SLIIT
Discover Your Future

Lecture 10
Internet Security

IT1100 – Internet and Web Technologies

Content

- How safe is the Internet?
- Internet security threats
- Internet security services
- Internet security
- E-life and security

HOW SAFE IS THE INTERENT?

How safe is the internet

eBay e-commerce platform under attack

Share this content:

A new credit card-stealing attack is underway on the eBay Magento e-commerce platform, which is used by more than 240,000 businesses worldwide.

The hack has been discovered by US security firm Sucuri, which says it's part of a wave of recent attacks in the wild by the same unnamed hacker group, and predict "we're in for a new trend of Magento-based credit card stealers".

Sucuri senior malware researcher Peter Gramantik said in a 23 June blog that the latest attack exploits a previously unknown vulnerability in the Magento core or one of its widely used modules/extensions.

"Using this vector, the attacker is able to inject malicious code into the Magento core file," he said.

This enables the hacker to intercept 'POST' request from the infected website, giving them all the credit card billing details being sent to the site server.

How safe is the internet

Credit card alert as hackers target 77 million PlayStation users

By SEAN POULTER FOR THE DAILY MAIL
UPDATED: 08:06 GMT, 28 April 2011

Share

- **Personal data of millions of users worldwide stolen**
- **Access to PlayStation Network was suspended a week ago, but Sony only revealed details of data theft today**
- **Fury as Sony announces breach in blog post just hours after launching tablets at high-profile event**

Millions of people may be issued with new credit cards over fears their banking details have been stolen by thieves hacking into the Sony PlayStation Network.

The personal information of 77million people around the world is thought to have been compromised.

Some three million Britons – who use the Sony system to play computer games against people in the UK and other countries – have been caught up in the biggest criminal hack on record.

How safe is the internet
And more recently…

'Panama papers' came from email server hack at Mossack Fonseca

Money-shuttling firm lost 2.6 TB of data and didn't even notice

5 Apr 2016 at 05:38, Richard Chirgwin 795

The staggering, Wikileaks-beating "Panama Papers" data exfiltration has been attributed to the breach of an email server last year.

The leak of documents from Panama-based, internationally-franchised firm Mossack Fonseca appears to confirm what has long been suspected but rarely proven: well-heeled politicians, businesses, investors, and criminals use haven-registered businesses to hide their wealth from the public and from taxmen.

Bloomberg says co-founder Ramon Fonseca told Panama's Channel 2 the leaked documents are authentic and were "obtained illegally by hackers".

According to *The Spanish*, the whistleblower (here in Spanish) accessed the vast trove of documents by breaching Mossack Fonseca's email server, with the company sending a message to clients saying it's investigating how the breach happened, and explaining that it's taking "all necessary steps to prevent it happening again".

The company added that it's engaged security consultants to close the horse-long-gone stable door.

How safe is the internet

A growing threat, Ransomware! ☹

How safe is the internet
What & Why Internet Security ?

- Process of creating rules and actions to protect against attacks over the Internet.

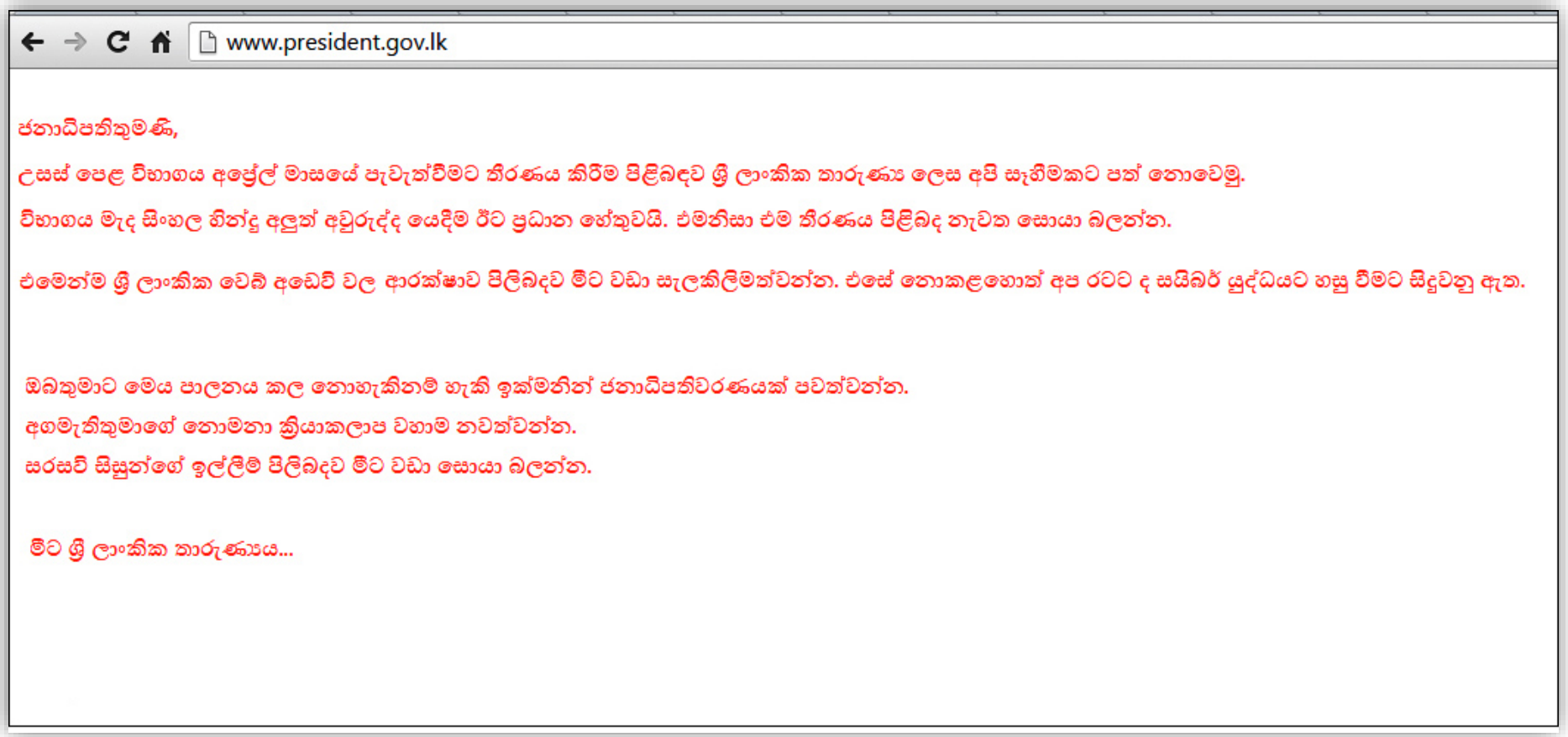
- Importance of Internet Security:
  - Privacy & Confidentiality
  - Prevents Data & Identity theft
  - Maintains productivity
  - Foils cyber-terrorism
  - Avoids legal consequences of not securing information
  - And many more

Internet Security Threats

- Threats are numerous
- Websites are particularly vulnerable
- Political activism is one motivation for Website defacement (Political Espionage)
- Theft of proprietary information is a major concern (Cooperate Espionage)
- Some do it for fun, or just to prove a point!

Internet Security Threats

Internet Security Threats



Internet Security Threats
Types of Attacks

Denial of Service Attacks

- An explicit attempt by attackers to prevent legitimate users of a service from using that service

- Flooding Attacks
  - Point-to-point attacks: TCP/UDP/ICMP flooding
  - SYN Flood, Ping of Death,
  - Smurf attacks

Distributed Denial of Service Attacks

- A DoS attack carried out using a large number of compromised systems improving its potency and reducing traceability of the originator.

Internet Security Threats
Types of Attacks

DNS Attacks

- An explicit attempt by attackers to modify a legitimate DNS service.

Active Code Attacks

- **Java Applets**
  - Java: developed by Sun Microsystems
  - Java programme runs in browser “sandbox”
  - Sandbox might have vulnerabilities
  - Problem: hostile applets

- **ActiveX**
  - Microsoft’s answer to Java technology
  - Web browser can download any type of document
  - Internet Explorer invokes handler (example: Word)
  - Problem: browser loses control

Internet Security Threats
Types of Attacks

SQL injection

- Attacker execute malicious SQL statements
- Any website or web application that use an SQL-based database could be vulnerable
- Attacker can use this to:
  - Bypass authentication and authorization mechanisms
  - Retrieve the contents of an entire database
  - Add, modify and delete records in a database
- Protection - Need to sanitize user input data

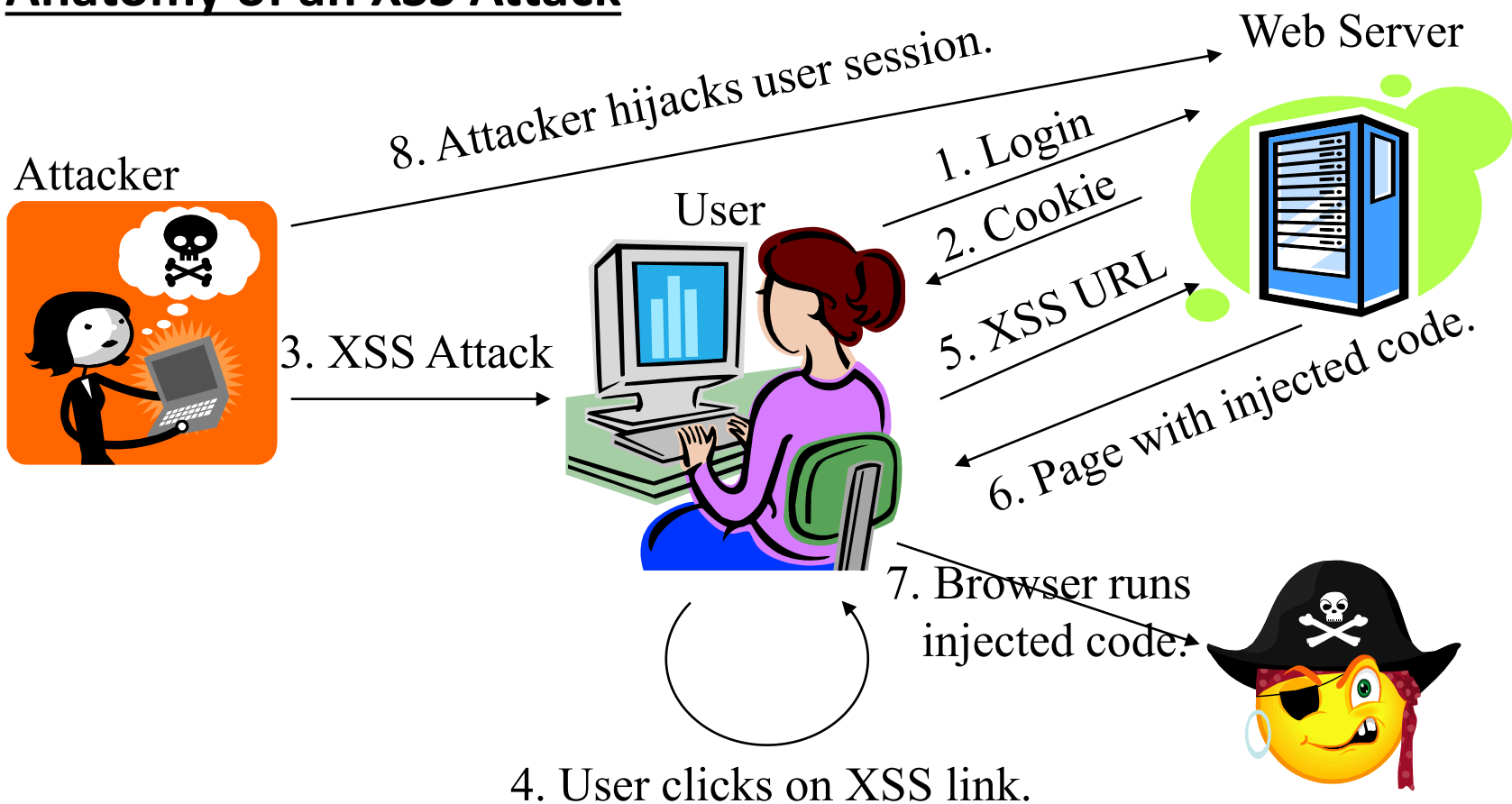
Internet Security Threats
Types of Attacks

Cross Site Scripting (XSS)

- Cross Site Scripting (CSS for short, but sometimes abbreviated as XSS) is one of the most common application level attacks that hackers use to sneak into web applications today.
- CSS attack involves three parties – the attacker, a client and the web site.
- The goal of the CSS attack is to steal the client cookies, or any other sensitive information, which can identify the client with the web site. With the token of the legitimate user at hand, the attacker can proceed to act as the user in his/her interaction with the site – specifically, impersonate the user.

Internet Security Threats
Types of Attacks

Anatomy of an XSS Attack



Internet Security Services

1. **Confidentiality**
2. **Integrity**
3. **Availability**

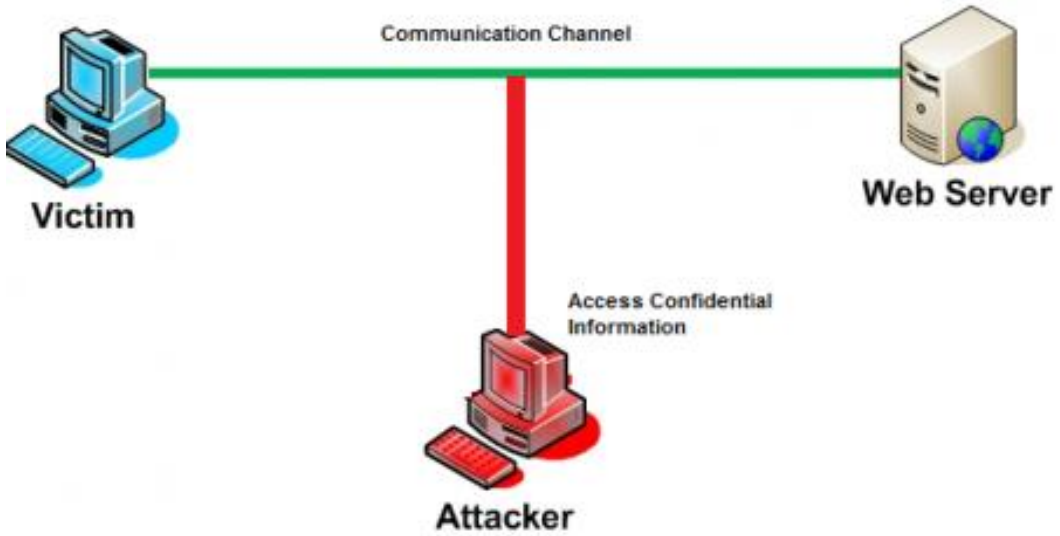
- Non-Repudiation
- Authentication
- Authorization (Access Control)

[Can be described as part of Integrity]

Internet Security Services

Confidentiality

- Can be defined as the **'Secrecy'** of the message
- Also known as **'Privacy'**

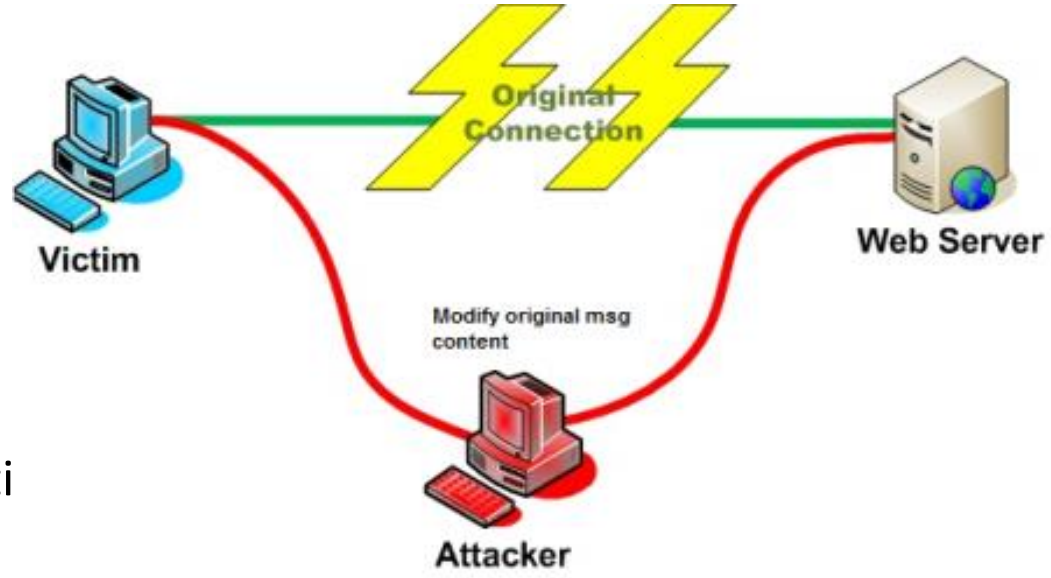


- Note: attacker doesn't change any information (Passive Intruder)

Internet Security Services

Integrity

- Can be defined as the **'Security'** of the message
- Ensure that the message will be delivered to the receiver **without being modified** in the middle by the intruder.



- Note: attacker acti

(Active Intruder)

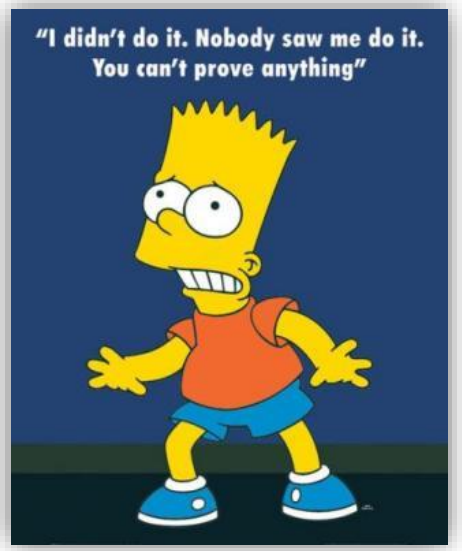
Availability

- Assuring information and communications services will be ready for use when expected.
- Information must be kept available to **authorized** persons when they need it.

Internet Security Services

Authentication

- Can be called as source verification
- Receiver can identify the actual sender
- Can be defined as a part of Origin Integrity
- Intruder is active and a malicious **impersonator**



Non – Repudiation

- Sender cannot deny that he/she sent the message
- Can be defined as a part of Origin Integrity

Authorization (Access Control)

- Access to resources should be in a controlled way.
- Intruders will be active. And try to access the resources which are not allowed.

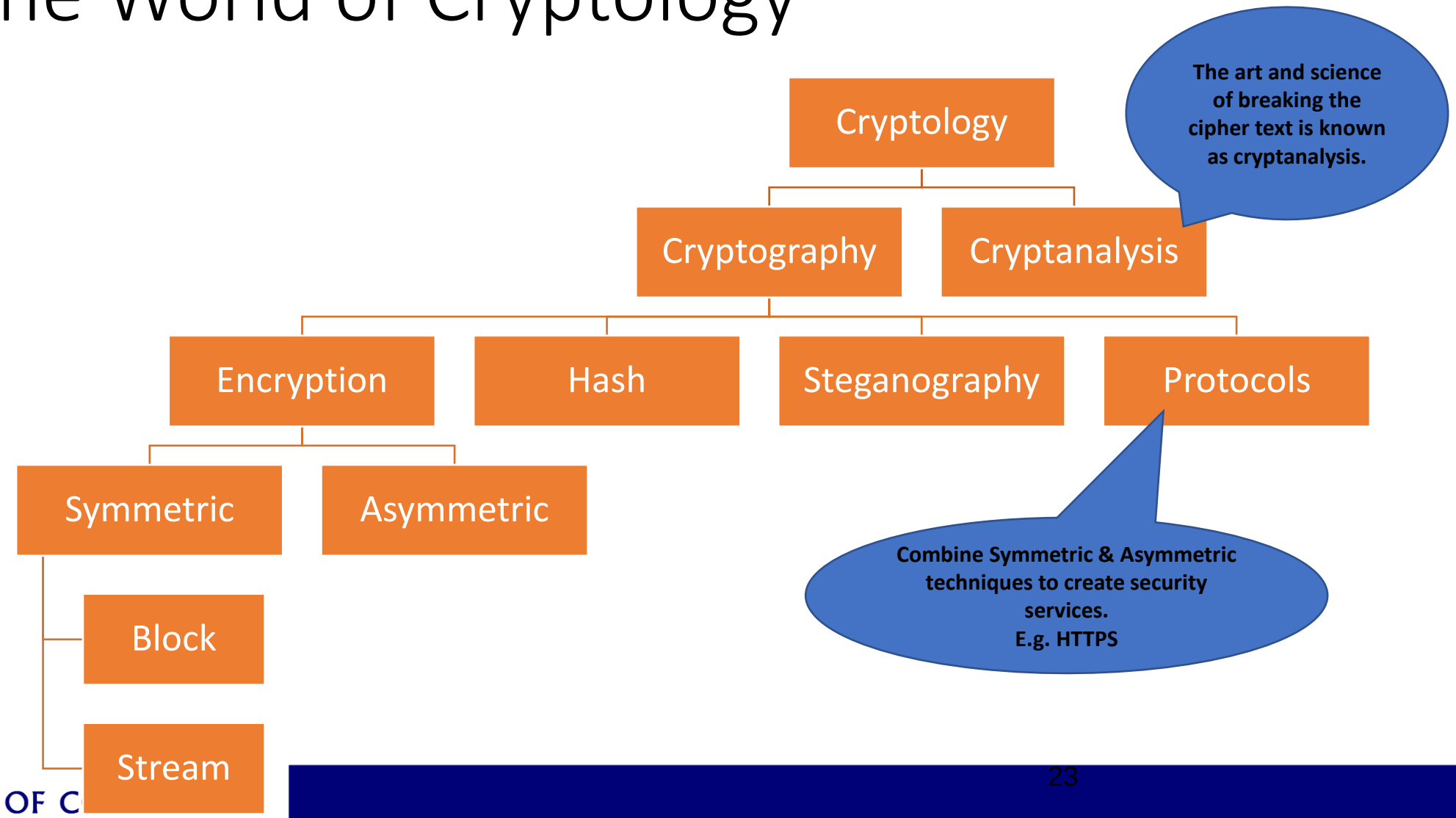
Internet Security

- **Why is it so difficult to achieve Internet Security?**
  - Internet was created as a product of research
  - Security was not a prime concern those days
  - Inherent protocols does not have security features
    - HTTP - Messages sent in plain-text ☹
    - Email - No authentication of the sender
    - FTP - Basic file transfer protocol has no encryption
  - Security had to be introduced as add-ons
    - New protocols had to be introduced

      (HTTPS, SMTP, SFTP etc.)
    - But cannot stop users from using old protocols! ☹
  - All these new protocols rely on **CRYPTOGRAPHY!**

Internet Security

The World of Cryptology

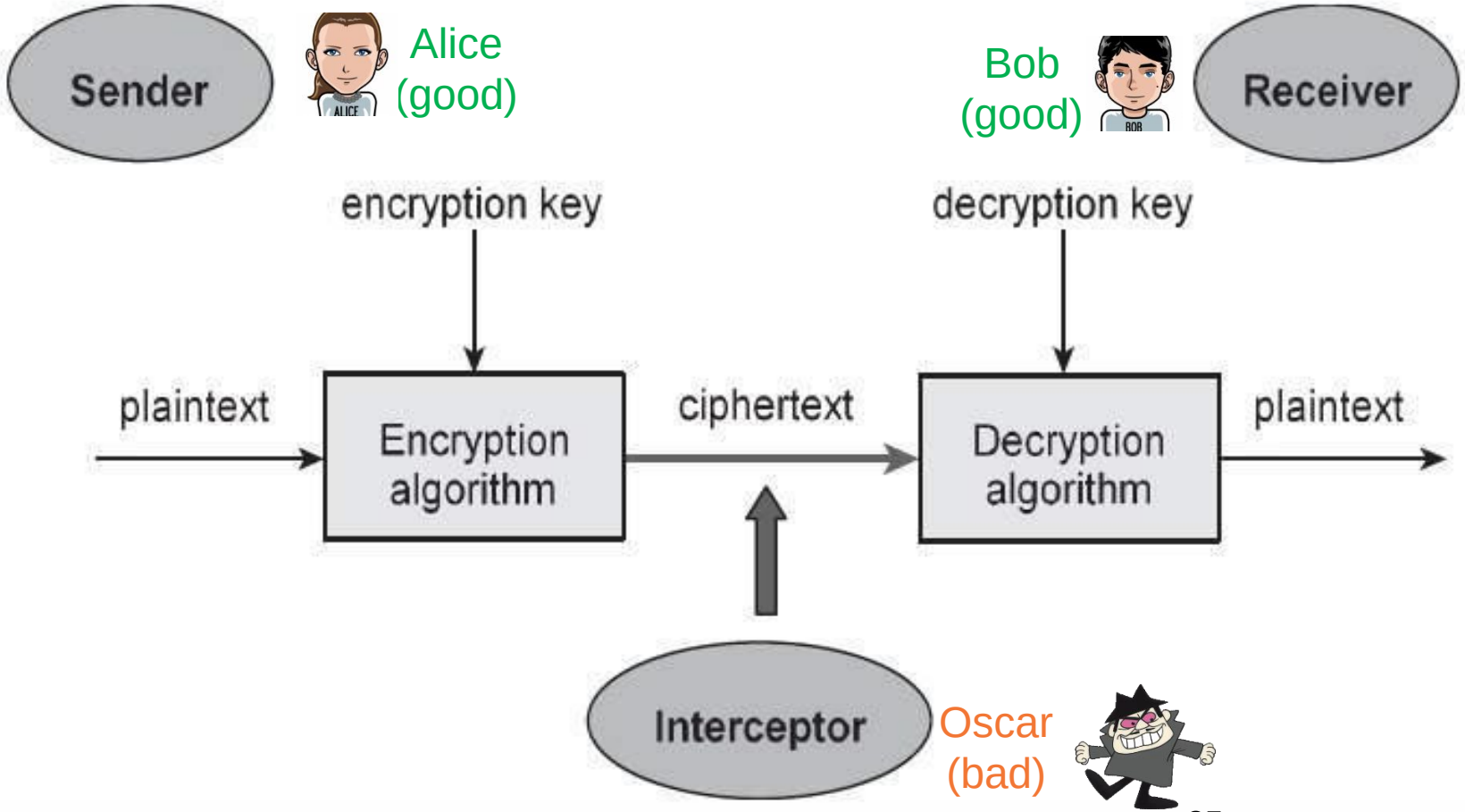


Keywords in Cryptography

- **Plain-text:** It is the data to be protected during transmission. Original message
- **Cipher-text:** It is the scrambled version of the plain-text produced by the encryption algorithm using a specific the encryption key. Text in unreadable format
- **Encryption Algorithm**: It is a mathematical process that produces a cipher-text for any given plain-text and encryption key.
- **Decryption Algorithm:** It is a mathematical process, that produces a unique plain-text for any given cipher-text and decryption key.
- **Encryption Key:** It is a value that is known to the sender. The sender inputs the encryption key into the encryption algorithm along with the plain-text in order to compute the cipher-text.
- **Decryption Key:** It is a value that is known to the receiver. The decryption key is related to the encryption key, but is **not always** identical to it. The receiver inputs the decryption key into the decryption algorithm along with the cipher-text in order to compute the plain-text.

Internet Security

Encryption



Encryption

- openSSL can be used to encrypt/decrypt
- Key generation
  - base64_encode(openssl_random_pseudo_bytes(32));

- Encryption
  - Algorithm: 3DES, AES(Rijndael)
  - Modes: ECB, CBC

Internet Security

Encryption

```
function encrypt($plaintext)
{
    $key = pack('H*', "bcb04b7e103a0cd8b54763051cef08bc55abe029fdebae5e1d417e2ffb2a00a3");
    $iv_size = mcrypt_get_iv_size(MCRYPT_RIJNDAEL_128, MCRYPT_MODE_CBC);
    $iv = mcrypt_create_iv($iv_size, MCRYPT_RAND);
    $ciphertext = mcrypt_encrypt(MCRYPT_RIJNDAEL_128, $key, $plaintext,
    MCRYPT_MODE_CBC, $iv);
    $ciphertext = $iv . $ciphertext;
    $ciphertext_base64 = base64_encode($ciphertext);

    return $ciphertext_base64;
}
```

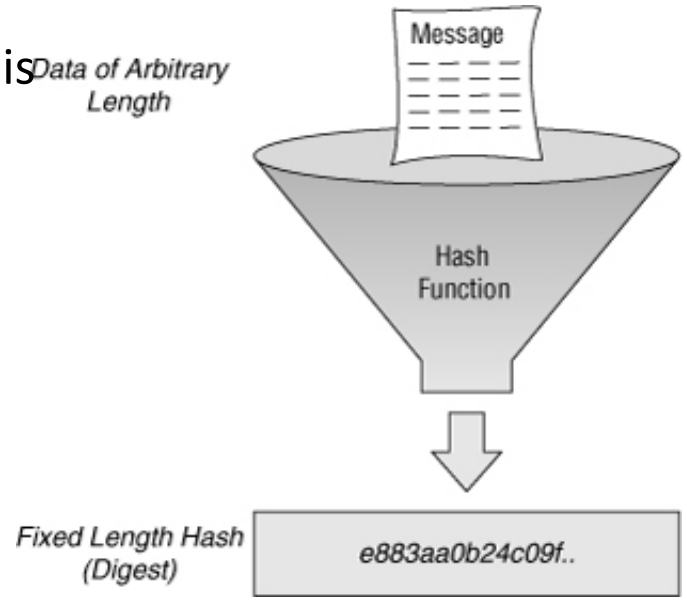
Internet Security

Decryption

```
function decrypt($cText)
{
    $ciphertext_dec = base64_decode($cText);
    $iv_size = mcrypt_get_iv_size(MCRYPT_RIJNDAEL_128, MCRYPT_MODE_CBC);
    $iv_dec = substr($ciphertext_dec, 0, $iv_size);
    $ciphertext_dec = substr($ciphertext_dec, $iv_size);
    $key = pack('H*',
    "bcb04b7e103a0cd8b54763051cef08bc55abe029fdebae5e1d417e2ffb2a00a3");
    $plaintext_dec = mcrypt_decrypt(MCRYPT_RIJNDAEL_128, $key, $ciphertext_dec,
    MCRYPT_MODE_CBC, $iv_dec);
    return $plaintext_dec;
}
```

Hash Functions

- A hash function is a mathematical function that converts a numerical input value into another compressed numerical value. The input to the hash function is of arbitrary length but output is always of fixed length. E.g. MD5, SHA1, SHA2



- Values returned by a hash function are called message digest or simply hash
  - (160 and 512 bits.)

- Can use for Message Integrity
  - Ideal for Password storage

Internet Security

Hash

- Cryptographic libraries can be used to secure the password using Hashing

- Hashing //Store the password's hash into the DB
  - password_hash($pw, PASSWORD_BCRYPT);

- Verify the password
  - password_verify($pw, $hashedPW);

Encryption Algorithms

- **Symmetric key cryptography**
  - Use of a single key for encrypting and decrypting the information
  - Key exchange problem!
  - Encryption, decryption algorithms are less complex
  - Faster!

- **Asymmetric key cryptography (Public Key)**
  - Each person has their own pair of keys,
    - private key
    - public key (Verified Certificate Authority)
  - Use one key to encrypt and another to decrypt.
  - Key exchange problem solved!
  - Encryption, decryption algorithms are very complex
  - Require far greater computation time, Slower!
  - impractical for large messages

Combine both techniques to create secure efficient security protocol suites!

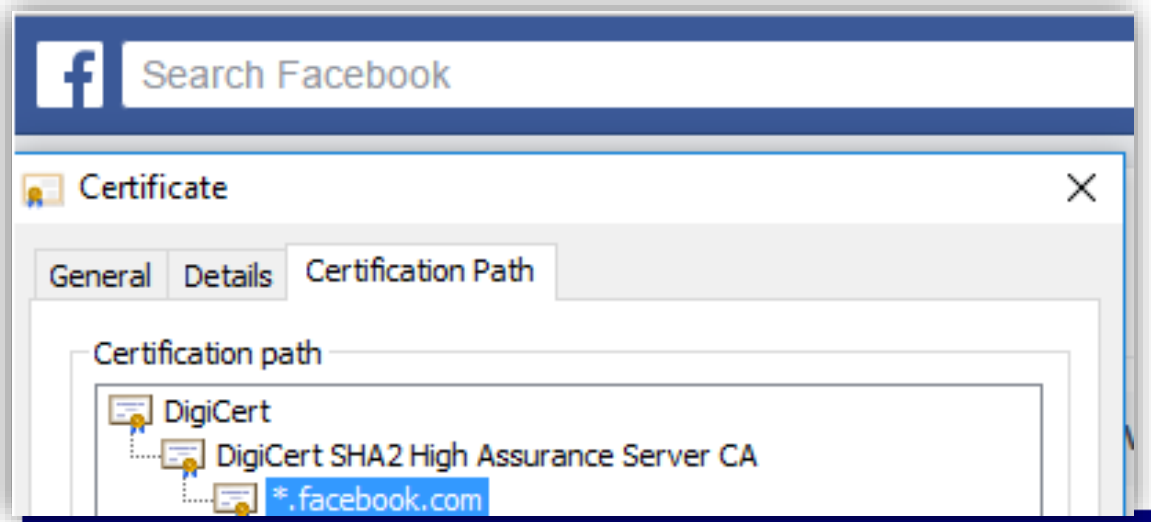
Certification Authorities - C A

What CA does ?

- Allow an individual to verify another person or company's public key
- The digital certificate is encrypted with the CA's private key.
- Each person must know the public key for the CA in order to verify the certificate
- Public keys for the main CA are encoded in latest versions of web browsers.

Certification Authorities - C A

- VeriSign - www.verisign.com
- GeoTrust - www.geotrust.com
- Comodo - www.comodo.com
- Digicert - www.digicert.com
- Thawte - www.thawte.com
- GoDaddy - www.godaddy.com
- Symantec - www.symantec.com



Protocols

- We can combine all the learnt techniques to create comprehensive security protocols.
- Secure Socket Layer **(SSL)** also known as Transport Layer Security **(TLS)**
- Secure IP Protocol **(IPSec)** signature helps to assure that the signer is who he or she claims to be.
- **HTTPS** (Conventional HTTP used inside TLS)
- And many more

Protocols – SSL/TLS

- Provide authentication for servers and browsers.
- Provide confidentiality and data integrity for communications.
- Operating lower in the network stack.
- Widely used on the web.
- SSL makes use of a combination of public key and symmetric cryptography, along with digital certificates for verification.
- Latest version SSL 3.0, TLS 1.2.

Internet Security

Protocols – SSL/TLS

e-Life & Security

Best Security Practices - Facebook

- Take control of your posts
  - Understand the importance of FB's **Audience Selector** tool.
- Manage posts other people have tagged you in using **Tag Review.**
- Give priority to your privacy.
  - "Who can see my stuff?" "Who can contact me?" "Who can look me up?"
- Protect your **password!**
- Avoid clicking on suspicious links or objects
- If required you **CAN** permanently delete your FB account.
- Use FB's security guidelines: https://www.facebook.com/facebookmedia/best-practices/security

Best Security Practices – YouTube

- Keep your account recovery information updated
- **Audience Selector** in YouTube.
- Videos violating your privacy ?
  - If you can’t reach an agreement with the uploader, or if you are uncomfortable contacting them, you can **request removal of content.**
- Unique & strong password!
- Don’t be a victim of phishing attacks:
  - YouTube will never ask you for your password, email address, or other account information.
  - Don't be fooled if someone contacts you pretending to be YouTube!

Best Security Practices – Gmail

- Constantly check recent account activity for anything suspicious. Use '**Recent Security Event'** tool.
- Enable '**Authentication icon for verified senders**' tool.
- Do not open 'Spam' emails unless 100% certain
- Unique & strong password!
- Update your web browser
- Complete Gmail's **Security Checkup**

Lessons Learned

- Internet is **NOT** safe, hence security techniques had to be introduced.
- Many threats exist and attackers use various techniques.
- Key Internet Security services are identified (CIA Triad).
- Cryptography provides solution for security requirements.
- We can combine cryptographic techniques to create comprehensive security protocol suites such as TLS.
- Always use best security practices for your daily internet based interactions.

Summary

- How safe is the Internet?
- Internet security threats
- Internet security services
- Internet security
- E-life and security