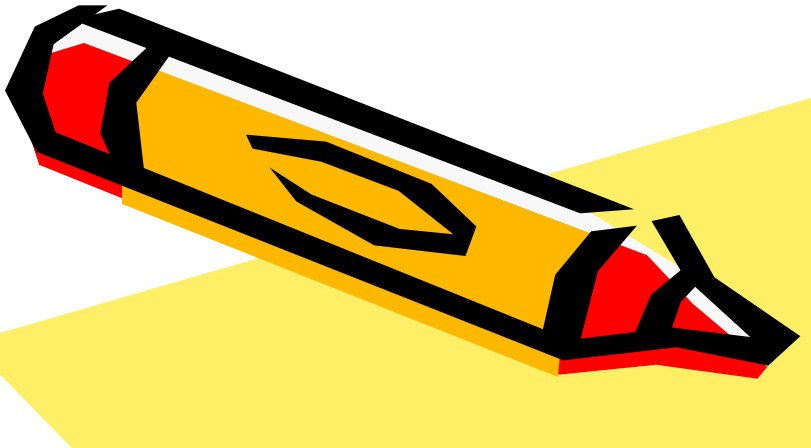
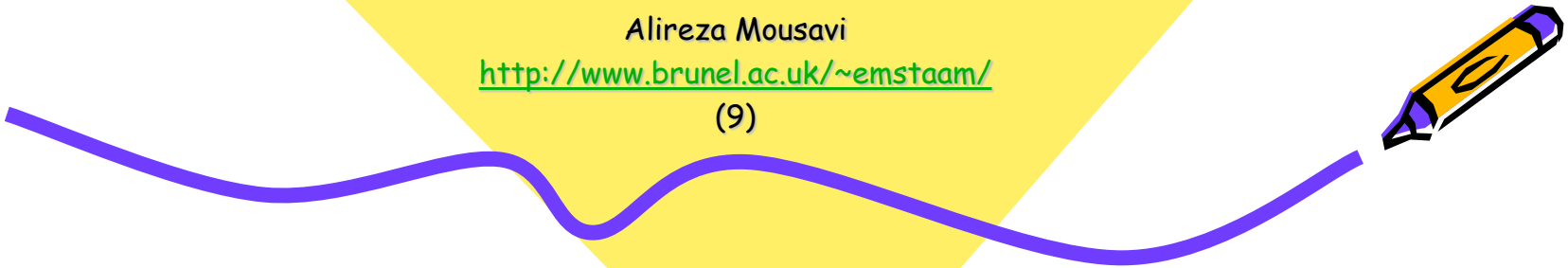


Electronic Business Systems

School of Engineering & Design

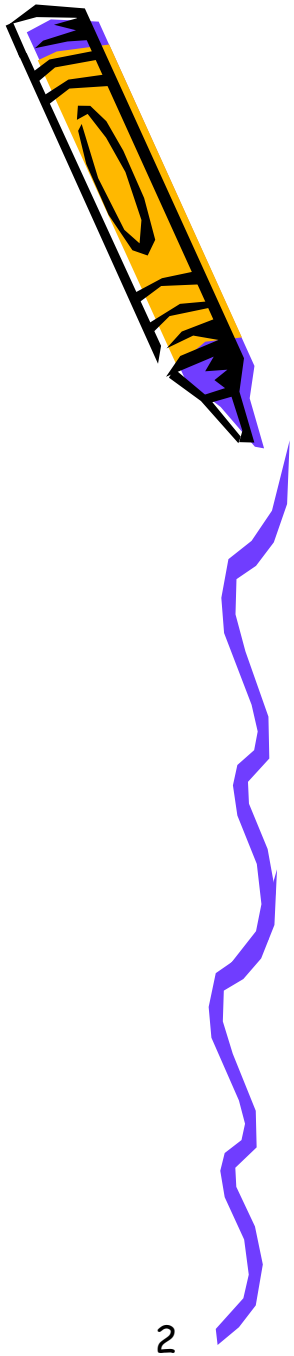
Alireza Mousavi
http://www.brunel.ac.uk/~emstaam/
(9)



E-Commerce Security

Chapter 7 topics:

- Secure electronic commerce
- Encryption and password control
- Single-key crypto systems
- Public key cryptosystems and digital signatures
- Key certificate
- Certifying authorities
- Firewalls
- Filters
- Attack classifications

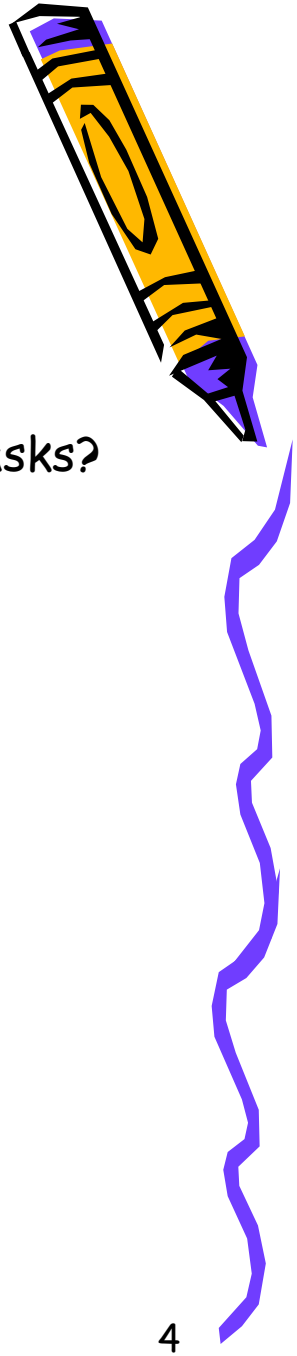


Safe & Secure communications

Ensuring a safe and secure communication passage from the sender to the receiver has been one of the most challenging aspects of communication systems.

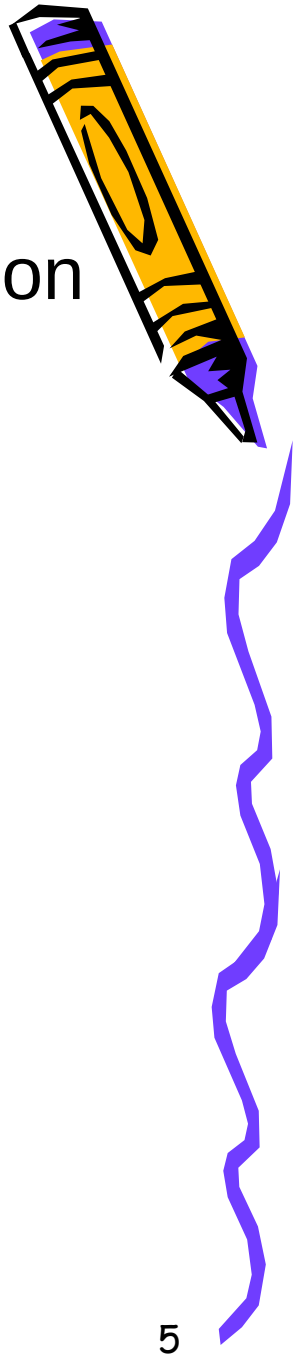
The science of encryption is therefore being constantly improved to eliminate or minimise the possible intrusion into communications systems.

Issues to be addressed



- Who can access the information?
- Is the person accessing the file authorised to perform any tasks?
- Is the users personal information protected?
- Is the information accessed valid?

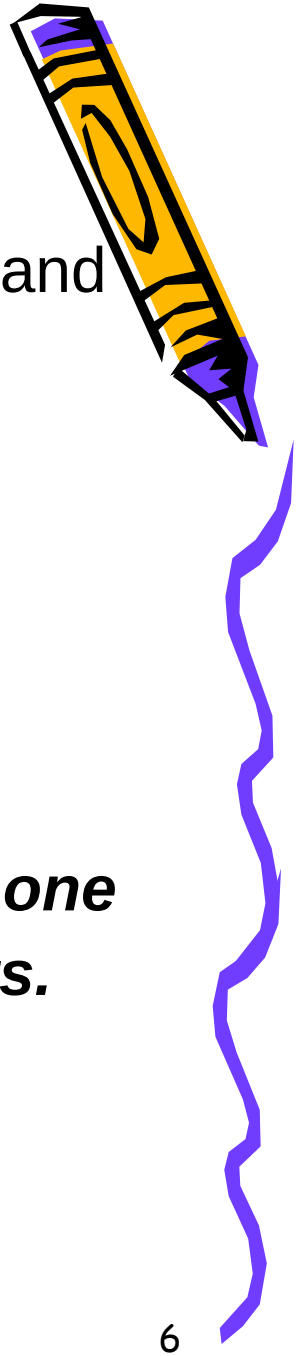
Intrusion



Individuals try to hack into restricted information zones:

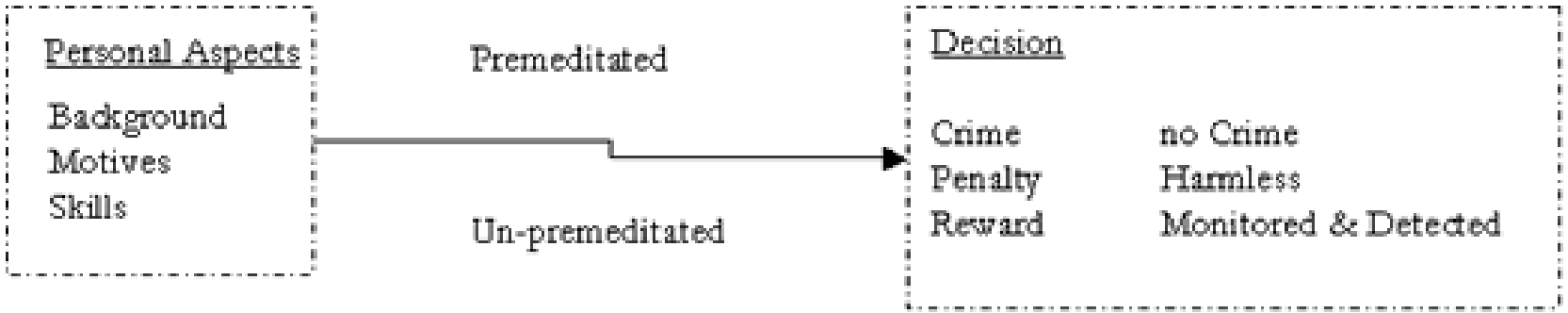
- Reasons:
  - Curiosity
  - Challenge
  - Criminal intent:
    - Sabotage commercial activities
    - Banking systems
    - Defence systems
    - Attack databases for secret information on others

Secure Electronic Commerce



- *Electronic Transaction:* Authentication of source and destination of payments
- *Identification of individuals:*
  - Username and password
  - Entry permits
  - Encryption keys …
- *Privacy:* Security over information that are the property of individuals. ***UK Data Act protection one of the most complete and comprehensive acts.***
- *Control Strategies:*
  - Sequential control
  - Layered control

Sequential strategy for network crime analysis



Encryption & Password control

- Encryption and password controls scramble information while they are being transmitted through the communication mediums.

- Unencrypted electronic transactions are relatively easy to intercept – Dangerous for companies

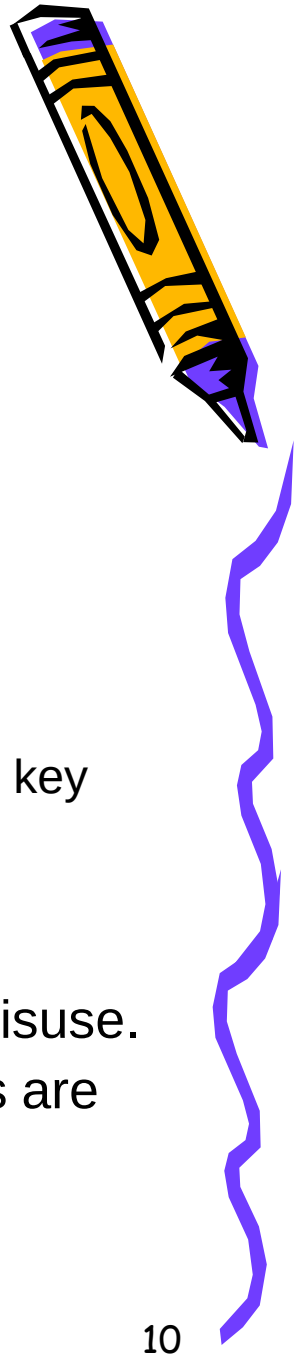
- Because of the vulnerability of electronic transactions, encryption has become an important control over networked computer system.

Crypto systems (1)

- **Single-key crypto systems:**
  - One-to-one system
  - Simple set of principles in their design
  - Encrypt(encipher) the message
  - Construct a key – only the key holder can decipher
  - Key message should be transmitted via a secure channel

- **Public key crypto systems and digital signatures**
  - Improved security
  - Two related & complementary keys (public & private – each unlock the other)
  - Public & Private keys are generated simultaneously – mathematical algorithm
  - Public keys are known to everyone – Private key are secret
  - On the user side the private key unlocks the public key

Crypto systems (2)



- **Key certificates**
  - Kept in individual "key certificates"
  - Key certificates include:
    - Person's username
    - Time stamp (date Public & Private key was generated)
    - Content of the public key
    - Private-key certificates contain the corresponding private key contents
- **Certifying authorities**

Public keys due to the publicity are prone to tampering and misuse. It is therefore necessary to make sure that only certified users are allowed to use the system.

Other security techniques

- **Automatic disconnection:**
  - time limitations or
  - number of trials to enter the network
  - Once the time or number of legitimate attempts expires the computer automatically disconnects or cancels the transactions or entry permit
- **Firewalls**
  - Filters between local network and Internet – Two types
    1. Packet-Level Filters: TCP/IP level – network address, ports, sender, and receiver ensuring traffic is authorised
    2. Application-Level Gateway: frequently checks the network by acting as surrogate for all the machines on the network

Attack Classification (Whitman et al)

"Attack is a deliberate act that exploits ICT vulnerability"

(Whitman et al)

- Malicious Code: execution of viruses, worms, Trojan horses, Spyware, and specific codes with the intent to sabotage or steal information.
- Hoaxes: Masked viruses under seemingly harmless messages and newsletters.
- Back Door: Using specific access mechanisms to enter networks and their sources. Mainly exploiting faults in system's administration setups.
- Password Crack: using tricks or algorithms to guess passwords. Normally the attack concentrates on Security Account Manger (SAM) data files.

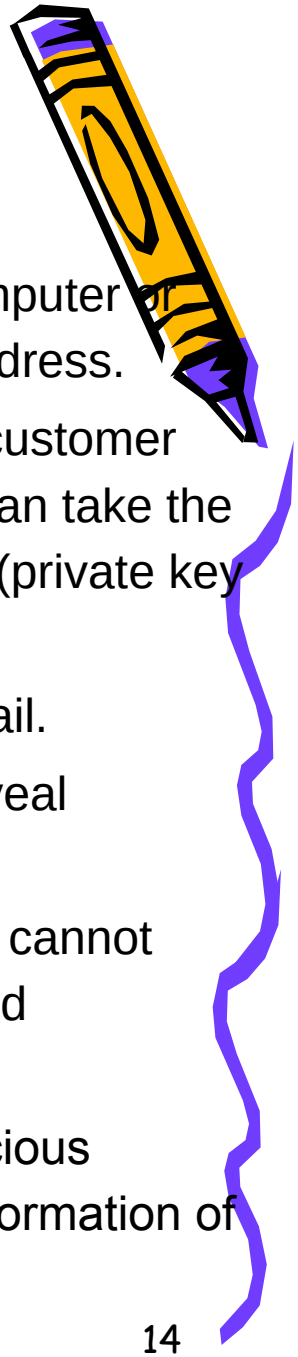
Attack Classification (2)

- Brute Force: Password guessing by narrowing down the search to a small number of accounts. Dangerous for low security systems.

- Dictionary: A form of Brute attack again by narrowing down the search to specific accounts and comparing commonly used passwords (dictionary)

- Denial of Service (DoS) and Distributed Denial of Service (DDoS): DoS case, the attacker overwhelms the system by large number of access request causing the system to slow down or crash. DDoS attacks are very difficult to handle since they are coordinated stream of simultaneous access request from different locations (zombies) causing the target system to crash.

Attack Classification (3)



- Spoofing: The spoofer tries to gain unauthorised access to a computer or network using an IP address indicating that the IP is a trusted address.
- TCP hijacking: the hacker comes between the company and its customer and controls the communication between them. They therefore can take the key information and fool the customer to reveal their information (private key stealing).
- Spam: Swarming email systems with unsolicited commercial email.
- Social Engineering: The attacker grooms and tricks people to reveal sensitive information by pretending they are someone else.
- Buffer overflow: Overflow of data sent to a buffer that the system cannot cope with. This results to mismatch between processing rates and communication rates resulting in collapse.
- Timing Attack: Exploits the web browser's cache. It creates malicious cookies stored on client's side. It allows the attacker to collect information of password protected sites

Also see

1. Whiteman M. E. and Mattord, H. J. (2003) Principals of Information Security, *THOMSON Course Technology.*
2. Rowley, J. (2002) E-Business principals and practice. *Palgrave.*