

Household INFOSEC in a Post-Sony Era

Steve Loughran
stevel@apache.org





Data Integrity
Data Privacy
Data
Availability
Resource Control



Don't upset a nation state





Worry about drive-by

3 pages Fax from 850-445-9826

850-445-9826 <brenda@sansomtimberframe.co.uk> 13:40 (58 minutes ago) Reply

to stevel

Ref: NY7DPXPO

Sender ID: 850-445-9826

Date: 14-12-2015

Open this fax using your Microsoft Word.

⚠ Anti-virus warning – 1 attachment contains a virus or blocked file. Downloading this attachment is disabled. Learn more

NY7DPXPO.doc Virus found

Open File - Security Warning

We can't verify who created this file. Are you sure you want to run this file?

Name: E:\Install\Java\jdk-8u74-windows-x64.exe
Type: Application
From: E:\Install\Java\jdk-8u74-windows-x64.exe

Run Cancel

This document contains macros.
Macros may contain viruses. Ensure current macro security setting is appropriate.
Therefore, some functionality may not be available.

OK

334_k74196-x7as

File Edit View Insert Format Tools Table Add-ons Help Last edit was seconds ago

Steve.loughran@gmail.com

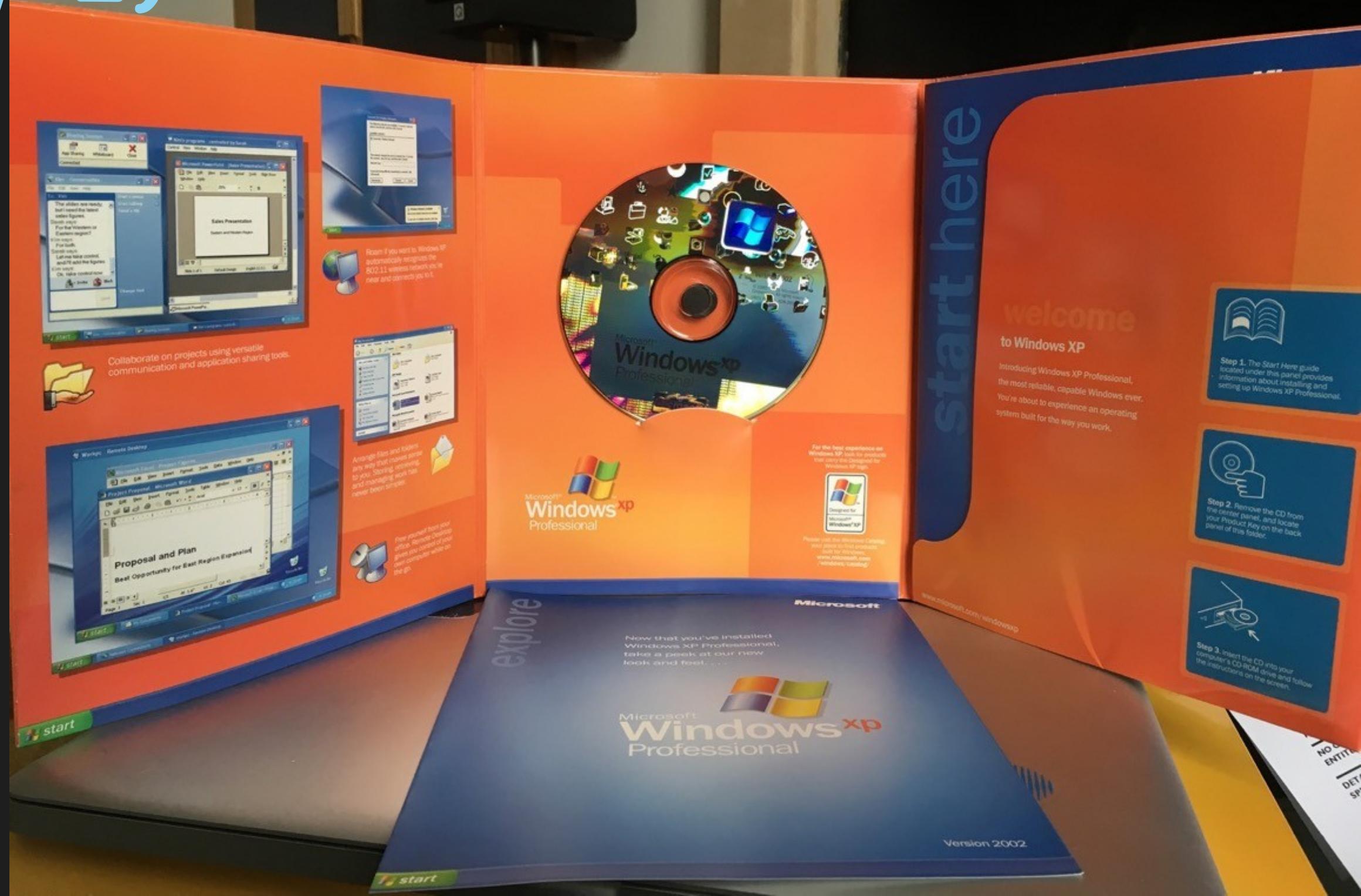
Comments Share

Privacy (lack of)

How to Quantify Risk?

Vulnerability

(11, 1)

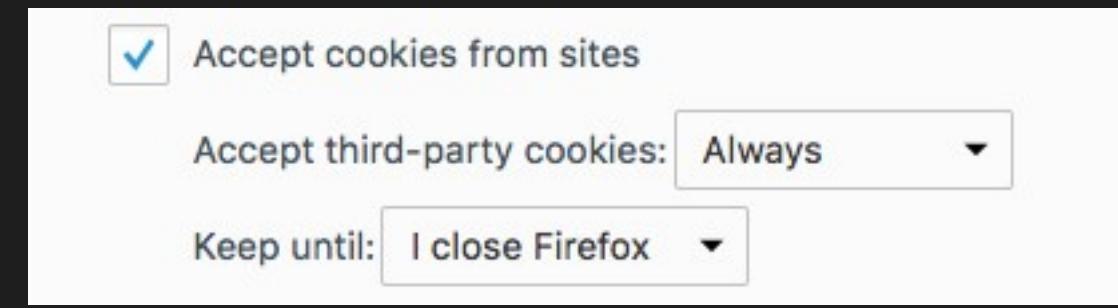


(*, 11)





Firefox (8, 2)



Adblock Plus Filter Preferences

Filter subscriptions Custom filters

Add filter subscription...

Filter rule	!	Enabled	Hits
! Last modified: 31 May 2016 09:10 UTC	!		
! Licence: https://easylist.github.io/pages/licence.html	!		
!			
! Please report any unblocked adverts or problems	!		
! in the forums (https://forums.lanik.us/)	!		
! or via e-mail (easylist.subscription@gmail.com).	!		
!			
-----General advert blocking filters-----			
! *** easylist:easylist/easylist_general_block.txt ***			
&ad_box=	<input checked="" type="checkbox"/>	0	
&ad_channel=	<input checked="" type="checkbox"/>	0	
&ad_classid=	<input checked="" type="checkbox"/>	0	
&ad_height=	<input checked="" type="checkbox"/>	0	
&ad_keyword=	<input checked="" type="checkbox"/>	0	
&ad_network_	<input checked="" type="checkbox"/>	0	
&ad_number=	<input checked="" type="checkbox"/>	0	
&ad_type=	<input checked="" type="checkbox"/>	0	
&ad_type_	<input checked="" type="checkbox"/>	0	

Find Filter actions Add filter

Filter subscriptions Custom filters

EasyList (Homepage, Filter list)
Last download: 31/05/2016, 10:19
(Success) Actions

EasyPrivacy (Homepage, Filter list)
Last download: 01/06/2016, 10:14
(Success) Actions

Disable Malware (Homepage, Filter list)
Last download: 01/06/2016, 10:14
(Success) Actions

Adblock Warning Removal List (Homepage, Filter list)
Last download: 31/05/2016, 16:42
(Success) Actions

Allow some non-intrusive advertising View list Read more

Backup and Restore Close

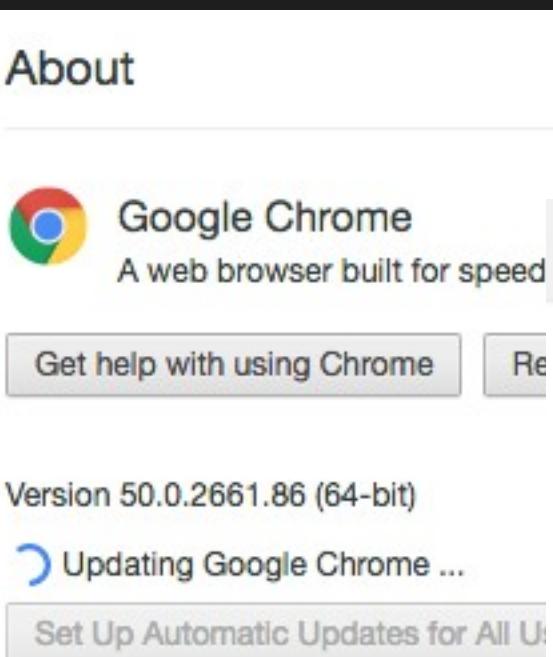


Chrome: (8, 10)

Chrome About

History
Extensions
Settings
About

Version 50.0.2661.86 (64-bit)
Updating Google Chrome ...
Set Up Automatic Updates for All U...



Google Chrome
A web browser built for speed

Get help with using Chrome Re...

Subscribe to filter lists

Don't subscribe to more than you need -- every one slows you down a tiny bit! Credits and more lists can be found [here](#).

I will fetch updates automatically; you can also [update now](#)

Ad Blocking Filter Lists

Acceptable Ads (recommended)
 AdBlock custom filters (recommended) updated 3 days ago
 EasyList (recommended) updated 4 days ago
Add filters for another language: [-- Select Language --](#)

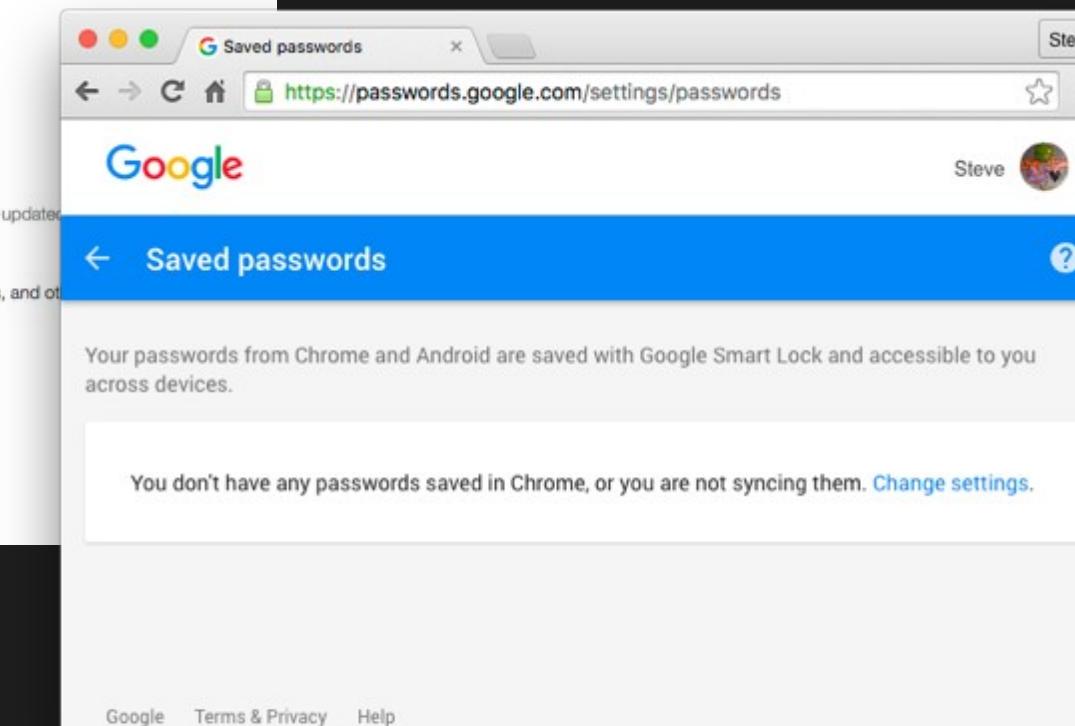
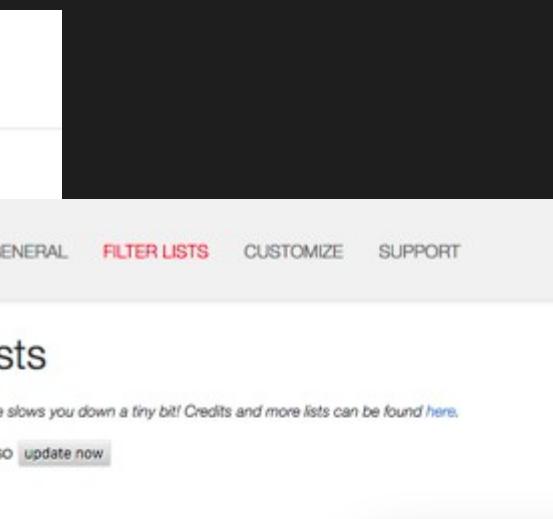
Other Filter Lists

Adblock Warning Removal list (removes warnings about using ad blockers)
 Antisocial filter list (removes social media buttons)
 EasyPrivacy (privacy protection)
 Fanboy's Annoyances (blocks in-page pop-ups, social media and related widgets, and other annoyances)
 Malware protection updated 13 seconds ago
 Should AdBlock notify you when it detects malware? [Beta](#)

Custom Filter Lists

Or enter a URL: [Subscribe](#)

Show links to the filter lists



Steve

https://passwords.google.com/settings/passwords

Google

Steve

Saved passwords

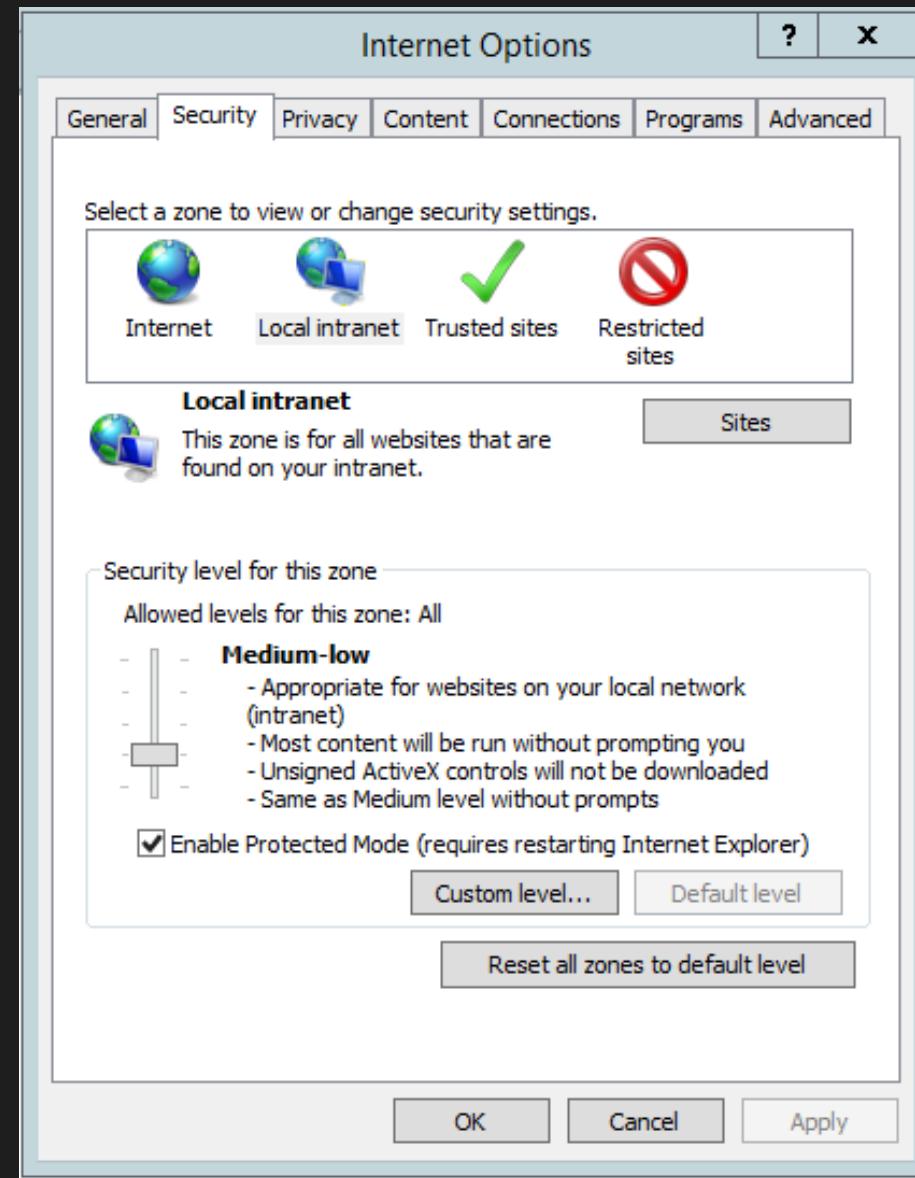
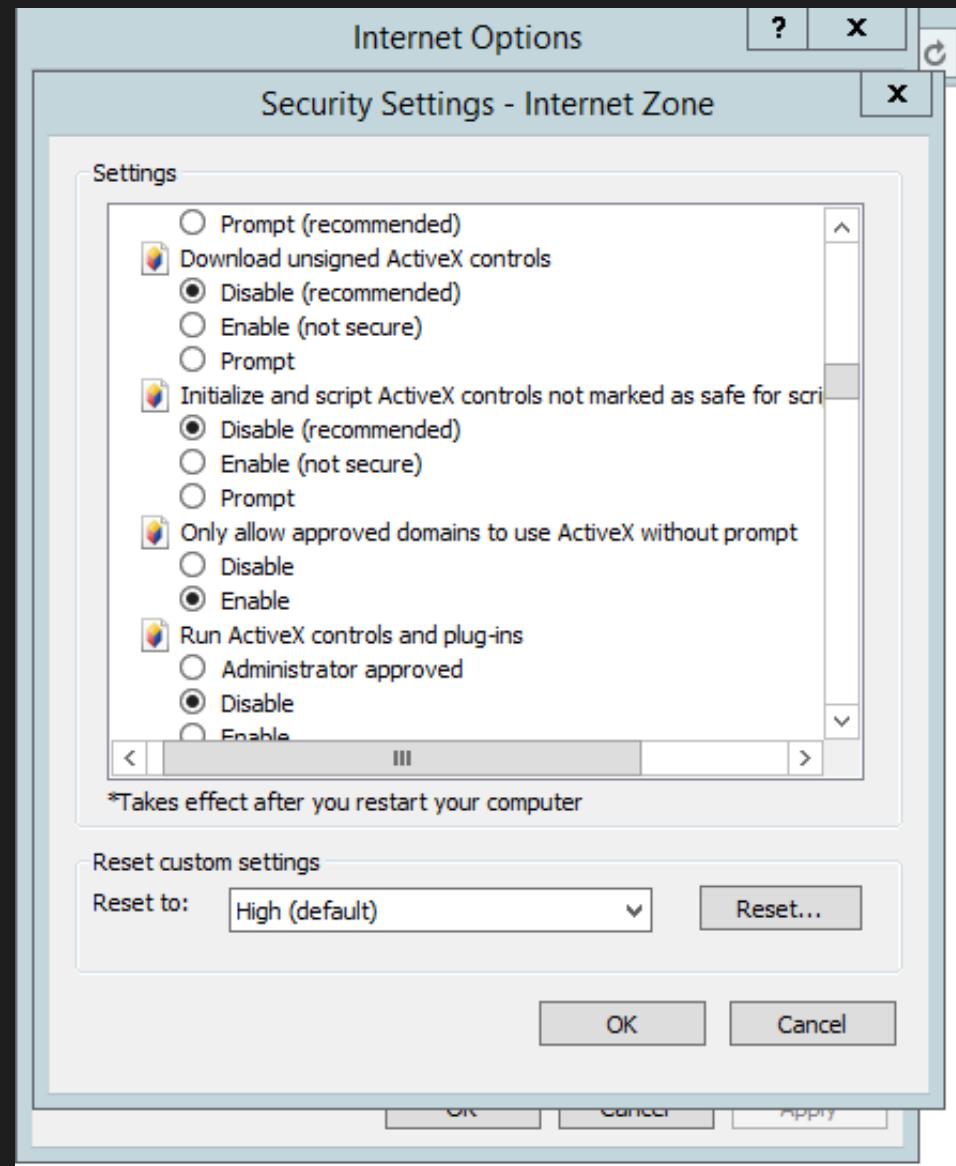
Your passwords from Chrome and Android are saved with Google Smart Lock and accessible to you across devices.

You don't have any passwords saved in Chrome, or you are not syncing them. [Change settings](#).

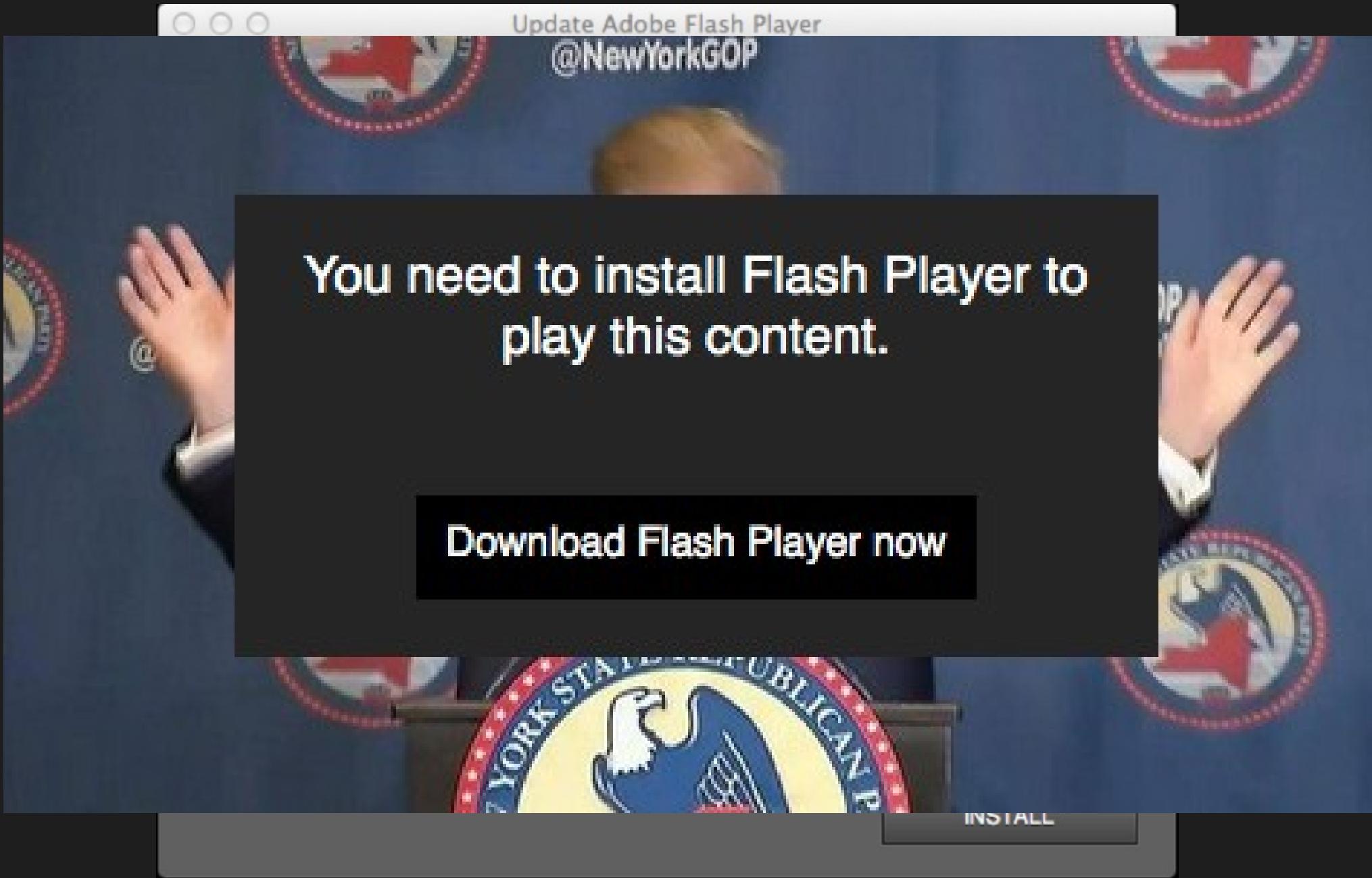
Google Terms & Privacy Help



IE 11 Use to D/L Firefox or Chrome



Flash (9->10, 4)



steve.loughran@gmail.com

pwned?

Oh no — pwned!

Pwned on 1 breached site and found no pastes (subscribe to search sensitive breaches)

 Notify me when I get pwned

 Donate



Breaches you were pwned in

A "breach" is an incident where a site's data has been illegally accessed by hackers and then released publicly. Review the types of data that were compromised (email addresses, passwords, credit cards etc.) and take appropriate action, such as changing passwords.



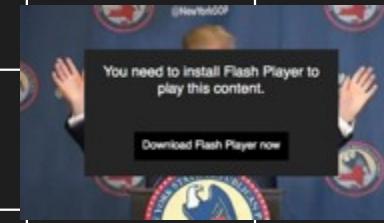
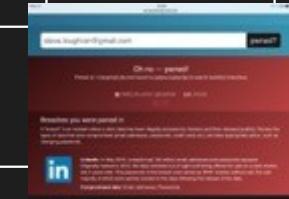
LinkedIn: In May 2016, LinkedIn had 164 million email addresses and passwords exposed.

Originally hacked in 2012, the data remained out of sight until being offered for sale on a dark market site 4 years later. The passwords in the breach were stored as SHA1 hashes without salt, the vast majority of which were quickly cracked in the days following the release of the data.

Compromised data: Email addresses, Passwords

Privacy (lack of)

Vulnerability



trouble-



iPad- -iPhone

-PS4

-Airplay
Amplifier

Select All Terms of Use Privacy Policy**Agree****Next**

our services are being used, and make improvements to them.

Apart from this Privacy Policy, you will be provided a specific opportunity to agree or disagree with the collection and use of Viewing Information. Please note, however, that anytime that you request to view content through a video on-demand service provided by LG, your LG Smart TV will transmit information to enable video playback to LG. This information will only be used to provide the content you request, unless you have agreed to the Viewing Information agreement (in which case it may be used for the additional purposes described in that agreement).

You may prevent the collection and use of your Viewing Information in connection with the Live Plus service by clicking the appropriate on-screen button in the Settings menu. Please note that if you do so, your Viewing Information will continue to be used for other LG Smart TV services.

How we use your Voice Information

Many LG Smart TVs come with a remote control or other input devices that can be operated using voice commands. We may use your Voice Information to power the voice activation used by the Smart TV or input device (e.g., remote control). If you do not agree to our use of your Voice Information then you will not be able to use the voice command and recognition features. Apart from this Privacy Policy, you will be provided a specific opportunity to agree or disagree with the collection and use of Voice Information. Please be aware that if your spoken word includes personal or other sensitive information, such information will be among the Voice Information captured through your use of voice recognition features.

LGTv3.pcapng [Wireshark 1.10.2 (SVN Rev 51934 from /trunk-1.10)]

File Edit View Go Capture Analyze Statistics Telephony Tools Internals Help

Filter: Expression... Clear Apply Save

Frame	Source IP	Destination IP	Protocol	Description
1529	312.39899100	192.168.1.2	igmp.mcast.net	IGMPv3 60 Membership Report / Join group 224.0.0.113 for any sources
1530	318.75345500	192.168.1.2	192.168.100.1	DNS 80 Standard query 0x9034 A GB.ibis.lgappstv.com
1531	318.78009700	192.168.100.1	192.168.1.2	DNS 96 Standard query response 0x9034 A 193.67.216.128
1532	318.78059400	192.168.1.2	GB.ibis.lgappstv.com	TCP 74 50596 > http [SYN] Seq=0 Win=14600 Len=0 MSS=1460 SACK_PERM=1 TSval=6684 TSecr=0 WS=32
1533	318.80634100	GB.ibis.lgappstv.com	192.168.1.2	TCP 74 http > 50596 [SYN, ACK] Seq=0 Ack=1 Win=5792 Len=0 MSS=1418 SACK_PERM=1 TSval=3302232552 TSecr=3302232552
1534	318.80651400	192.168.1.2	GB.ibis.lgappstv.com	TCP 66 50596 > http [ACK] Seq=1 Ack=1 Win=14624 Len=0 TSval=6689 TSecr=3302232552
1535	318.80691500	192.168.1.2	GB.ibis.lgappstv.com	HTTP 1149 POST /ibs/v2.2/service/watchInformation.xml HTTP/1.1 (application/x-www-form-urlencoded)
1536	318.84226300	GB.ibis.lgappstv.com	192.168.1.2	TCP 66 http > 50596 [ACK] Seq=1 Ack=1084 Win=8704 Len=0 TSval=3302232588 TSecr=6689
1537	318.84950400	GB.ibis.lgappstv.com	192.168.1.2	HTTP/XML 1174 HTTP/1.1 200 OK
1538	318.84953900	GB.ibis.lgappstv.com	192.168.1.2	TCP 66 http > 50596 [FIN, ACK] Seq=1109 Ack=1084 Win=8704 Len=0 TSval=3302232594 TSecr=6689
1539	318.84975100	192.168.1.2	GB.ibis.lgappstv.com	TCP 66 50596 > http [ACK] Seq=1084 Ack=1109 Win=16832 Len=0 TSval=6698 TSecr=3302232594
1540	318.85021000	192.168.1.2	GB.ibis.lgappstv.com	TCP 66 50596 > http [FIN, ACK] Seq=1084 Ack=1110 Win=16832 Len=0 TSval=6698 TSecr=3302232594
1541	318.87602700	GB.ibis.lgappstv.com	192.168.1.2	TCP 66 http > 50596 [ACK] Seq=1110 Ack=1085 Win=8704 Len=0 TSval=3302232622 TSecr=6698

X-Device-Platform:NC4M\r\nX-Device-Model:HE_DTV_NC4M_AFAAABAA\r\nX-Device-Netcast-Platform-Version:0004.0002.0000\r\nX-Device-Country:GB\r\nX-Device-Country-Group:EU\r\nX-Device-ID:2yxQ5kEhf45fjUD35G+E/xdq7xxWE2ghu0j4an9kbGoNcyWaSsoLgyk8JJJoMtjRrYRsVS6mHKy/Zdd6nZp+Y+gK6DVqnbQeDqr16YgacdZKU80sCKw0Ai1TwIQov/S1B\r\nX-Authentication:YMu3V1dv8m8JD0ghrsmEToxONDI=\r\ncookie:JSESSIONID=3BB87277C55EED9489B6E6B2DEA7C9FD.node_sdplibis10; Path=/\r\nContent-Length: 463\r\nContent-Type: application/x-www-form-urlencoded\r\n\r\n[Full request URI: <http://GB.ibis.lgappstv.com/ibs/v2.2/service/watchInformation.xml>]\r\n[HTTP request 1/1]\r\n[Response in frame: 1537]\r\nLine-based text data: application/x-www-form-urlencoded\r\n[truncated] &chan_name=BBC NEWS&device_src_idx=1&dvtv_standard_type=2&broadcast_type=2&device_platform_name=NETCAST 4.0_mtk5398&chan_code=251533447-AF06B3CC8ACE450D32BF26439B8I

02a0 75 72 6c 65 6e 63 6f 64 65 64 0d 0a 0d 0a 26 63 urlencod ed....&c
02b0 68 61 6e 5f 6e 61 6d 65 3d 42 42 43 20 4e 45 57 han_name =BBC NEW
02c0 53 26 64 65 76 69 63 65 5f 73 72 63 5f 69 64 78 S&device_src_idx
02d0 3d 31 26 64 74 76 5f 73 74 61 6e 64 61 72 64 5f =1&dvtv_s standard
02e0 74 79 70 65 3d 32 26 62 72 6f 61 64 63 61 73 74 type=2&b roadcast
02f0 5f 74 79 70 65 3d 32 26 64 65 76 69 63 65 5f 70 _type=2& device_p
0300 6c 61 74 66 6f 72 6d 5f 6e 61 6d 65 3d 4e 45 54 latform_name=NET
0310 43 41 53 54 20 34 2e 30 5f 6d 74 6b 35 33 39 38 CAST 4.0 mtk5398

Text item (text) Packets: 2463 · Displayed: 2463 (100.0%) · Load time: 0:00.169 Profile: Default

doctorbeet.blogspot.co.uk(?,10)



router manager
N600 Wireless Dual Band Router model WNDR3400

Select Language:

Auto

Apply

- Setup Wizard
- Add WPS Client

Setup

- Basic Settings
- Wireless Settings
- Guest Network

USB Storage

- Basic Settings
- Advanced Settings

Content Filtering

- Logs
- Block Sites
- Block Services
- Schedule

E-mail

Maintenance

- Router Status
- Attached Devices
- Backup Settings

Firmware Version Check

No new firmware version available.

Back

Router Upgrade Help

You install new versions of the router's software using the Router Upgrade screen.

Click the **Check** button to go to the NETGEAR website to get **new versions** of the router software. After downloading the file, you will need to unzip (or unstuff) it before upgrading the router.

Select the check box if you want to check for a new version upon login.

IMPORTANT! Once you click **Upload**, do not interrupt the process of sending the software to the router and restarting the router. If you think the process might be interrupted in some way, click **Cancel** to keep the current router software.

Locate and select the upgrade file on your hard disk.

1. Go to www.NETGEAR.com and download the updated software.
2. If it is not done automatically, uncompress the file.
You might want to read the *Release Notes* before continuing.
3. Click **Browse**.
4. Locate and select the file you just

(?, 0)

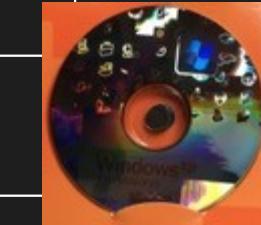
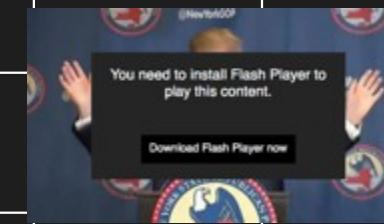
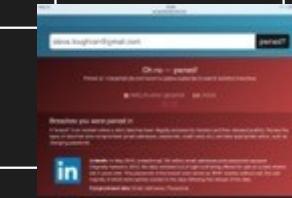


```
hadoop-trunk — fish /Users/steve/Projects/Hortonworks/Projects/hadoop-trunk — fish — 158x43
fish /Users/steve/Projects/Hortonworks/Pr... fish /Users/steve/Projects/Hortonworks/Pr... fish /Users/steve/Projects/Hortonworks/Pr... fish /Users/steve/Projects/Hortonworks/Pr... fish /Users/steve/Projects/Hortonworks/Pr...
[INFO] Apache Hadoop YARN Applications ..... SUCCESS [ 0.037 s]
[INFO] Apache Hadoop YARN DistributedShell ..... SUCCESS [ 0.576 s]
[INFO] Apache Hadoop YARN Unmanaged Am Launcher ..... SUCCESS [ 0.314 s]
[INFO] Apache Hadoop YARN Site ..... SUCCESS [ 0.034 s]
[INFO] Apache Hadoop YARN Registry ..... SUCCESS [ 0.861 s]
[INFO] Apache Hadoop YARN Project ..... SUCCESS [ 0.077 s]
[INFO] Apache Hadoop MapReduce Client ..... SUCCESS [ 0.068 s]
[INFO] Apache Hadoop MapReduce Core ..... SUCCESS [ 3.656 s]
[INFO] Apache Hadoop MapReduce Common ..... SUCCESS [ 1.765 s]
[INFO] Apache Hadoop MapReduce Shuffle ..... SUCCESS [ 0.397 s]
[INFO] Apache Hadoop MapReduce App ..... SUCCESS [ 2.176 s]
[INFO] Apache Hadoop MapReduce HistoryServer ..... SUCCESS [ 1.085 s]
[INFO] Apache Hadoop MapReduce JobClient ..... SUCCESS [ 2.580 s]
[INFO] Apache Hadoop MapReduce HistoryServer Plugins ..... SUCCESS [ 0.166 s]
[INFO] Apache Hadoop MapReduce Examples ..... SUCCESS [ 1.121 s]
[INFO] Apache Hadoop MapReduce ..... SUCCESS [ 0.086 s]
[INFO] Apache Hadoop MapReduce Streaming ..... SUCCESS [ 0.712 s]
[INFO] Apache Hadoop Distributed Copy ..... SUCCESS [ 2.001 s]
[INFO] Apache Hadoop Archives ..... SUCCESS [ 0.265 s]
[INFO] Apache Hadoop Archive Logs ..... SUCCESS [ 0.500 s]
[INFO] Apache Hadoop Rumen ..... SUCCESS [ 0.797 s]
[INFO] Apache Hadoop Gridmix ..... SUCCESS [ 0.871 s]
[INFO] Apache Hadoop Data Join ..... SUCCESS [ 0.426 s]
[INFO] Apache Hadoop Ant Tasks ..... SUCCESS [ 0.232 s]
[INFO] Apache Hadoop Extras ..... SUCCESS [ 0.444 s]
[INFO] Apache Hadoop Pipes ..... SUCCESS [ 0.075 s]
[INFO] Apache Hadoop OpenStack support ..... SUCCESS [ 0.729 s]
[INFO] Apache Hadoop Amazon Web Services support ..... SUCCESS [ 0.733 s]
[INFO] Apache Hadoop Azure support ..... SUCCESS [ 0.692 s]
[INFO] Apache Hadoop Client ..... SUCCESS [ 1.176 s]
[INFO] Apache Hadoop Mini-Cluster ..... SUCCESS [ 0.223 s]
[INFO] Apache Hadoop Scheduler Load Simulator ..... SUCCESS [ 1.718 s]
[INFO] Apache Hadoop Tools Dist ..... SUCCESS [ 0.356 s]
[INFO] Apache Hadoop Tools ..... SUCCESS [ 0.035 s]
[INFO] Apache Hadoop Distribution ..... SUCCESS [ 0.079 s]
[INFO] -----
[INFO] BUILD SUCCESS
[INFO] -----
[INFO] Total time: 02:58 min
[INFO] Finished at: 2016-06-03T15:13:33+01:00
[INFO] Final Memory: 245M/961M
[INFO] -----
~/P/H/P/hadoop-trunk (branch-2) $
```

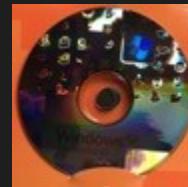
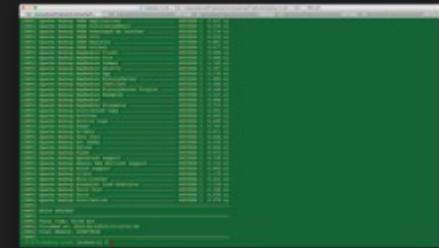
Privacy (lack of)



Vulnerability



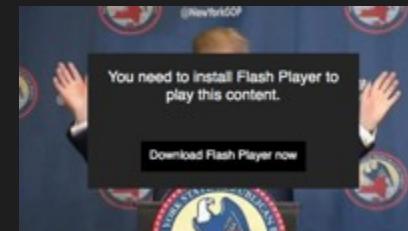
CRITICAL



USB

DD-WRT

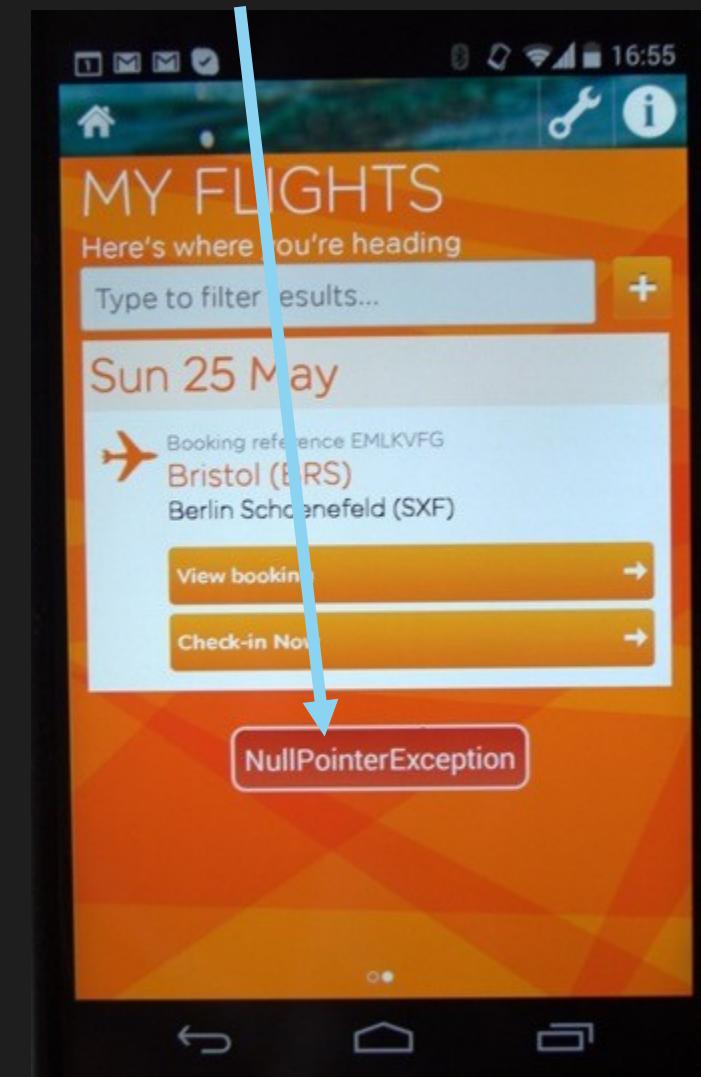
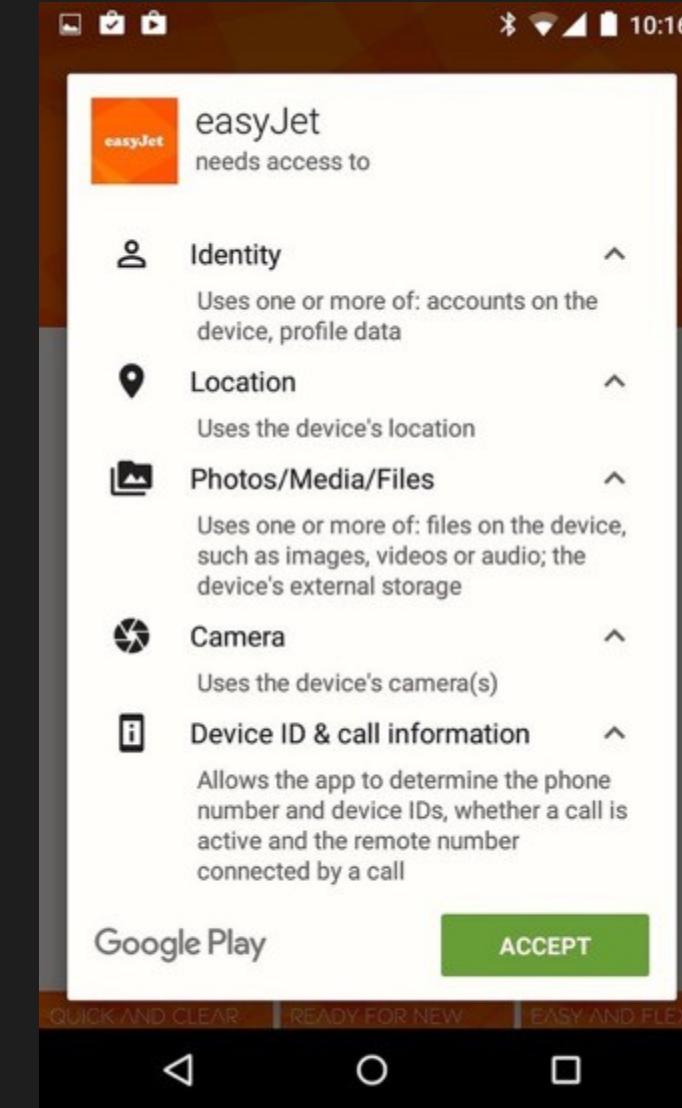
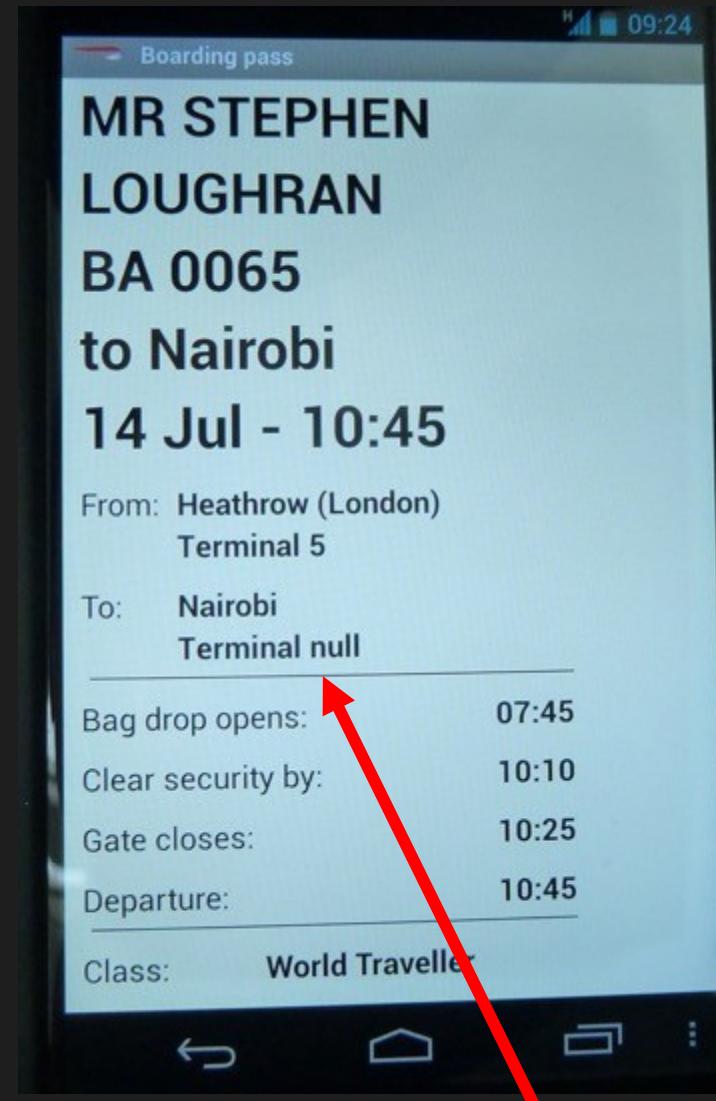
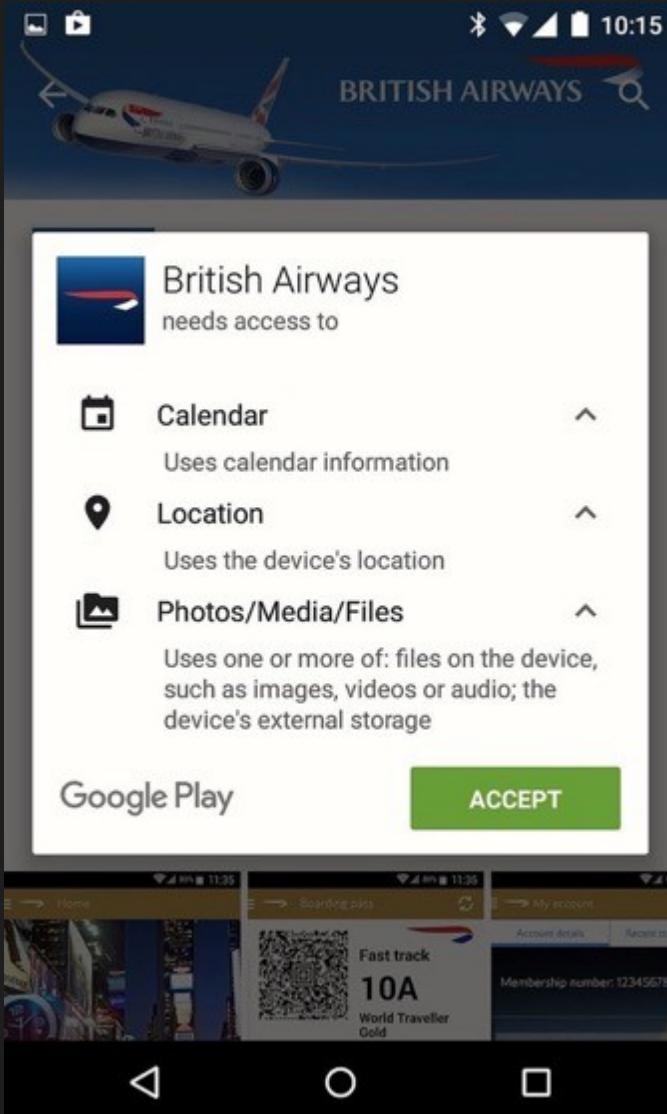
DMZ



...

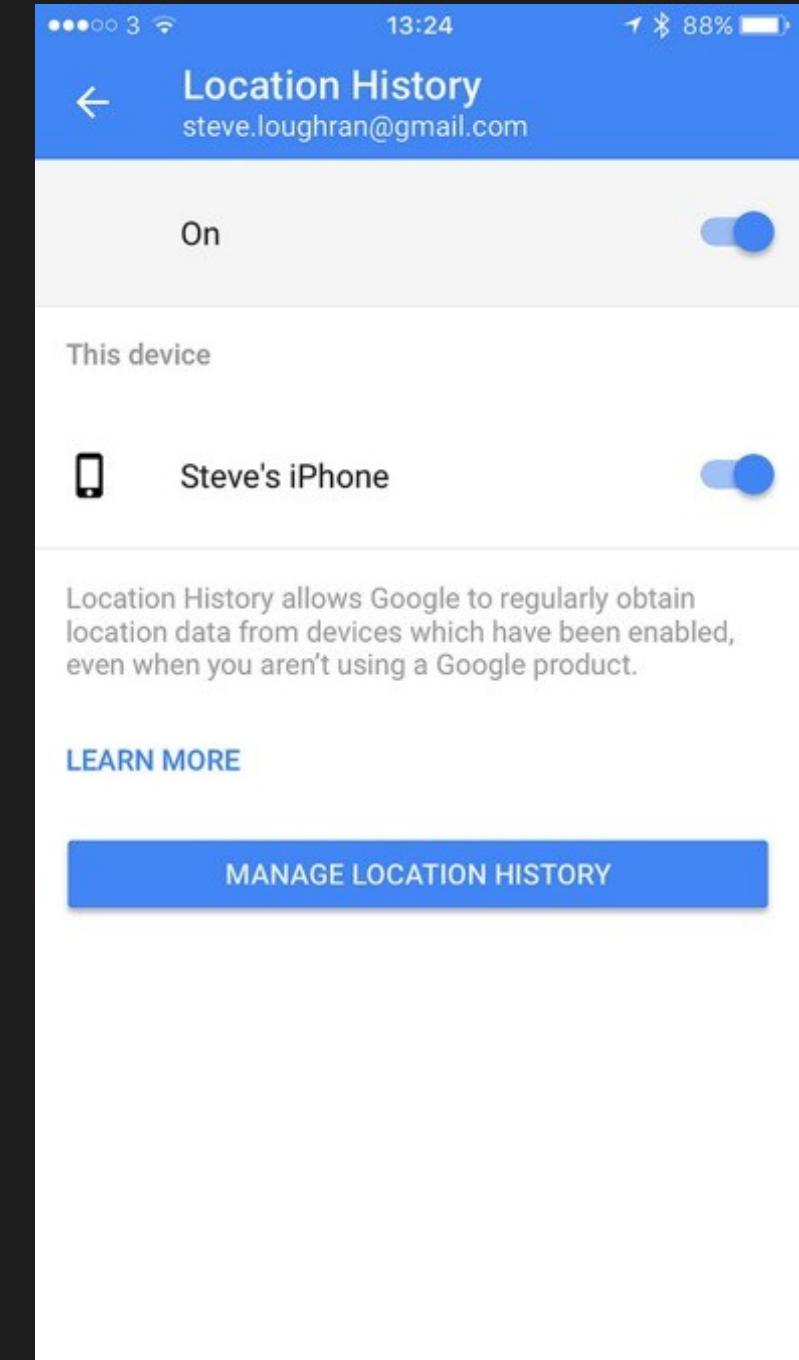
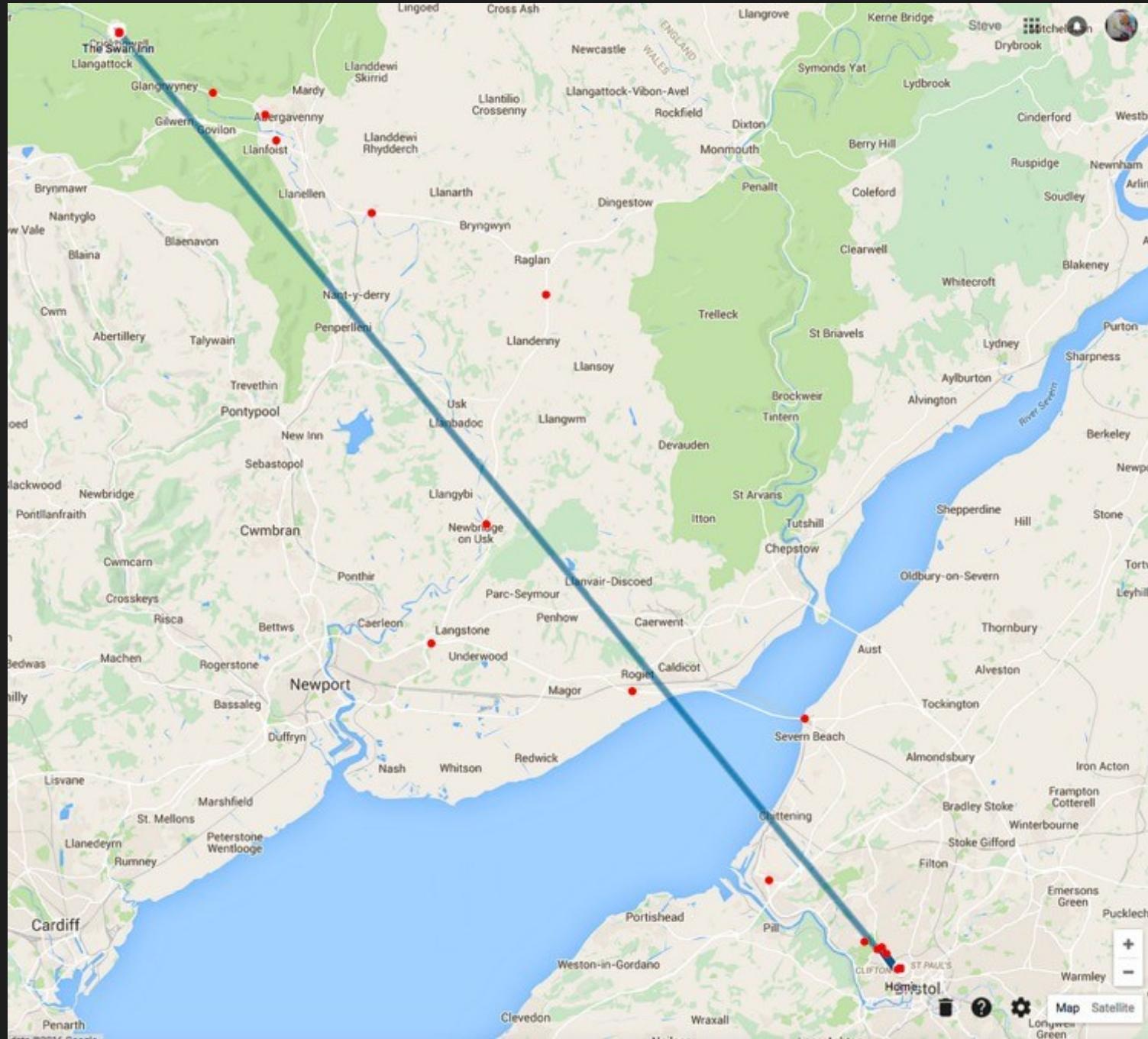
New Netgear
Firewall

Other?



SQL vulnerability?

(?, 11)



iPhone + Google photos (5,1)



(3,1)



Settings

Activating/deactivating sound

1. Call up "Options".
2. "Sound"

Suppressing cookies

1. Call up "Options".
2. "Block cookies"

Change to mobile web page view

1. Call up "Options".
2. "Activate Flash plugin"

Suppressing pop-ups

1. Call up "Options".
2. "Block pop-ups"

Suppress HTTPS warnings

1. Call up "Options".
2. "Block warnings"

Delete personal settings

1. Call up "Options".
2. "Clear personal settings"

HTTPS certificates and history are deleted.

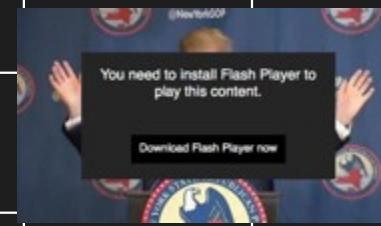
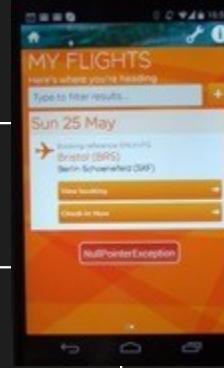


((9?,,

Game over



Privacy (lack of)



Vulnerability

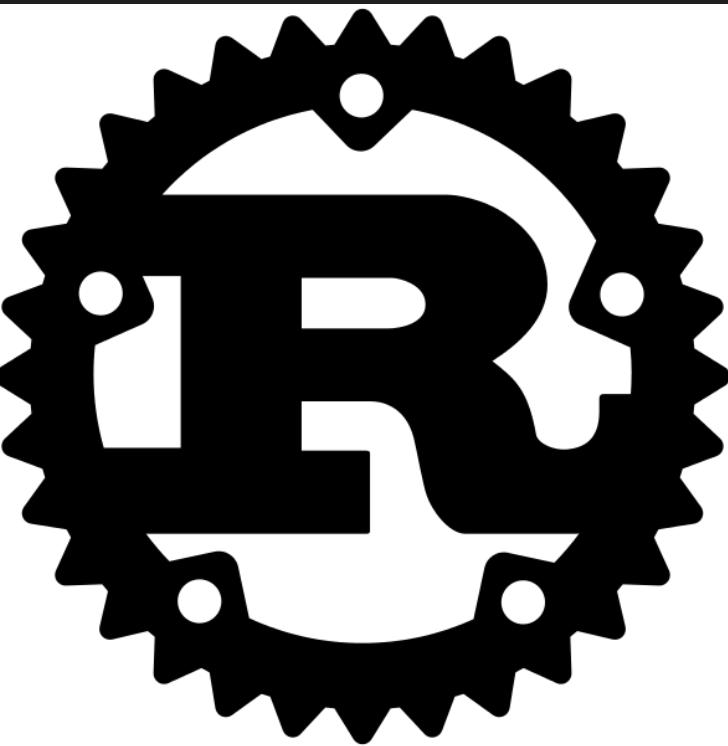




We must fix this in our
code

All external data is malicious

All remote interactions leak
privacy



```
new URL("http://www.starcon.net.kp")  
.toString()
```

java.net.URL (>2, >2)

```
def objectFile[T: ClassTag](  
    path: String,  
    minPartitions: Int): RDD[T] = withScope {  
    sequenceFile(path,  
        classOf[NullWritable],  
        classOf[BytesWritable], minPartitions)  
    .flatMap(x =>  
        Utils.deserialize[Array[T]](  
            x._2.getBytes,  
            Utils.getContextOrSparkClassLoader))  
}
```

SparkContext (0, 9)

OSS everywhere => target



```
apache-hadoop — fish /Users/stevel/Hadoop/commit/apache-hadoop — fish — 136x37
~/H/c/apache-hadoop (branch-2.8) $ git apply --verbose --whitespace=fix \
|   ~./hadoop-patches/incoming/HADOOP-13405.patch
Checking patch hadoop-common-project/hadoop-common/src/main/resources/core-default.xml...
Hunk #1 succeeded at 941 (offset -32 lines).
Checking patch hadoop-tools/hadoop-aws/src/main/java/org/apache/hadoop/fs/s3a/Constants.java...
Hunk #1 succeeded at 133 (offset 5 lines).
Checking patch hadoop-tools/hadoop-aws/src/site/markdown/tools/hadoop-aws/index.md...
Hunk #1 succeeded at 551 (offset -3 lines).
Applied patch hadoop-common-project/hadoop-common/src/main/resources/core-default.xml cleanly.
Applied patch hadoop-tools/hadoop-aws/src/main/java/org/apache/hadoop/fs/s3a/Constants.java cleanly.
Applied patch hadoop-tools/hadoop-aws/src/site/markdown/tools/hadoop-aws/index.md cleanly.
~/H/c/apache-hadoop (branch-2.8) $ git status
On branch branch-2.8
Your branch is up-to-date with 'apache/branch-2.8'.
Changes not staged for commit:
  (use "git add <file>..." to update what will be committed)
  (use "git checkout -- <file>..." to discard changes in working directory)

    modified:   hadoop-common-project/hadoop-common/src/main/resources/core-default.xml
    modified:   hadoop-tools/hadoop-aws/src/main/java/org/apache/hadoop/fs/s3a/Constants.java
    modified:   hadoop-tools/hadoop-aws/src/site/markdown/tools/hadoop-aws/index.md

no changes added to commit (use "git add" and/or "git commit -a")
~/H/c/apache-hadoop (branch-2.8) $ git commit -a -m "HADOOP-13405 doc for fs.s3a.acl.default indicates incorrect values. Contributed by Shen Yinjie"
[branch-2.8 c09797c] HADOOP-13405 doc for fs.s3a.acl.default indicates incorrect values. Contributed by Shen Yinjie
 3 files changed, 8 insertions(+), 8 deletions(-)
~/H/c/apache-hadoop (branch-2.8) $ git push apache
Counting objects: 24, done.
Delta compression using up to 8 threads.
Compressing objects: 100% (16/16), done.
Writing objects: 100% (24/24), 1.82 KiB | 0 bytes/s, done.
Total 24 (delta 12), reused 0 (delta 0)
remote: hadoop git commit: HADOOP-13405 doc for fs.s3a.acl.default indicates incorrect values. Contributed by Shen Yinjie
To https://git-wip-us.apache.org/repos/asf/hadoop.git
 1fe08c9..c09797c branch-2.8 -> branch-2.8
~/H/c/apache-hadoop (branch-2.8) $
```

Apache & github keys

build dependencies

apt-get upgrade

brew upgrade

mvn install

npm update

yum update

pip install

docker pull

...

We need to address this!

(?, ?)

Isolation: containers?

Authentication: PGP validate
mvn...

Audit logs

Questions?

