Fundamentals

Trap-door

Mis-representation

Visual spying

Logical scavenging

Eavesdropping

Interference

Physical removal

Spoofing

Logic bombs

Trojan horse

Authorizati attack

Threats

Author: Prof Bill Buchanan

Threats
Introduction

Cyberterrorism. This can be attacks against critical national infrastructures, such as power plants, oil refineries, and so on,

Natural Disasters

Natural Disasters. This includes storms, hurricanes, fire, floods, earthquakes, and natural events

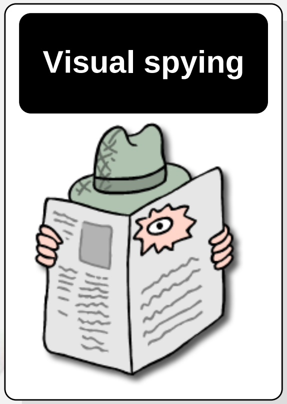
Cyberterror

Threats: Cyberterrorism/Nature Disasters

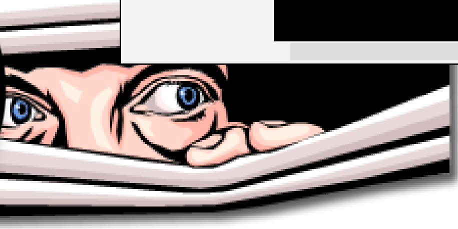
Threats: Visual spying/misrepresentation

Fundamentals

Threats



Visual spying. This actual physical viewing a user's activities, such as their keystrokes or mouse clicks.

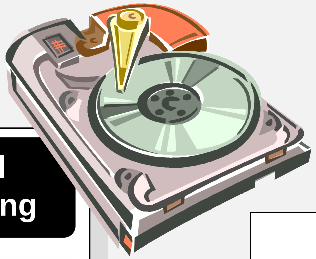


Misrepresentation. This involves the actual deception of users and system operators.

Author: Prof Bill Buchanan

Threats: Visual spying/misrepresentation

Eavesdropping. This involves intercepting communications.



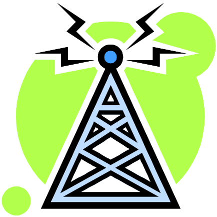
Logical scavenging. This involves scavenging through discarded media.

Author: Prof Bill Buchanan

Threats

Fundamentals

Interference



Interference. This involves the actual interference of communications, such as jamming communications, or modifying it in some way.

Physical attacks

Physical removal

Physical attacks. This involves an actual physical attack on the hardware. **Physical removal**. This involves the actual physical removal of hardware.

Author: Prof Bill Buchanan

Threats: Interference/Physical attacks

Threats

Fundamentals

Spoofing. This involves the spoofing of devices.

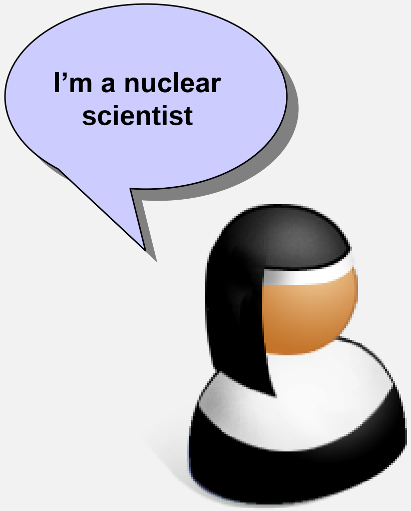
Spoofing

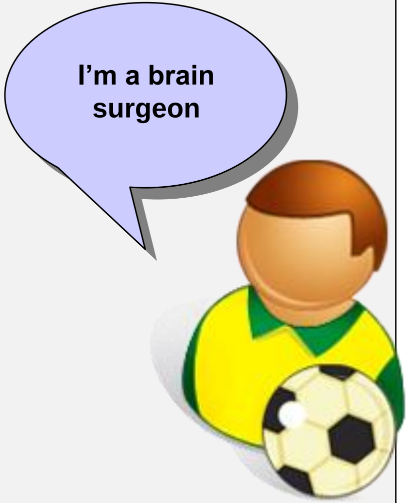
Bob

Eve

Im-personation

Impersonation. This involves the impersonation of a user/device.





Author: Prof Bill Buchanan

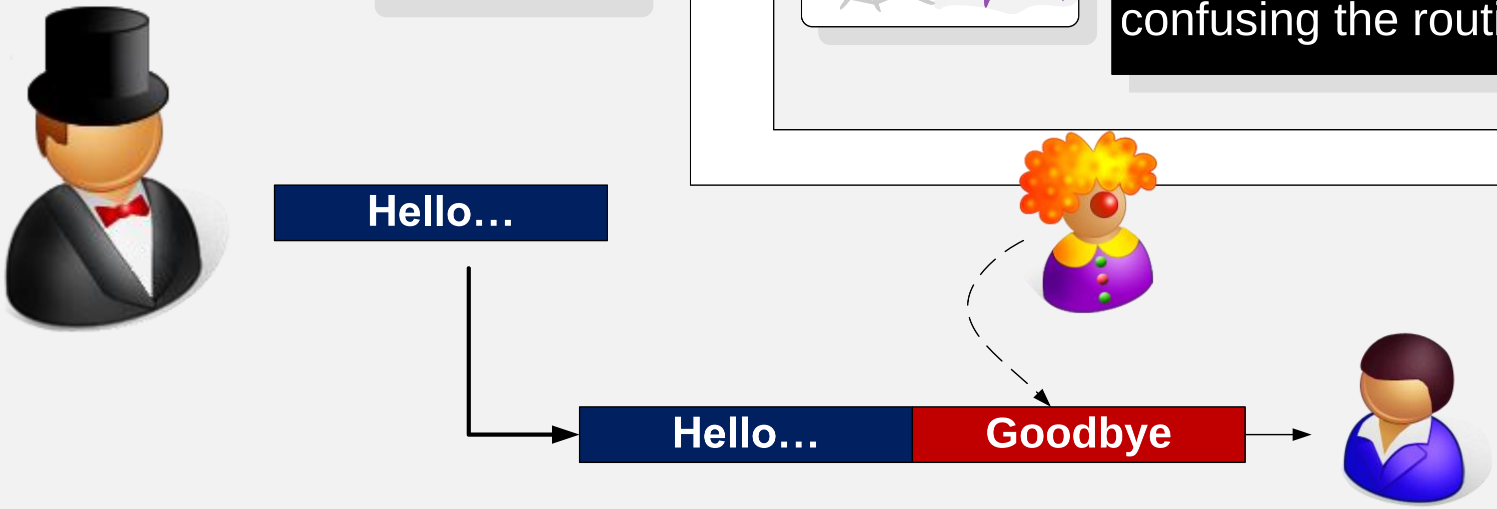
Threats: Spoofing/impersonation

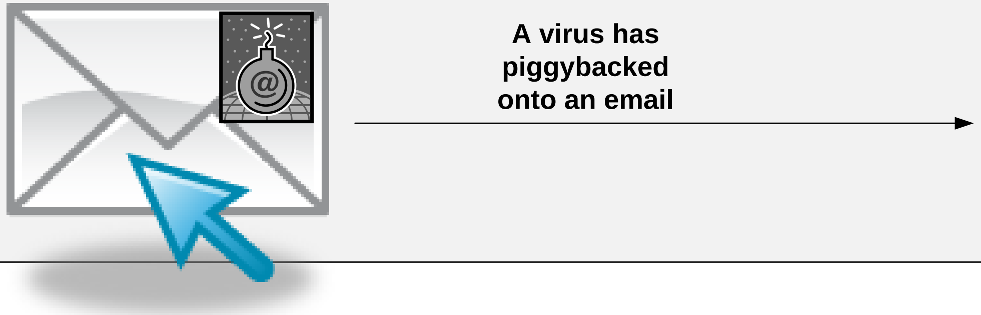
Piggy back attacks. This involves adding data onto valid data packets.

Piggy back

Network weaving

Network weaving. This involves confusing the system onto the whereabouts of a device, or confusing the routing.





Threats

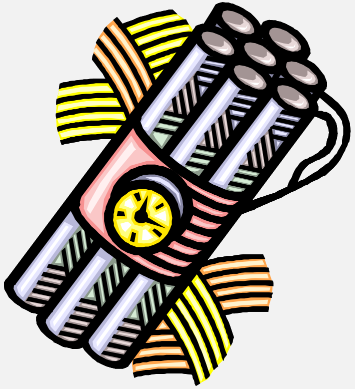
Fundamentals

Author: Prof Bill Buchanan

Threats: Piggy back/network weaving

Threats:Trojan/logical bomb

Trojan horses. This involves users running programs which look valid, but install an illicit program which will typically do damage to the host.



Logic bombs. This involves the installation of a program which will trigger some time in the future based on time or an event.

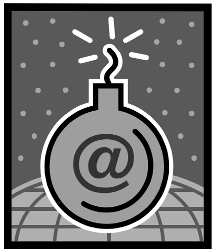
Best project ever! Click here

→

The email contains a Trojan virus

Trojan horse

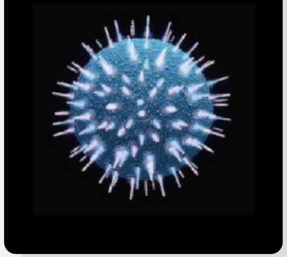
Logic bombs



Threats: Worms/viruses

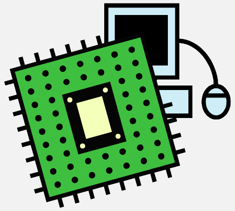
Malevolent worms. This involves a worm program which mutates in a given way which will eventually reduce the quality of service on the network, such as using up CPU resources or network bandwidth.

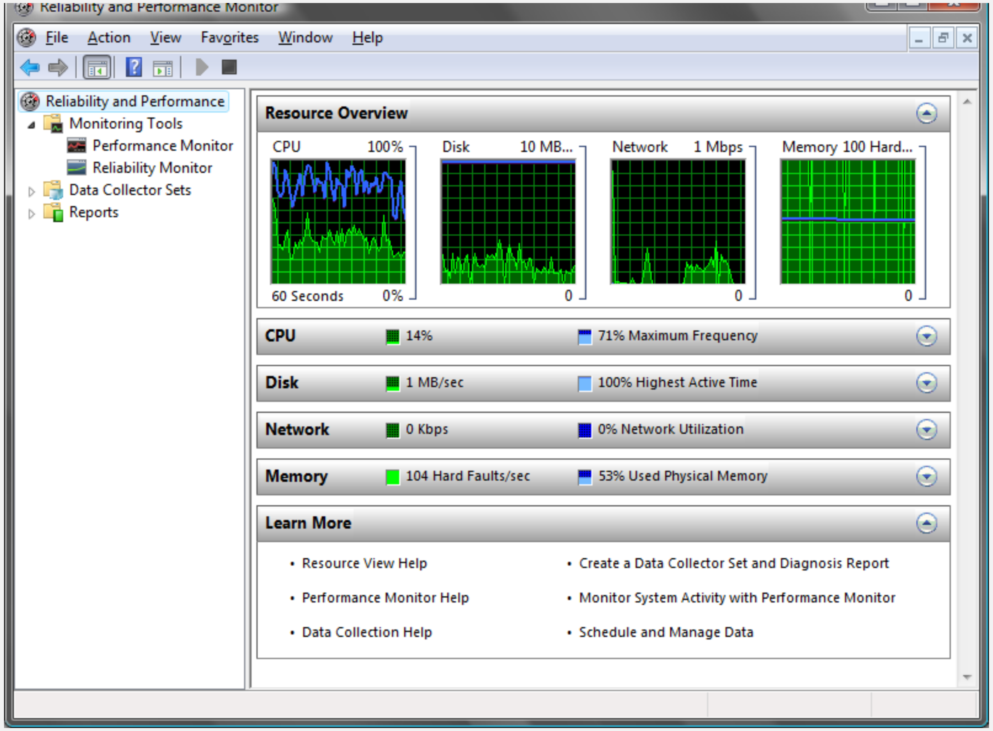
Viruses



Viruses. This involves attaching program which self replicate themselves.

Worms





Resource Overview

CPU 🟩 14% 🟦 71% Maximum Frequency

Disk 🟩 1 MB/sec 🟦 100% Highest Active Time

Network 🟩 0 Kbps 🟦 0% Network Utilization

Memory 🟩 104 Hard Faults/sec 🟦 53% Used Physical Memory

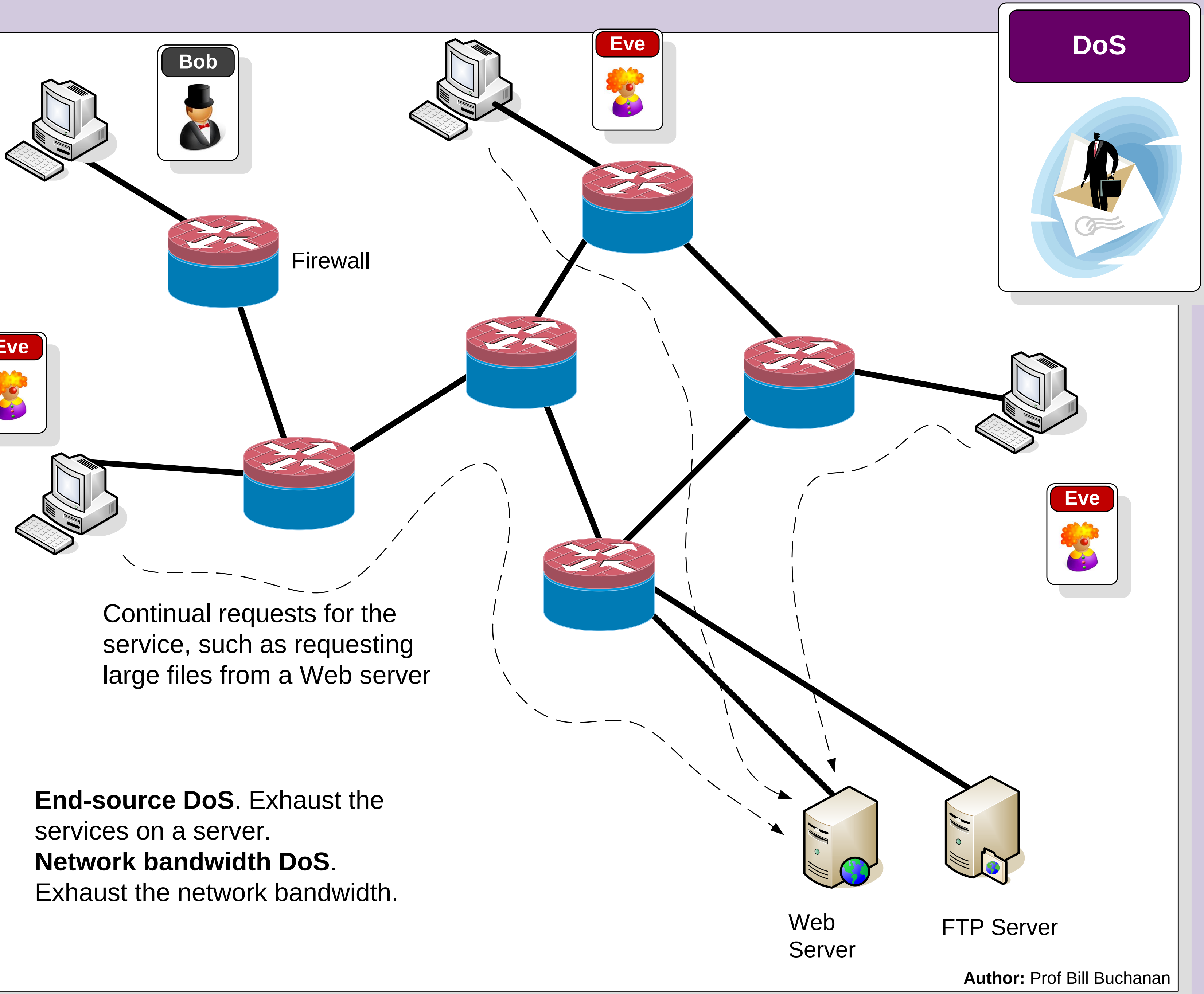
Learn More

- Resource View Help
- Performance Monitor Help
- Data Collection Help
- Create a Data Collector Set and Diagnosis Report
- Monitor System Activity with Performance Monitor
- Schedule and Manage Data

Threats

Fundamentals

DoS



Continual requests for the service, such as requesting large files from a Web server

End-source DoS. Exhaust the services on a server.
Network bandwidth DoS.
Exhaust the network bandwidth.

Author: Prof Bill Buchanan

Inference

Inference. This involves exploiting database weaknesses using inferences.

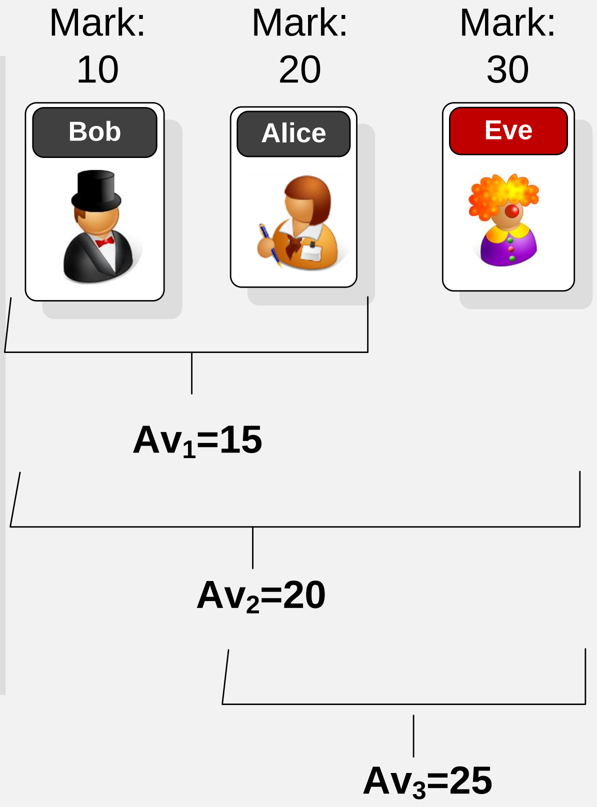
For example … the marks for any student is not allowed, but the average a number of students is allowed.

Query: Average(Bob,Alice) -> Av_1= (B+A)/2
Query: Average(Bob,Eve) -> Av_2= (B+E)/2
Query: Average(Alice,Eve) -> Av_3= (A+E)/2

Av_1-Av_2=(A-E)/2

Av_1-Av_2+Av_3 = (A-E)/2+(A+E)/2=A

Alice’s mark is Av_1-Av_2+Av_3



Alice’s mark=Av_1-Av_2+Av_3=15-20+25=20

Author: Prof Bill Buchanan

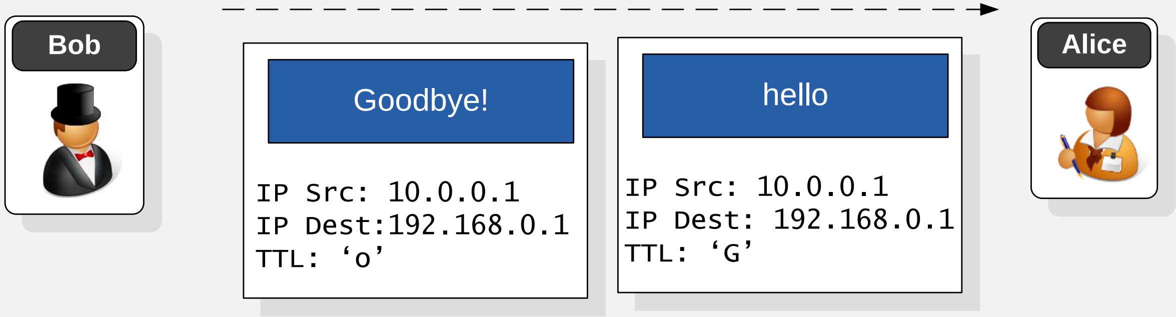
Threats: Inference

Covert channel

Covert channels. This involves hiding data in valid network traffic.

Timing channel. Transmit with relative timing of events.

Storage channel. Modify an object (such as adding to network packet headers).



```
IP Src: 10.0.0.1
IP Dest:192.168.0.1
TTL: ‘o’
```

```
IP Src: 10.0.0.1
IP Dest: 192.168.0.1
TTL: ‘G’
```

Eve reads the data packets, and the message seems valid, but the message “Go” is hidden in the packet headers.

Author: Prof Bill Buchanan

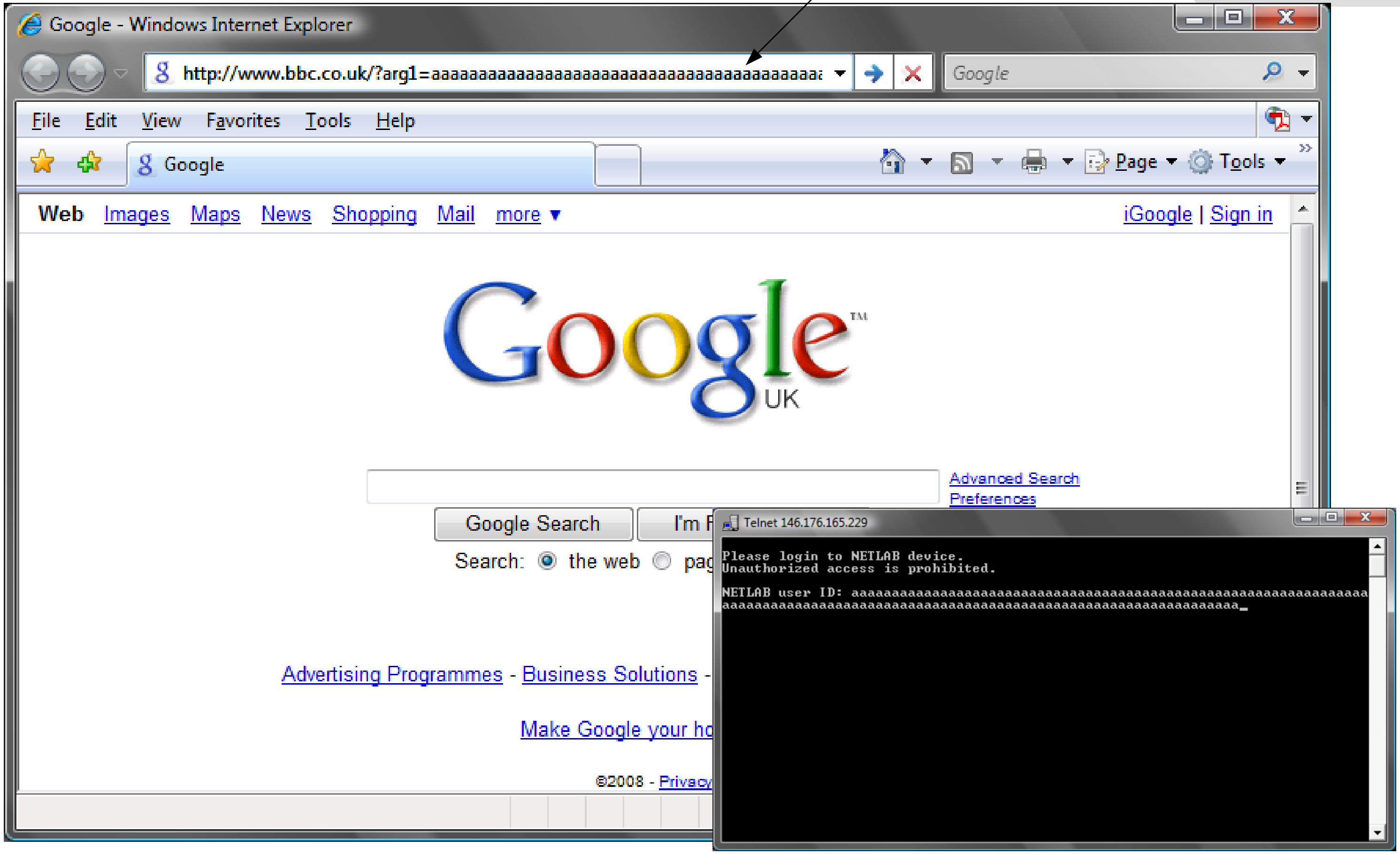
Threats: Covert channels

Threats: Active attacks

Active attack

Active attack. This entering incorrect data with the intention to do damage to the system.

Possible buffer overflow attack where the intruder tries to put incorrect information into the page



```
http://www.bbc.co.uk/?arg1=aaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaa
```

```
Please login to NETLAB device.
Unauthorized access is prohibited.

NETLAB user ID: aaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaa
aaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaa_
```

Author: Prof Bill Buchanan

Threats: Authorization attack/trap door

Threats

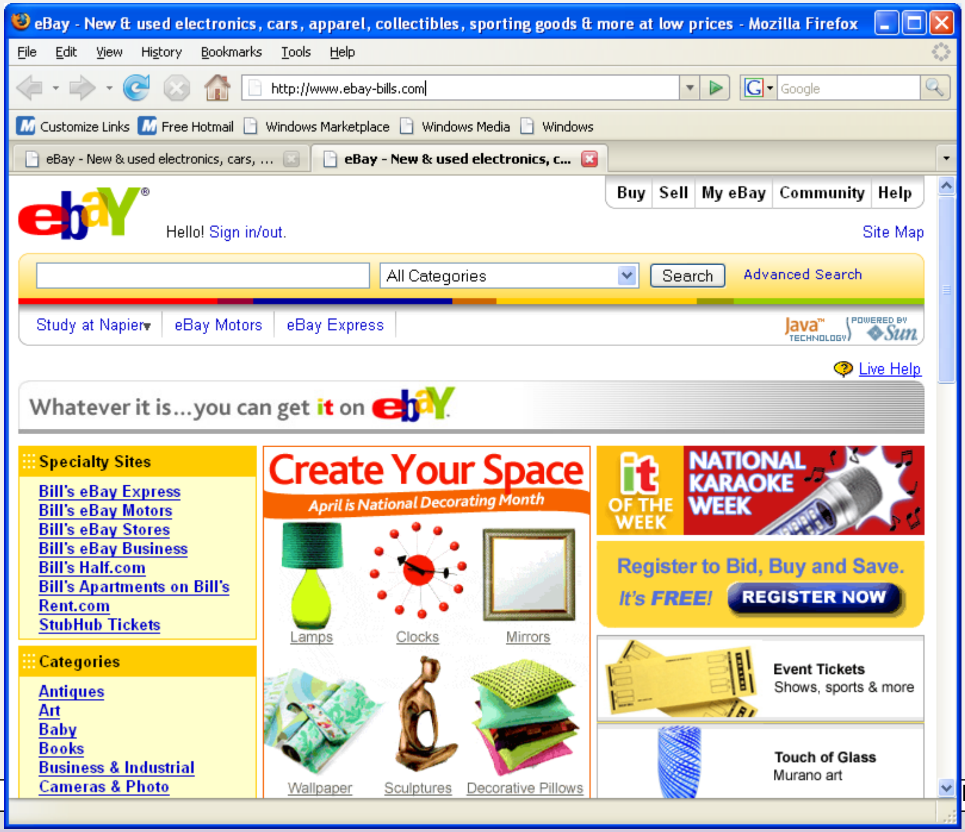
Fundamentals

Authorization attacks. This involves trying to gain access to a higher level of authorization than is valid for the user, such as with password attacks.

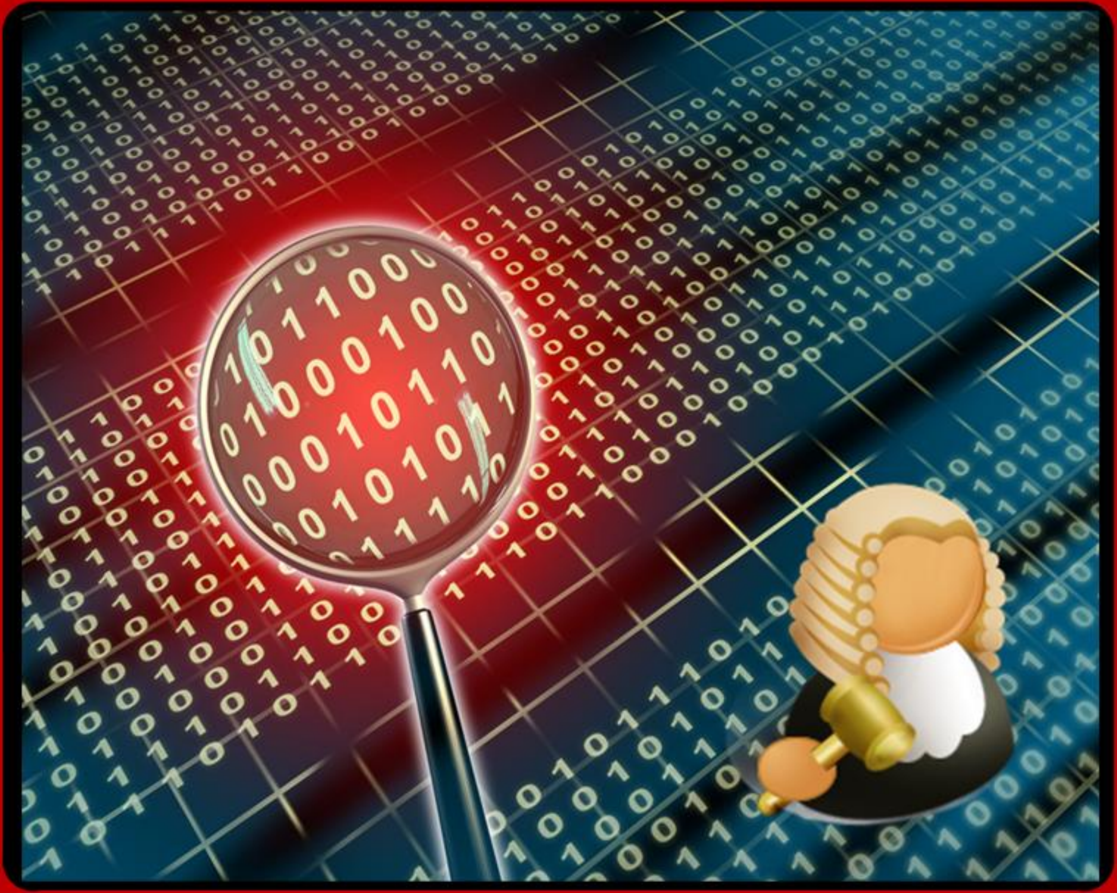
Trap-door

Trap door impersonation. This involves the creation of pages or login screens which look valid, but are used to gain information from a user, such as their bank details, or login password.

Authorization attack



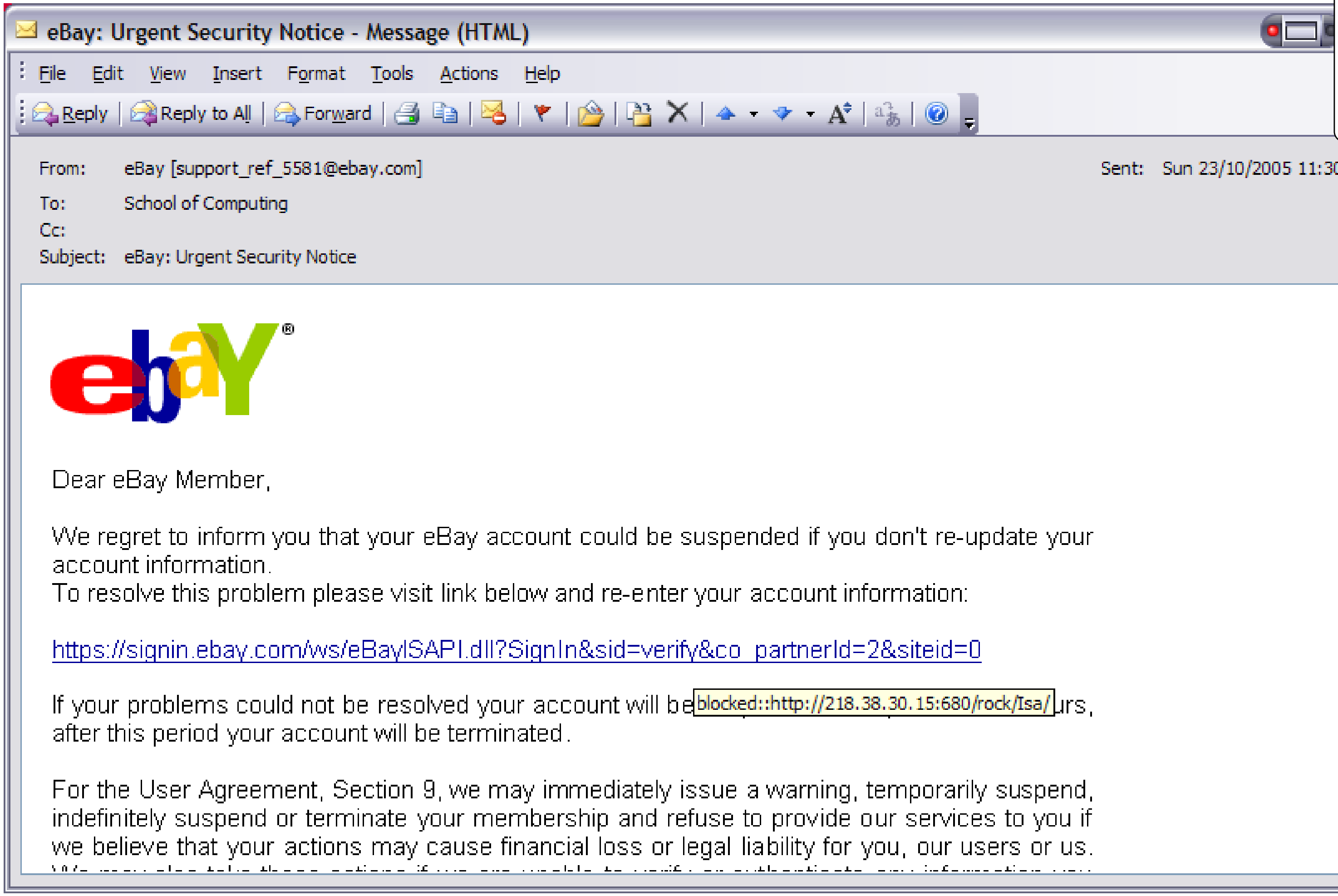
Threat Analysis



Phishing

Author: Prof Bill Buchanan

Trap-door


eBay: Urgent Security Notice - Message (HTML)
File Edit View Insert Format Tools Actions Help
Reply
Reply to All
Forward

From: eBay [support_ref_5581@ebay.com]

Sent: Sun 23/10/2005 11:30

To: School of Computing

Cc:

Subject: eBay: Urgent Security Notice

Dear eBay Member,

We regret to inform you that your eBay account could be suspended if you don't re-update your account information.
To resolve this problem please visit link below and re-enter your account information:

https://signin.ebay.com/ws/eBayISAPI.dll?SignIn&sid=verify&co_partnerId=2&siteid=0

If your problems could not be resolved your account will be urs, after this period your account will be terminated.

blocked::http://218.38.30.15:680/rock/Isa/

For the User Agreement, Section 9, we may immediately issue a warning, temporarily suspend, indefinitely suspend or terminate your membership and refuse to provide our services to you if we believe that your actions may cause financial loss or legal liability for you, our users or us. We may also take these actions if we are unable to verify or authenticate any information you

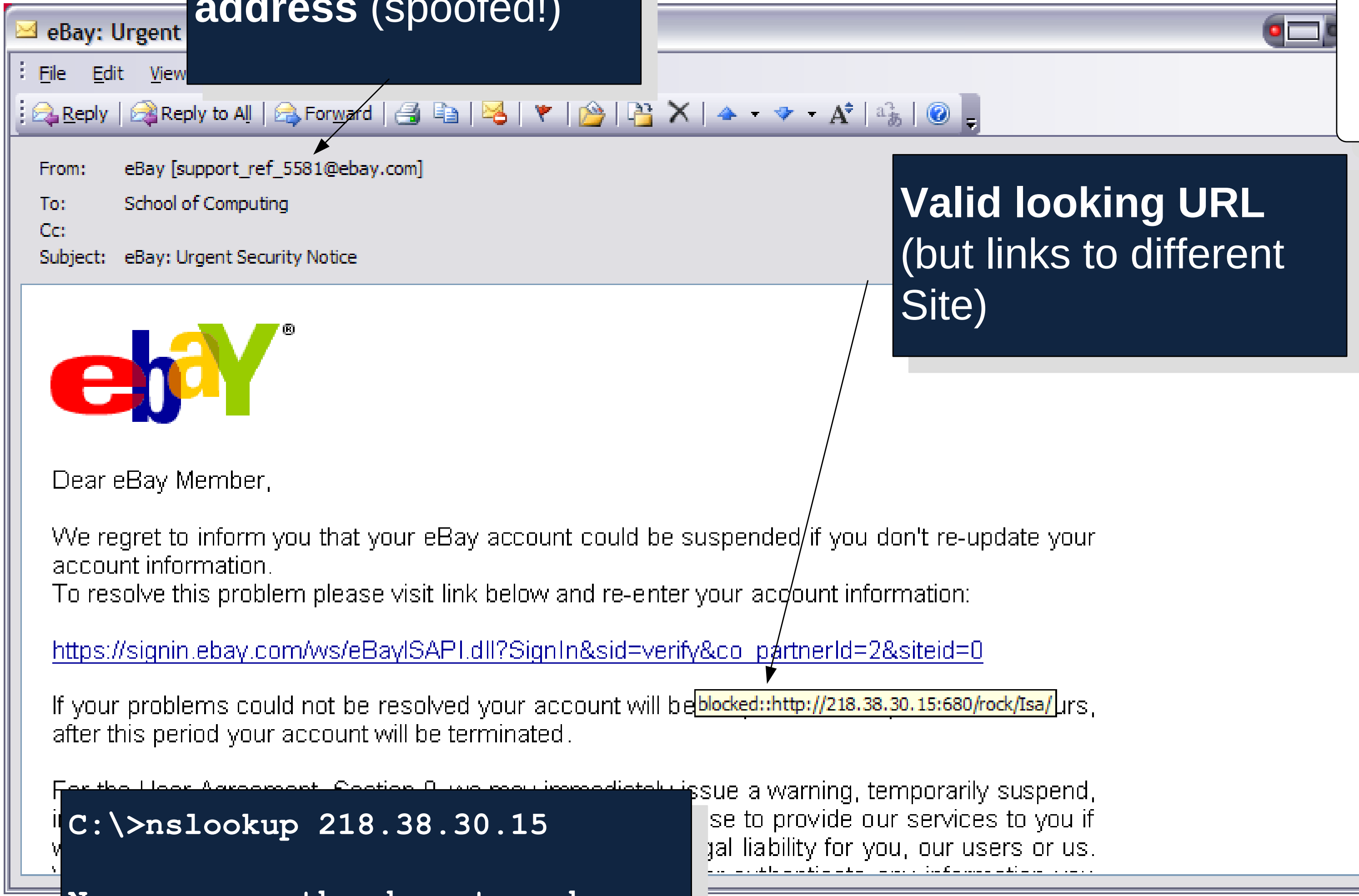
Threats

Fundamentals

Author: Prof Bill Buchanan

Threats: Authorization attack/trap door

Trap-door



Valid looking email address (spoofed!)

From: eBay [support_ref_5581@ebay.com]
To: School of Computing
Cc:
Subject: eBay: Urgent Security Notice

Valid looking URL (but links to different Site)

Dear eBay Member,

We regret to inform you that your eBay account could be suspended if you don't re-update your account information.
To resolve this problem please visit link below and re-enter your account information:

https://signin.ebay.com/ws/eBayISAPI.dll?SignIn&sid=verify&co_partnerId=2&siteid=0

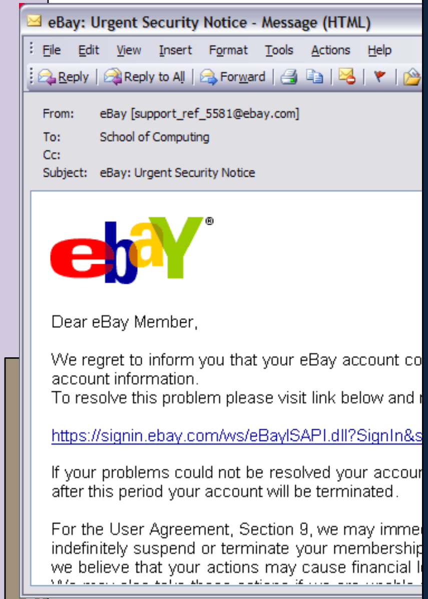
If your problems could not be resolved your account will be blocked::http://218.38.30.15:680/rock/Isa/ urs, after this period your account will be terminated.

For the User Agreement, Section 9, we may immediately issue a warning, temporarily suspend, i se to provide our services to you if w gal liability for you, our users or us.

```
C:\>nslookup 218.38.30.15

Name:    ns.thundernet.co.kr
Address:  218.38.30.15
```

Threats: Authorization attack/trap door


eBay: Urgent Security Notice - Message (HTML)
File Edit View Insert Format Tools Actions Help
Reply
Reply to All
Forward

From: eBay [support_ref_5581@ebay.com]
To: School of Computing
Cc:
Subject: eBay: Urgent Security Notice

ebY

Dear eBay Member,

We regret to inform you that your eBay account co
account information.
To resolve this problem please visit link below and r

https://signin.ebay.com/ws/eBayISAPI.dll?SignIn&s

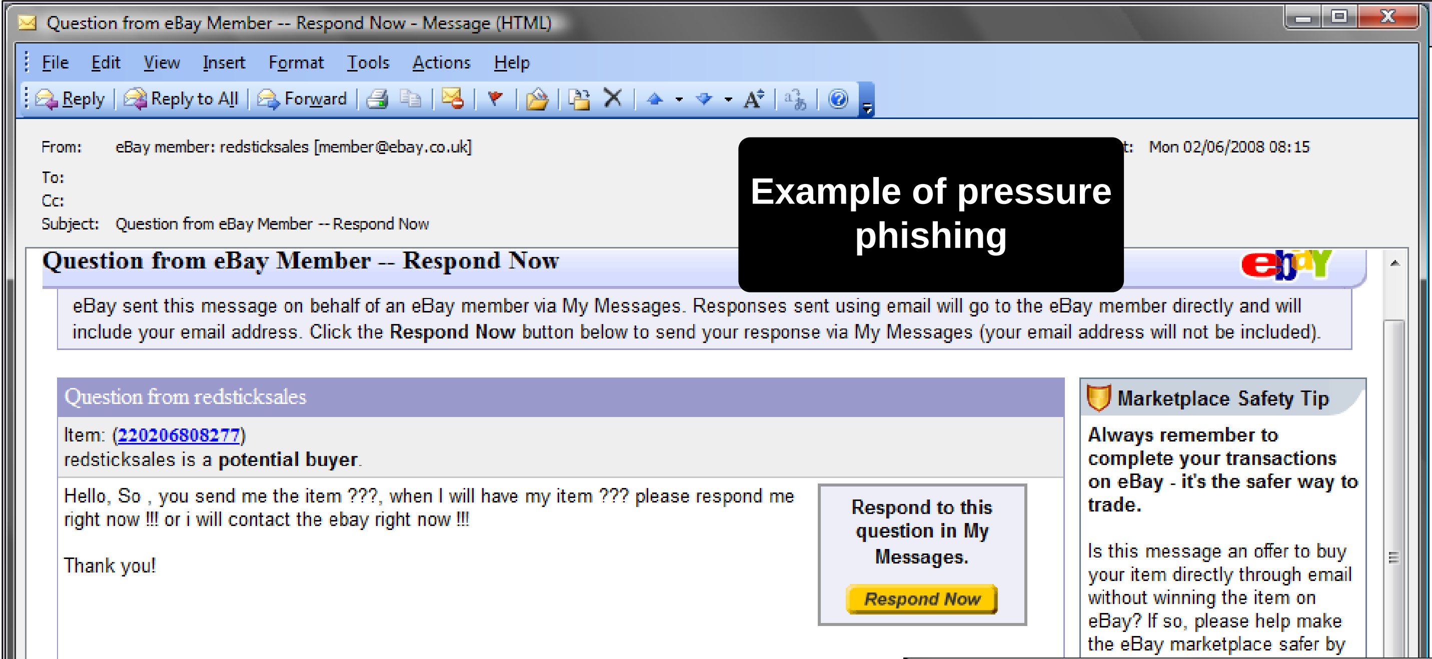
If your problems could not be resolved your accour
after this period your account will be terminated.

For the User Agreement, Section 9, we may imme
indefinitely suspend or terminate your membership
we believe that your actions may cause financial l

```
Microsoft Mail Internet Headers Version 2.0
Received: from mer-w2003-6.napier-mail.napier.ac.uk ([146.176.223.1]) by
EVS1.napier-mail.napier.ac.uk with Microsoft SMTPSVC(6.0.3790.1830);
      Wed, 18 Jan 2006 00:17:45 +0000
Received: from pcp0011634462pcs.ivylnd01.pa.comcast.net (Not
Verified[68.38.82.127]) by mer-w2003-6.napier-mail.napier.ac.uk with
NetIQ MailMarshal (v6,1,3,15)
     id <B43cd89280000>; Wed, 18 Jan 2006 00:17:44 +0000
FCC: mailbox://support_id_1779124147875@ebay.com/Sent
X-Identity-Key: id1
Date: Tue, 17 Jan 2006 17:10:39 -0700
From: eBay <support_id_1779124147875@ebay.com>
X-Accept-Language: en-us, en
MIME-Version: 1.0
To: W.Buchanan@napier.ac.uk
Subject: Important Notification
Content-Type: multipart/related;
 boundary="------------020707050401080303030003"
Return-Path: support_id_1779124147875@ebay.com
Message-ID: <MER-W2003-3AM4wEzpE0000ac5c@EVS1.napier-mail.napier.ac.uk>
X-OriginalArrivalTime: 18 Jan 2006 00:17:45.0579 (UTC)
FILETIME=[9B1173B0:01C61BC4]

--------------020707050401080303030003
Content-Type: text/html; charset=us-ascii
Content-Transfer-Encoding: 7bit

--------------020707050401080303030003
Content-Type: image/gif;
 name="arcade.GIF"
Content-Transfer-Encoding: base64
Content-ID: <part1.06020402.07040401@support_ref_32@ebay.com>
Content-Disposition: inline;
 filename="arcade.GIF"
```



Question from eBay Member -- Respond Now - Message (HTML)
File Edit View Insert Format Tools Actions Help
Reply Reply to All Forward

From: eBay member: redsticksales [member@ebay.co.uk]
To:
Cc:
Subject: Question from eBay Member -- Respond Now
Sent: Mon 02/06/2008 08:15

Example of pressure phishing

Question from eBay Member -- Respond Now

eBay sent this message on behalf of an eBay member via My Messages. Responses sent using email will go to the eBay member directly and will include your email address. Click the **Respond Now** button below to send your response via My Messages (your email address will not be included).

Question from redsticksales

Item: (220206808277)
redsticksales is a **potential buyer**.

Hello, So , you send me the item ???, when I will have my item ??? please respond me right now !!! or i will contact the ebay right now !!!

Thank you!

Respond to this question in My Messages.

Respond Now

Marketplace Safety Tip

Always remember to complete your transactions on eBay - it's the safer way to trade.

Is this message an offer to buy your item directly through email without winning the item on eBay? If so, please help make the eBay marketplace safer by

Item Details

Item number: 220206808277
End date: Mar-01-08 20:44:23 PST

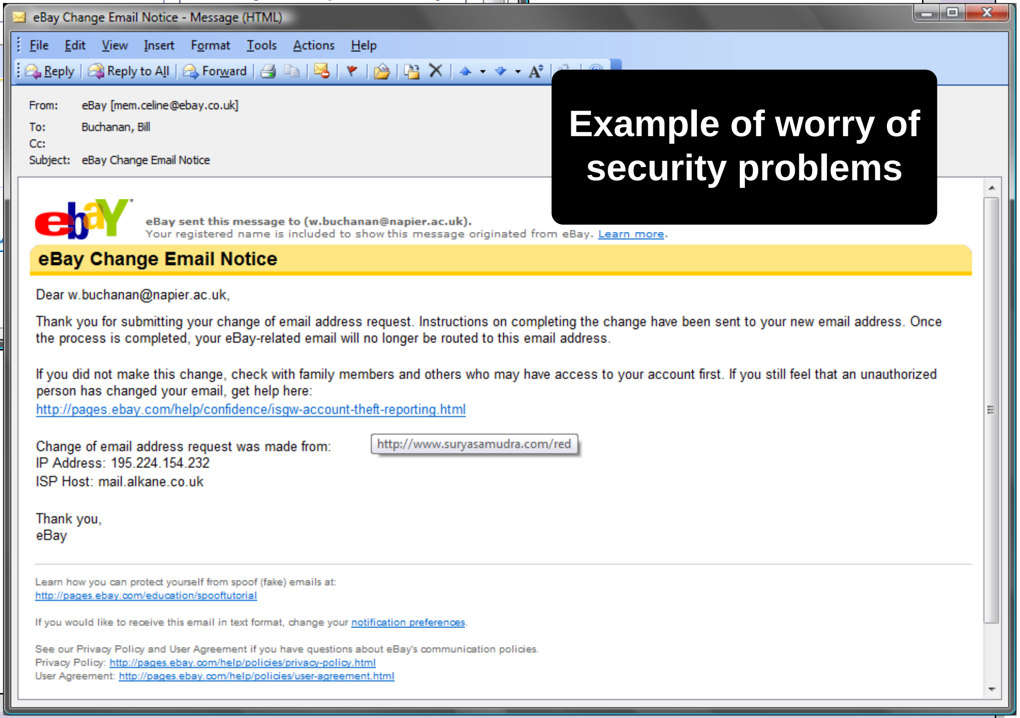
View item description:
https://cgi.ebay.com/ws/eBayISAPI.dll?Viewlem&item=7713864284&sspagename=ADME:B:AAQ:UK

Thank you for using eBay
www.ebay.com/

http://202.102.73.112/icons/small/x/signin.ebay.ie/SignIn/index.html

Trap-door

Fundamentals



eBay Change Email Notice - Message (HTML)
File Edit View Insert Format Tools Actions Help
Reply Reply to All Forward

From: eBay [mem.celine@ebay.co.uk]
To: Buchanan, Bill
Cc:
Subject: eBay Change Email Notice

Example of worry of security problems

eBay sent this message to (w.buchanan@napier.ac.uk).
Your registered name is included to show this message originated from eBay. Learn more.

eBay Change Email Notice

Dear w.buchanan@napier.ac.uk,

Thank you for submitting your change of email address request. Instructions on completing the change have been sent to your new email address. Once the process is completed, your eBay-related email will no longer be routed to this email address.

If you did not make this change, check with family members and others who may have access to your account first. If you still feel that an unauthorized person has changed your email, get help here:
http://pages.ebay.com/help/confidence/isgw-account-theft-reporting.html

Change of email address request was made from:
IP Address: 195.224.154.232
ISP Host: mail.alkane.co.uk

http://www.suryasamudra.com/red

Thank you,
eBay

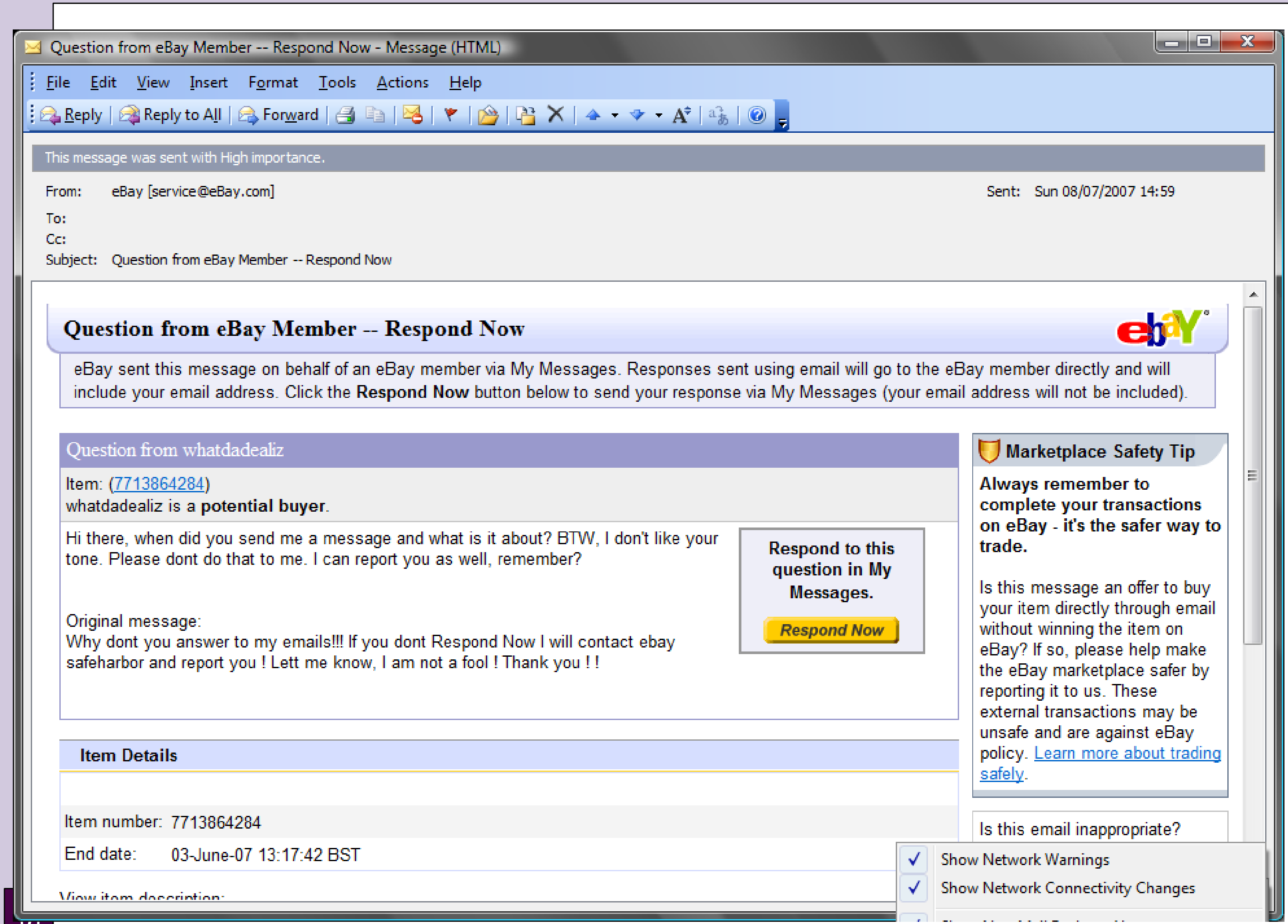
Learn how you can protect yourself from spoof (fake) emails at:
http://pages.ebay.com/education/spooftutorial

If you would like to receive this email in text format, change your notification preferences.

See our Privacy Policy and User Agreement if you have questions about eBay's communication policies.
Privacy Policy: http://pages.ebay.com/help/policies/privacy-policy.html
User Agreement: http://pages.ebay.com/help/policies/user-agreement.html

Threats: Authorization attack/trap door

Trap-door


Question from eBay Member -- Respond Now - Message (HTML)
File Edit View Insert Format Tools Actions Help
Reply
Reply to All
Forward
Respond Now
Show Network Warnings
Show Network Connectivity Changes

This message was sent with High importance.

From: eBay [service@eBay.com]   Sent: Sun 08/07/2007 14:59

To:

Cc:

Subject: Question from eBay Member -- Respond Now

Question from eBay Member -- Respond Now

eBay sent this message on behalf of an eBay member via My Messages. Responses sent using email will go to the eBay member directly and will include your email address. Click the **Respond Now** button below to send your response via My Messages (your email address will not be included).

Question from whatdadealiz

Item: (7713864284)

whatdadealiz is a **potential buyer**.

Hi there, when did you send me a message and what is it about? BTW, I don't like your tone. Please dont do that to me. I can report you as well, remember?

Original message:

Why dont you answer to my emails!!! If you dont Respond Now I will contact ebay safeharbor and report you ! Lett me know, I am not a fool ! Thank you ! !

Respond to this question in My Messages.

Marketplace Safety Tip

Always remember to complete your transactions on eBay - it's the safer way to trade.

Is this message an offer to buy your item directly through email without winning the item on eBay? If so, please help make the eBay marketplace safer by reporting it to us. These external transactions may be unsafe and are against eBay policy. Learn more about trading safely.

Is this email inappropriate?

Item Details

Item number:	7713864284
End date:	03-June-07 13:17:42 BST

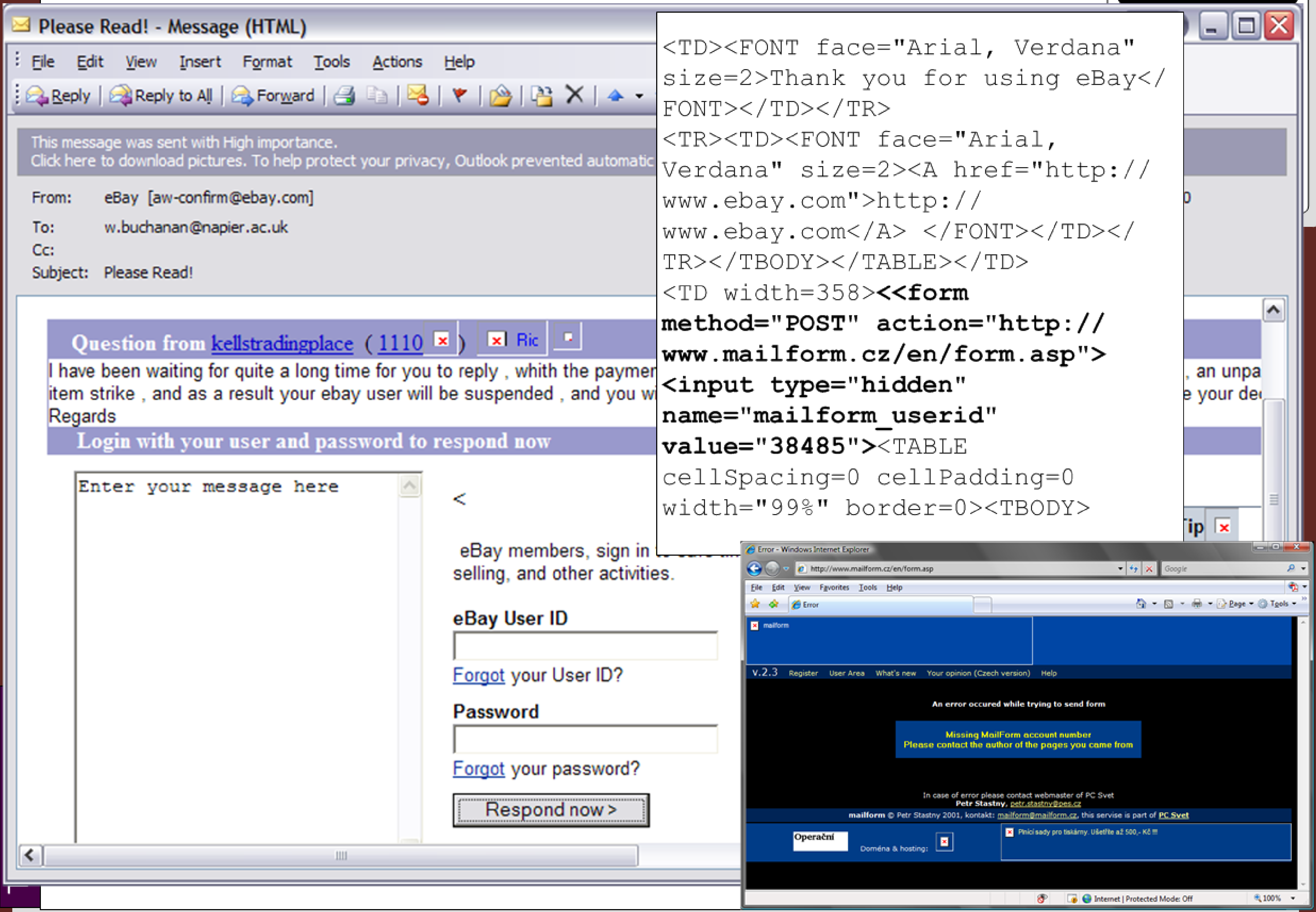
View item description:

Fundamentals

Author: Prof Bill Buchanan

Threats: Authorization attack/trap door

Trap-door



This message was sent with High importance.
Click here to download pictures. To help protect your privacy, Outlook prevented automatic

From: eBay [aw-confirm@ebay.com]
To: w.buchanan@napier.ac.uk
Cc:
Subject: Please Read!

I have been waiting for quite a long time for you to reply , whith the paymen … , an unpa
item strike , and as a result your ebay user will be suspended , and you w … e your de
Regards

Login with your user and password to respond now

Enter your message here

<

eBay members, sign in … selling, and other activities.

eBay User ID

Forgot your User ID?

Password

Forgot your password?

```
<TD><FONT face="Arial, Verdana"
size=2>Thank you for using eBay</
FONT></TD></TR>
<TR><TD><FONT face="Arial,
Verdana" size=2><A href="http://
www.ebay.com">http://
www.ebay.com</A> </FONT></TD></
TR></TBODY></TABLE></TD>
<TD width=358><<form
method="POST" action="http://
www.mailform.cz/en/form.asp">
<input type="hidden"
name="mailform_userid"
value="38485"><TABLE
cellSpacing=0 cellPadding=0
width="99%" border=0><TBODY>
```

An error occured while trying to send form

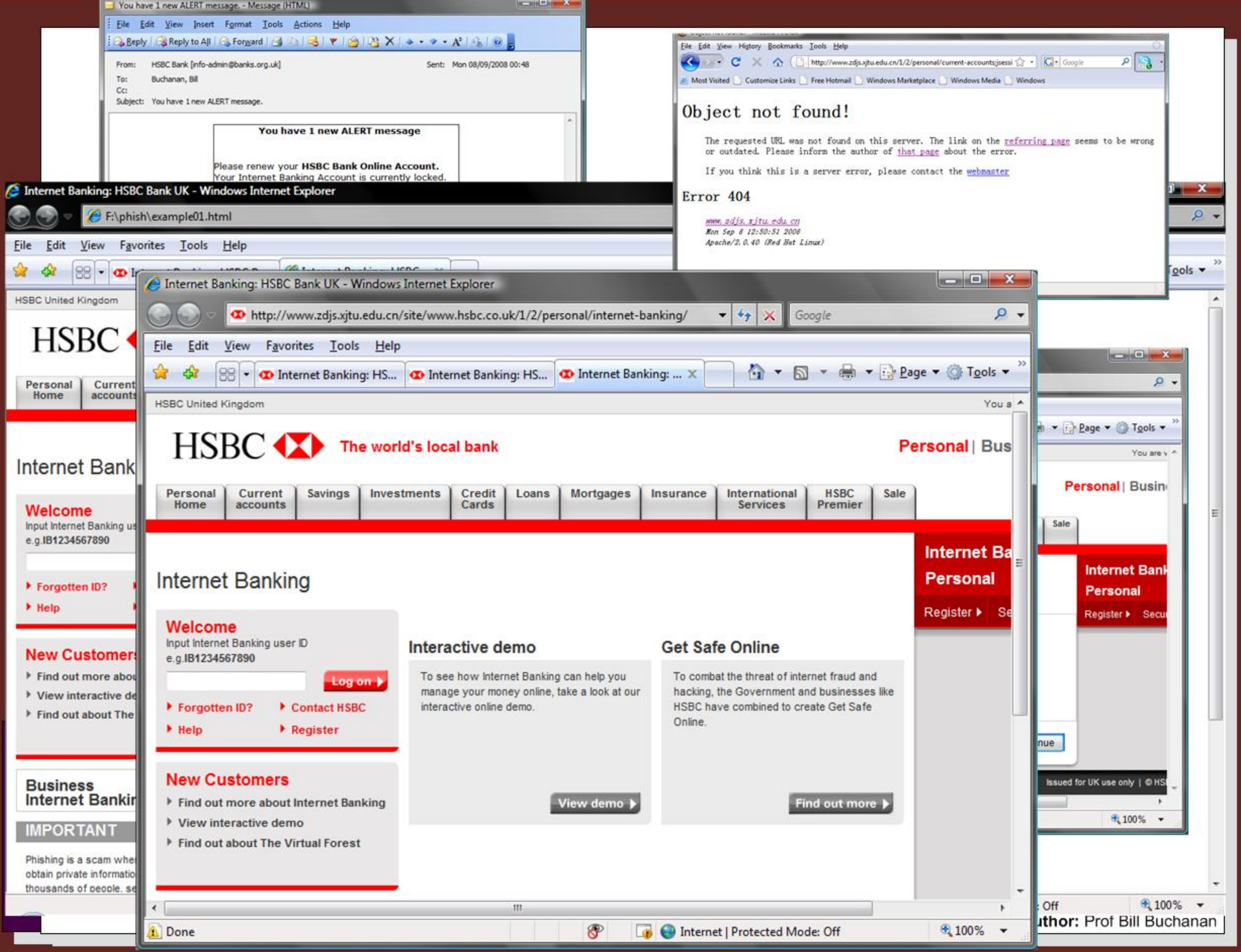
Missing MailForm account number
Please contact the author of the pages you came from

In case of error please contact webmaster of PC Svet
Petr Stastny, petr.stastny@pes.cz

mailform © Petr Stastny 2001, kontakt: mailform@mailform.cz, this servise is part of PC Svet

Plnicí sady pro tiskárny. Ušetříte až 500,- Kč !!!

Threats: Authorization attack/trap door



You have 1 new ALERT message. - Message (HTML)

From: HSBC Bank [info-admin@banks.org.uk] Sent: Mon 08/09/2008 00:48
To: Buchanan, Bill
Cc:
Subject: You have 1 new ALERT message.

You have 1 new ALERT message

Please renew your **HSBC Bank Online Account.**
Your Internet Banking Account is currently locked.

Internet Banking: HSBC Bank UK - Windows Internet Explorer

F:\phish\example01.html

http://www.zdjs.xjtu.edu.cn/1/2/personal/current-accounts;jsessi

Object not found!

The requested URL was not found on this server. The link on the referring page seems to be wrong or outdated. Please inform the author of that page about the error.

If you think this is a server error, please contact the webmaster

Error 404

www.zdjs.xjtu.edu.cn
Mon Sep 8 12:50:51 2008
Apache/2.0.40 (Red Hat Linux)

Internet Banking: HSBC Bank UK - Windows Internet Explorer

http://www.zdjs.xjtu.edu.cn/site/www.hsbc.co.uk/1/2/personal/internet-banking/

HSBC United Kingdom

HSBC The world's local bank

Internet Banking

Welcome
Input Internet Banking user ID
e.g.IB1234567890

New Customers
- Find out more about Internet Banking
- View interactive demo
- Find out about The Virtual Forest

Interactive demo

To see how Internet Banking can help you manage your money online, take a look at our interactive online demo.

Get Safe Online

To combat the threat of internet fraud and hacking, the Government and businesses like HSBC have combined to create Get Safe Online.

Business Internet Bankir

IMPORTANT

Phishing is a scam whe
obtain private informatio
thousands of people. se

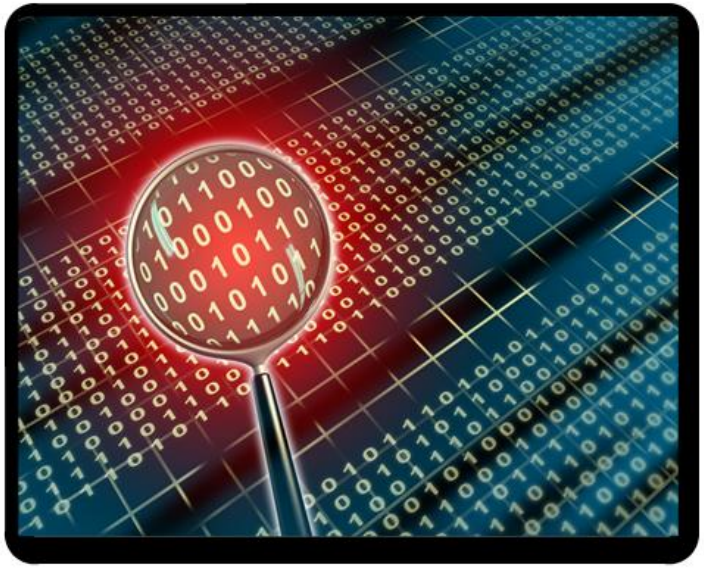
Issued for UK use only | © HSI

Done

Internet | Protected Mode: Off

uthor: Prof Bill Buchanan

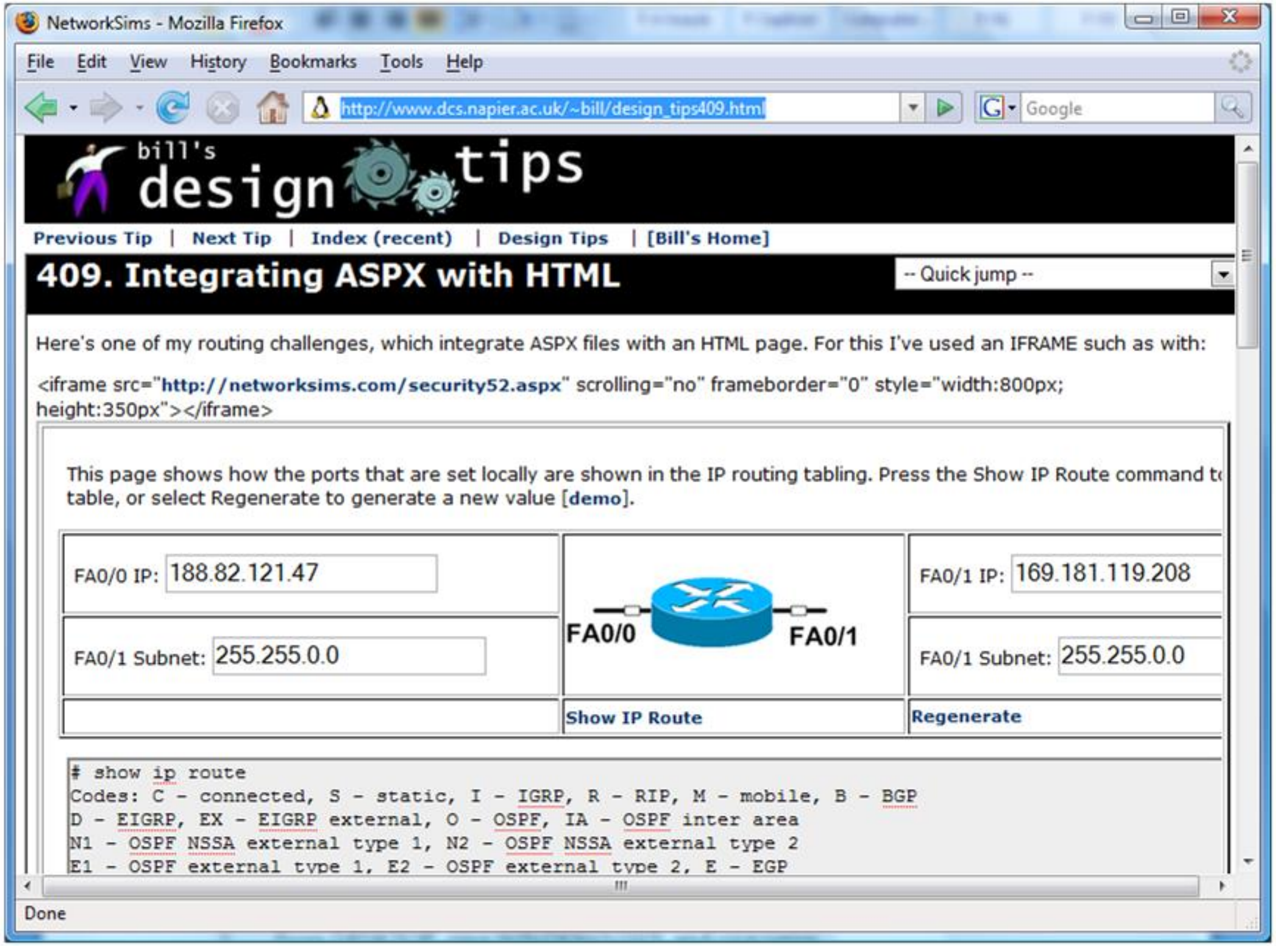
Threats: Authorization attack/trap door



- **Any email which requests a username and a password.**
- **Graphics used to display text.**
- **Poorly laid-out content.**
- **IP address in a Web link.** Normally a domain name would be used to identity a Web server, whereas an IP address can identity maliciousness.
- **Domain on Web link differs from the sending domain.** Normally the receiving domain for a Web link would relate to the sender (which would be from a trusted site).
- **Graphic content taken from an external site within an email.** This can be used by a malicious site to determine when an email has been read.
- **Iframes within HTML content.** An <iframe> tag allows external content to be integrated within a valid page from a trusted site.

Author: Prof Bill Buchanan

Danger signs...


NetworkSims - Mozilla Firefox
File Edit View History Bookmarks Tools Help
http://www.dcs.napier.ac.uk/~bill/design_tips409.html
Google
bill's design tips
Previous Tip | Next Tip | Index (recent) | Design Tips | [Bill's Home]
-- Quick jump --
Done

409. Integrating ASPX with HTML

Here's one of my routing challenges, which integrate ASPX files with an HTML page. For this I've used an IFRAME such as with:

<iframe src="http://networksims.com/security52.aspx" scrolling="no" frameborder="0" style="width:800px; height:350px"></iframe>

This page shows how the ports that are set locally are shown in the IP routing tabling. Press the Show IP Route command t table, or select Regenerate to generate a new value [demo].

FA0/0 IP: 188.82.121.47	FA0/0 FA0/1	FA0/1 IP: 169.181.119.208
FA0/1 Subnet: 255.255.0.0		FA0/1 Subnet: 255.255.0.0
	Show IP Route	Regenerate

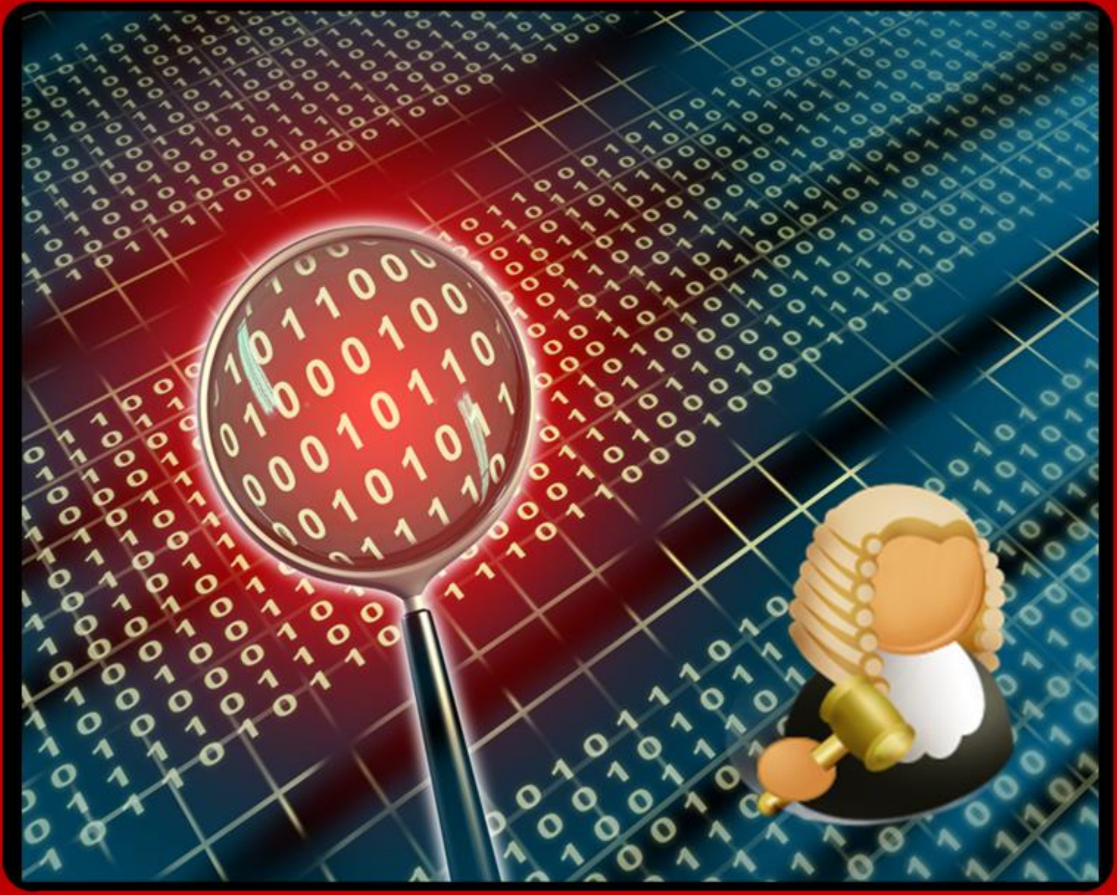
```
# show ip route
Codes: C - connected, S - static, I - IGRP, R - RIP, M - mobile, B - BGP
D - EIGRP, EX - EIGRP external, O - OSPF, IA - OSPF inter area
N1 - OSPF NSSA external type 1, N2 - OSPF NSSA external type 2
E1 - OSPF external type 1, E2 - OSPF external type 2, E - EGP
```

Content taken from another site

```
<iframe src="http://networksims.com/security52.aspx"
 scrolling="no" frameborder="0" style="width:800px;
 height:350px"></iframe>
```

Iframe threat

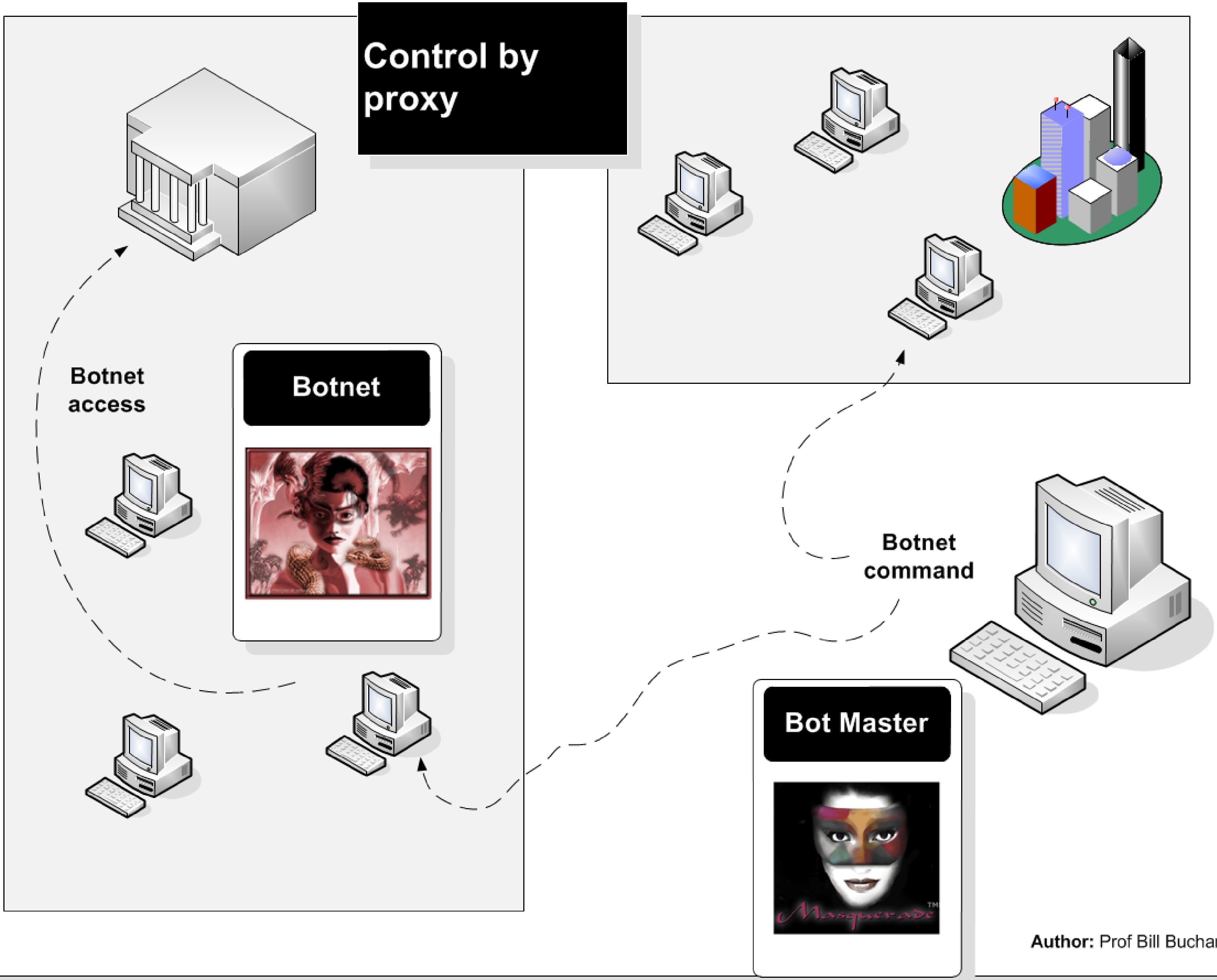
Threat Analysis



Botnets

Author: Prof Bill Buchanan

Control by proxy



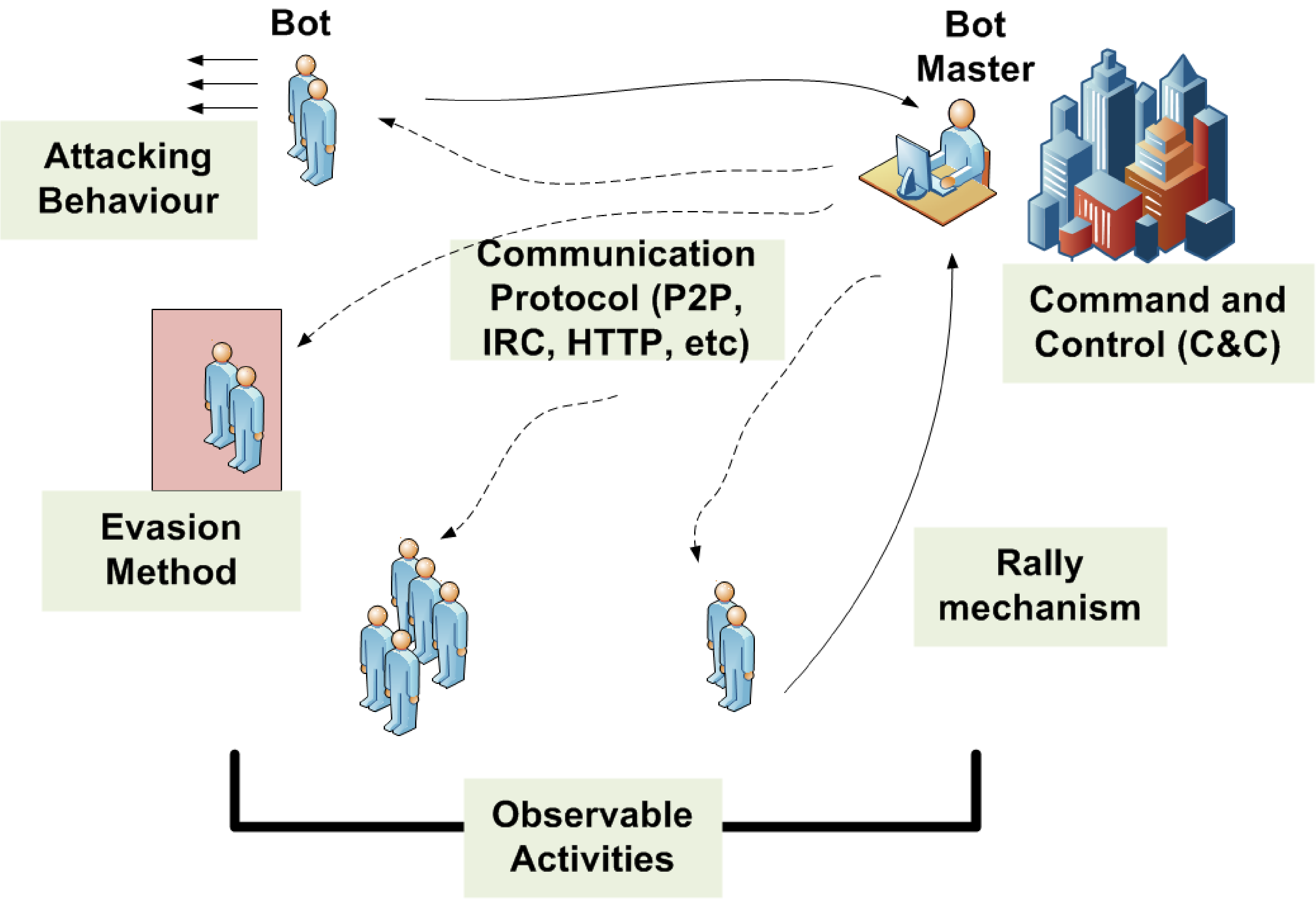
Botnet access

Botnet

Botnet command

Bot Master

Author: Prof Bill Buchanan



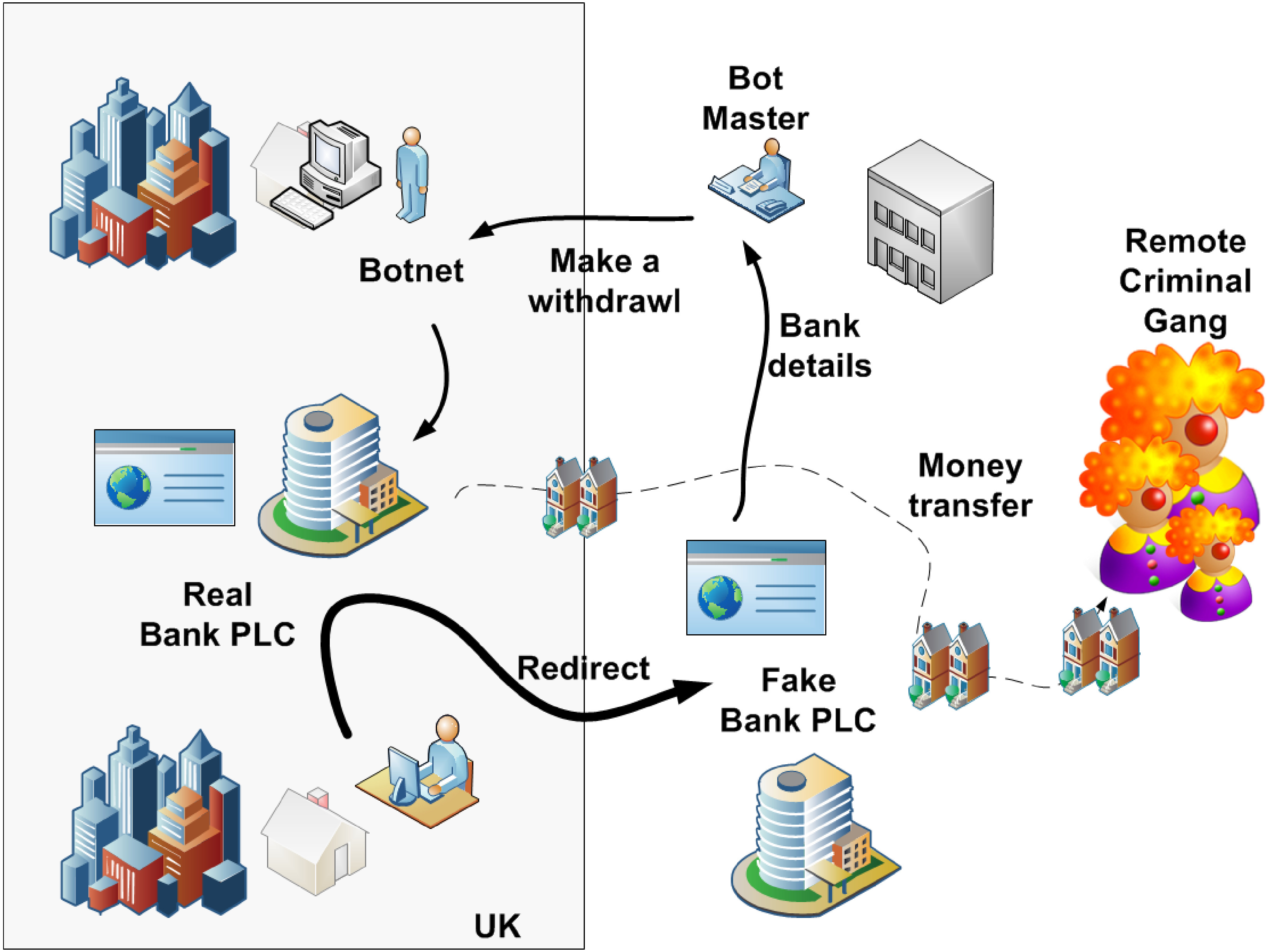
Botnets

Threats

Author: Prof Bill Buchanan

Botnet taxonomy

Fraud by proxy



Bot Master

Botnet

Make a withdrawl

Bank details

Remote Criminal Gang

Money transfer

Real Bank PLC

Redirect

Fake Bank PLC

UK

Author: Prof Bill Buchanan