Copyright 2015 Carnegie Mellon University

This material is based upon work funded and supported by the Department of Defense under Contract No. FA8721-05-C-0003 with Carnegie Mellon University for the operation of the Software Engineering Institute, a federally funded research and development center.

Any opinions, findings and conclusions or recommendations expressed in this material are those of the author(s) and do not necessarily reflect the views of the United States Department of Defense.

NO WARRANTY. THIS CARNEGIE MELLON UNIVERSITY AND SOFTWARE ENGINEERING INSTITUTE MATERIAL IS FURNISHED ON AN “AS-IS” BASIS. CARNEGIE MELLON UNIVERSITY MAKES NO WARRANTIES OF ANY KIND, EITHER EXPRESSED OR IMPLIED, AS TO ANY MATTER INCLUDING, BUT NOT LIMITED TO, WARRANTY OF FITNESS FOR PURPOSE OR MERCHANTABILITY, EXCLUSIVITY, OR RESULTS OBTAINED FROM USE OF THE MATERIAL. CARNEGIE MELLON UNIVERSITY DOES NOT MAKE ANY WARRANTY OF ANY KIND WITH RESPECT TO FREEDOM FROM PATENT, TRADEMARK, OR COPYRIGHT INFRINGEMENT.

DM-0002553

Web Traffic Analysis with CERT Tapioca

Software Engineering Institute
Carnegie Mellon University
Pittsburgh, PA 15213

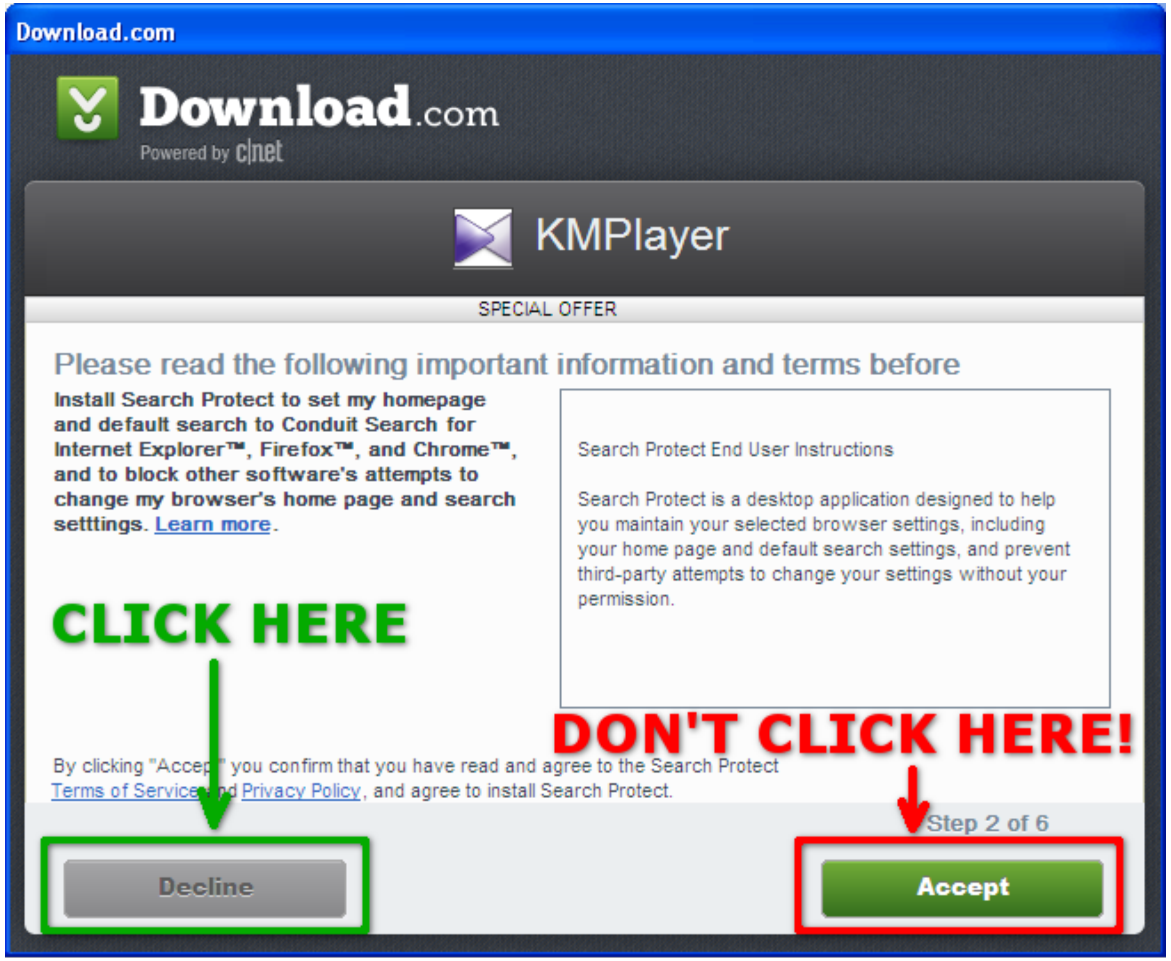
Will Dormann

Web Traffic Analysis with CERT Tapioca

Background

History

Download.com



Please read the following important information and terms before

Install Search Protect to set my homepage and default search to Conduit Search for Internet Explorer™, Firefox™, and Chrome™, and to block other software's attempts to change my browser's home page and search setttings. Learn more.

Search Protect End User Instructions

Search Protect is a desktop application designed to help you maintain your selected browser settings, including your home page and default search settings, and prevent third-party attempts to change your settings without your permission.

By clicking "Accept" you confirm that you have read and agree to the Search Protect Terms of Service and Privacy Policy, and agree to install Search Protect.

http://www.cert.org/blogs/certcc/post.cfm?EntryID=199

Identical installers

Installers from Download.com are the same:

```
5a275a569dce6e2f2f0284d82d31310b *cbsidlm-cbsi213-
Enable__Disable_Registry_Tool-SEO-75812481.exe
5a275a569dce6e2f2f0284d82d31310b *cbsidlm-cbsi213-
KMPlayer-SEO-10659939.exe
```

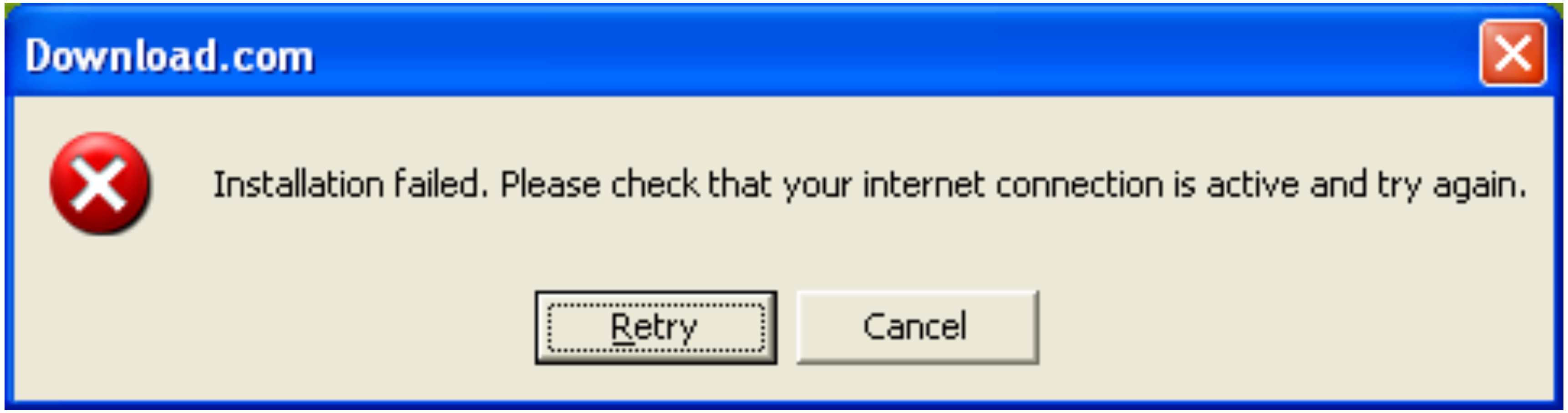
Software retrieval (HTTP)

```
GET /rest/v1.0/softwareProductLink?productSetId=10659939&partTag=dlm&path=SEO&build=213 HTTP/1.1
Host: api.cnet.com
HTTP/1.1 200 OK
<?xml version="1.0" encoding="utf-8"?>
<CNETResponse xmlns="http://api.cnet.com/restApi/v1.0/ns" xmlns:xlink="http://www.w3.org/1999/
xlink" version="1.0"><SoftwareProductLink id="13819308" setId="10659939" appVers="1.0"><Name><!
[CDATA[KMPlayer - 3.9.1.129]]></Name><ProductName><![CDATA[KMPlayer]]></
ProductName><ProductVersion><![CDATA[3.9.1.129]]></ProductVersion><FileName><!
[CDATA[KMPlayer_3.9.1.129.exe]]></FileName><FileSize><![CDATA[35872504]]></
FileSize><FileMd5Checksum><![CDATA[5d0e7d17fc4ef0802a9332c83075047c]]></
FileMd5Checksum><PublishDate><![CDATA[2014-10-06]]></PublishDate><CategoryId><![CDATA[13632]]></
CategoryId><Category><![CDATA[Downloads^Video Software^Video Players]]></Category><License><!
[CDATA[Free]]></License><DownloadLink>http://software-files-a.cnet.com/s/software/13/81/93/08/
KMPlayer_3.9.1.129.exe?token=1413054436_d56f7814cd5af230f782dd28550e185a</
DownloadLink><TrackedDownloadLink>http://dw.cbsi.com/redir?
edId=1174&amp;siteId=4&amp;lop=feed.dl&amp;ontId=13632&amp;tag=tdw_dlman&amp;pid=13819308&amp;de
stUrl=http%3A%2F%2Fsoftware-files-a.cnet.com%2Fs%2Fsoftware
%2F13%2F81%2F93%2F08%2FKMPlayer_3.9.1.129.exe%3Ftoken
%3D1413054436_2defb65a1350a3b035964c18f30fb06e%26fileName%3DKMPlayer_3.9.1.129.exe
```

Just MITM it!

Set up a proxy to modify content as it's transferred

Problem: Installer isn't proxy-aware!



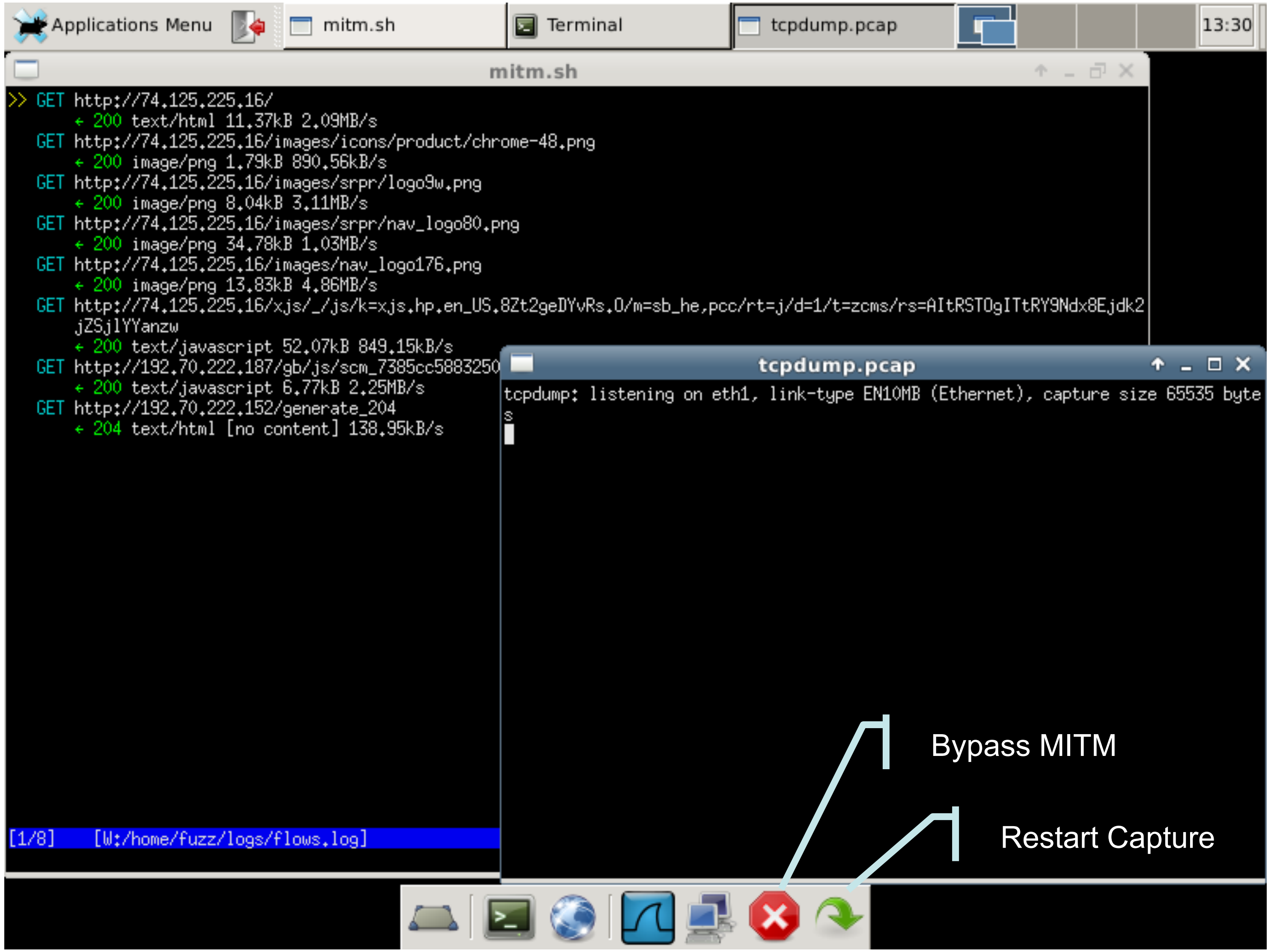
Download.com

Installation failed. Please check that your internet connection is active and try again.

Solution: CERT Tapioca

Transparent Proxy Capture Appliance

UbuFuzz + iptables + mitmproxy

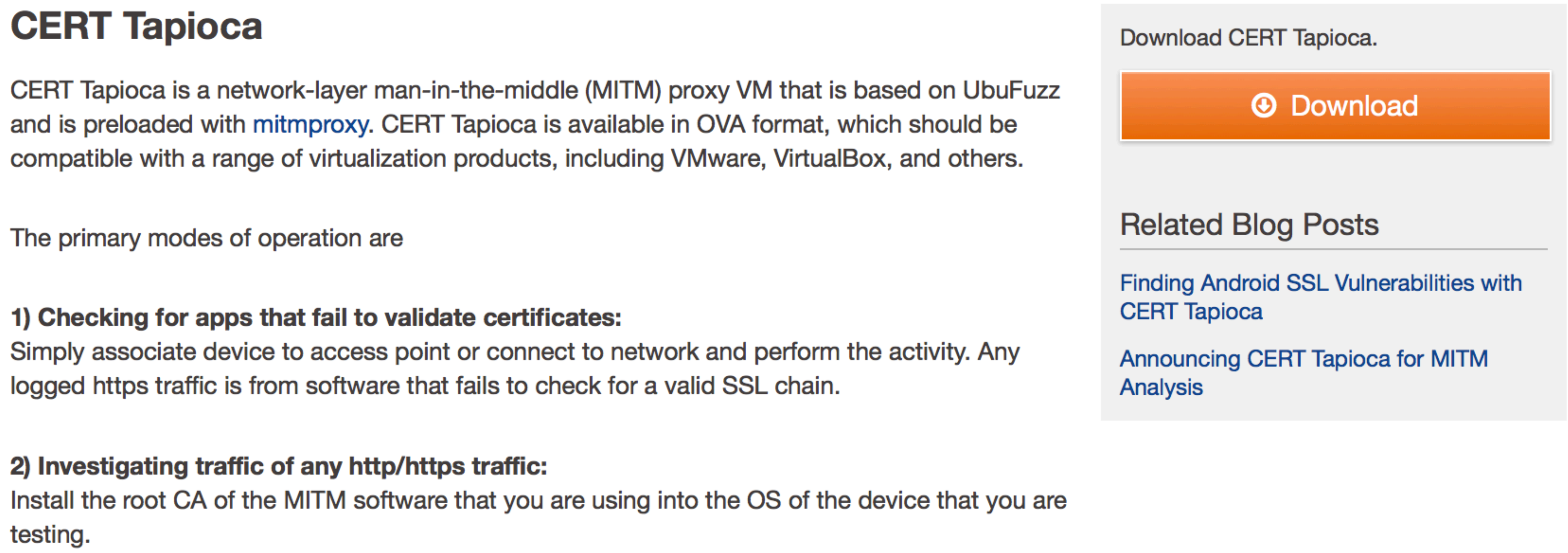


```
>> GET http://74.125.225.16/
       ← 200 text/html 11.37kB 2.09MB/s
   GET http://74.125.225.16/images/icons/product/chrome-48.png
       ← 200 image/png 1.79kB 890.56kB/s
   GET http://74.125.225.16/images/srpr/logo9w.png
       ← 200 image/png 8.04kB 3.11MB/s
   GET http://74.125.225.16/images/srpr/nav_logo80.png
       ← 200 image/png 34.78kB 1.03MB/s
   GET http://74.125.225.16/images/nav_logo176.png
       ← 200 image/png 13.83kB 4.86MB/s
   GET http://74.125.225.16/xjs/_/js/k=xjs.hp.en_US.8Zt2geDYvRs.0/m=sb_he,pcc/rt=j/d=1/t=zcms/rs=AItRSTOgITtRY9Ndx8Ejdk2
       jZSjlYYanzw
       ← 200 text/javascript 52.07kB 849.15kB/s
   GET http://192.70.222.187/gb/js/scm_7385cc5883250
       ← 200 text/javascript 6.77kB 2.25MB/s
   GET http://192.70.222.152/generate_204
       ← 204 text/html [no content] 138.95kB/s

[1/8]    [W:/home/fuzz/logs/flows.log]
```

```
tcpdump: listening on eth1, link-type EN10MB (Ethernet), capture size 65535 byte
s
```

CERT Tapioca



CERT Tapioca

CERT Tapioca is a network-layer man-in-the-middle (MITM) proxy VM that is based on UbuFuzz and is preloaded with mitmproxy. CERT Tapioca is available in OVA format, which should be compatible with a range of virtualization products, including VMware, VirtualBox, and others.

The primary modes of operation are

1) Checking for apps that fail to validate certificates:
Simply associate device to access point or connect to network and perform the activity. Any logged https traffic is from software that fails to check for a valid SSL chain.

2) Investigating traffic of any http/https traffic:
Install the root CA of the MITM software that you are using into the OS of the device that you are testing.

Download CERT Tapioca.

Related Blog Posts

Finding Android SSL Vulnerabilities with CERT Tapioca

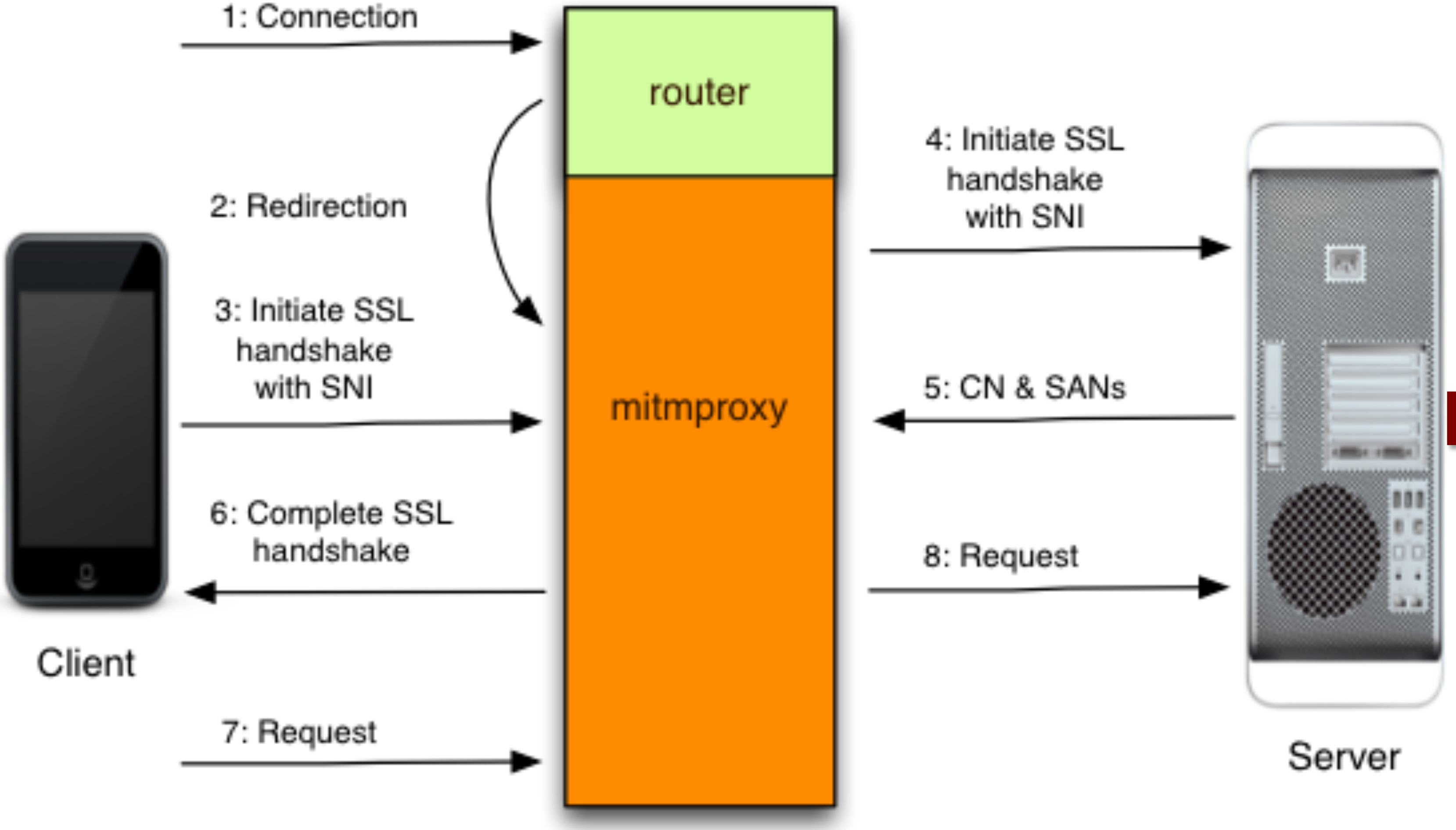
Announcing CERT Tapioca for MITM Analysis

http://www.cert.org/vulnerability-analysis/tools/cert-tapioca.cfm

How it works

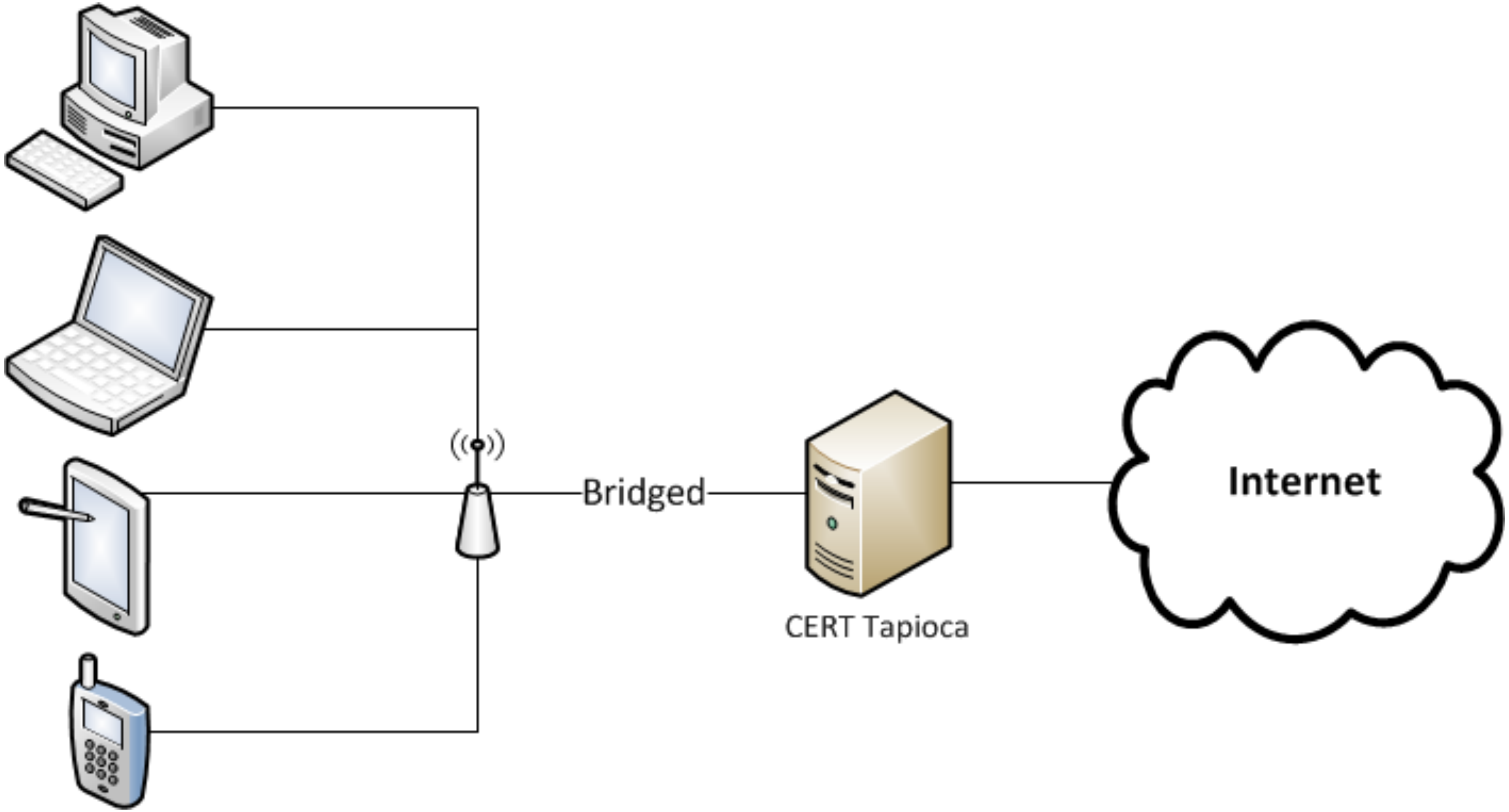
I can see everything if the client doesn’t validate SSL

Invalid SSL handshake

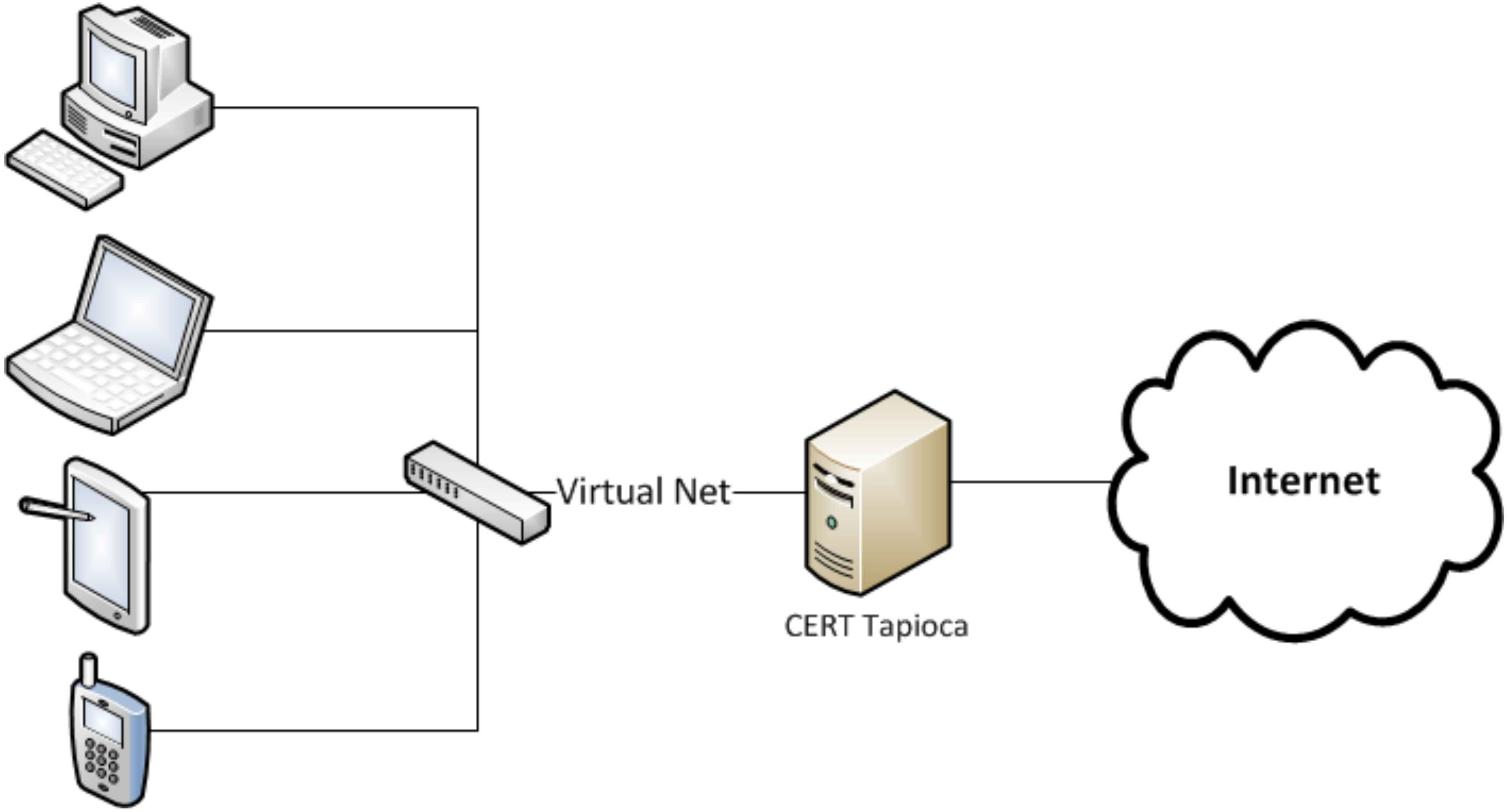

1: Connection
router
2: Redirection
3: Initiate SSL handshake with SNI
mitmproxy
4: Initiate SSL handshake with SNI
5: CN & SANs
6: Complete SSL handshake
Client
7: Request
8: Request
Server

Valid SSL handshake

Tapioca architecture



Tapioca architecture



CERT Tapioca Operating Modes

Without certificate installed:

- Every application that passes HTTPS traffic is failing to validate SSL certificates
- Useful for finding insecure applications

With certificate installed:

- I can view traffic that would otherwise be protected
- Useful for knowing what data is being sent over the network

Polling Question

When you visit a site on the internet, how do you know you're viewing the actual, legitimate site?

Web Traffic Analysis with CERT Tapioca

Android Apps and SSL Validation

Investigating Android

Use a phone and a wireless access point

Automation Improvement

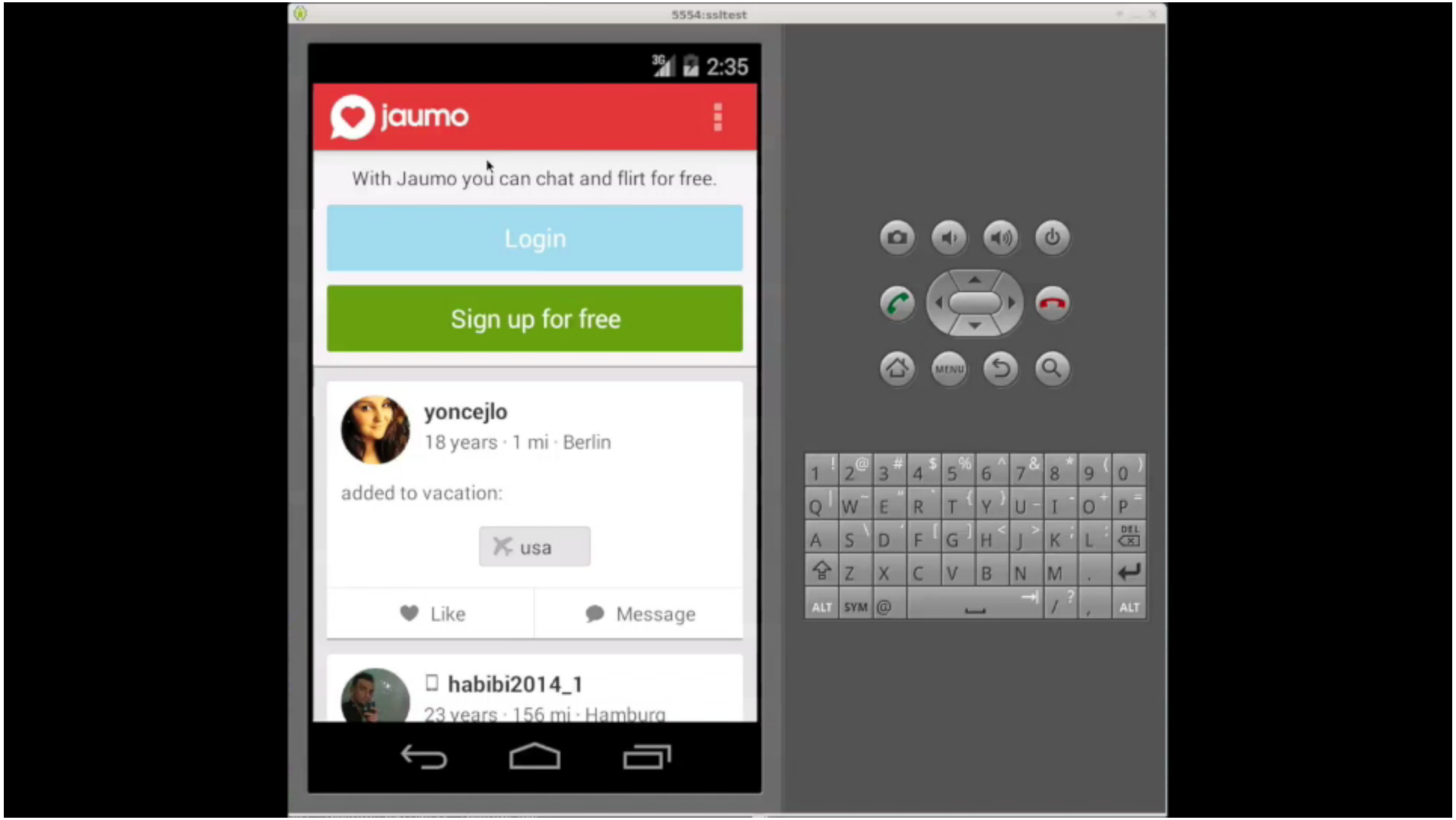
Emulation and Automation

- google-play-crawler
- VMware
- Android SDK
- AVD
- Monkeyrunner
- Monkey

Now I can test when I sleep!

https://github.com/Akdeniz/google-play-crawler
http://developer.android.com/tools/help/monkeyrunner_concepts.html
http://developer.android.com/tools/help/monkey.html
http://www.cert.org/blogs/certcc/post.cfm?EntryID=204

Automated Android



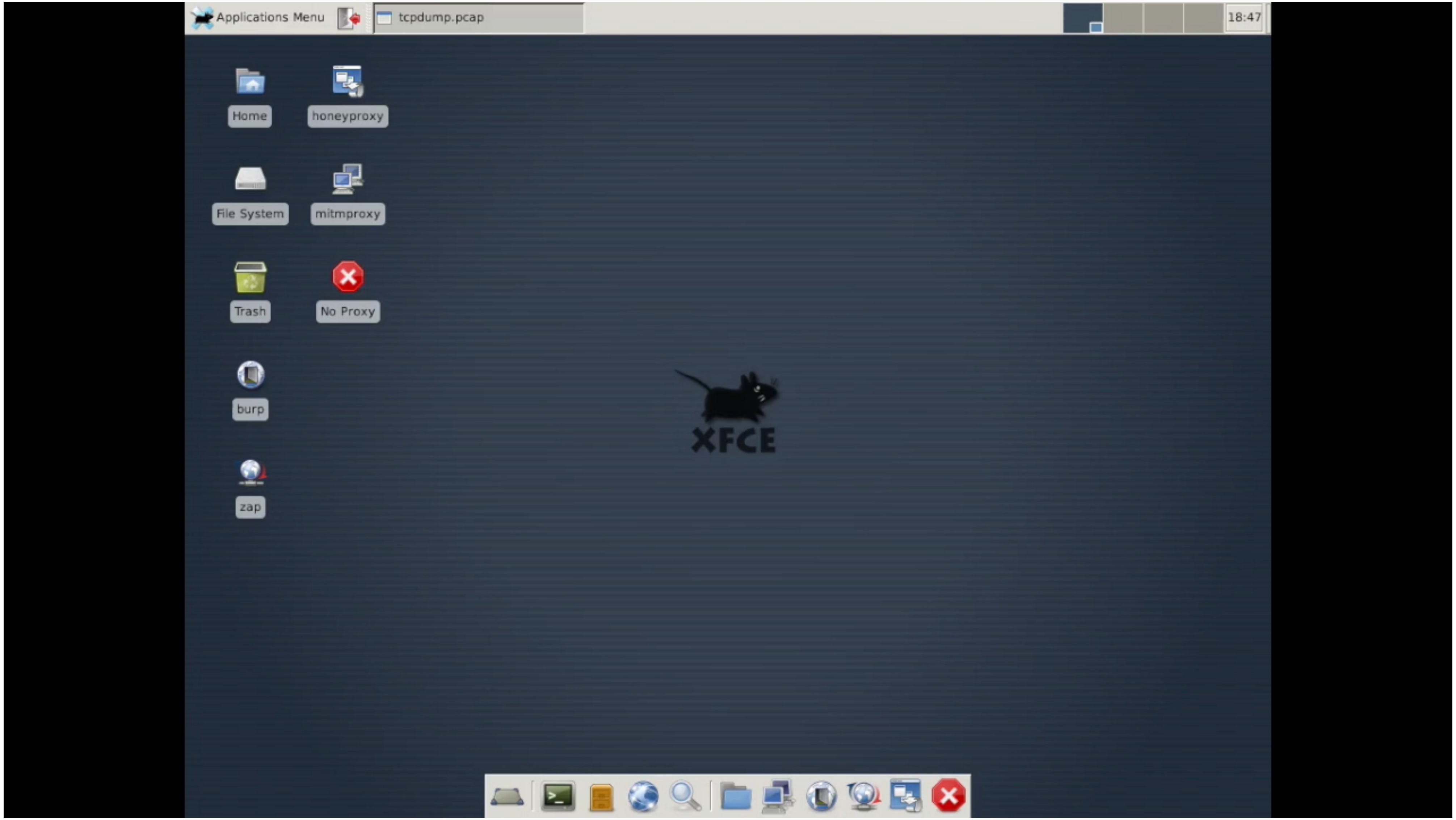
With Jaumo you can chat and flirt for free.

yoncejlo
18 years · 1 mi · Berlin

added to vacation:

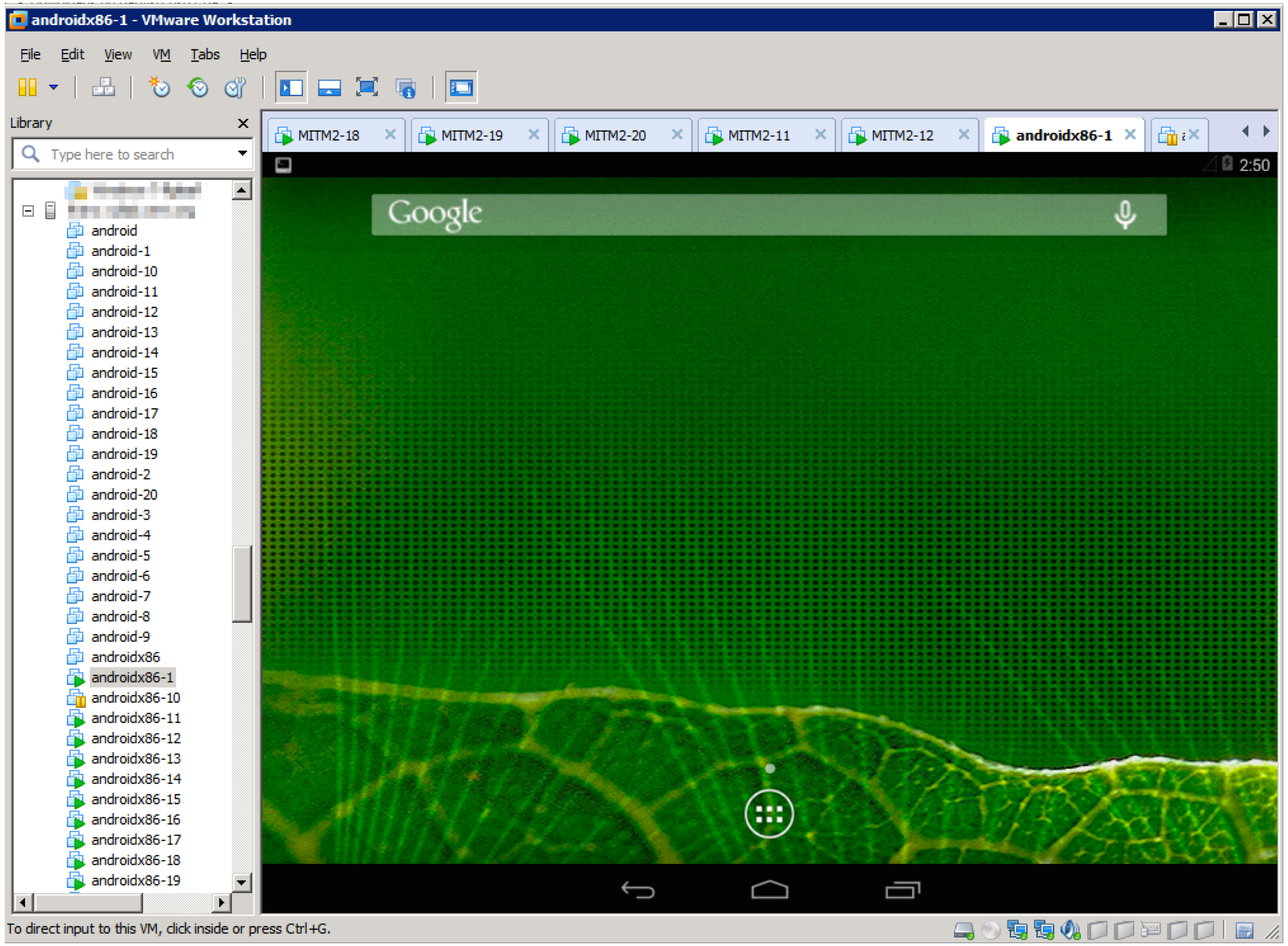
habibi2014_1
23 years · 156 mi · Hamburg

CERT Tapioca



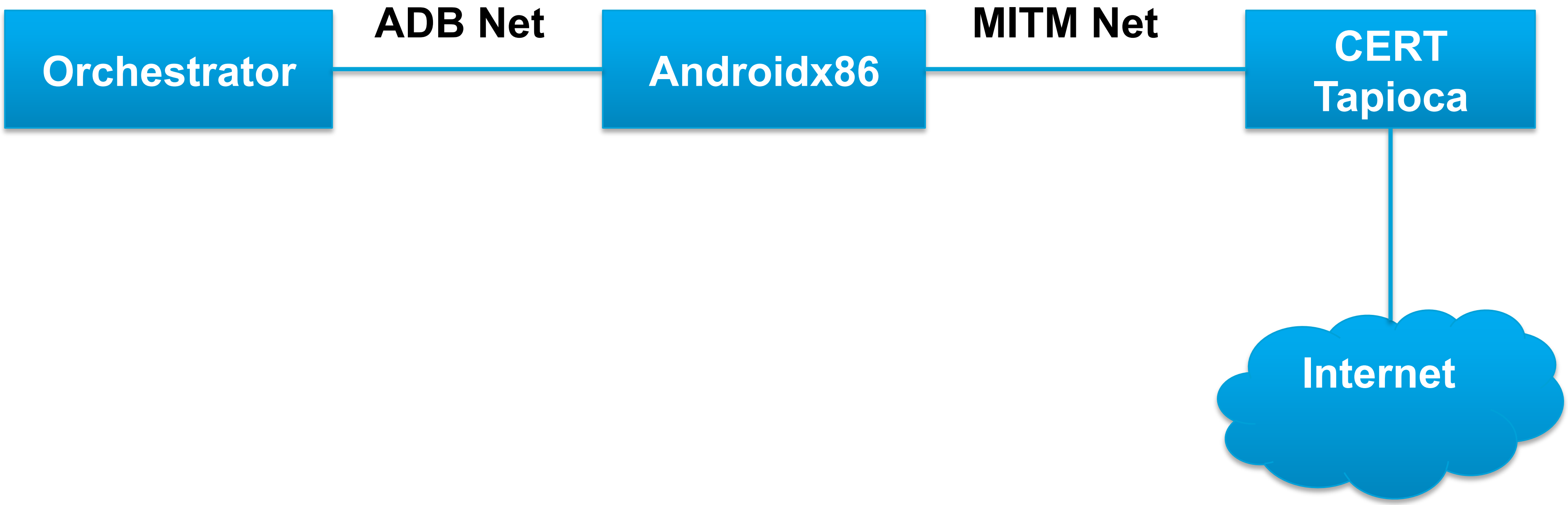
Virtualization

http://www.android-x86.org/

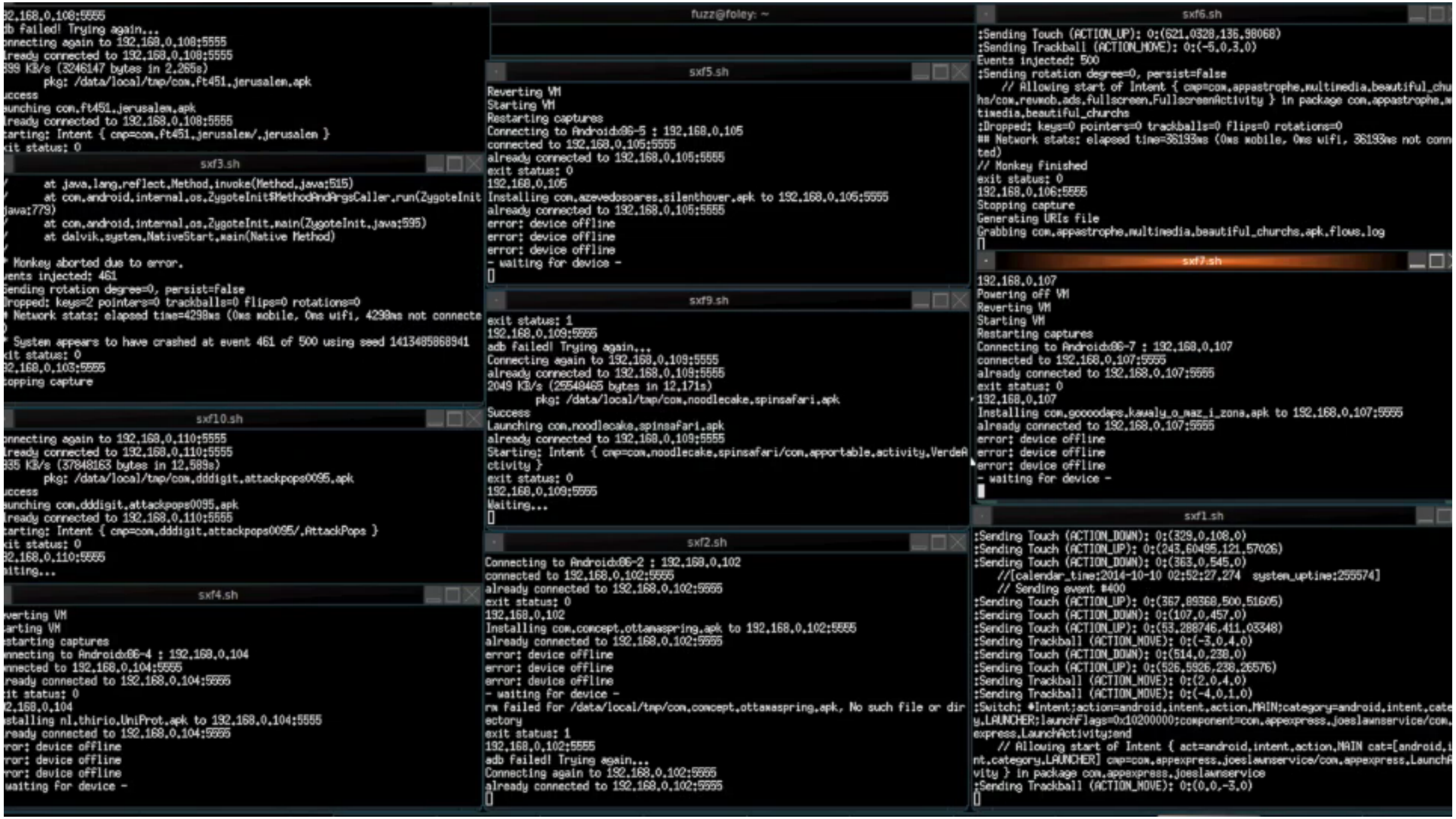


To direct input to this VM, click inside or press Ctrl+G.

Androidx86 SSL Test Architecture



Automation of 20 VMs



```
2.168.0.108:5555
db failed! Trying again...
onnecting again to 192.168.0.108:5555
lready connected to 192.168.0.108:5555
399 KB/s (3246147 bytes in 2.265s)
        pkg: /data/local/tmp/com.ft451.jerusalem.apk
uccess
aunching com.ft451.jerusalem.apk
lready connected to 192.168.0.108:5555
tarting: Intent { cmp=com.ft451.jerusalem/.jerusalem }
xit status: 0
```

sxf3.sh

```
/       at java.lang.reflect.Method.invoke(Method.java:515)
/       at com.android.internal.os.ZygoteInit$MethodAndArgsCaller.run(ZygoteInit
java:779)
/       at com.android.internal.os.ZygoteInit.main(ZygoteInit.java:595)
/       at dalvik.system.NativeStart.main(Native Method)
/
* Monkey aborted due to error.
vents injected: 461
Sending rotation degree=0, persist=false
Dropped: keys=2 pointers=0 trackballs=0 flips=0 rotations=0
# Network stats: elapsed time=4298ms (0ms mobile, 0ms wifi, 4298ms not connecte
)
* System appears to have crashed at event 461 of 500 using seed 1413485868941
xit status: 0
2.168.0.103:5555
topping capture
```

sxf10.sh

```
onnecting again to 192.168.0.110:5555
lready connected to 192.168.0.110:5555
935 KB/s (37848163 bytes in 12.589s)
        pkg: /data/local/tmp/com.dddigit.attackpops0095.apk
uccess
aunching com.dddigit.attackpops0095.apk
lready connected to 192.168.0.110:5555
tarting: Intent { cmp=com.dddigit.attackpops0095/.AttackPops }
xit status: 0
2.168.0.110:5555
aiting...
```

sxf4.sh

```
verting VM
arting VM
starting captures
nnecting to Androidx86-4 : 192.168.0.104
nnected to 192.168.0.104:5555
ready connected to 192.168.0.104:5555
it status: 0
2.168.0.104
stalling nl.thirio.UniProt.apk to 192.168.0.104:5555
ready connected to 192.168.0.104:5555
ror: device offline
ror: device offline
ror: device offline
waiting for device -
```

fuzz@foley: ~

sxf5.sh

```
Reverting VM
Starting VM
Restarting captures
Connecting to Androidx86-5 : 192.168.0.105
connected to 192.168.0.105:5555
already connected to 192.168.0.105:5555
exit status: 0
192.168.0.105
Installing com.azevedosoares.silenthover.apk to 192.168.0.105:5555
already connected to 192.168.0.105:5555
error: device offline
error: device offline
error: device offline
- waiting for device -
▯
```

sxf9.sh

```
exit status: 1
192.168.0.109:5555
adb failed! Trying again...
Connecting again to 192.168.0.109:5555
already connected to 192.168.0.109:5555
2049 KB/s (25548465 bytes in 12.171s)
        pkg: /data/local/tmp/com.noodlecake.spinsafari.apk
Success
Launching com.noodlecake.spinsafari.apk
already connected to 192.168.0.109:5555
Starting: Intent { cmp=com.noodlecake.spinsafari/com.apportable.activity.VerdeA
ctivity }
exit status: 0
192.168.0.109:5555
Waiting...
▯
```

sxf2.sh

```
Connecting to Androidx86-2 : 192.168.0.102
connected to 192.168.0.102:5555
already connected to 192.168.0.102:5555
exit status: 0
192.168.0.102
Installing com.concept.ottawaspring.apk to 192.168.0.102:5555
already connected to 192.168.0.102:5555
error: device offline
error: device offline
error: device offline
- waiting for device -
rm failed for /data/local/tmp/com.concept.ottawaspring.apk, No such file or dir
ectory
exit status: 1
192.168.0.102:5555
adb failed! Trying again...
Connecting again to 192.168.0.102:5555
already connected to 192.168.0.102:5555
▯
```

sxf6.sh

```
:Sending Touch (ACTION_UP): 0:(621.0328,136.98068)
:Sending Trackball (ACTION_MOVE): 0:(-5.0,3.0)
Events injected: 500
:Sending rotation degree=0, persist=false
    // Allowing start of Intent { cmp=com.appastrophe.multimedia.beautiful_chu
hs/com.revmob.ads.fullscreen.FullscreenActivity } in package com.appastrophe.m
timedia.beautiful_churchs
:Dropped: keys=0 pointers=0 trackballs=0 flips=0 rotations=0
## Network stats: elapsed time=36193ms (0ms mobile, 0ms wifi, 36193ms not conn
ted)
// Monkey finished
exit status: 0
192.168.0.106:5555
Stopping capture
Generating URIs file
Grabbing com.appastrophe.multimedia.beautiful_churchs.apk.flows.log
▯
```

sxf7.sh

```
192.168.0.107
Powering off VM
Reverting VM
Starting VM
Restarting captures
Connecting to Androidx86-7 : 192.168.0.107
connected to 192.168.0.107:5555
already connected to 192.168.0.107:5555
exit status: 0
192.168.0.107
Installing com.goooodaps.kawaly_o_maz_i_zona.apk to 192.168.0.107:5555
already connected to 192.168.0.107:5555
error: device offline
error: device offline
error: device offline
- waiting for device -
█
```

sxf1.sh

```
:Sending Touch (ACTION_DOWN): 0:(329.0,108.0)
:Sending Touch (ACTION_UP): 0:(243.60495,121.57026)
:Sending Touch (ACTION_DOWN): 0:(363.0,545.0)
    //[calendar_time:2014-10-10 02:52:27.274  system_uptime:255574]
    // Sending event #400
:Sending Touch (ACTION_UP): 0:(367.89368,500.51605)
:Sending Touch (ACTION_DOWN): 0:(107.0,457.0)
:Sending Touch (ACTION_UP): 0:(53.288746,411.03348)
:Sending Trackball (ACTION_MOVE): 0:(-3.0,4.0)
:Sending Touch (ACTION_DOWN): 0:(514.0,238.0)
:Sending Touch (ACTION_UP): 0:(526.5926,238.26576)
:Sending Trackball (ACTION_MOVE): 0:(2.0,4.0)
:Sending Trackball (ACTION_MOVE): 0:(-4.0,1.0)
:Switch: #Intent;action=android.intent.action.MAIN;category=android.intent.cate
y.LAUNCHER;launchFlags=0x10200000;component=com.appexpress.joeslawnservice/com.
express.LaunchActivity;end
    // Allowing start of Intent { act=android.intent.action.MAIN cat=[android.i
nt.category.LAUNCHER] cmp=com.appexpress.joeslawnservice/com.appexpress.LaunchA
vity } in package com.appexpress.joeslawnservice
:Sending Trackball (ACTION_MOVE): 0:(0.0,-3.0)
▯
```

The Numbers

	Total	Percent
Free Apps Tested	1,000,500	Most?
Vulnerable Apps Discovered	23,667	2.4%
Vulnerable App Authors Notified	23,301	98.5%
Email responses	1,593	6.8%
Email responses with fix details	25	0.1%

“There are now 1 million apps in the Google Play store.”

July 24, 2013

http://mashable.com/2013/07/24/google-play-1-million/

Web Traffic Analysis with CERT Tapioca

SSL Inspecting Proxies

HTTPS Background

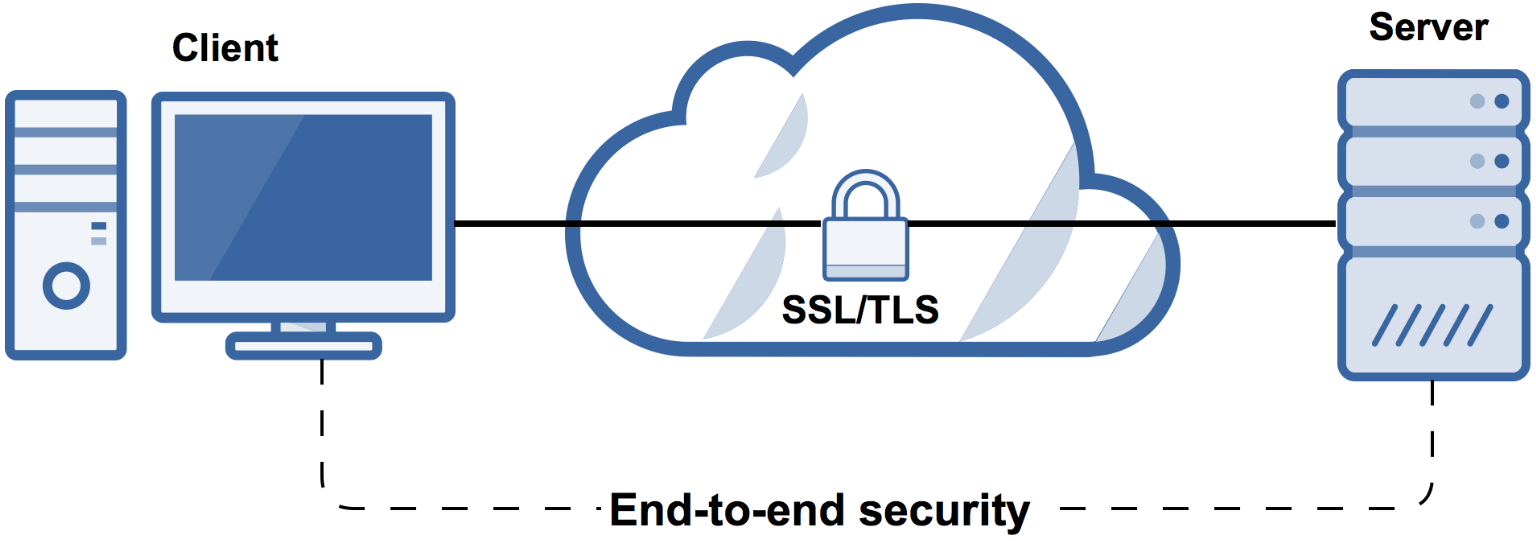
Often referred to as simply “SSL”, there are several technologies involved.

- HTTPS is HTTP secured by either
  - SSL (obsolete)
  - TLS

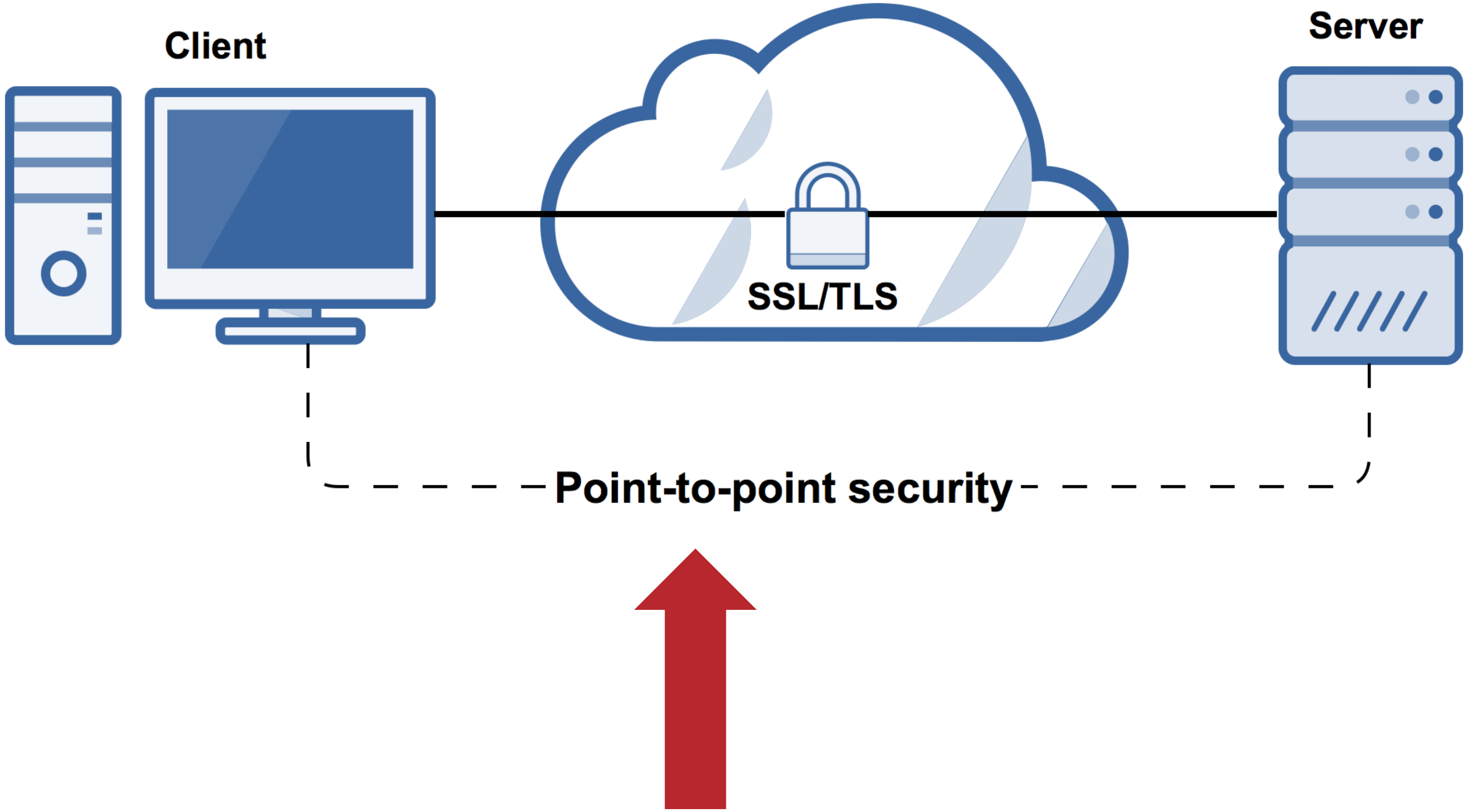
Goals:

- Authentication of visited site
- Privacy and integrity of data

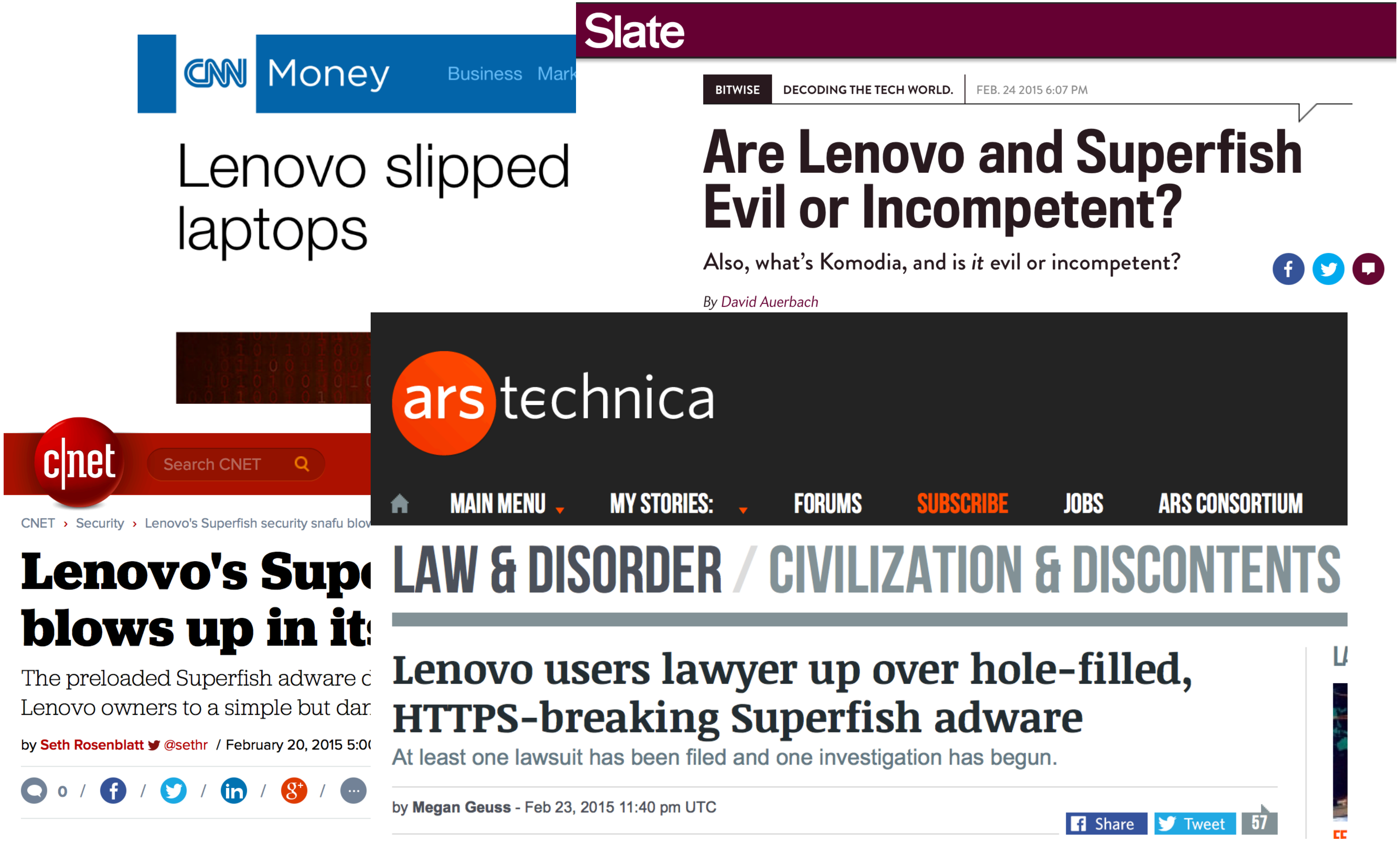
HTTPS Expectation



HTTPS Reality



Superfish



CNN Money

Lenovo slipped laptops

Slate

BITWISE | DECODING THE TECH WORLD. | FEB. 24 2015 6:07 PM

Are Lenovo and Superfish Evil or Incompetent?

Also, what's Komodia, and is *it* evil or incompetent?

By David Auerbach

cnet

CNET › Security › Lenovo's Superfish security snafu blow

Lenovo's Sup blows up in it

The preloaded Superfish adware c Lenovo owners to a simple but dar

by Seth Rosenblatt @sethr / February 20, 2015 5:0

ars technica

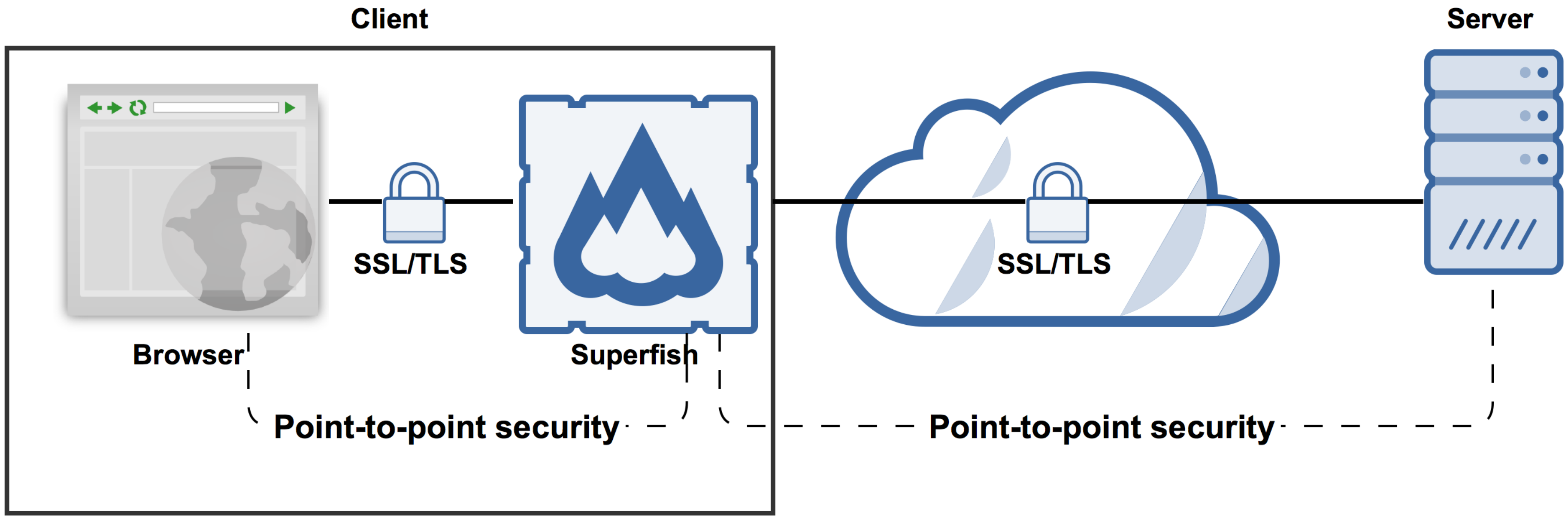
LAW & DISORDER / CIVILIZATION & DISCONTENTS

Lenovo users lawyer up over hole-filled, HTTPS-breaking Superfish adware

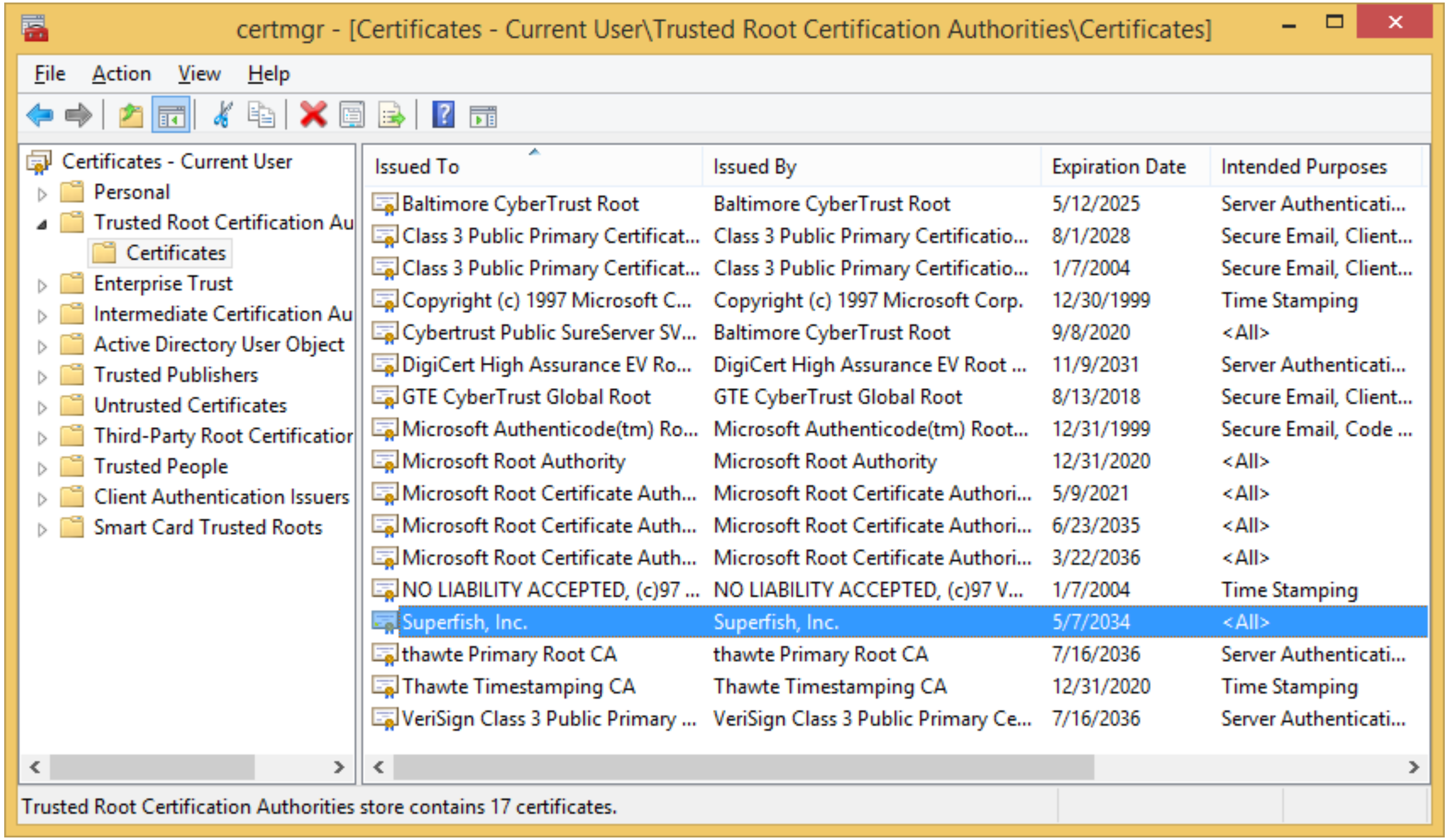
At least one lawsuit has been filed and one investigation has begun.

by **Megan Geuss** - Feb 23, 2015 11:40 pm UTC

How Can Superfish Work?



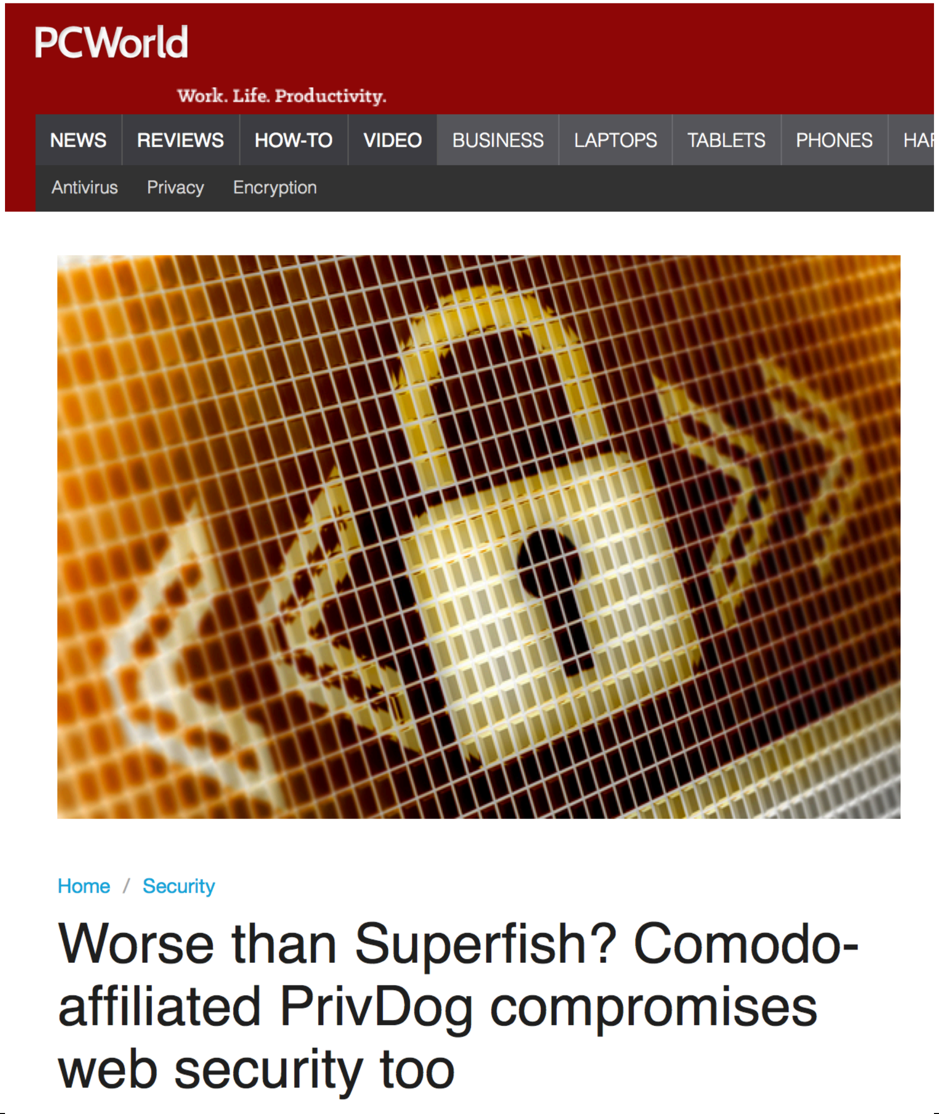
How Can Superfish Work?


certmgr - [Certificates - Current User\Trusted Root Certification Authorities\Certificates]
File
Action
View
Help
Certificates - Current User
Personal
Trusted Root Certification Au
Certificates
Enterprise Trust
Intermediate Certification Au
Active Directory User Object
Trusted Publishers
Untrusted Certificates
Third-Party Root Certification
Trusted People
Client Authentication Issuers
Smart Card Trusted Roots

Issued To	Issued By	Expiration Date	Intended Purposes
Baltimore CyberTrust Root	Baltimore CyberTrust Root	5/12/2025	Server Authenticati...
Class 3 Public Primary Certificat...	Class 3 Public Primary Certificatio...	8/1/2028	Secure Email, Client...
Class 3 Public Primary Certificat...	Class 3 Public Primary Certificatio...	1/7/2004	Secure Email, Client...
Copyright (c) 1997 Microsoft C...	Copyright (c) 1997 Microsoft Corp.	12/30/1999	Time Stamping
Cybertrust Public SureServer SV...	Baltimore CyberTrust Root	9/8/2020	<All>
DigiCert High Assurance EV Ro...	DigiCert High Assurance EV Root ...	11/9/2031	Server Authenticati...
GTE CyberTrust Global Root	GTE CyberTrust Global Root	8/13/2018	Secure Email, Client...
Microsoft Authenticode(tm) Ro...	Microsoft Authenticode(tm) Root...	12/31/1999	Secure Email, Code ...
Microsoft Root Authority	Microsoft Root Authority	12/31/2020	<All>
Microsoft Root Certificate Auth...	Microsoft Root Certificate Authori...	5/9/2021	<All>
Microsoft Root Certificate Auth...	Microsoft Root Certificate Authori...	6/23/2035	<All>
Microsoft Root Certificate Auth...	Microsoft Root Certificate Authori...	3/22/2036	<All>
NO LIABILITY ACCEPTED, (c)97 ...	NO LIABILITY ACCEPTED, (c)97 V...	1/7/2004	Time Stamping
Superfish, Inc.	Superfish, Inc.	5/7/2034	<All>
thawte Primary Root CA	thawte Primary Root CA	7/16/2036	Server Authenticati...
Thawte Timestamping CA	Thawte Timestamping CA	12/31/2020	Time Stamping
VeriSign Class 3 Public Primary ...	VeriSign Class 3 Public Primary Ce...	7/16/2036	Server Authenticati...

Trusted Root Certification Authorities store contains 17 certificates.

Not Just Superfish



Worse than Superfish? Comodo-affiliated PrivDog compromises web security too

What Else?

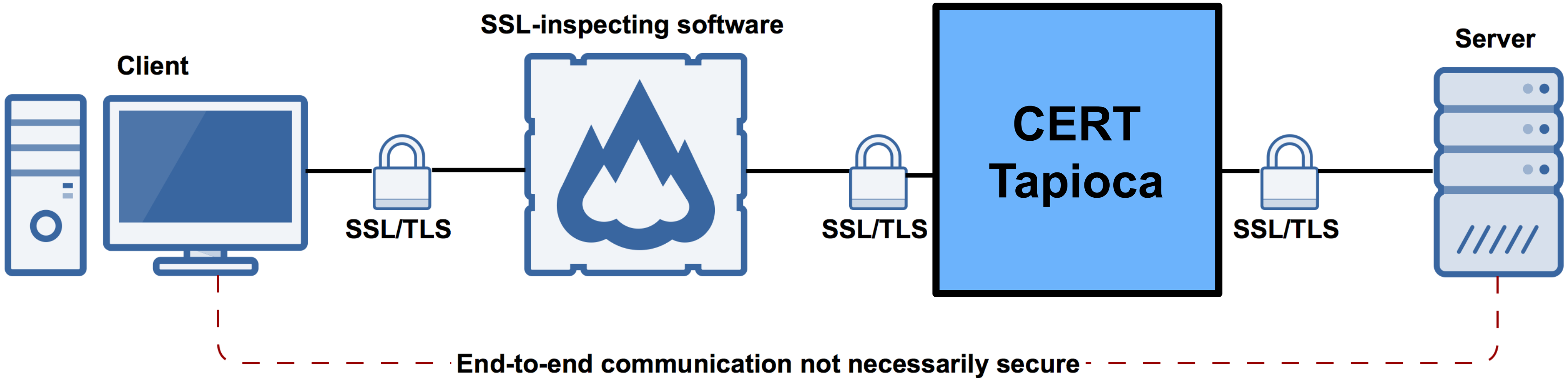
SSL-inspecting proxies

How Common Is SSL Inspection?

1. A10 vThunder
2. Arbor Networks Pravail
3. Baracuda Web Filter
4. BASCOM School Web Filter
5. Bloxx Web Filter
6. Blue Coat SSL Visibility Appliance
7. Check Point Data Loss Prevention (DLP), Anti Virus, Anti-Bot, Application Control, URL Filtering, Threat Emulation and IPS.
8. Cisco ScanCenter
9. Citrix NetScaler AppFirewall
10. Clearswift SECURE Web Gateway
11. ContentKeeper
12. Cymphonix Internet Management Suite
13. Dell SonicWALL
14. EdgeWave iPrism Web Security
15. ESET Smart Security
16. F5 BIG-IP
17. Fortinet FortiGate
18. Fidelis Security XPS
19. Finjan Vital Security (pdf)
20. GFI WebMonitor
21. GigaMon GigaSmart
22. IBM Security Network Protection
23. iboss Web Security
24. iSHERIFF Cloud Security
25. Juniper IDP devices
26. Kaspersky Anti-Virus
27. Komodia SSL Decoder
28. M86 Secure Web Gateway (pdf)
29. McAfee Web Gateway and Firewall Enterprise (pdf)
30. Microsoft Forefront TMG
31. NetNanny
32. NextGig Netronome
33. Optenet WebFilter (pdf)
34. Palo Alto PAN-OS
35. Panda Cloud Internet Protection
36. PrivDog
37. Radware AppXcel
38. SafeNet eSafe Web Security Gateway
39. Sangfor IAM (pdf)
40. Smoothwall Secure Web Gateway
41. Sophos Cyberoam
42. Sourcefire SSL Appliance
43. Squid
44. Symantec Web Gateway
45. Thomason Technologies Next Gen IPS
46. Trend Micro Deep Security (pdf)
47. Trustwave WebMarshal, Secure Web Gateway
48. Untangle NG Firewall
49. Venafi TrustAuthority
50. VSS Monitoring vInspector (pdf)
51. WatchGuard HTTPS Proxy
52. Wavecrest CyBlock
53. WebSense Content Gateway
54. WebTitan
55. Qbik WinGate
56. WolfSSL SSL Inspection
57. Zscaler
58. ZyXel Firewall

https://www.cert.org/blogs/certcc/post.cfm?EntryID=221

SSL Inspection Software



SSL Inspection Software Mistakes

- Incomplete validation of upstream certificate validity
- Not conveying validation of upstream certificate to the client
- Overloading of certificate Canonical Name (CN) field
- Use of application layer to convey certificate validity
- Use of a User-Agent HTTP header to determine when to validate a certificate
- Communication before warning
- Same root CA certificate

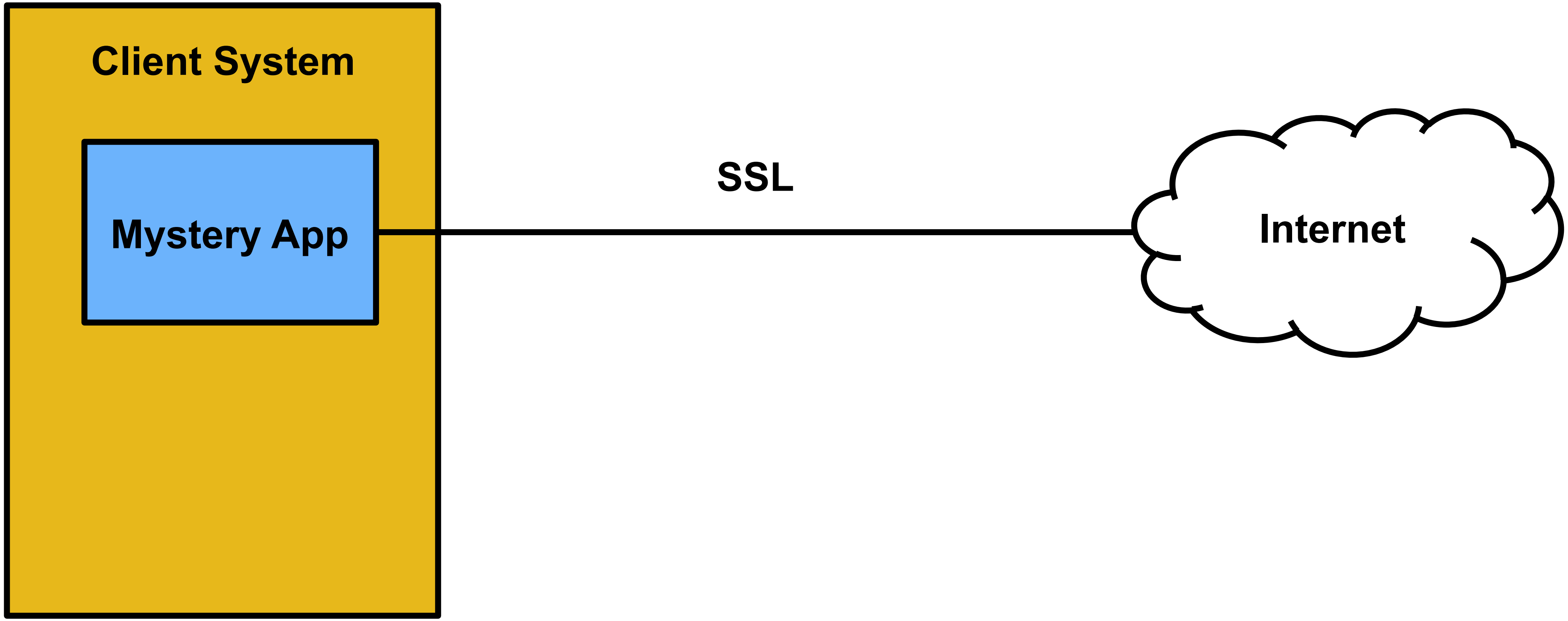
Polling Question

What type of SSL validation mistakes would you like more details about?

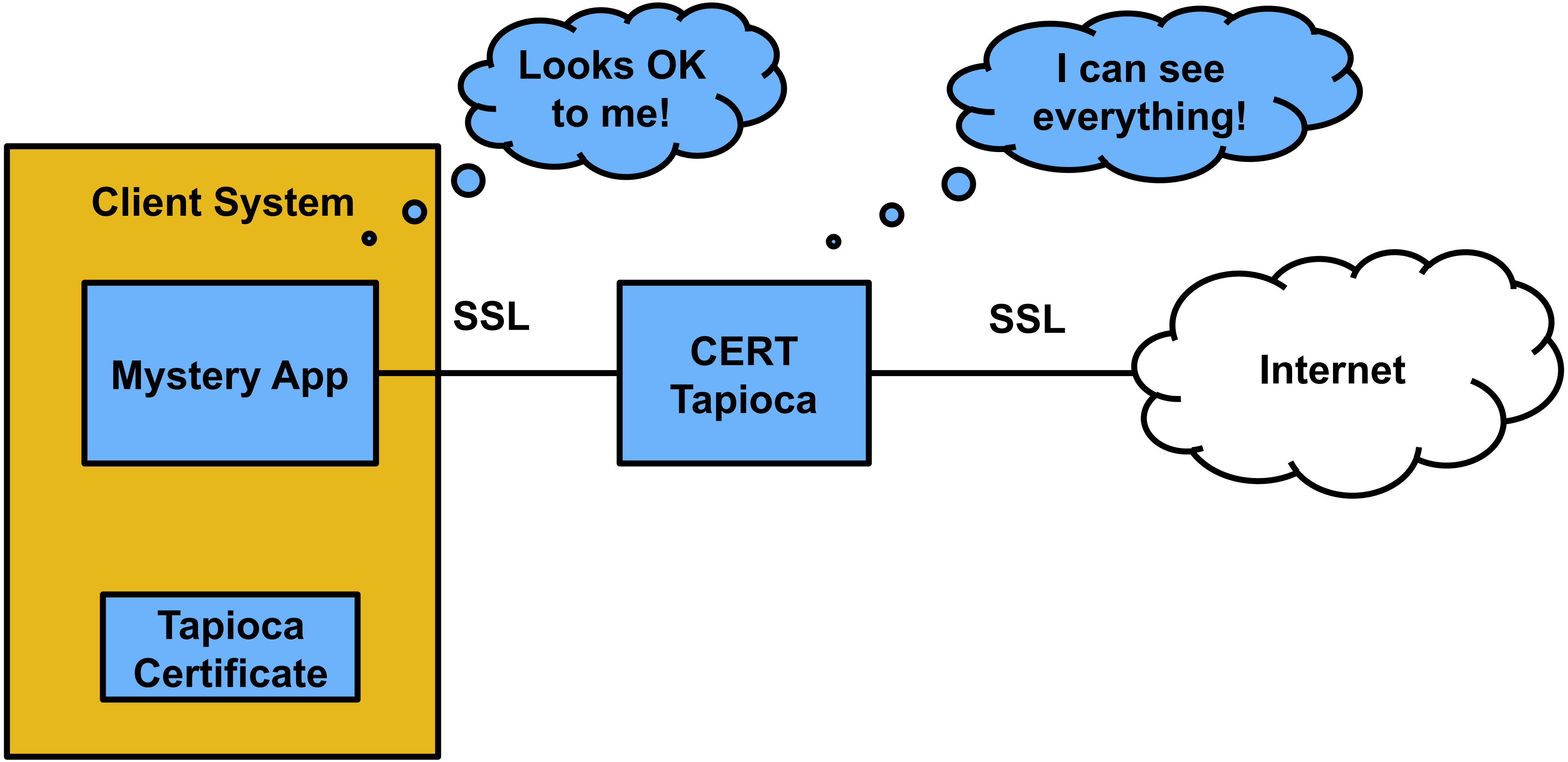
Web Traffic Analysis with CERT Tapioca

Inspection of all SSL Traffic

Observing SSL Traffic



Observing SSL Traffic



* As long as there's no certificate pinning

CERT Tapioca and Trust

By using CERT Tapioca, you can verify trust in applications that are communicating on the network:

- Is the application communicating insecurely by failing to properly validating SSL certificates?
- Is the application sending unexpected information over the network?