Impersonation

CS 161: Computer Security
Prof. Vern Paxson
TAs: Devdatta Akhawe, Mobin Javed
& Matthias Vallentin

http://inst.eecs.berkeley.edu/~cs161/

March 1, 2011
Announcements

• Midterm next Tuesday March 8th
  – Scope is course material up through today
  – You can bring a *single sheet* of notes
    • Two-sided, viewable w/o assistance
    • (FYI: you might want to keep this for the final)

• My office hours the week of March 7th will be by appointment

• **Guest lecture** this Thursday (March 3rd), Prof. David Wagner

• Reminder, HW #2 due **5PM** on Friday
Goals For Today

• A broad look at the problem of *impersonation*: threats based on something not being what it appears to be
• Web attacks: misleading users regarding their clicks
• Phishing: misleading users regarding with whom they are interacting
• CAPTCHAs: telling humans apart from “bots”
• Analyzing email headers for legitimacy (time permitting)
Attacks on User Volition

• Browser assumes clicks & keystrokes = clear indication of what the user wants to do
  – Constitutes part of the user’s trusted path

• Attack #1: commandeer the focus of user-input

• Attack #2: mislead the user regarding true focus ("click-jacking")
Click-Jacking

• Demo #1: you think you’re typing to a familiar app, but you’re not (demo)
Click-Jacking

• Demo #1: you think you’re typing to a familiar app, but you’re not

• Demo #2: you don’t think you’re typing to a familiar app, but you are (demo)
BEST GAME EVER!
Global Security Settings panel

Some websites may access information from other sites using an older system of security. This is usually harmless, but it is possible that some sites could obtain unauthorized information using the older system. When a website attempts to use the older system to access information:

- Always ask
- Always allow
- Always deny

Always trust files in these locations:
Click-Jacking

• Demo #1: you think you’re typing to a familiar app, but you’re not

• Demo #2: you don’t think you’re typing to a familiar app, but you are
  • You might click on what the attacker wants no matter where you click! (demo)
Click-Jacking

• Demo #1: you think you’re typing to a familiar app, but you’re not

• Demo #2: you don’t think you’re typing to a familiar app, but you are

• Demo #3: you definitely meant to click somewhere else
Adblock Plus 1.1.3
by Wladimir Palant

Ever been annoyed by all those ads and banners on the internet that often take longer to download than everything else on the page? Install Adblock Plus now and get rid of them.

For a quick overview watch http://www.youtube.com/watch?v=ONvb2Jvjl

See All Privacy & Security Add-ons

Other add-ons by Wladimir Palant
- Adblock Plus

Need help with this add-on?
- Visit the support site
Install add-ons only from authors whom you trust.

Malicious software can damage your computer or violate your privacy.

You have asked to install the following item:

Adblock Plus  (Wladimir Palant)

Cancel  Install (5)
Install add-ons only from authors whom you trust.

Malicious software can damage your computer or violate your privacy.

You have asked to install the following item:

Adblock Plus  (Wladimir Palant)

[Buttons: Cancel, Install (4)]
Install add-ons only from authors whom you trust.

Malicious software can damage your computer or violate your privacy.

You have asked to install the following item:

Adblock Plus  (Wladimir Palant)
Install add-ons only from authors whom you trust.
Malicious software can damage your computer or violate your privacy.

You have asked to install the following item:

Adblock Plus  (Wladimir Palant)

[Buttons: Cancel, Install (2)]
Install add-ons only from authors whom you trust.

Malicious software can damage your computer or violate your privacy.

You have asked to install the following item:

Adblock Plus  (Wladimir Palant)

[Buttons: Cancel, Install (1)]
Why Does Firefox Make You Wait?

... to keep you from being tricked into clicking!
Defending Against Clickjacking

• Main defense: *frame busting*
• Web site ensures that its “vulnerable” pages can’t be included as a *frame* inside another browser frame
Attacker implements this by placing Twitter’s page in a “Frame” inside their own page. Otherwise they wouldn’t overlap.
Defending Against Clickjacking

- Main defense: *frame busting*
- Web site ensures that its “vulnerable” pages can’t be included as a frame inside another browser frame
  - So user can’t be looking at it with something invisible overlaid on top …
  - … nor have the site invisible above something else
- Conceptually implemented with Javascript like:
  
  ```javascript
  if (top.location != self.location)
    top.location = self.location;
  ```
- (Note: actually quite tricky to get this right!)
Related UI Sneakiness

• Demo #1: you think you’re typing to a familiar app, but you’re not
• Demo #2: you don’t think you’re typing to a familiar app, but you are
• Demo #3: you definitely meant to click somewhere else

• Demo #4: you’ve got a lot on your mind (demo)
Related UI Sneakiness

• Demo #1: you think you’re typing to a familiar app, but you’re not
• Demo #2: you don’t think you’re typing to a familiar app, but you are
• Demo #3: you definitely meant to click somewhere else

• Demo #4: you’ve got a lot on your mind (demo)
  • Tabnabbing
Related UI Sneakiness

• Demo #1: you think you’re typing to a familiar app, but you’re not
• Demo #2: you don’t think you’re typing to a familiar app, but you are
• Demo #3: you definitely meant to click somewhere else

• Demo #4: you’ve got a lot on your mind (demo)
  • Tabnabbing
• Demo #5: you’re living in *The Matrix*
“Browser in Browser”

Apparent browser is just a **fully interactive image** generated by script running in real browser!
5 Minute Break

Questions Before We Proceed?
Phishing
I can do for $385.00 with shipping. Waiting for your answer asap.

Thank you.

Did this answer your question? If not, let the seller know.

View Item:  http://cgi.ebay.com/ws/eBayISAPI.dll?ViewItem&item=130312669787

Item Id:  130312669787
End time:  Mar 03, 2011 09:38:06 PDT
Buyer:  pajv21 ( 381 ⭐ )
Feedback: 100 % Positive
Member: since 26-May-06
Location: United States

Listing Status: This message was sent while the listing was active.

Marketplace Safety Tip

- Keep your money safe - never pay for items with cash or instant money transfer services, such as Western Union or MoneyGram. In the past some sellers have exploited these payment methods in order to defraud buyers, so eBay has banned them from the site.
Welcome to eBay

Ready to bid and buy? Register here

Join the millions of people who are already a part of the eBay family. Don't worry, we have room for one more.

Register as an eBay Member and enjoy privileges including:
- Bid, buy and find bargains from all over the world
- Shop with confidence with PayPal Buyer Protection
- Connect with the eBay community and more!

Sign in to your account

Back for more fun? Sign in now to buy, bid and sell, or to manage your account.

User ID
I forgot my user ID

Password
I forgot my password

Keep me signed in for today. Don't check this box if you're at a public or shared computer.

Sign in

Having problems with signing in? Get help.

Protect your account: Create a unique password by using a combination of letters and numbers that are not
Welcome to eBay

Ready to bid and buy? Register here

Join the millions of people who are already a part of the eBay family. Don't worry, we have room for one more.

Register as an eBay Member and enjoy privileges including:

- Bid, buy and find bargains from all over the world
- Shop with confidence with PayPal Buyer Protection
- Connect with the eBay community and more!

Sign in to your account

Back for more fun? Sign in now to buy, bid and sell, or to manage your account.

User ID: joebob
I forgot my user ID

Password: ************
I forgot my password

Keep me signed in for today. Don't check this box if you're at a public or shared computer.

Having problems with signing in? Get help.

Protect your account: Create a unique password by using a combination of letters and numbers that are not
Please confirm your identity jbieber

Please answer security question below.

What is your mother’s maiden name?

Smith

Answer the secret question you provided.

What is your other eBay user ID or another’s member in your household?

NA

What email used to be associated with this account?

bieberlicious@hotmail.com

Have you ever sold something on eBay?
Thanks j Bieber. Your identity has been confirmed.

Now you can pick up where you left off.

Save Profile
This listing (350121605127) has been removed, or this item is not available.

- Please check that you've entered the correct item number.
- Listings that have ended 90 or more days ago will not be available for viewing.
The Problem of Phishing

• Arises due to mismatch between reality & user’s:
  – Perception of how to assess legitimacy
  – Mental model of what attackers can control
    • Both Email and Web

• Coupled with:
  – Deficiencies in how web sites authenticate
    • In particular, “replayable” authentication that is vulnerable to theft

• How can we tell when we’re being phished?
I can do for $385.00 with shipping. Waiting for your answer asap.

Thank you.

View Item:  http://cgi.ebay.com/ws/eBayISAPI.dll?ViewItem&item=130312669787

Item Id:  130312669787
End time:  Mar 03, 2011 09:38:06 PDT
Buyer:  pajv21 ( 381 ⭐️ )
Feedback: 100 % Positive
Member:  since 26-May-06
Location:  United States

Listing Status:  This message was sent while the listing was active.

Marketplace Safety Tip

- Keep your money safe - never pay for items with cash or instant money transfer services, such as Western Union or MoneyGram. In the past some sellers have exploited these payment methods in order to defraud buyers, so eBay has banned them from the site.
Message from eBay member, pajv21

Do not respond to the sender if this message requests that you complete the transaction outside of eBay. This type of offer is against eBay policy, may be fraudulent, and is not covered by buyer protection programs. Learn More.

I can do for $385.00 with shipping. Waiting for your answer asap.

Thank you.

View Item:  http://cgi.ebay.com/ws/eBayISAPI.dll?ViewItem&item=130312669787

Item Id:  130312669787
End time:  Mar 03, 2011 09:38:06 PDT
Buyer:  pajv21 ( 381 ⭐️ )
Feedback: 100 % Positive
Member: since 26-May-06
Location: United States
Listing Status: This message was sent while the listing was active.

Marketplace Safety Tip

- Keep your money safe - never pay for items with cash or instant money transfer services, such as Western Union or MoneyGram. In the past some sellers have exploited these payment methods in order to defraud buyers, so eBay has banned them from the site.
Check the URL before clicking?

<a href="http://www.ebay.com/
onclick="location='http://hackrz.com/"">
Welcome to eBay

Ready to bid and buy? Register here

Join the millions of people who are already a part of the eBay family. Don't worry, we have room for one more.

Register as an eBay Member and enjoy privileges including:

- Bid, buy and find bargains from all over the world
- Shop with confidence with PayPal Buyer Protection
- Connect with the eBay community and more!

Sign in to your account

Back for more fun? Sign in now to buy, bid and sell, or to manage your account.

User ID
I forgot my user ID

Password
I forgot my password

Keep me signed in for today. Don't check this box if you're at a public or shared computer.

Sign in

Having problems with signing in? Get help.

Protect your account: Create a unique password by using a combination of letters and numbers that are not
Exploits a misfeature in IE that interprets a number here as a 32-bit IP address
dig -x 189.89.71.227

; <<>> DiG 9.6.0-APPLE-P2 <<>> -x 189.89.71.227
;; global options: +cmd
;; Got answer:
;; ->>HEADER<<- opcode: QUERY, status: NOERROR, id: 24037
;; flags: qr rd ra; QUERY: 1, ANSWER: 1, AUTHORITY: 2, ADDITIONAL: 0

;; QUESTION SECTION:
;227.71.89.189.in-addr.arpa. IN PTR

;; ANSWER SECTION:
227.71.89.189.in-addr.arpa. 86400 IN PTR 227.71.89.189.cliente.interjato.com.br.

;; AUTHORITY SECTION:
71.89.189.in-addr.arpa. 86399 IN NS ns2.interjato.com.br.
71.89.189.in-addr.arpa. 86399 IN NS ns1.interjato.com.br.

;; Query time: 511 msec
;; SERVER: 128.32.153.21#53(128.32.153.21)
;; WHEN: Tue Mar 1 17:37:52 2011
;; MSG SIZE  rcvd: 132
whois 189.89.71.227

# The following results may also be obtained via:
# http://whois.arin.net/rest/nets;q=189.89.71.227?showDetails=true&showA
#
#

NetRange: 189.0.0.0 - 189.255.255.255
CIDR: 189.0.0.0/8
OriginAS:
NetName: NET189
NetHandle: NET-189-0-0-0-1
Parent:
NetType: Allocated to LACNIC
...
...
inetnum: 189.89.64/20
aut-num: AS28184
abuse-c: EMR5
owner: TECHNET NETWORKING LTDA
ownerid: 000.872.797/0001-17
responsible: Erich matos Rodrigues
country: BR
Check the URL in address bar?
Welcome to eBay

Ready to bid and buy? Register here

Join the millions of people who are already a part of the eBay family. Don't worry, we have room for one more.

Register as an eBay Member and enjoy privileges including:

- Bid, buy and find bargains from all over the world
- Shop with confidence with PayPal Buyer Protection
- Connect with the eBay community and more!

Register

Sign in to your account

Back for more fun? Sign in now to buy, bid and sell, or to manage your account.

User ID
I forgot my user ID

Password
I forgot my password

Keep me signed in for today. Don't check this box if you're at a public or shared computer.

Sign In

Having problems with signing in? Get help.

Protect your account: Check that the Web address in your browser starts with https://signin.ebay.com/. More account security tips.
Homograph Attacks

• International domain names can use international character set
  – E.g., Chinese contains characters that look like / . ? =

• **Attack**: Legitimately register var.cn ...

• ... buy legitimate set of HTTPS certificates for it ...

• ... and then create a subdomain:
  www.pnc.com/webapp/unsec/homepage.var.cn
Check for padlock?
Add a clever .favicon with a picture of a padlock
Check for “green glow” in address bar?
Check for everything?
“Browser in Browser”
“Spear Phishing”

From: Lab.senior.manager@gmail.com
Subject: FW: Agenda
Body: This below agenda just came in form from Susan, please look at it.
>From: Norris, Susan (ORO)
>To: Manager, Senior; Rabovsky, Joel MJ
>Subject: Agenda
>Thanks, nice to know that you all care this so much!
>
>Susan Norris
>norrissg@oro.doe.gov
Attached: Agenda Mar 4.pdf

Targeted phishing that includes details that seemingly must mean it’s legitimate
Russian spear phishing attack against .mil and .gov employees

A "relatively large" number of U.S. government and military employees are being taken in by a spear phishing attack which delivers a variant of the Zeus trojan. The email address is spoofed to appear to be from the NSA or InteLink concerning a report by the National Intelligence Council named the "2020 Project". It's purpose is to collect passwords and obtain remote access to the infected hosts.

Security Update for Windows 2000/XP/Vista/7 (KB823988)

About this download: A security issue has been identified that could allow an attacker to remotely compromise a computer running Microsoft Windows and gain complete control over it. You can help protect your computer by installing this update from Microsoft. After you install this item, you may have to restart your computer.

Download:

http://mv.net.md/update/update.zip

or

http://www.sendspace.com/file/xwc1pi

Yep, this is itself a spear-phishing attack!

Jeffrey Carr is the CEO of GreyLogic, the Founder and Principal Investigator of Project Grey Goose, and the author of "Inside Cyber Warfare".
jeffreyc@greylogic.us
Sophisticated phishing

- Context-aware phishing – 10% users fooled
  - Spoofed email includes info related to a recent eBay transaction/listing/purchase
- Social phishing – 70% users fooled
  - Send spoofed email appearing to be from one of the victim’s friends (inferred using social networks)
- West Point experiment
  - Cadets received a spoofed email near end of semester: “There was a problem with your last grade report; click here to resolve it.” 80% clicked.
CAPTCHAs
By clicking the “Create My Account” button below, I certify that I have read and agree to the Yahoo! Terms of Service, Yahoo! Privacy Policy and Communication Terms of Service, and to receive account related communications from Yahoo! electronically. Yahoo! automatically identifies items such as words, links, people, and subjects from your Yahoo! communications services to deliver product features and relevant advertising.
CAPTCHAs

- **Reverse Turing Test**: present “user” a challenge that’s easy for a human to solve, hard for a program to solve
- One common approach: distorted text that’s difficult for character-recognition algorithms to decipher
Figure 1: Examples of CAPTCHAs from various Internet properties.
Issues with CAPTCHAs

• Inevitable arms race: as solving algorithms get better, defense erodes, or gets harder for humans
Click 3 pictures of kittens to submit

The KittenAuth system. Source: ThePCSpy.com.
Issues with CAPTCHAs

- Inevitable arms race: as solving algorithms get better, defense erodes, or gets harder for humans

- **Accessibility**: not all humans can see!
- **Granularity**: not all bots are bad! (e.g., crawlers)
Issues with CAPTCHAs, con’t

• If generating a CAPTCHA is somewhat expensive, *the mechanism itself is a DoS vulnerability*
Clicking this link loads 120,000 copies of the RIAA's captcha. Clicking would be wrong, don't do it. (antisocial.propagation.net)
Issues with CAPTCHAs, con’t

• If generating a CAPTCHA is somewhat expensive, *the mechanism itself is a DoS vulnerability*

• Final problem: CAPTCHAs are inherently vulnerable to *outsourcing* attacks
  – Attacker gets real humans to solve them
Using the advertisement in blogs, social networks, etc significantly increases the efficiency of the business. Many services use pictures called CAPTCHAs in order to prevent automated use of these services.

Solve CAPTCHAs with the help of this portal, increase your business efficiency now!

Following these steps:
1. Register
2. Login and follow the link inside to load funds to your account.
   Your request will be processed ASAP.

**You pay for correctly recognized CAPTCHAs only**
The price is $2 for 1000 CAPTCHAs. We accept payments from $10.

If you use a third-party software the price could be different, contact the software vendor for more information.

Hi! I want to bypass captcha from my bots. Bots have different IPs. Is it possible to use your service from many IPs?
We have no restrictions about IP: with DeCaptcha you can bypass CAPTCHA from as many IPs as you need.

Hi. I need to crack captcha. Do you provide a captcha decoder?
DeCaptcha CAPTCHA solving is processed by humans. So the accuracy is much better than an automated captcha solver ones.
<table>
<thead>
<tr>
<th>Language</th>
<th>Example</th>
<th>AG</th>
<th>BC</th>
<th>BY</th>
<th>CB</th>
<th>DC</th>
<th>IT</th>
<th>All</th>
</tr>
</thead>
<tbody>
<tr>
<td>English</td>
<td>one two three</td>
<td>51.1</td>
<td>37.6</td>
<td>4.76</td>
<td>40.6</td>
<td>39.0</td>
<td>62.0</td>
<td>39.2</td>
</tr>
<tr>
<td>Chinese (Simp.)</td>
<td></td>
<td>48.4</td>
<td>31.0</td>
<td>0.00</td>
<td>68.9</td>
<td>26.9</td>
<td>35.8</td>
<td>35.2</td>
</tr>
<tr>
<td>Chinese (Trad.)</td>
<td></td>
<td>52.9</td>
<td>24.4</td>
<td>0.00</td>
<td>63.8</td>
<td>30.2</td>
<td>33.0</td>
<td>34.1</td>
</tr>
<tr>
<td>Spanish</td>
<td>uno dos tres</td>
<td>1.81</td>
<td>13.8</td>
<td>0.00</td>
<td>2.90</td>
<td>7.78</td>
<td>56.8</td>
<td>13.9</td>
</tr>
<tr>
<td>Italian</td>
<td>uno due tre</td>
<td>3.65</td>
<td>8.45</td>
<td>0.00</td>
<td>4.65</td>
<td>5.44</td>
<td>57.1</td>
<td>13.2</td>
</tr>
<tr>
<td>Tagalog</td>
<td>isá dalawá tatló</td>
<td>0.00</td>
<td>5.79</td>
<td>0.00</td>
<td>0.00</td>
<td>7.84</td>
<td>57.2</td>
<td>11.8</td>
</tr>
<tr>
<td>Portuguese</td>
<td>um dois três</td>
<td>3.15</td>
<td>10.1</td>
<td>0.00</td>
<td>1.48</td>
<td>3.98</td>
<td>48.9</td>
<td>11.3</td>
</tr>
<tr>
<td>Russian</td>
<td>один два три</td>
<td>24.1</td>
<td>0.00</td>
<td>0.00</td>
<td>11.4</td>
<td>0.55</td>
<td>16.5</td>
<td>8.76</td>
</tr>
<tr>
<td>Tamil</td>
<td>ஒன்று இரண்டு மூன்று</td>
<td>2.26</td>
<td>21.1</td>
<td>3.26</td>
<td>0.74</td>
<td>12.1</td>
<td>5.36</td>
<td>7.47</td>
</tr>
<tr>
<td>Dutch</td>
<td>een twee drie</td>
<td>4.09</td>
<td>1.36</td>
<td>0.00</td>
<td>0.00</td>
<td>1.22</td>
<td>31.1</td>
<td>6.30</td>
</tr>
<tr>
<td>Hindi</td>
<td>एक दो तीन</td>
<td>10.5</td>
<td>5.38</td>
<td>2.47</td>
<td>1.52</td>
<td>6.30</td>
<td>9.49</td>
<td>5.94</td>
</tr>
<tr>
<td>German</td>
<td>eins zwei drei</td>
<td>3.62</td>
<td>0.72</td>
<td>0.00</td>
<td>1.46</td>
<td>0.58</td>
<td>29.1</td>
<td>5.91</td>
</tr>
<tr>
<td>Malay</td>
<td>satu dua tiga</td>
<td>0.00</td>
<td>1.42</td>
<td>0.00</td>
<td>0.00</td>
<td>0.55</td>
<td>29.4</td>
<td>5.23</td>
</tr>
<tr>
<td>Vietnamese</td>
<td>molt hai ba</td>
<td>0.46</td>
<td>2.07</td>
<td>0.00</td>
<td>0.00</td>
<td>1.74</td>
<td>18.1</td>
<td>3.72</td>
</tr>
<tr>
<td>Korean</td>
<td>일 이 삼</td>
<td>0.00</td>
<td>0.00</td>
<td>0.00</td>
<td>0.00</td>
<td>0.00</td>
<td>20.2</td>
<td>3.37</td>
</tr>
<tr>
<td>Greek</td>
<td>ένα δύο τρία</td>
<td>0.45</td>
<td>0.00</td>
<td>0.00</td>
<td>0.00</td>
<td>15.5</td>
<td>2.65</td>
<td></td>
</tr>
<tr>
<td>Arabic</td>
<td>ثلاثة اثنين واحد</td>
<td>0.00</td>
<td>0.00</td>
<td>0.00</td>
<td>0.00</td>
<td>0.00</td>
<td>15.3</td>
<td>2.56</td>
</tr>
<tr>
<td>Bengali</td>
<td>এক দুই তিন</td>
<td>0.45</td>
<td>0.00</td>
<td>9.89</td>
<td>0.00</td>
<td>0.00</td>
<td>0.00</td>
<td>1.72</td>
</tr>
<tr>
<td>Kannada</td>
<td>ಎರಡು ತಿಂಗಳು</td>
<td>0.91</td>
<td>0.00</td>
<td>0.00</td>
<td>0.00</td>
<td>0.55</td>
<td>6.14</td>
<td>1.26</td>
</tr>
<tr>
<td>Klingon</td>
<td></td>
<td>0.00</td>
<td>0.00</td>
<td>0.00</td>
<td>0.00</td>
<td>0.00</td>
<td>1.12</td>
<td>0.19</td>
</tr>
<tr>
<td>Farsi</td>
<td></td>
<td>0.45</td>
<td>0.00</td>
<td>0.00</td>
<td>0.00</td>
<td>0.00</td>
<td>0.00</td>
<td>0.08</td>
</tr>
</tbody>
</table>

Table 2: Percentage of responses from the services with correct answers for the language CAPTCHAs.
Analyzing Email Headers
To: vern@ee.lbl.gov
Subject: RE: Russian spear phishing attack against .mil and .gov employees
From: jeffreyc@cia.gov
Date: Wed, 10 Feb 2010 19:51:47 +0100

Russian spear phishing attack against .mil and .gov employees

A "relatively large" number of U.S. government and military employees are being taken in by a spear phishing attack which delivers a variant of the Zeus trojan. The email address is spoofed to appear to be from the NSA or InteLink concerning a report by the National Intelligence Council named the "2020 Project". It's purpose is to collect passwords and obtain remote access to the infected hosts.

Security Update for Windows 2000/XP/Vista/7 (KB823988)

About this download: A security issue has been identified that could allow an attacker to remotely compromise a computer running Microsoft Windows and gain complete control over it. You can help protect your computer by installing this update from Microsoft. After you install this item, you may have to restart your computer.

Download:

http://mv.net.md/update/update.zip

or

http://www.sendspace.com/file/xwc1pi

Jeffrey Carr is the CEO of GreyLogic, the Founder and Principal Investigator of Project Grey Goose, and the author of "Inside Cyber Warfare".
jeffreyc@greylogic.us
To: vern@ee.lbl.gov
Subject: RE: Russian spear phishing attack against .mil and .gov emp
From: jeffreyc@cia.gov
Message-Id: <E1NfHf9-0002n7-Md@uw03.uniweb.no>
Date: Wed, 10 Feb 2010 19:51:47 +0100

To/Subject/From/etc. are completely under the attacker’s control
Any headers below them *may also be under the attacker’s control*

To: vern@ee.lbl.gov  
Subject: RE: Russian spear phishing attack against .mil and .gov employees  
From: jeffreyc@cia.gov  
Message-Id: <E1NfHf9-0002n7-Md@uw03.uniweb.no>  
Date: Wed, 10 Feb 2010 19:51:47 +0100  
X-Virus-Scanned: clamav-milter 0.95.3 at ee.lbl.gov  
X-Virus-Status: Clean  
Content-Length: 1116
This header tells us about the first delivery “hop”. It’s supposedly reported by a machine uw03.uniweb.no, but who knows ...

Received: from w63697 by uw03.uniweb.no with local (Exim 4.66) (envelope-from <w63697@uw03.uniweb.no>)
   id 1NfHf9-0002n7-Md
   for vern@ee.lbl.gov; Wed, 10 Feb 2010 19:51:47 +0100
To: vern@ee.lbl.gov
Subject: RE: Russian spear phishing attack against .mil and .gov em...
From: jeffreyc@cia.gov
Message-Id: <E1NfHf9-0002n7-Md@uw03.uniweb.no>
Date: Wed, 10 Feb 2010 19:51:47 +0100
X-Virus-Scanned: clamav-milter 0.95.3 at ee.lbl.gov
X-Virus-Status: Clean
Content-Length: 1116
However, headers for subsequent hops are * prepended. 

So we can start at the **top** of the headers, which came from our trusted mailer, and decide how much trustworthy information we can find …

Received: from w63697 by uw03.uniweb.no with local (Exim 4.66)  
(envelope-from <w63697@uw03.uniweb.no>)  
id 1NfHf9-0002n7-Md  
for vern@ee.lbl.gov; Wed, 10 Feb 2010 19:51:47 +0100  
To: vern@ee.lbl.gov  
Subject: RE: Russian spear phishing attack against .mil and .gov emĚ  
From: jeffreyc@cia.gov  
Message-Id: <E1NfHf9-0002n7-Md@uw03.uniweb.no>  
Date: Wed, 10 Feb 2010 19:51:47 +0100  
X-Virus-Scanned: clamav-milter 0.95.3 at ee.lbl.gov  
X-Virus-Status: Clean  
Content-Length: 1116
This header is my own system (vpmini.icir.org) stating that it retrieved the message from mailhost.icsi.berkeley.edu.

I trust vpmini.icir.org, and therefore I believe the previous hop really was mailhost.icsi.berkeley.edu.
mailhost.icsi.berkeley.edu is integrated with fruitcake.icsi.berkeley.edu (that’s why the name is different in this header).

I trust the ICSI mailer, so I will trust this Received header too. It tells me that the prior hop was ee.lbl.gov (which I also trust).
Delivery-Date: Wed Feb 10 10:51:55 2010
Received: from mailhost.icsi.berkeley.edu [192.150.186.11] by vpmini.icir.org with IMAP (fetchmail-6.3.11) for <vern@localhost> (single-drop); Wed, 10 Feb 2010 10:51:54 -0800 (PST)
Received: from ee.lbl.gov (ee.lbl.gov [131.243.2.201]) by fruitcake.ICSI.Berkeley.EDU (8.12.11.20060614/8.12.11) with ESMTP id o1AIpmOf002895 for <vern@icsi.berkeley.edu>; Wed, 10 Feb 2010 10:51:50 -0800 (PST)
Received: from uw03.uniweb.no (uw03.uniweb.no [91.207.158.135]) by ee.lbl.gov (8.14.4/8.14.4) with ESMTP id o1AIpmOf002895 for <vern@ee.lbl.gov>; Wed, 10 Feb 2010 10:51:48 -0800 (PST)

ee.lbl.gov reports that the message came from uw03.uniweb.no.

I trust that information, but I do not trust that host. So any information from that point below is untrustworthy.
However, I have reliably learned that the message was sent by a machine in Norway ... probably not where the CIA has a mail server!