INTERNET SECURITY AND THE WWW

OVERVIEW

A. Major Components of the Internet

B. Attacks against Web Servers

C. Risks the Internet user faces

D. Attack Points on the Internet

Image by rawpixel.com

A. MAJOR COMPONENTS OF THE INTERNET

1.1 World Wide Web (WWW)

- The **WWW** is a collection of standards, programs, and protocols which enable multimedia hypertext files to be accessed over the Internet
- The **Internet** is made up of a large number of smaller, interconnected networks.
    - It was originally developed as a military project and later handed over to the National Science Foundation to be used for research and academics.

Without the Web, the Internet might appear as something like a library without books. The Internet is populated with content and substance by the Web.

1.2 Cloud Infrastructure

- **Cloud Computing** provides access to communications, applications, and information over the Internet. Without it, computers would run software only locally.
- In addition to revolutionized accessibility, the expansion of cloud computing can largely be attributed to the process of **convergence**. This is where a single product is capable of performing the functionalities of several different devices.

Primary Cloud Service Types:

1. **Software as a Service (SaaS)**
    a. Software provided to end-users, often subscription or fee based
    b. Examples – Dropbox, Office 365

2. **Platform as a Service (PaaS)**
    a. Provides access to operating systems, developer tools, programming languages
    b. Examples – Windows Azure, AWS Elastic Beanstalk
3. **Infrastructure as a Service (IaaS)**
    a. Cloud provider manages a network and provides organizations with access to:
        i. Network equipment
        ii. Virtualized network services
        iii. Storage, Software, Supporting Network Infrastructure
    b. Examples – Amazon Web Services, DigitalOcean

1.3 E-mail & Instant Messaging (IM) Systems

- **Electronic mail (E-mail)** is one method of sending messages between computing devices using the Internet (e.g. Gmail, Outlook, Yahoo..)
- **E-mail & Web-mail**: webmail is sent through a browser; e-mails are sent through a particular application and browser

  Gmail is an example of a browser-based email, whereas Microsoft Office 365 is an email service used outside a browser.

1.4 Forums

- **Forums** are online discussion boards which allow users to seek help and advice about a topic

  Examples: Reddit, Quora, Stack Overflow

B. Attacks Against Web Servers

- Web Applications
  - Web apps. are supported by Web servers, usually running embedded OSs
  - Components such as an application, server, and OS have their own individual vulnerabilities. When combined, there is a higher risk that a Web app. becoming compromised will affect a network's security

    (e.g. a vulnerability exploited within a Web mail app. could lead to attacks being launched against an OS)
  - Database servers store Web page information that users interact with. If web servers becoming compromised, perpetrators could:
    - Deface the Website
    - Destroy, Alter, or Sell Database Contents
    - Gain control of stored User Accounts
    - Access other servers part of the network
- Scripting Languages
  - HTML Web pages contain forms and scripting languages (e.g. JavaScript)
  - Scripting languages are attributed to over half of Web server attacks
- Security Testing
  - Determine whether dynamic or static Web pages are being used
  - Determine if a separate server is implemented to authenticate users
  - Determine if a Web app. is connected to a back-end DB
  - Analyze what platform was used in developing the target Web app.

Tools: Burp Suite and **Wpiti** are used to test and attack Web servers. OWASP helps inform security professionals of Web app. vulnerabilities

C. Risks the Internet User Faces

- Malware
  - Trojans, Keyloggers, Spyware/Adware, Virus.. see **Attack Techniques** Document
- Social Engineering
  - Perpetrators seeking to divulge information by using techniques such as authority impersonation, urgency, kindness, etc..
- Network Attacks
  - Attacks on the user's network that might include denial of service or interception of traffic (man-in-the-middle)
- Password Attacks
  - Credential cracking to gain access to personal accounts and data
- Online information (posted on public domain & social media)
  - Crowdsourced information (user posts voluntarily) such as pet names, birthdays, family members and other personally identifiable information could be used against you (especially if you name those in passwords)
  - Publicly accessible information such as phone numbers, company directory, etc..

D. Attack Points on the Internet

1) **Client**
    a. Any computing device on a network which requests services from another computing device on the Internet
2) **Server**
    a. Any computer which sends an output to requests from clients (e.g. Web servers handle web-related requests)
3) **Webpage**
    a. Any digital page or document which is accessible on the Internet
4) **Web Site**
    a. A collection of interconnected webpages (designed to fulfill a particular goal)
5) **Web Portal**
    a. A web site or service which offers resources such as e-mail, search engines, and forums (e.g. Yahoo, Google..)
6) **Web Browser**
    a. A program or software on a client which retrieves data from the WWW