Information Security Threats

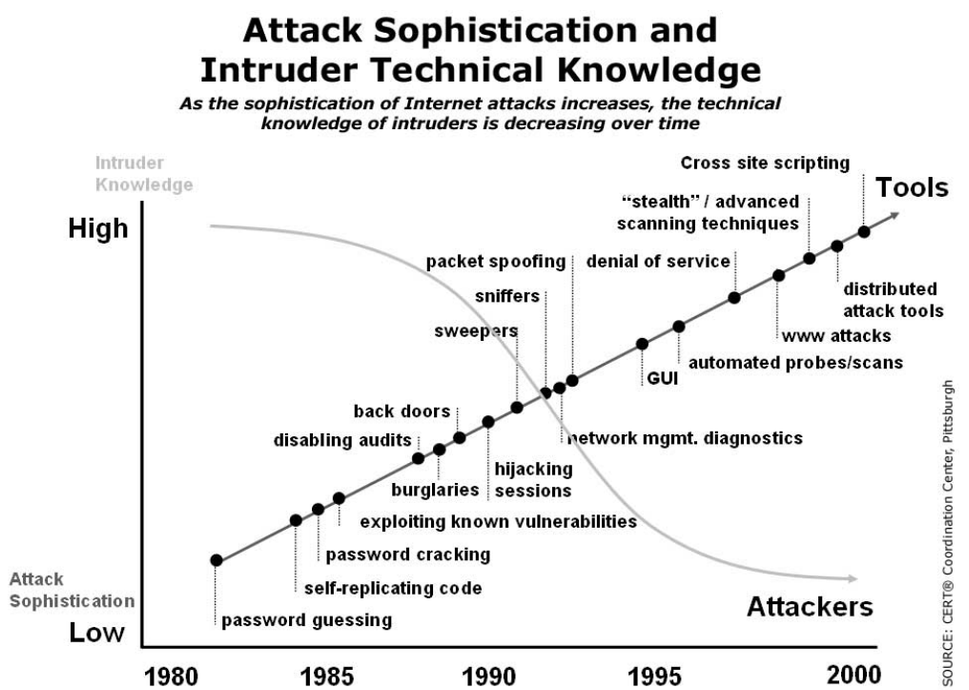
Rana Tassabehji
University of Bradford, UK

INFORMATION SECURITY: EVOLUTION TO PROMINENCE

Information security is an old concept where people, businesses, politicians, military leaders, and others have been trying to protect "sensitive" information from unauthorised or accidental loss, destruction, disclosure, modification, misuse, or access. Since antiquity, information security has been a decisive factor in a large number of military and other campaigns (Wolfram 2002)—one of the most notable being the breaking of the German Enigma code in the Second World War.

With the invention of computers, information has moved from a physical paper-based format to an electronic bit-based format. In the early days, mainframe infrastructures were based on a single sequential execution of programmes with no sharing of resources such as databases and where information could be relatively easily secured with a password and locked doors (Solms 1998). The development and widespread implementation of multi-processor personal computers and networks to store and transmit information, and the advent of the Internet, has moved us into an information age where the source of wealth creation is changing from atoms (physical goods), to bits (digital goods and services) (Negroponte 1995). Information is now a valuable asset and consequently, information security is increasingly under threat as vulnerabilities in systems are being exploited for economic and other gain. The CERT Co-ordination Center at Carnegie Mellon

Figure 1. Relationship between attack sophistication and knowledge required by attackers (Source: http://www.cert.org/archive/ppt/crime-legislation.ppt)



University has charted the increase in sophistication of attacks as knowledge required decreases since technical attack tools are more readily available and indiscriminately accessible (Figure 1). Even novices can launch the most sophisticated attacks at the click of a mouse button (Anthes 2003).

MEASURING INFORMATION SECURITY THREATS

It is impossible to get accurate figures for the number and cost of information security breaches, mainly because organisations are either not aware that the breach has occurred, or are reluctant to publicise it, for fear of ruining their reputation or destroying the trust of their stakeholders. However, in one instance the impact of malicious software in the form of worm/virus attacks on the Internet was estimated to have caused $32.8 billion in economic damages for August 2003 (Berghel 2003).

The types of information security threats come from a number of sources, which can be broadly divided into two main categories the technical and non-technical which will be examined in more detail in the next section.

TECHNICAL INFORMATION SECURITY THREATS

Information is increasingly transmitted and stored on interconnected and networked infrastructures, so the threats to information security can come from a variety of technical sources, including:

- **Intrusion attacks:** where hackers or unauthorised intruders gain access to stored information to either steal or vandalise it (such as defacing a Web site).
- **Probing or scanning:** where an automated tool is used to find and exploit vulnerabilities to gain access to an information system as a prelude to theft or modification of information. Increasingly home users are unknowing victims of scans that detect unprotected ports allowing attackers to gain access to their information or take control of their computer to launch other types of attack.
- **Automated eavesdropping:** uses sniffer programmes that monitor and analyse information in transit. They capture information such as usernames, passwords, or other text being transmitted over a network, which might not always be encrypted, for instance e-mail.
- **Automated password attacks:** the most common and successful kind of threat to information security. They exploit people's poor password practices (see Table 1) and their tendency to rely on passwords that are easy to remember and have some personal relevance. Once attackers have a user's password, they can legitimately access all their privileges and information. Some techniques used include:
  - **Brute-force attacks:** where programmed scripts run through every single combination of characters until the password is found. This takes time and is the slowest method since for an eight-character lower case alphabet there are 200 billion combinations, but powerful processors can reduce the time considerably. It is most effective for short and simple passwords.
  - **Dictionary attacks:** where programmed scripts run through every word in one or more dictionaries that include different languages, common names, and terms from popular culture such as films, music, or sport until the password is found.
  - **Password cracking:** a more advanced method where attackers launch a brute-force dictionary attack to find out encrypted passwords. Common words (found in dictionaries) are encrypted and compared to stored encrypted passwords until a match is found. The success of this attack depends upon the completeness of the dictionary of encrypted passwords and the processor power of the machines being used.
- **Spoofing:** where a person or machine impersonates another to gain access to a resource, making it easy for an attacker to modify original information or change its destination. This technique is effective in disguising an attacker's identity, preventing victims from identifying the culprits who breach their systems. A more recent trend is *"phishing",* where the mass distribution of "spoofed" e-mail messages with