacy Enhanced Mail and Pretty Good Privacy provide secrecy and authentication services for email
 - B. Schneiser, “E-Mail security: how to keep your electronic messages private”, Wiley, 1995
- Anonymous Remailers (1990)
 - servers act as mail forwarder, hiding the identity of the sender by substituting a random string for the senders name
 - C. Gulcu, G. Tsudik, “Mixing E-mail with BABEL”, proceedings of the symposium on network and distributed systems security, 1996

Cracking - the early years

- Wiley hacker attack
 - an attacker intruded into computers at Lawrence Berkeley Laboratory, apparently looking for secret information. Clifford Stoll was a system manager at LBL and helped authorities arrest the attacker who was being paid by a foreign government.
 - C. Stoll, “The cuckoo’s egg”, Doubleday, 1989
 - C. Stoll, “Stalking the wily hacker”, CACM, 31(5), 1988

Growth in the Internet



Potted history of cracking

- 1969 John Draper (Cap'n Crunch) starts phreaking
- 1981 Chaos Computer Club (CCC) founded
- Kevin Mitnick first jailed
- 1984 the 2600 magazine founded
- 1985 Phrach e-zine founded
- C. Stoll publishes Cuckoo's egg
 - Doubleday 1989

Packet spoofing and network sniffing - the early days

- Sniffing and spoofing 1993
- Internet protocols were designed on the assumption that no one could access the actual wires and listen observe the packets
 - in the last few years crackers have start to do just that
 - Steve Bellovin, "Security problems in the TCP/IP protocol suite", Computer Communications Review, 19(2), 1989
- methods called sniffing have been used to detect passwords transmitted in cleartext
 - attackers have also started to transmit their own packets containing false information
 - called spoofing

Java security problems

- there are many!
- Java is a language that allows you to write small applications called applets
- an applet can be down-loaded from a remote machine and executed on your local machine!
- can the user trust an applet?
- G. McGraw & E.W. Felton, Java Security, Wiley, 1997
- Scott Oaks, Java Security, O'Reilly, 1996

Potted history of cracking

- 2000 CD Universe broken into a 30,000 credit card numbers stolen

Potted history of cracking

- 1988 Robert T. Morris releases Internet Worm
- 1989 CERT founded (<http://www.cert.org>)

Definition of Threat

- a possible danger to the system
 - Michael E. Kabay, Enterprise Security: protecting information asserts, McGraw-Hill, 1996
- a circumstance that has the potential to cause loss or harm
 - Charles P. Pfleeger, Security in Computing, Addison Wesley, 1997
- a circumstance or event that could cause harm by violating security
 - Rita C. Summers, Secure Computing: Threats and safeguards, McGraw-Hill, 1997

Potted history of cracking

- 1990 Computer Misuse Act (CMA) becomes law in UK
- 1991 Kevin Lee Poulsen (“Dark Dante”) arrested
- 1993 Bedworth acquitted in first major Computer Misuse Act Trial
- 1994 Citibank hacked Vladimir Levin
- 1995 “Ardita”, son of Argentinian General hacks NASA
- 1998 East Timorese Internet Domain Name Removed (.tp)
- 1998 cracker sentenced to death by a court in eastern China

Types of computer misuse

| | Mode | Example |
|----|----------------------|---|
| | Pest programs | |
| 12 | Trojan horse attacks | Implanting malicious code, sending letter bombs |
| 13 | Logic bombs | Setting up time or event bombs (a form of Trojan horse) |
| 14 | Malevolent worms | acquiring distributed resources (rabbits and bacteria) |
| 15 | Virus attacks | attaching to programs and replicating |

Types of computer misuse

| | Mode | Example |
|---|------------------------|--|
| | External misuse | |
| 1 | Visual Spying | observation of keystrokes or screen |
| 2 | Misrepresentation | deceiving operators and users |
| | Hardware misuse | |
| 3 | Logical scavaging | Examining discarded/stolen media |
| 4 | Eavesdropping | Intercepting electronic or other data |
| 5 | Interference | Jamming, electronic or otherwise |
| 6 | Physical attack | Damaging or modifying equipment or power |
| 7 | Physical removal | Removing equipment and storage media |

Types of computer misuse

| | Mode | Example |
|----|----------------------|--|
| | Masquerading | |
| 8 | Impersonation | using false identities external to the computer system |
| 9 | Piggybacking attacks | usurping communication lines |
| 10 | Spoofing attacks | Using playback, creating bogus nodes and systems |
| 11 | Network weaving | Masking physical whereabouts or routing |

Types of computer misuse

| | Mode | Example |
|----|---------------------------|--|
| | Bypasses | |
| 16 | Trapdoor Impersonation | utilising existing flaws in the system |
| 17 | Authorisation attacks | Password cracking etc |
| | Active misuse | |
| 18 | Basic active attack | creating, modifying, entering false or misleading data |
| 19 | Incremental attack | Using salami attacks |

Types of computer misuse

| | Mode | Example |
|----|-----------------------------|--|
| 20 | Denial of service | Perpetrating saturation attacks |
| | Passive misuse | |
| 21 | Browsing | making random and selective searches |
| 22 | Interference, aggression | Exploiting database inferences and traffic analysis |
| 23 | Covert channels | Exploiting covert channels and other data leakage |