Usable Security and User Training

KAMI VANIEA
JANUARY 25
Equifax was serving up spyware

[Image: Randy-abrams.blogspot.com]

Equifax Credit Assistance Site Served Spyware

OCT 17

Big-three consumer credit bureau Equifax says it has removed third-party code from its credit report assistance Web site that prompted visitors to download spyware disguised as an update for Adobe’s Flash Player software.

On Wednesday, security expert and blogger Randy Abrams documented how browsing a page at Equifax’s consumer information services portal caused his browser to be served with a message urging him to download Adobe Flash Player.

“As I tried to find my credit report on the Equifax website I clicked on an Equifax link and was redirected to a malicious URL,” Abrahms wrote. “The URL brought up one of the ubiquitous fake Flash Player Update screens.”

https://krebsonsecurity.com/2017/10/equifax-credit-assistance-site-served-spyware/
Equifax was serving up spyware

In a follow-up statement shared with KrebsOnSecurity this afternoon, however, Equifax said the problem stemmed from a “third-party vendor that Equifax uses to collect website performance data,” and that “the vendor’s code running on an Equifax Web site was serving malicious content.”

https://krebsonsecurity.com/2017/10/equifax-credit-assistance-site-served-spyware/
What do they mean by “third party vendor”?
Websites are made up of many elements from many sources
You can easily see this list on most browsers in the “Network” developer tool.
Sites I went to intentionally

All the ▲ are trackers or content sources contacted by the main site.
The user visits a “first party website” such as cnn.com or theguardian.com.

That webpage then instructs your computer to fetch other websites to load content such as ads, images, calendars, Facebook, etc.

Those websites then in turn have more requests.
Fascinating, but what has all this got to do with Equifax serving Spyware?
Imagine that this node is a Javascript library that Equifax loads. Like jQuery or Bootstrap.

Except one day it goes out of business and no one notices because it is a very small company. And its domain registration lapses.

Then an ingenious malicious person registers the domain and starts serving spyware along with the old library.
Usable Security
People account for 90% of all security incidents

Misc Errors
Crimeware
Insider Misuse
Physical Theft/Loss
Web App Attacks
Denial of Service
Cyber-espionage
POS Intrusions
Payment Card Services

“At this point, take your finger, place it on your chest, and repeat: “I am the problem” as long as it takes for you to believe it. Good -- the first step to recovery is admitting the problem.”

Verizon 2015 Data Breach Investigations Report
Users are not the enemy

• Malicious actors are the enemy
• Users are a partner in keeping the system secure
• Like any partner:
  ◦ They have skills you don’t have
  ◦ They are missing skills you do have
• Think about what skills they have that you need
• Use the skills you have to make good decisions on users’ behalf
Three reasons people don’t use security or privacy technologies

1. They do not care about security and privacy

2. They do not know about security or privacy issues

3. They cannot use security and privacy technologies
Today and next lecture:

- How do I be safe online? Formulating good security advice
- Famous studies
- Passwords
- Phishing
- Warning and communications
- Trust. How it is built and supported
How do I be safe online?

The single most common question I get asked.
Opinion of security professionals and normal users.

They don’t match...

Common advice:

- Install an anti-virus scanner (Windows 8+ installed one for you)
- Keep your software updated
- Select a strong passcode for important things you use all the time
- Use a password manager for less important things that you use rarely
- If you have important things you use rarely, pick a strong password and write it down somewhere safe (this is ok)
- Install an ad blocker
- Remove software you don’t use
- If you are not sure about a website Google for it
Software I use:

• **Ad-blockers** – they are not just about ads, they reduce the amount of content loading

• **Ghostery** and **Privacy Badger** – Will block trackers

• **Lightbeam** – visualizes the trackers, though it does not protect you from them very well

• **Password managers** – LastPass, OnePassword, and KeePass are the most recommended

• 2-Factor like **YubiKey** – Extra protection for accounts like Facebook

• If you are really serious, and do not mind major usability issues
  ◦ UMatrix and NoScript - both block code from running off of third party sites
Famous studies
Why Johnny Can’t Encrypt: A Usability Evaluation of PGP 5.0 by Whitten and Tygar

- Asked 12 Carnegie Mellon Computer Scientists to correctly send an encrypted email using PGP 5.0
- Only 4 managed to accomplish this within 90 minutes
- Dangerous errors
  - Accidentally emailing without encrypting
  - Confusions around key system
  - Giving up
Bob would like to send Alice an encrypted email. So he first **Encrypt** the message with **Private** key and then **Encrypt** the message with **Public** key.

Alice gets a message supposedly from Bob. So she **Decrypt** the message using **Public** key. She then verifies the **Signature** using **Private** key.
Compose E-mail

frankchou1116@gmail.com

Add recipient

Happy birthday!

Encrypt attachments

E-mail will be signed digitally

Sign message with key: Qingyu Zhou <frankchou1116@yahoo.com> - 01C23B375BC3

Sign all messages with primary key

Options

Sign Only

Cancel

Encrypt

Send
### Task 2: Write an encrypted email

<table>
<thead>
<tr>
<th></th>
<th>Webmail login</th>
<th>Composing email on</th>
<th>Opening Mailvelope popup</th>
<th>Sending encrypted email</th>
</tr>
</thead>
<tbody>
<tr>
<td>T1</td>
<td>Success (hint)</td>
<td>Webmail editor</td>
<td>Failure</td>
<td>Failure</td>
</tr>
<tr>
<td>T2</td>
<td>Success (hint)</td>
<td>Webmail editor</td>
<td>Failure</td>
<td>Failure</td>
</tr>
<tr>
<td>T3</td>
<td>Success (hint)</td>
<td>Webmail editor</td>
<td>Failure</td>
<td>Failure</td>
</tr>
<tr>
<td>T4</td>
<td>Success (hint)</td>
<td>Webmail editor</td>
<td>Failure</td>
<td>Failure</td>
</tr>
<tr>
<td>T5</td>
<td>Success (hint)</td>
<td>Webmail editor</td>
<td>Failure</td>
<td>Failure</td>
</tr>
<tr>
<td>T6</td>
<td>Success</td>
<td>Webmail editor</td>
<td>Failure</td>
<td>Failure</td>
</tr>
<tr>
<td>T7</td>
<td>Success</td>
<td>Webmail editor</td>
<td>Failure</td>
<td>Failure</td>
</tr>
<tr>
<td>T8</td>
<td>Success</td>
<td>Webmail editor</td>
<td>Failure</td>
<td>Failure</td>
</tr>
<tr>
<td>T9</td>
<td>Success (hint)</td>
<td>Mailvelope popup</td>
<td>Success</td>
<td>Success</td>
</tr>
<tr>
<td>T10</td>
<td>Success</td>
<td>Webmail editor</td>
<td>Failure</td>
<td>Failure</td>
</tr>
</tbody>
</table>

Table 4.3: Completion details of Task 2 for each participant.
So why did they all fail?
Cognitive Walkthrough

Step 2: Click on the “Options” button.

Q1. Will users try to achieve the outcome of clicking on this button?

Q2. Will users see this button for the action?

Q3. Once users find this button, will users recognize that clicking on it will produce the effect they want?

Q4. After the action is performed, will users understand the feedback, so they can confidently continue on to the next action?
Security experts are not typically trained in usability.

Usability experts tend to leave out very important security steps (like key verification).
Passwords
Passwords

• Most popular method of authentication
  ◦ A character string (password) is agreed upon between the user and the system
  ◦ User proves their identity by providing the password

• Convenient system design
  ◦ Easy to store encrypted
  ◦ Easy to enter on many systems
  ◦ No special equipment needed
  ◦ Scales well

• Problem: people choose easy to guess passwords
  ◦ Low entropy, so easy to guess
  ◦ Hard to remember

Most common passwords in RockYou data
### Rockyou

<table>
<thead>
<tr>
<th>Count</th>
<th>Password</th>
</tr>
</thead>
<tbody>
<tr>
<td>290729</td>
<td>123456</td>
</tr>
<tr>
<td>79076</td>
<td>12345</td>
</tr>
<tr>
<td>76789</td>
<td>123456789</td>
</tr>
<tr>
<td>59462</td>
<td>password</td>
</tr>
<tr>
<td>49952</td>
<td>iloveyou</td>
</tr>
<tr>
<td>33291</td>
<td>princess</td>
</tr>
<tr>
<td>21725</td>
<td>1234567</td>
</tr>
<tr>
<td>20901</td>
<td>rockyou</td>
</tr>
<tr>
<td>20553</td>
<td>12345678</td>
</tr>
<tr>
<td>16648</td>
<td>abc123</td>
</tr>
<tr>
<td>16227</td>
<td>nicole</td>
</tr>
<tr>
<td>15308</td>
<td>daniel</td>
</tr>
</tbody>
</table>

### Phpbb

<table>
<thead>
<tr>
<th>Count</th>
<th>Password</th>
</tr>
</thead>
<tbody>
<tr>
<td>2650</td>
<td>123456</td>
</tr>
<tr>
<td>1244</td>
<td>password</td>
</tr>
<tr>
<td>708</td>
<td>phpbb</td>
</tr>
<tr>
<td>562</td>
<td>qwerty</td>
</tr>
<tr>
<td>418</td>
<td>12345</td>
</tr>
<tr>
<td>371</td>
<td>12345678</td>
</tr>
<tr>
<td>343</td>
<td>letmein</td>
</tr>
<tr>
<td>313</td>
<td>111111</td>
</tr>
<tr>
<td>273</td>
<td>1234</td>
</tr>
<tr>
<td>253</td>
<td>123456789</td>
</tr>
<tr>
<td>224</td>
<td>abc123</td>
</tr>
<tr>
<td>223</td>
<td>test</td>
</tr>
</tbody>
</table>

### Myspace

<table>
<thead>
<tr>
<th>Count</th>
<th>Password</th>
</tr>
</thead>
<tbody>
<tr>
<td>75</td>
<td>password1</td>
</tr>
<tr>
<td>56</td>
<td>abc123</td>
</tr>
<tr>
<td>34</td>
<td>fuckyou</td>
</tr>
<tr>
<td>29</td>
<td>monkey1</td>
</tr>
<tr>
<td>28</td>
<td>iloveyou1</td>
</tr>
<tr>
<td>24</td>
<td>myspace1</td>
</tr>
<tr>
<td>24</td>
<td>fuckyou1</td>
</tr>
<tr>
<td>18</td>
<td>number1</td>
</tr>
<tr>
<td>18</td>
<td>football1</td>
</tr>
<tr>
<td>17</td>
<td>nicole1</td>
</tr>
<tr>
<td>17</td>
<td>123456</td>
</tr>
<tr>
<td>16</td>
<td>iloveyou2</td>
</tr>
</tbody>
</table>
Standard password guidance

What does a **good** password look like?
- At least 8 characters, longer better
- No words (any language, especially English)
- Avoid common patterns
  - Upper case letter as first letter
  - Putting the number at the end
  - Putting the special character at the end
- High entropy
  - Lowercase letters
  - Upper case letters
  - Numbers
  - Special characters

What does a **bad** password look like?
- Short
- Easy to guess (significant other attack)
- Uses common patterns
- Low entropy
  - Word (in any language)
  - Same combination other people use
Password entropy

- A good password should be drawn randomly from a large set of possible passwords
- A bad password is drawn from either a small set or not randomly

https://xkcd.com/936/
UK guidance on simplifying passwords

1. Change all default passwords
2. Help users cope with password overload
3. Understand the limitations of user-generated passwords
4. Understand the limitations of machine generated passwords
5. Prioritize administrator and remote user accounts
6. Use account lockout and protective monitoring
7. Don’t store passwords as plain text

Common (possibly wrong) wisdom

- Reset passwords every 30 days
- Use long passwords
- Use a different password for every site
- Don’t ever give out your password
- Don’t use easy to guess passwords
User generated passwords

• People are somewhat ok at generating passwords they can remember

• People are bad at generating passwords that are hard to guess

• User-generated passwords:
  ◦ Low entropy
  ◦ Tend to have facts about themselves such as their pet’s name
  ◦ Guessable by someone who knows them
  ◦ Easy to lookup in a password dictionary
PassFaces

• Humans are better at recognizing things than they are at recalling information.
• High feature information, like faces, are easier to recognize
• Idea: Use high feature information as the pin, so humans can recognize their password
• Problem: People select faces that mean something to them. If you know basic characteristics about someone you can easily guess their PassFace.
PassFaces

- Password length = 4
- Each password selected from a set of 9 faces like what is shown on the right
- Theoretical password space = 6561
- What is the best way to break someone’s password?
  - If the person is a white male, you can guess the correct password in about two guesses by selecting all the pretty white females.
Machine generated passwords

• Computers are better at selecting passwords that are challenging for other computers to guess

• Computers are less good at selecting passwords that are easy to remember

• Tactics:
  ◦ Some algorithms produce passwords which are pronounceable, or are made up of words (correct battery horse staple)
  ◦ Let users choose from a small number of passwords
Phishing

• Phishing – Attempting to trick someone into taking the “bait” and interacting in a way they should not.
  ◦ Typically involves the impersonator pretending to be someone else that the person trusts
  ◦ Interactions: Clicking a link, opening a file, replying with information, transferring money, etc.
• Spear phishing – Phishing, but with a small number of targets and each email is crafted for that individual
• Whaling – Phishing for people with a lot of money, i.e. CEO
• QRishing – Phishing attacks through QR codes
What on this email can be trusted?

From: "Fletcher, Freya" <ffletcher@conejousd.org>

Subject: FW: ITS Administrative Support

To: undisclosed-recipients:

Day User,

Your password will expire within 24hrs. Click on: Staff & faculty update to validate your e-mail.

This email has been scanned by the Symantec Email Security.cloud service. For more information please visit http://www.symanteccloud.com

http://staffupgrade.moonfruit.com/
(Wrong) Trust indicators

Authority figure that often sends emails to do things

Clear threat to recipient’s ability to log in

(False) statement saying the email has been scanned and is safe
Sneaky email to get the recipient to open the attachment, which is an html document.

Dear Damon,

Unfortunately we failed to deliver the postal package you have sent in time because the recipient's address is erroneous. Please fill out the attached form and bring it to our local office so that you can retrieve your package.

Thank you,
Customer Care

This is an automated email. Do not respond as the email address is not checked and you will not receive a response.
Problem: Users click on links and attachments

• Scan all incoming attachments and links for blacklisted content
• Teach users
  ◦ Only click if you are expecting the email
  ◦ Do not open attachments unless you are expecting them
  ◦ If you are not sure, contact the person or company separately and ask if they sent the email
  ◦ If you are not sure, contact the IT department
  ◦ Banks and credit card companies will never contact you this way
Anti-Phishing Phill

- Serious game to help people learn to spot dangerous URLs
- Training sometimes works
- But it takes time
- And people forget
PhishGuru

- Comic to train people to spot phishing attacks
- Best time to train is after a user has already fallen for an attack
- Send out fake attacks and train those who click on them
Give users options that make sense and work for them
PhishGuru

- Users know what they are expecting
- Users know who the email looks like it is from
- Users can do an out-of-band contact (phone call)
- Users do not want to ignore a serious issue
In Summary...

- Academics say in-the-moment training works
- Chief Security Officers (CSOs) have mixed opinions
- Everybody thinks that users clicking on links and attachments is a big problem
Warnings and communication
Why show warnings at all?

• Determined users might disable Safe Browsing. Which would prevent future warnings.

• User could also open the website in another browser that is less safe and does not block the website.
  ◦ America Online users used to go to a friend’s house to open malicious sites because the ISP blocked malicious sites.
  ◦ Different browsers block different sets of sites, we don’t want to teach users to use less safe browsers.
Chrome malware warning

- Huffington post was blocked because a content provider images.buddytv.com had malware
Why do people click through the warnings?

• The site is used often and trusted
  ◦ “YouTube is a well known website. I’d assume that the malware block is in error.”

• The person who posted the link is trusted
  ◦ “I find it harder to believe [the warning] when my Facebook friend just posted it and had no problems.”

• The site where the link is assumed to have good security
  ◦ “I presume that visiting YouTube from a Facebook link would be safe.”

• They think they are safe
  ◦ “I use Linux I’m not afraid of anything.”
  ◦ “I have an anti virus”
Improved warning

- Added “for now”
- Added “even if ... visited safely in the past”
- Consider special warning for common websites
Are users correct to ignore the warnings?

• Studied TLS activity of more than 300,000 users
  ◦ Collected certificates passively at egress points of 10 network sites
  ◦ Over 9 month period
  ◦ Validated certificate chains using local browser logic
  ◦ 98.46% of the filtered connections validate correctly, implying a false warning rate of 1.54%

• In a scenario with a hypothetical Man-In-The-Middle chance of 1 in 1,000,000
  ◦ 1,000,000 connections would produce 15.401 warnings
  ◦ Out of which 15.4 would be false warnings

Devdatta Akhawe, Bernhard Amann, Matthias Vallentin, and Robin Sommer; Here’s My Cert, So Trust Me, Maybe? Understanding TLS Errors on the Web, 2013
Human in the Loop Framework
This is a regular monthly email from the School of Informatics Computing Team which summarises your recent account activity. For the month of September 2016 your account 'kvaniea' was used to access Informatics computing resources from remote locations on 84 occasions.

Please review all these hosts listed below and check for any activity which appears to be unusual (i.e. logins from locations you do not recognise).

Sac68545.bb.sky.com (Cosign: 11, SSH: 21)
Sac8e505.bb.sky.com (Cosign: 13, SSH: 16)
172.20.107.180 {EdLAN} (SSH: 4)
172.20.105.173 {EdLAN} (Cosign: 5)
172.20.107.42 {EdLAN} (SSH: 2)
94.197.129.254.threemb.co.uk (Cosign: 2)
172.20.104.174 {EdLAN} (Cosign: 2)
172.20.104.182 {EdLAN} (SSH: 1)
94.197.129.37.threemb.co.uk (SSH: 1)
172.20.104.14 {EdLAN} (Cosign: 1)
172.20.105.217 {EdLAN} (Cosign: 1)
172.20.106.190 {EdLAN} (SSH: 1)
172.20.106.229 {EdLAN} (Cosign: 1)
172.20.106.255 {EdLAN} (Cosign: 1)
172.20.110.7 {EdLAN} (SSH: 1)
172.20.105.98 {EdLAN} (Cosign: 1)
172.20.104.83 {EdLAN} (SSH: 1)

For a more detailed view you can access the logs of all authentication
NEAT and SPRUCE

• Developed at Microsoft Research
• Guidance on how to create effective security messaging for end users
NEAT

**Necessary** – Can you change the architecture to eliminate or defer this user decision?

**Explained** - Does your user experience present all the information the user needs to make this decision? (See SPRUCE)

**Actionable** – Have you determined a set of steps the user will realistically be able to take to make the decision correctly?

**Tested** – Have you checked that your user experience is NEAT for all scenarios, both benign and malicious? Have you tested it on a human who is not a member of your team?
SPRUCE

Source – State who or what is asking the user to make a decision

Process – Give the user actionable steps to follow to make a good decision

Risk – Explain what bad thing could happen if they user makes the wrong decision

Unique knowledge the user has – Tell the user what information they bring to the decision

Choices – List available options and clearly recommend one

Evidence – Highlight information the user should factor in or exclude in making a decision
Questions