

# **Computer Security**

## **Introduction**

**Threats, Risks, Vulnerabilities and Impacts**

**Mark D. Ryan – [M.D.Ryan@cs.bham.ac.uk](mailto:M.D.Ryan@cs.bham.ac.uk)**

What is computer security?

# Some example definitions

- Java is an object-oriented programming language developed by Sun Microsystems and released in 1995.
- Islam is a monotheistic religion originating with the teachings of Muhammad in the 7<sup>th</sup> century.
- China is the most populous country in the world, and the largest country in East Asia, bordering Mongolia, Russia, Vietnam, Laos, India and others.

# What is computer security?

- What kind of thing is security?
- What does computer security try to achieve?
- How does it try to achieve it?

*Computer security is . . .*

# Possible answer

Computer security is a field of engineering concerned with the development and deployment of measures to ensure the protection of computer systems from hostile acts or influences.

- What are we trying to secure?
- From whom are we trying to secure those things?
- What do we want to prevent them from doing?

# Computer Security: definitions

- **Assets:** Things we want to protect (data, systems, services)
- **Threats:** Events that can happen to assets (e.g. loss of confidentiality)
- **Attacks:** Attempts to realise threats
- **Vulnerabilities:** Weaknesses of systems which make attacks possible
- **Risk:** A measure of the likelihood of occurrence of an attack
- **Impact:** A measure of how serious an attack would be
- **Computer security:**

- Analysing *risk* and *impact* of *threats*
- Protecting *assets* against *attacks*
- Overcoming *vulnerabilities*
- Mitigating *risks*
- Reducing impacts of *attacks*

# Computer Security: *impact vs. risk*

- **Security engineering:**

- Evaluating risks and impacts of attacks
- Deciding appropriate responses (avoidance, reduction, acceptance)

	<i>Low Impact</i>	<i>High Impact</i>
<i>Low Risk</i>		
<i>High Risk</i>		

# Computer Security: *impact vs. risk*

- **Security engineering:**

- Evaluating risks and impacts of attacks
- Deciding appropriate responses (avoidance, reduction, acceptance)

	<b><i>Low Impact</i></b>	<b><i>High Impact</i></b>
<b><i>Low Risk</i></b>	Gaining unauthorised access to the University's wireless network	Gaining unauthorised access to Pentagon nuclear weapon systems
<b><i>High Risk</i></b>	A large-scale spam attack	A large-scale virus attack against Microsoft Windows

# Some aspects of security

- Confidentiality
- Integrity
- Availability
- Authentication
- Non-repudiation

# Some methods of computer security

# Authentication

- Authenticating people, using passwords, biometrics, RSA tokens, smartcards
- Authenticating platforms, e.g. for network access
- Authenticating software, before you install it
- Authenticating services, before you use them

# Access control

- Deciding whether an agent can access a resource
  - agents can be users, or software
- Deciding whether a packet can reach its destination (firewalls)
- ...

# Intrusion detection

- Host intrusion detection
  - pattern analysis on servers
  - anti-virus software
- Network intrusion detection
- ...

# Cryptography

- Encryption
  - Encryption is a method to transform data to render it unusable except by agents possessing certain knowledge, called a key
- Digital signature
  - A digital signature is some data that provides evidence that a certain agent asserted certain other data
- ...

# Who are the attackers?

– Used to be:

People who get kicks out of vandalism

- They get attention and the feeling of power

– Now it's:

Organised criminals

- They get money

# Today's attacker



# Today's security



# How to interpret this mail?

From: Verification <verify50@halifax.co.uk>  
To: M.d.ryan <m.d.ryan@bham.ac.uk>  
Subject: Halifax E-mail Verification: m.d.ryan@bham.ac.uk  
Date: Sun, 26 Oct 2003 06:49:54 +0000

Dear Halifax Bank Member,

This email was sent by the Halifax server to verify your e-mail address. You must complete this process by clicking on the link below and entering in the small window your Halifax username and password. This is done for your protection --- because some of our members no longer have access to their email addresses and we must verify it.

To verify your e-mail address and access your bank account, click on the link below. If nothing happens when you click on the link (or if you use AOL), copy and paste the link into the address bar of your web browser.

**<http://halifax.co.uk:ac=AA6FDxthlNmaz70OuYbH@ShOrTwAy.To/x66f94/?7312hL2M5ZHFzNj>**

# How to interpret this mail?

From: Verification <verify50@halifax.co.uk>  
To: M.d.ryan <m.d.ryan@bham.ac.uk>  
Subject: Halifax E-mail Verification: m.d.ryan@bham.ac.uk  
Date: Sun, 26 Oct 2003 06:49:54 +0000

Dear Halifax Bank Member,

This email was sent by the Halifax server to verify your e-mail address. You must complete this process by clicking on the link below and entering in the small window your Halifax username and password. This is done for your protection --- because some of our members no longer have access to their email addresses and we must verify it.

To verify your e-mail address and access your bank account, click on the link below. If nothing happens when you click on the link (or if you use AOL), copy and paste the link into the address bar of your web browser.

<http://halifax.co.uk:ac=AA6FDxthlNmaz70OuYbH@ShOrTwAy.To/x66f94/?7312hL2M5ZHFzNj>

# Discussion

- **Phishing:**

- This is a type of attack known as phishing
- It relies on uninformed parties parting with personal details
- Phishing attacks cost \$500m per year! [The Register, 29/09/04]

- **Syntax: `http://a.b@domain.com/path` means:**

- access `http://domain.com/path`
- citing username [a] and password [b]
- `http://shortway.to` has disappeared, but was available at time of this message.

- **But wait, there's more...**

# Scenario: Part 2

*Is this real or another fraud?*

From: "Halifax plc" <response@halifax-mail.co.uk>  
Sender: "Halifax plc" <response@halifax-mail.co.uk>  
To: "mdr@cs.bham.ac.uk" <M.D.Ryan@cs.bham.ac.uk>  
Subject: IMPORTANT NOTICE: From Halifax and Bank of Scotland  
Date: Sat, 1 Nov 2003 12:24:24 GMT

As you may have heard on the news recently a number of fraudulent emails are currently circulating in the UK encouraging bank customers to visit a website where personal card or internet security details are then requested. Please note that we would never send emails that ask you for confidential or personal security information - other than your usual sign-ins to online banking.

If you have already received, or receive such an email in the future, please forward this to [onlineemailinvestigations@hbosplc.com](mailto:onlineemailinvestigations@hbosplc.com) and then delete it immediately without responding or visiting any site it details. If you are concerned that you may have divulged any personal or security details please call our Helpdesk on 0845 602 0000.

Halifax plc. Registered In England No. 2367076. Registered Office: Trinity Road, Halifax, West Yorkshire HX1 2RG.

Bank of Scotland. The Governor and Company of the Bank of Scotland, constituted under an Act of Parliament 1695. Head Office: The Mound, Edinburgh EH1 1YZ.

# Countermeasures

- **Authenticated email**
  - Digital signatures
  - Public key certificates
- **Better software**
  - Avoid compromising security for user convenience
- **User education**

# An ongoing saga

- **December 2003, vulnerability announcement:**

- IE6 can display a different URL in address bar to the one accessed
- Same as before, but include non-printing character (%01) before "@"
- See: <http://www.zapheddingbat.com/security/ex01/vun1.htm>

- **September 2004, vulnerability announcement:**

- JPEG Bug – Attacker can insert malicious code into a JPEG file
- File can be e-mailed or downloaded whilst browsing the web
- When image is viewed, inserted code is executed
- See: <http://news.bbc.co.uk/1/hi/technology/3684552.stm>

# An ongoing saga

- **September 2006, vulnerability announcement:**

- Stack-based buffer overflow in the Vector Graphics Rendering engine (vgx.dll), as used in Microsoft Outlook and Internet Explorer 6.0 on Windows XP SP2, and possibly other versions, allows remote attackers to execute arbitrary code via a Vector Markup Language (VML) file with a long fill parameter within a rect tag.
- <http://www.cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2006-4868>

# The padlock

- Meaning: https, i.e. traffic between browser and server is encrypted.
- What if a form is *secure* (https) but it posts its data back *insecurely*? How should your browser behave?
  - It probably means the web designer doesn't understand what s/he is doing, since he is securing the blank form (which is unlikely to be confidential) but then passing the data (likely to be confidential) in the clear.
  - Tim Williams: "I reported the problem twice [to the web site owners], but they never replied and never bothered fixed the problem."

# The padlock, continued

- How do the browsers behave?
  - IE: initially, warns user about *any* switch between http and https. Everyone turns this off of course. It doesn't give you any warning after that.
  - Both KDE Konqueror and Mozilla web browsers warn the user of this particular situation, regardless of whether they have turned off standard warnings.

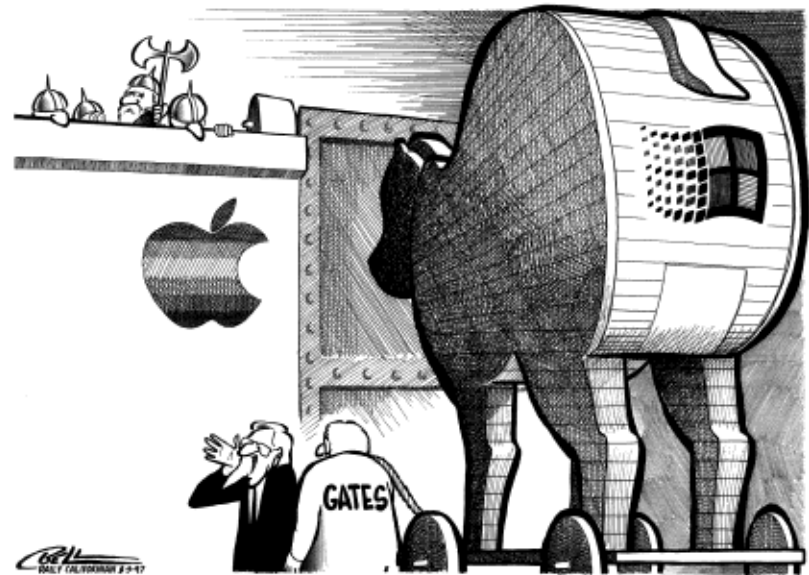
*Warning. This is a secure form but it is attempting to send your data back unencrypted. A third party may be able to intercept and view this information. Are you sure you wish to continue?*
- Demo: <https://hotstuff.my-place.org.uk/encrypttest.html>

# Some kinds of attack

- Malware
- Denial of service
- Website defacing
- "Social engineering"
- Phishing (identity theft)
- Key logging

## The CIA:

- **C**onfidentiality
- **I**ntegrity
- **A**vailability



"He says he comes bearing gifts!"