Network Security

AA 2015/2016

Privacy in networks

Dr. Luca Allodi

Recall: O*utright malicious* attacker

- **Typically the malicious attacker aims at reading or modifying the communication (in part or fully)**
- **In this contest, this attacker is typically called "man in the middle"**
  - Or "man in the browser"
- Attacker can intercept and act upon a communication between client and server
  - Channel redirection, Block communication entirely, Spoofing..
- Example: injection of malicious content
  - Manipulation of server response
    - Client's answer can also be modified by the attacker
  - Connection Hijack
    - Attacker injects him/herself in the communication and spoofs the victim's identity

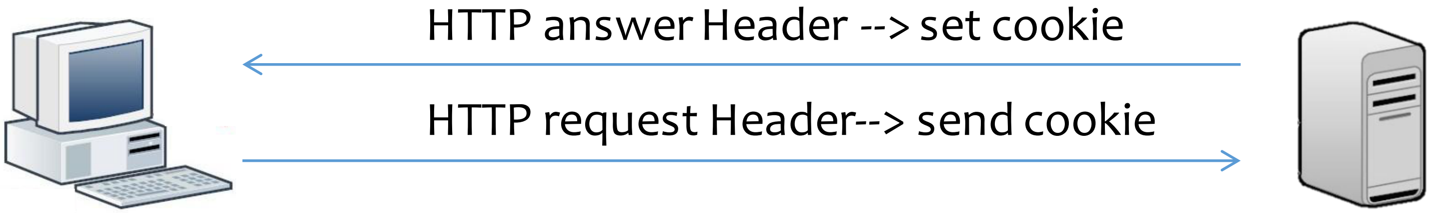
Recall: Honest-but-curious attacker

- **The goal of this attacker is to use the client's information after correctly handling the service**
  - Typically resides at the service level
    - E.g. IPS, router
  - Typically implies confidentiality and possibly integrity losses
- Example
  - DB Server is the attacker. Provides agreed service correctly.
    - E.g. answers queries with correct data
  - After the query is delivered to the client, the server uses the query's information to perform user profiling

Content security

Browser cookies - reprise

- Cookies are set by the server during an HTTP answer



HTTP answer Header --> set cookie

HTTP request Header--> send cookie

- Used to set variable's values that are useful at the service level
- Example:
  - Server sets cookie "ThemePreference"
    - **Set-cookie** ThemePreference=red
  - At the next interaction, client will send "ThemePreference" to server
    - **Cookie** ThemePreference=red

Attributes that can be defined at cookie level

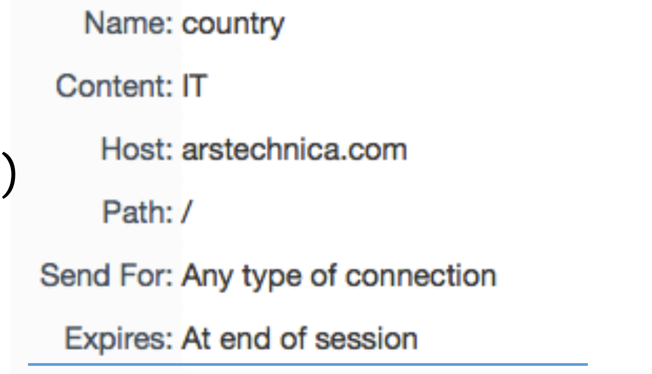
- Pre-defined attributes
  - **Name** (of cookie) (User)
  - **Content** (value of cookie) (mario)
  - **Host** (name of the server that set the cookie) (mario.net)
    - → remember: **same origin policy**
    - **Browser sends cookies only to the domain who created them**
  - **Path** (server path onto which the cookie is valid) (/)
  - **Send for** (all connections/ only encrypted)
  - **Expires** (expiry date) (19 Giu 2015)

Different cookie types, by attribute

- **Temporary (session cookie)**
  - Typically deleted at end of session
  - **expires: NULL**
- **Persistent**
  - Remain until expiry date
  - **expires: Fri, 19-Jun-2015**
- **Secure**
  - Set by a domain communicating over an HTTPS channel over SSL/TLS
  - Secure transmission, harder to intercept

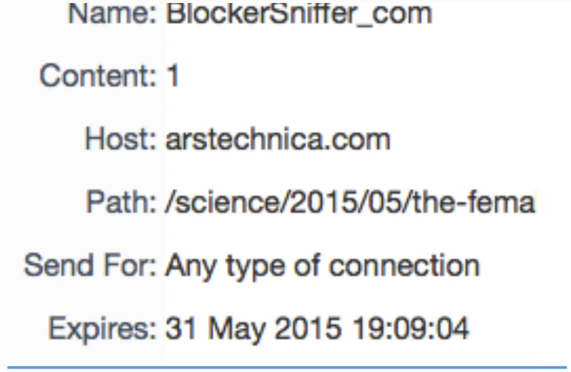
Cookies example

A)



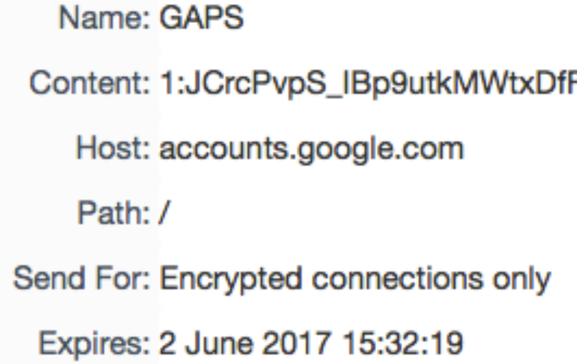
Name: country
Content: IT
Host: arstechnica.com
Path: /
Send For: Any type of connection
Expires: At end of session

B)



Name: BlockerSniffer_com
Content: 1
Host: arstechnica.com
Path: /science/2015/05/the-fema
Send For: Any type of connection
Expires: 31 May 2015 19:09:04

C)



Name: GAPS
Content: 1:JCrcPvpS_lBp9utkMWtxDfF
Host: accounts.google.com
Path: /
Send For: Encrypted connections only
Expires: 2 June 2017 15:32:19

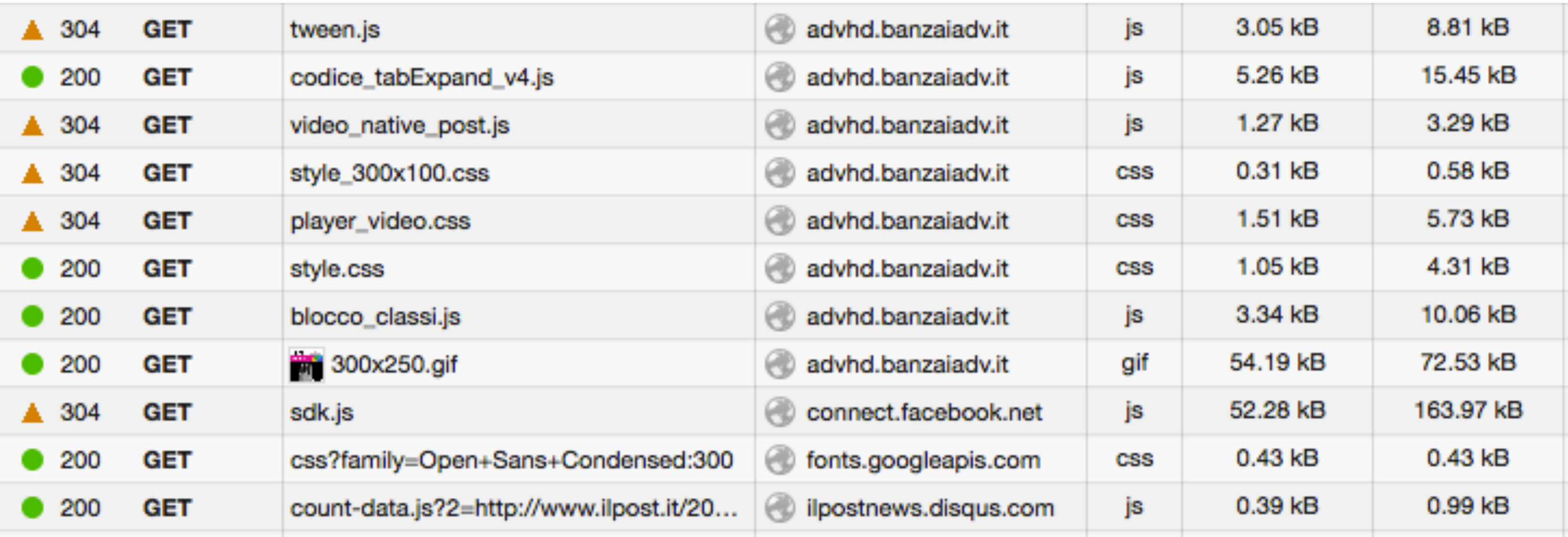
- A, B set by arstechnica.com
  - On different paths
- C → accounts.google.com
- Google can’t read cookies set by arstechnica, and vice-versa
- Expiry date set for B and C (**persistent**), but not for A (**temporary**)
- C is sent only over secure connections (**secure cookie**)

Different types of cookies, by setting

- **Third parties**
  - Set by domains other than the one requested by the user
  - Can be used to track user
- **Supercookies**
  - Like cookies, but associated to first-level domain names (e.g. .com ; .it)
  - *Malicious.it* can read supercookies set by *anotherdomain.it* ("same origin" policy)

Third party cookies (1)

- Cookies can be set by domains called by the browser
  - Not necessarily correspond to the domain displayed in the address bar
- e.g. Requests from www.ilpost.it



▲ 304	GET	tween.js	advhd.banzaiadv.it	js	3.05 kB	8.81 kB
● 200	GET	codice_tabExpand_v4.js	advhd.banzaiadv.it	js	5.26 kB	15.45 kB
▲ 304	GET	video_native_post.js	advhd.banzaiadv.it	js	1.27 kB	3.29 kB
▲ 304	GET	style_300x100.css	advhd.banzaiadv.it	css	0.31 kB	0.58 kB
▲ 304	GET	player_video.css	advhd.banzaiadv.it	css	1.51 kB	5.73 kB
● 200	GET	style.css	advhd.banzaiadv.it	css	1.05 kB	4.31 kB
● 200	GET	blocco_classi.js	advhd.banzaiadv.it	js	3.34 kB	10.06 kB
● 200	GET	300x250.gif	advhd.banzaiadv.it	gif	54.19 kB	72.53 kB
▲ 304	GET	sdk.js	connect.facebook.net	js	52.28 kB	163.97 kB
● 200	GET	css?family=Open+Sans+Condensed:300	fonts.googleapis.com	css	0.43 kB	0.43 kB
● 200	GET	count-data.js?2=http://www.ilpost.it/20...	ilpostnews.disqus.com	js	0.39 kB	0.99 kB

Third party cookies (2)

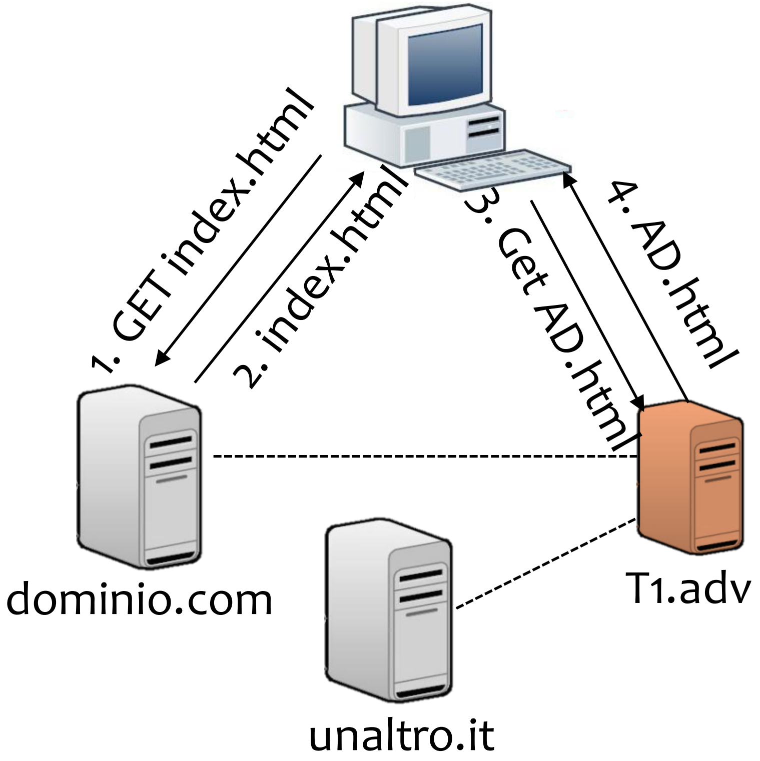
- Other domains can be contacted by the server on behalf of the client
  - e.g. third party services(e.g. facebook), advertisers
  - These services can be requested by multiple, unrelated domains
    - Domains managed by different organizations, collecting diverse data about the same user, and complying to different policies may use/embed the same third party service.

→ This way third party services can track users over different domains

Supercookies

- Not limited to a single domain, but rather to a **first level** domain
- Stored in cache
  - In the browser → the browser’s cookie deletion procedure does not affect supercookies
  - Proprietary plugins (e.g. Flash, Silverlight)
    - Permanent (no expiry date)
    - More info (<100KB vs <4KB of standard cookies)
    - Saved also when using “private browsing mode”
    - Now Flash API permits deletion of supercookies from browser interface

Attacks: honest-but-curious attacker - tracking



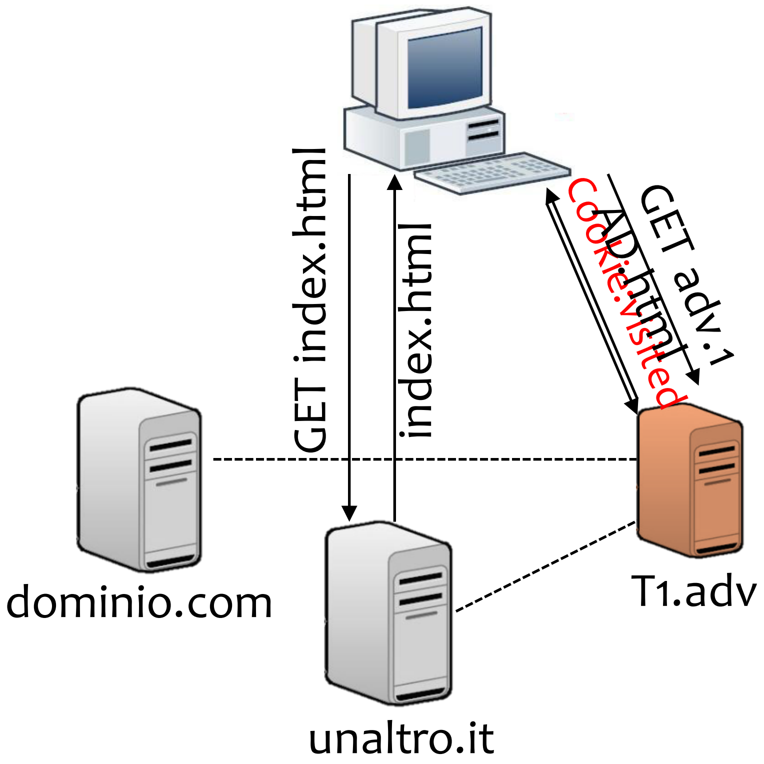
Cookies

Current website

Name: preference
Content: F
Host:dominio.co
m
Path: /
Expires=19-Jun-15

Name: visited
Content:
dominio.com
Host:T1.adv
Path: /
Expires=19-Jun-15

Attacks: honest-but-curious attacker - tracking

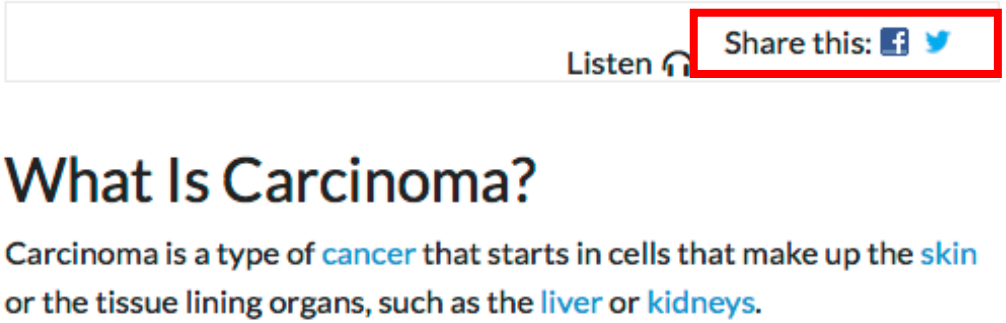


Cookies

Past website	Current website
Name: preference Content: F Host:dominio.co m Path: / Expires=19-Jun-15	Name: bckcolor Content: blue Host:unaltro.it Path: / Expires=21-Jun-15
Name: visited Content: dominio.com Host:T1.adv Path: / Expires=19-Jun-15	Name: visited Content: unaltro.it Host:T1.adv Path: / Expires=21-Jun-15

Tracking: a persistent case

- Almost anybody as a Facebook account
  - Visit www.facebook.com and FB sets cookies on the browser
- That’s however now persistent behavior among majority of domains

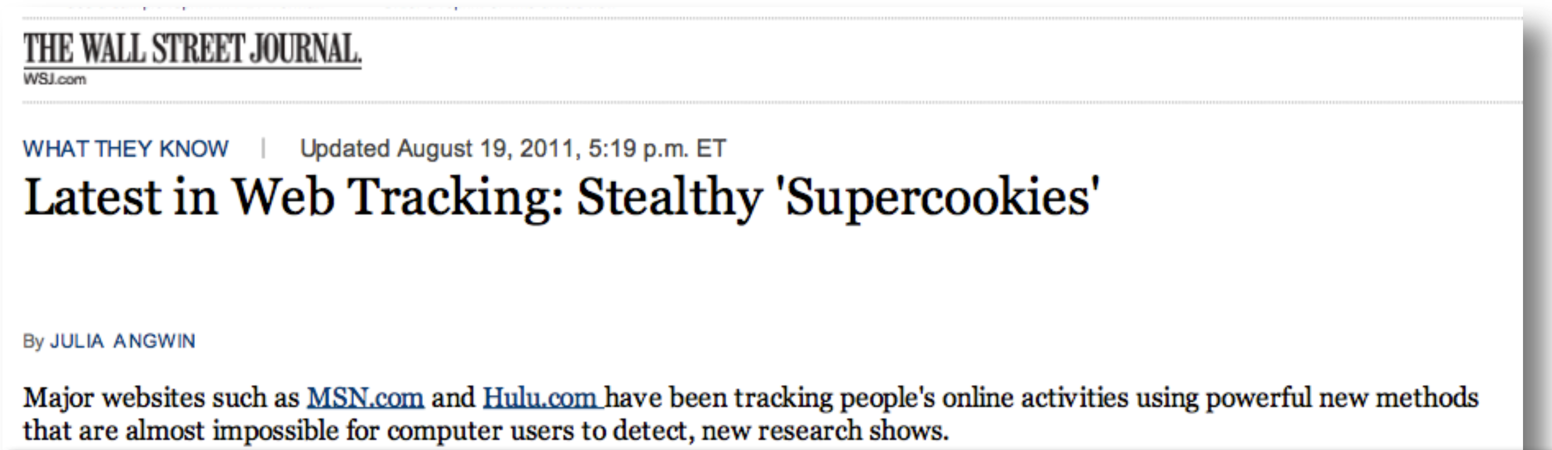


What Is Carcinoma?

Carcinoma is a type of cancer that starts in cells that make up the skin or the tissue lining organs, such as the liver or kidneys.

- No FB account?
  - 3rd party cookies are set anyway when loading page elements that are not on the requested domain
  - Tracking still possible

Honest-but-curious – Examples “in the wild”



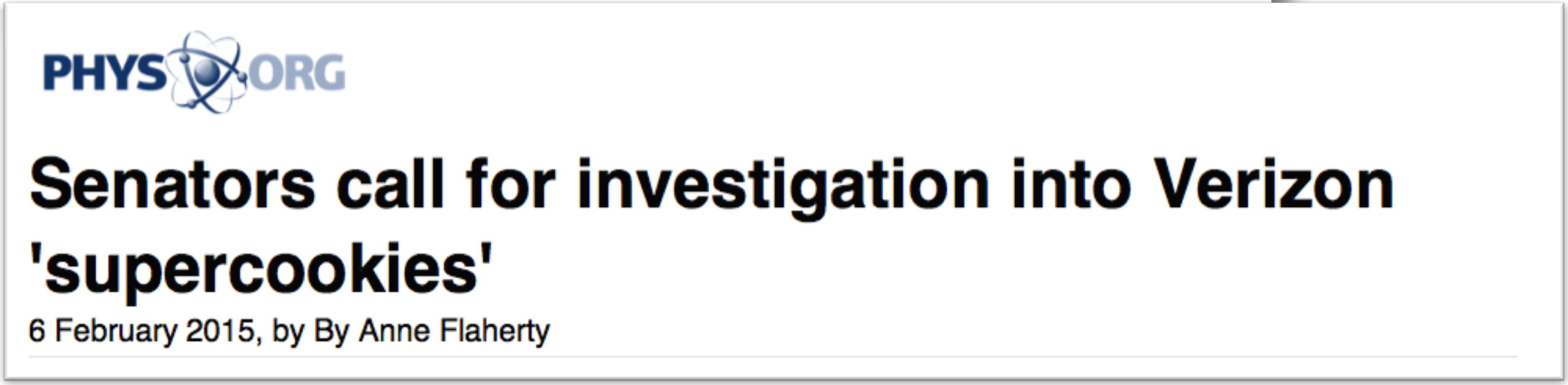
THE WALL STREET JOURNAL.
WSJ.com

WHAT THEY KNOW | Updated August 19, 2011, 5:19 p.m. ET

Latest in Web Tracking: Stealthy 'Supercookies'

By JULIA ANGWIN

Major websites such as MSN.com and Hulu.com have been tracking people's online activities using powerful new methods that are almost impossible for computer users to detect, new research shows.



PHYS.ORG

Senators call for investigation into Verizon 'supercookies'

6 February 2015, by By Anne Flaherty

Risk matrix: non secure cookie (in the clear)

Severity level	Low	Medium	HIgh	Critical

Honest but curious attacker	**Domain cookie**	**Third party**	**Super cookie**
Temporary			
Persistent			

Malicious attacker	**Domain cookie**	**Third party**	**Super cookie**
Temporary			
Persistent			

Risk matrix: secure cookie (enc. Channel)

Severity level	Low	Medium	HIgh	Critical

Honest but curious attacker	**Domain cookie**	**Third party**	**Super cookie**
Temporary			
Persistent			

Malicious attacker	**Domain cookie**	**Third party**	**Super cookie**
Temporary			
Persistent			

“Private” browsing

- Private browsing does **not** prevent user tracking or identification
- It only disassociate past browsing history from future
- Past browsing history + browser cookies can not be accessed by websites visited using private browsing
- Safari & Firefox → “Private browsing”
- Chrome → “Incognito”
- Internet Explorer → “InPrivate browsing”
- Some type of supercookies can be passed by in between private sessions

Browser extensions

- Browser extensions are basically third-party code that is executed by the browser
- **Trust issue → browser will trust the code, but should you?**
- Some extensions can help the user in preserving (or limiting violations to) his privacy online
  - **AdBlock** → blocks ads and other tracking content
  - **Ghostery** → like AdBlock, but specialised in tracking
    - MIT Tech Review → Ghostery is closed course and it may be re-selling anonimized browsing data to advertisers
  - **uBlock** → Open source, more memory efficient
  - **noScript** → guerrilla version of the above, blocks all JS/scripts

Extensions: to trust or not to trust?

- Browser extensions allow the user to add new functionalities to the browser
  - Typically written in JS
  - Can access browser environment using APIs (i.e. software interfaces)
- Some APIs may allow the extension to access information outside of the private browsing env
  - Some extensions are clearly a security threat
    - e.g. Firefox' ***commandrun*** extension
  - Can access all open browser windows
    - If private browsing does not close current session (e.g. FF 20), extension can reach over and link private and non-private sessions

Plugins

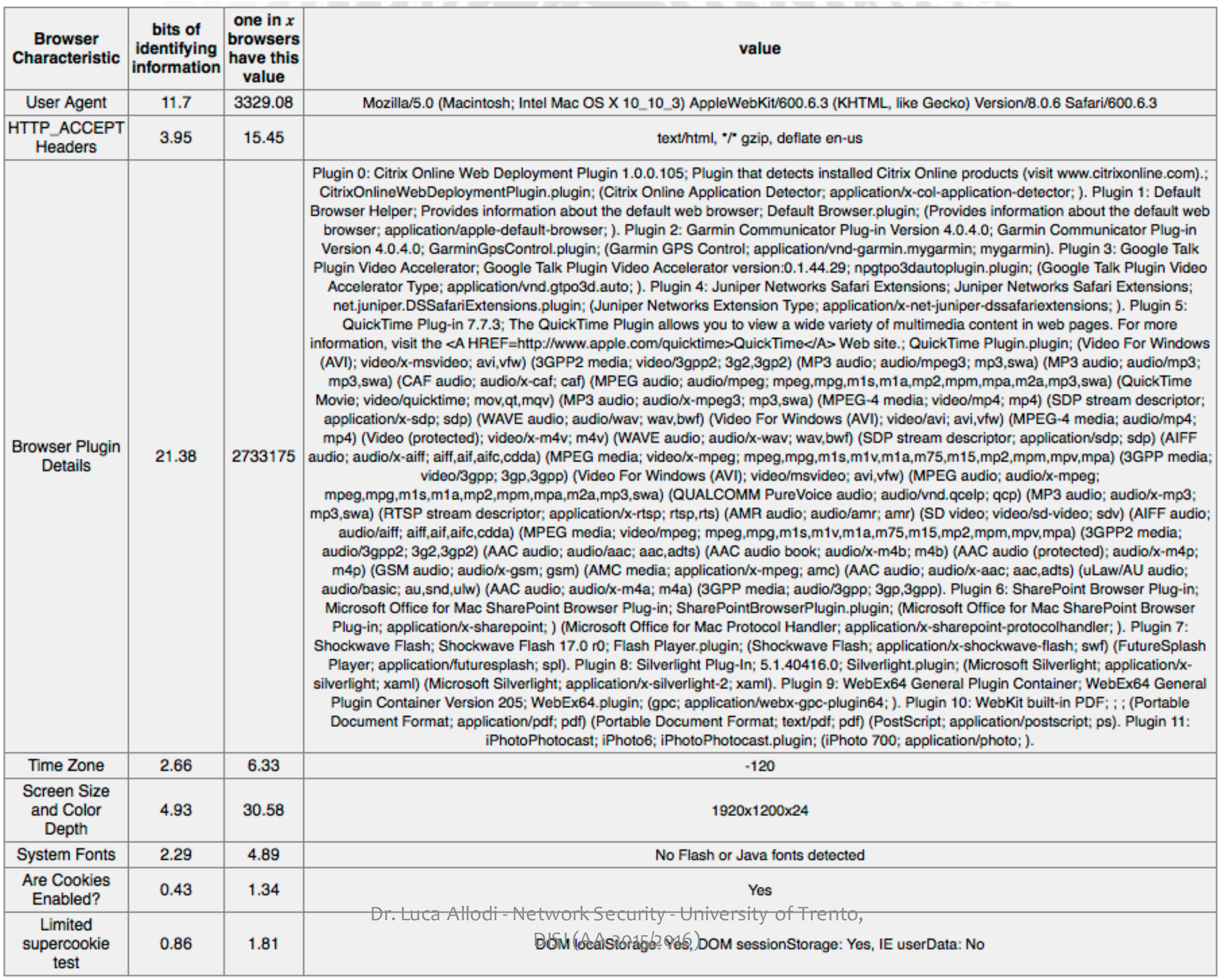
- Plugins pose a similar problem
  - Do not directly depend on the browser
  - Third party applications that may or may not comply to the browser’s (security) policies
    - Cookie and supercookie setting
    - Communication of system’s IP address
    - Direct access to system functionalities
      - Chrome executes Flash in a sandbox

Browser Fingerprinting

- Tracking typically happens using cookies
- It is however possible to achieve reasonable tracking precision even for users with a “clean” browsing history
- **Browser Fingerprinting** is a technique that can uniquely identify a browser over a set of rather stable metrics:
  - User agent
  - Header HTTP
  - Screen resolution
  - PLUGINS/Fonts
  - Supercookie settings
- https://panopticlick.eff.org

UNIVERSITÀ DEGLI STUDI DI TRENTO

Browser identification (1/~5M)



Browser Characteristic	bits of identifying information	one in *x* browsers have this value	value
User Agent	11.7	3329.08	Mozilla/5.0 (Macintosh; Intel Mac OS X 10_10_3) AppleWebKit/600.6.3 (KHTML, like Gecko) Version/8.0.6 Safari/600.6.3
HTTP_ACCEPT Headers	3.95	15.45	text/html, */* gzip, deflate en-us
Browser Plugin Details	21.38	2733175	Plugin 0: Citrix Online Web Deployment Plugin 1.0.0.105; Plugin that detects installed Citrix Online products (visit www.citrixonline.com).; CitrixOnlineWebDeploymentPlugin.plugin; (Citrix Online Application Detector; application/x-col-application-detector;). Plugin 1: Default Browser Helper; Provides information about the default web browser; Default Browser.plugin; (Provides information about the default web browser; application/apple-default-browser;). Plugin 2: Garmin Communicator Plug-in Version 4.0.4.0; Garmin Communicator Plug-in Version 4.0.4.0; GarminGpsControl.plugin; (Garmin GPS Control; application/vnd-garmin.mygarmin; mygarmin). Plugin 3: Google Talk Plugin Video Accelerator; Google Talk Plugin Video Accelerator version:0.1.44.29; npgtpo3dautoplugin.plugin; (Google Talk Plugin Video Accelerator Type; application/vnd.gtpo3d.auto;). Plugin 4: Juniper Networks Safari Extensions; Juniper Networks Safari Extensions; net.juniper.DSSafariExtensions.plugin; (Juniper Networks Extension Type; application/x-net-juniper-dssafariextensions;). Plugin 5: QuickTime Plug-in 7.7.3; The QuickTime Plugin allows you to view a wide variety of multimedia content in web pages. For more information, visit the <A HREF=http://www.apple.com/quicktime>QuickTime</A> Web site.; QuickTime Plugin.plugin; (Video For Windows (AVI); video/x-msvideo; avi,vfw) (3GPP2 media; video/3gpp2; 3g2,3gp2) (MP3 audio; audio/mpeg3; mp3,swa) (MP3 audio; audio/mp3; mp3,swa) (CAF audio; audio/x-caf; caf) (MPEG audio; audio/mpeg; mpeg,mpg,m1s,m1a,mp2,mpm,mpa,m2a,mp3,swa) (QuickTime Movie; video/quicktime; mov,qt,mqv) (MP3 audio; audio/x-mpeg3; mp3,swa) (MPEG-4 media; video/mp4; mp4) (SDP stream descriptor; application/x-sdp; sdp) (WAVE audio; audio/wav; wav,bwf) (Video For Windows (AVI); video/avi; avi,vfw) (MPEG-4 media; audio/mp4; mp4) (Video (protected); video/x-m4v; m4v) (WAVE audio; audio/x-wav; wav,bwf) (SDP stream descriptor; application/sdp; sdp) (AIFF audio; audio/x-aiff; aiff,aif,aifc,cdda) (MPEG media; video/x-mpeg; mpeg,mpg,m1s,m1v,m1a,m75,m15,mp2,mpm,mpv,mpa) (3GPP media; video/3gpp; 3gp,3gpp) (Video For Windows (AVI); video/msvideo; avi,vfw) (MPEG audio; audio/x-mpeg; mpeg,mpg,m1s,m1a,mp2,mpm,mpa,m2a,mp3,swa) (QUALCOMM PureVoice audio; audio/vnd.qcelp; qcp) (MP3 audio; audio/x-mp3; mp3,swa) (RTSP stream descriptor; application/x-rtsp; rtsp,rts) (AMR audio; audio/amr; amr) (SD video; video/sd-video; sdv) (AIFF audio; audio/aiff; aiff,aif,aifc,cdda) (MPEG media; video/mpeg; mpeg,mpg,m1s,m1v,m1a,m75,m15,mp2,mpm,mpv,mpa) (3GPP2 media; audio/3gpp2; 3g2,3gp2) (AAC audio; audio/aac; aac,adts) (AAC audio book; audio/x-m4b; m4b) (AAC audio (protected); audio/x-m4p; m4p) (GSM audio; audio/x-gsm; gsm) (AMC media; application/x-mpeg; amc) (AAC audio; audio/x-aac; aac,adts) (uLaw/AU audio; audio/basic; au,snd,ulw) (AAC audio; audio/x-m4a; m4a) (3GPP media; audio/3gpp; 3gp,3gpp). Plugin 6: SharePoint Browser Plug-in; Microsoft Office for Mac SharePoint Browser Plug-in; SharePointBrowserPlugin.plugin; (Microsoft Office for Mac SharePoint Browser Plug-in; application/x-sharepoint;) (Microsoft Office for Mac Protocol Handler; application/x-sharepoint-protocolhandler;). Plugin 7: Shockwave Flash; Shockwave Flash 17.0 r0; Flash Player.plugin; (Shockwave Flash; application/x-shockwave-flash; swf) (FutureSplash Player; application/futuresplash; spl). Plugin 8: Silverlight Plug-In; 5.1.40416.0; Silverlight.plugin; (Microsoft Silverlight; application/x-silverlight; xaml) (Microsoft Silverlight; application/x-silverlight-2; xaml). Plugin 9: WebEx64 General Plugin Container; WebEx64 General Plugin Container Version 205; WebEx64.plugin; (gpc; application/webx-gpc-plugin64;). Plugin 10: WebKit built-in PDF; ; ; (Portable Document Format; application/pdf; pdf) (Portable Document Format; text/pdf; pdf) (PostScript; application/postscript; ps). Plugin 11: iPhotoPhotocast; iPhoto6; iPhotoPhotocast.plugin; (iPhoto 700; application/photo;).
Time Zone	2.66	6.33	-120
Screen Size and Color Depth	4.93	30.58	1920x1200x24
System Fonts	2.29	4.89	No Flash or Java fonts detected
Are Cookies Enabled?	0.43	1.34	Yes
Limited supercookie test	0.86	1.81	DOM localStorage: Yes, DOM sessionStorage: Yes, IE userData: No

Add one more privacy tool..

- Fingerprint's precision increases with the uniqueness of the user's configuration
- The more you "personalize" your browser, the least common its configuration will be
  - **Disable 3rd party cookies**
  - **Install Ghostery**
  - **Install uBlock**
  - **Kill plugins**
  - **Install new system fonts**
  - **..**

Fingerprinting: disclaimer

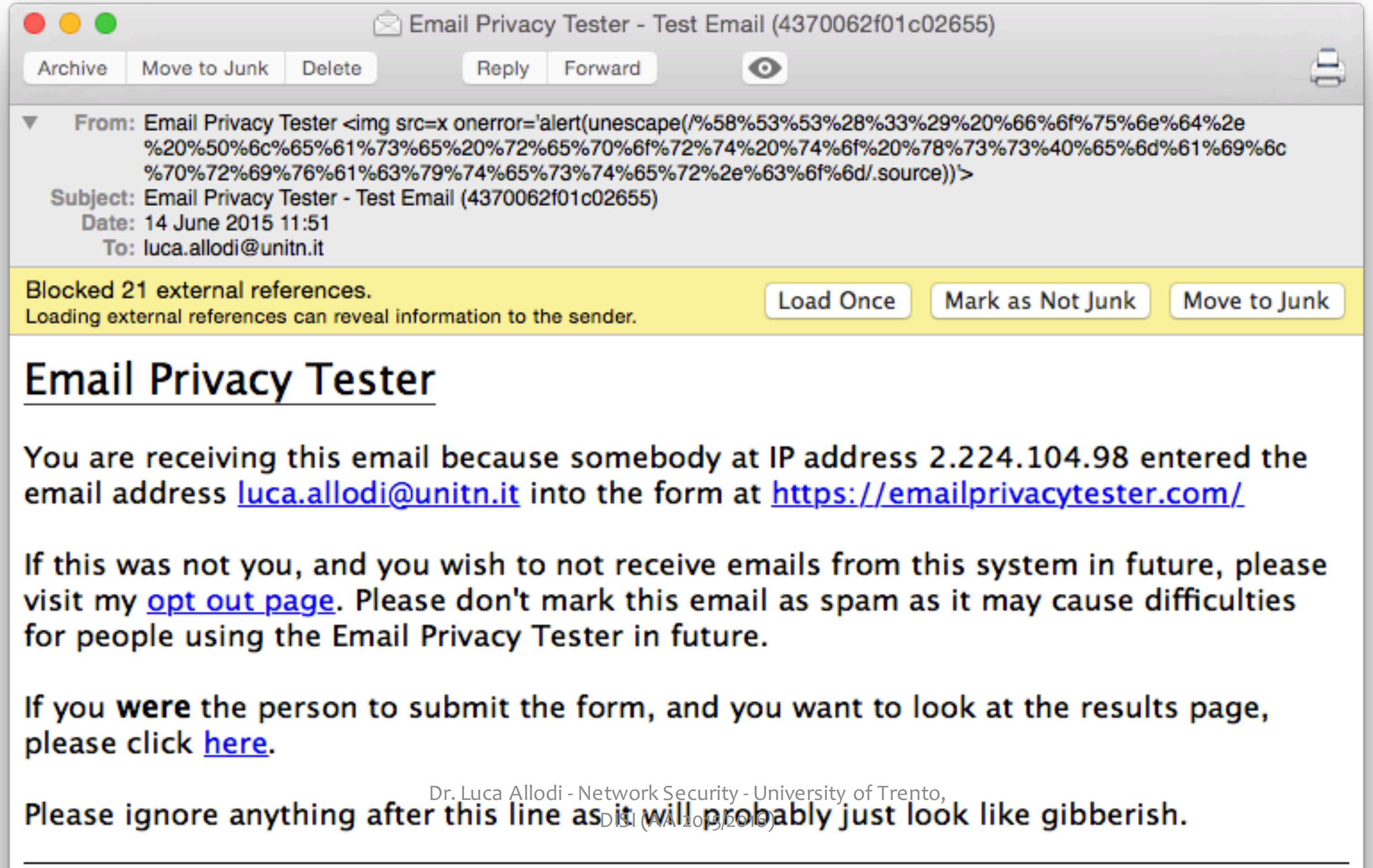
- Being unique is not the same as being trackable
- Fingerprint must be **stable** in time
    - Or at least change in a somewhat predictable manner
- Some implementations can predict a browser's fingerprint with good precision
    - 65% detection
    - 99.1% true positives

Attacks out of the browser: email

- We already know that email is an attack vector for social engineering attacks such as phishing
- There are however other, more technical attacks that allow the attacker to obtain private information from within the email client
  - Emails are basically webpages
  - Can include a number of objects
    - Video, picture, sound files
    - Javascript, VB script, ..
    - CSS, iFrames
- This can be exploited by the attacker to access to information about the user and/or deliver remote attacks to the email client
  - Example of type of info:
  - This email address is valid, therefore I can send spam to it. The user appears to be Italian, and works/studies at the University of Trento. The user read this email on day X at time Y from the IP address Z.

Email attacks: example (1)

- https://emailprivacytester.com (Mike Cardwell)



From: Email Privacy Tester <img src=x onerror='alert(unescape(/%58%53%53%28%33%29%20%66%6f%75%6e%64%2e%20%50%6c%65%61%73%65%20%72%65%70%6f%72%74%20%74%6f%20%78%73%73%40%65%6d%61%69%6c%70%72%69%76%61%63%79%74%65%73%74%65%72%2e%63%6f%6d/.source))'>
Subject: Email Privacy Tester - Test Email (4370062f01c02655)
Date: 14 June 2015 11:51
To: luca.allodi@unitn.it

Blocked 21 external references.
Loading external references can reveal information to the sender.

Email Privacy Tester

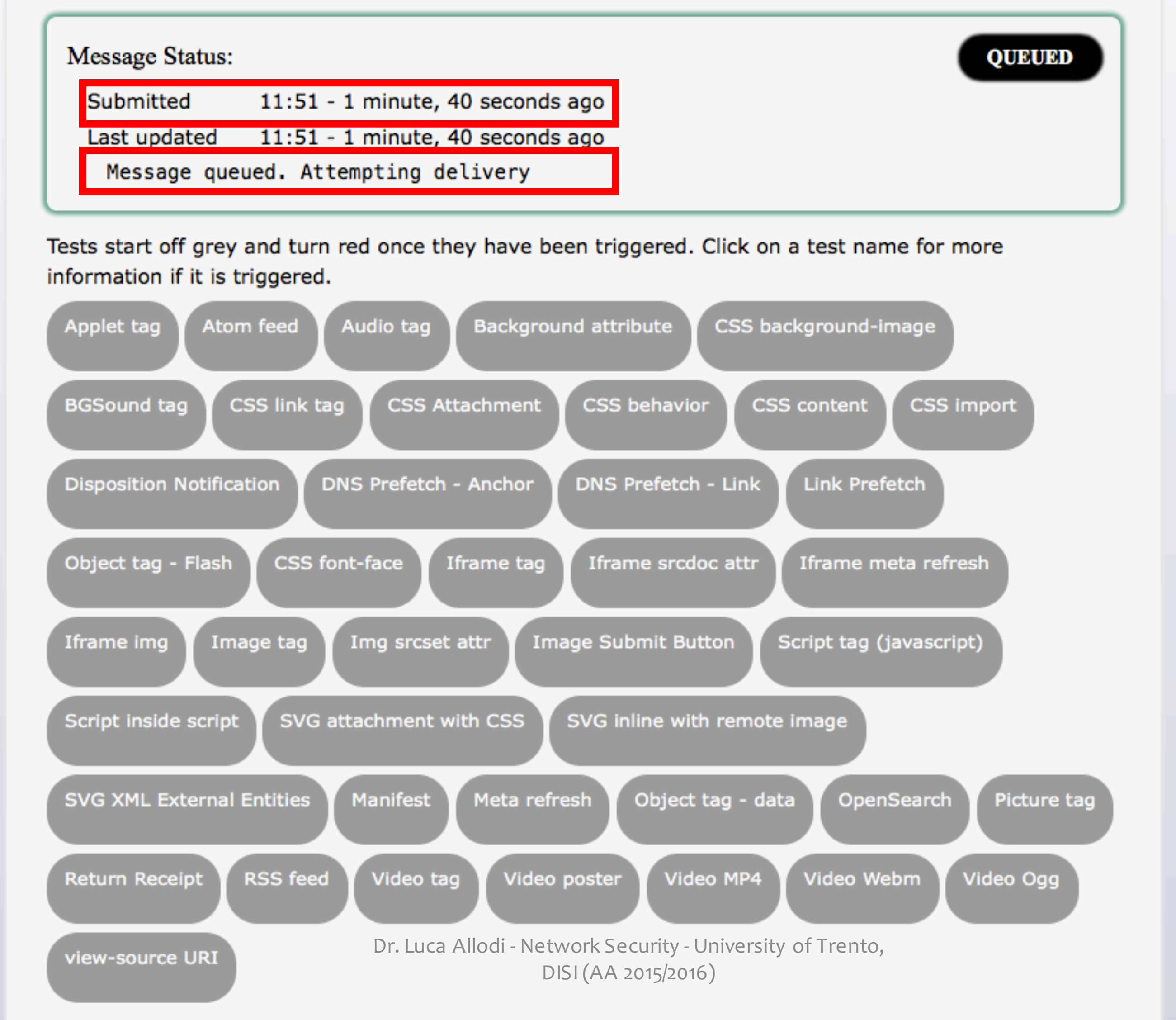
You are receiving this email because somebody at IP address 2.224.104.98 entered the email address luca.allodi@unitn.it into the form at https://emailprivacytester.com/

If this was not you, and you wish to not receive emails from this system in future, please visit my opt out page. Please don't mark this email as spam as it may cause difficulties for people using the Email Privacy Tester in future.

If you **were** the person to submit the form, and you want to look at the results page, please click here.

Please ignore anything after this line as it will probably just look like gibberish.

Email attacks: example (2)



Message Status:

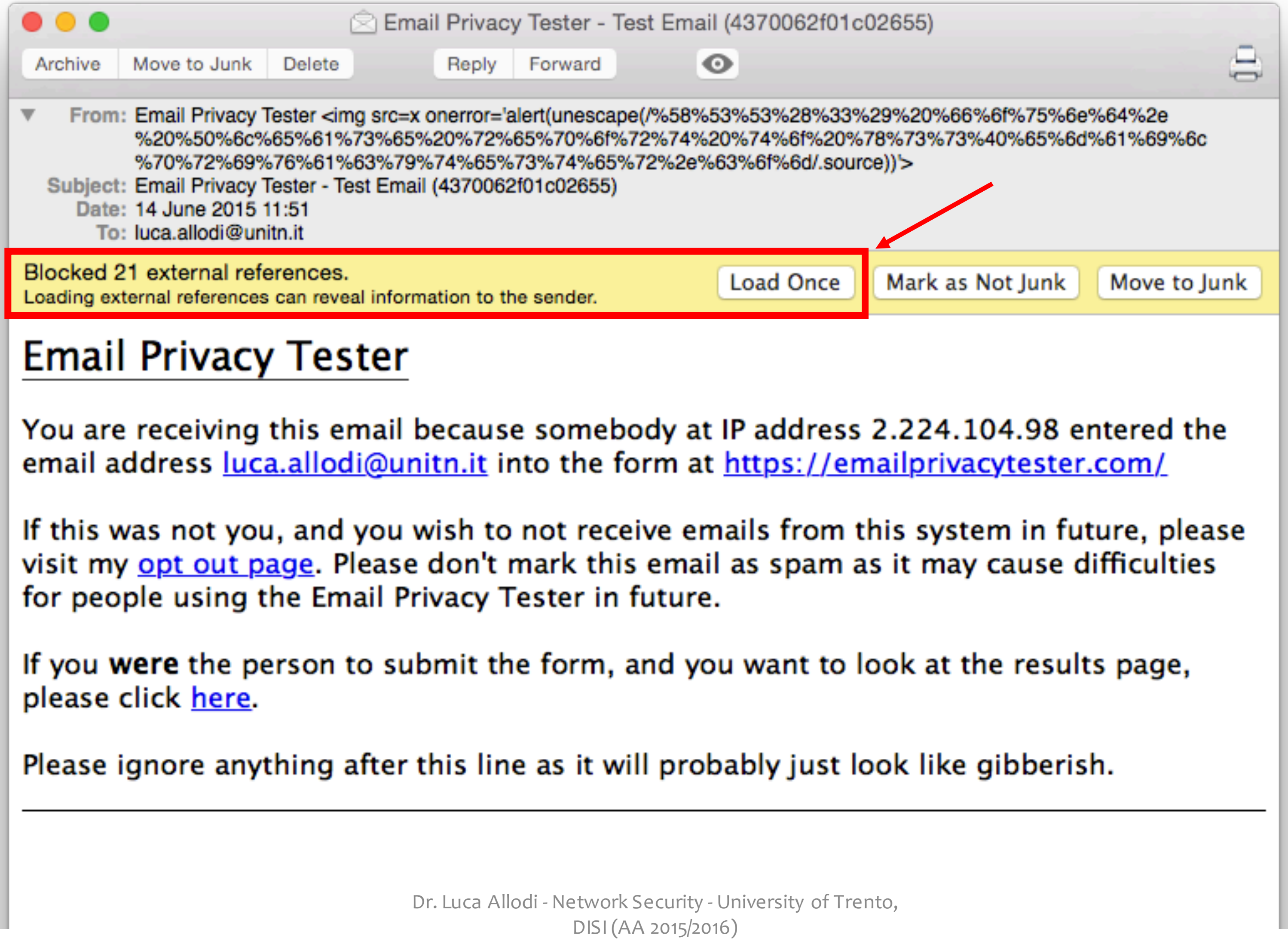
Submitted 11:51 - 1 minute, 40 seconds ago

Last updated 11:51 - 1 minute, 40 seconds ago

```
Message queued. Attempting delivery
```

Tests start off grey and turn red once they have been triggered. Click on a test name for more information if it is triggered.

Email attacks: example (3)



From: Email Privacy Tester <img src=x onerror='alert(unescape(/%58%53%53%28%33%29%20%66%6f%75%6e%64%2e%20%50%6c%65%61%73%65%20%72%65%70%6f%72%74%20%74%6f%20%78%73%73%40%65%6d%61%69%6c%70%72%69%76%61%63%79%74%65%73%74%65%72%2e%63%6f%6d/.source))'>
Subject: Email Privacy Tester - Test Email (4370062f01c02655)
Date: 14 June 2015 11:51
To: luca.allodi@unitn.it

Blocked 21 external references.
Loading external references can reveal information to the sender.

Email Privacy Tester

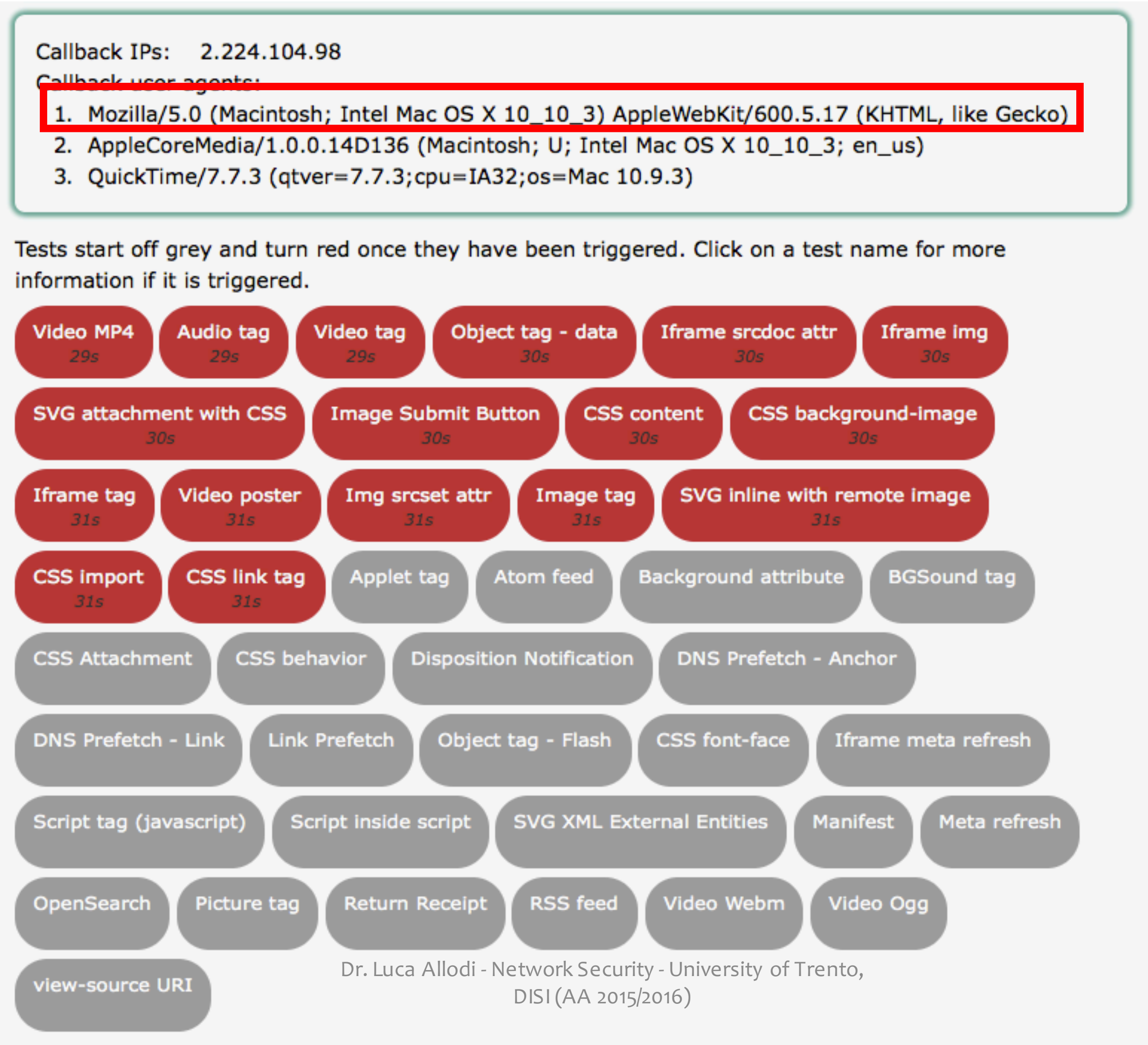
You are receiving this email because somebody at IP address 2.224.104.98 entered the email address luca.allodi@unitn.it into the form at https://emailprivacytester.com/

If this was not you, and you wish to not receive emails from this system in future, please visit my opt out page. Please don't mark this email as spam as it may cause difficulties for people using the Email Privacy Tester in future.

If you **were** the person to submit the form, and you want to look at the results page, please click here.

Please ignore anything after this line as it will probably just look like gibberish.

Email attacks: example (4)



Callback IPs: 2.224.104.98

Callback user agents:

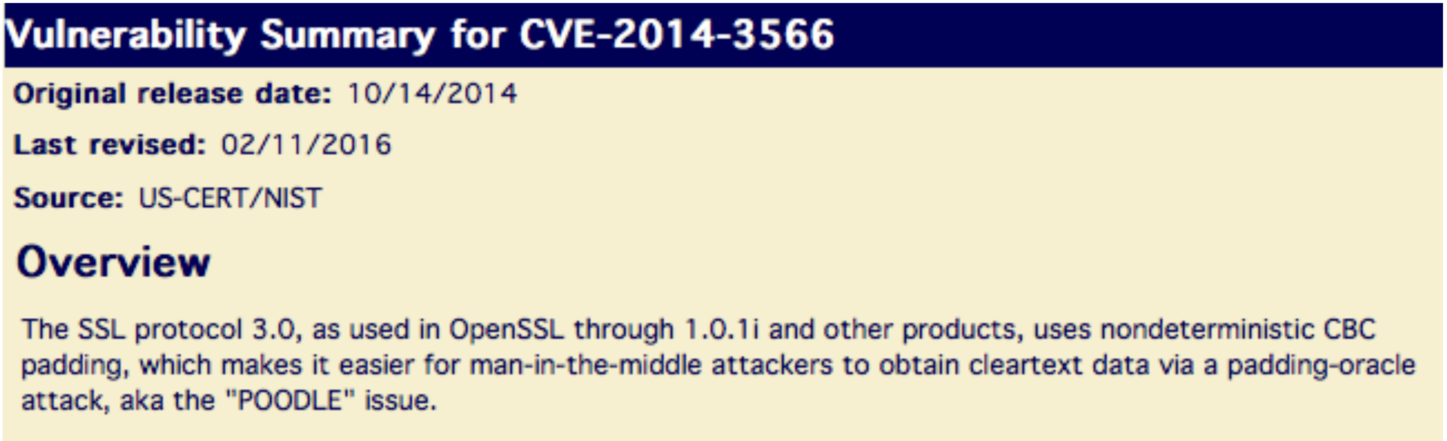
1. Mozilla/5.0 (Macintosh; Intel Mac OS X 10_10_3) AppleWebKit/600.5.17 (KHTML, like Gecko)
2. AppleCoreMedia/1.0.0.14D136 (Macintosh; U; Intel Mac OS X 10_10_3; en_us)
3. QuickTime/7.7.3 (qtver=7.7.3;cpu=IA32;os=Mac 10.9.3)

Tests start off grey and turn red once they have been triggered. Click on a test name for more information if it is triggered.

3. Channel security

Channel crypto

- Most Internet web traffic happens through HTTP
  - User data transmission over the channel
  - Confidentiality / integrity problem
- HTTPS → HTTP over **TLS (Transport Layer Security)**
  - Asymmetric key encryption
  - Every user/server has a public/private key
- Originally deployed over **SSL (Secure Sockets Layer)**
  - SSL 1.0, 2.0 (<1996) → insecure → 2.0 deprecated in 2011
  - SSL 3.0 → 1996 → redesign of previous protocols → deprecated in 2015



Vulnerability Summary for CVE-2014-3566

Original release date: 10/14/2014

Last revised: 02/11/2016

Source: US-CERT/NIST

Overview

The SSL protocol 3.0, as used in OpenSSL through 1.0.1i and other products, uses nondeterministic CBC padding, which makes it easier for man-in-the-middle attackers to obtain cleartext data via a padding-oracle attack, aka the "POODLE" issue.

TLS

- Same protocol design of SSL, crypto is different
- Current TLS 1.2
- Supported by every browser
  - Also used in VoIP communication, several other systems
- **Handshake Protocol**
  - Public-key crypto to exchange shared secret keys
  - Negotiate protocol version and crypto algorithms
  - Authenticate server
    - Optionally authenticate client (mutual)
- **Record Protocol**
  - Exchange of information encrypted with secret keys

Shared Secret Key exchange

- Several protocols can be implemented to exchange secret key
- We've seen Diffie-Hellman
  - Does not authenticate parties (needed typically for the server, sometimes both client and server → mutual authentication)
  - Alice initiates exchange with Bob and establish secret key
    - No mechanism to guarantee that Bob is Bob → MitM
- **Public-key certificates**
  - Trusted electronic certificate that signs the public key of a server
  - **Certification authority** signs the certificate with its private key (X.509)
  - Public Keys of CAs are known (e.g. Shipped with browser)
  - Client can verify the signature and thus trust the certified identity
  - Security is transferred to trust in CA

Certification Authority (CA)

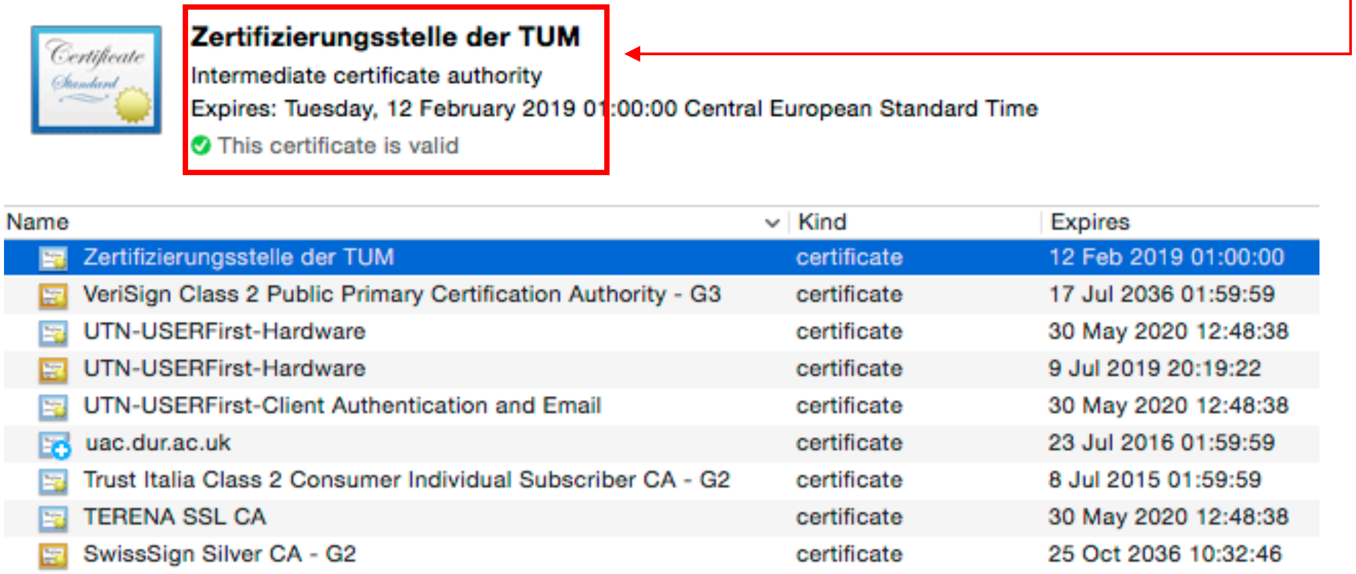
- CAs act as a third-party, independent intermediary that certifies the tuple <identity, public key>
- CAs
  - Verify subject's identity
  - Creates digital certificate with associated identity/public key
  - CA signs association with its private key
    - Certificate authenticity can be verified by the user
- Browsers are shipped with list of public keys of several CAs
- Hierarchical structure similar to DNS
  - Root certificate signs intermediate certificates that sign server's public key

Certificates: a technological problem?

- Certificates are a technological solution
  - Can be release by anybody with the correct technology and technological knowledge (i.e. any CS MSc student, me, you)
- List of trusted CAs can vary from from system to system
- Authenticity of the certificate is verified by the user using the public key of the CA (verify signature)
  - This is again a technological approach
  - Does **not** guarantee that the certificate **actually certificates a meaningful pair <identity, key>.**
- Still, attacks are possible by which a forged certificate can be evaluated as authentic → **Flame malware**
    - Software modules falsely certified as Microsoft's

Certificates: a trust problem

- The certificate may be valid, but who released it?
- Do you trust **ZERTIFIZIERUGSSTELLE DER TUM?**
  - The cert is technically valid, but who is this?
  - VeriSign looks like a more legitimate CA..



Zertifizierungsstelle der TUM

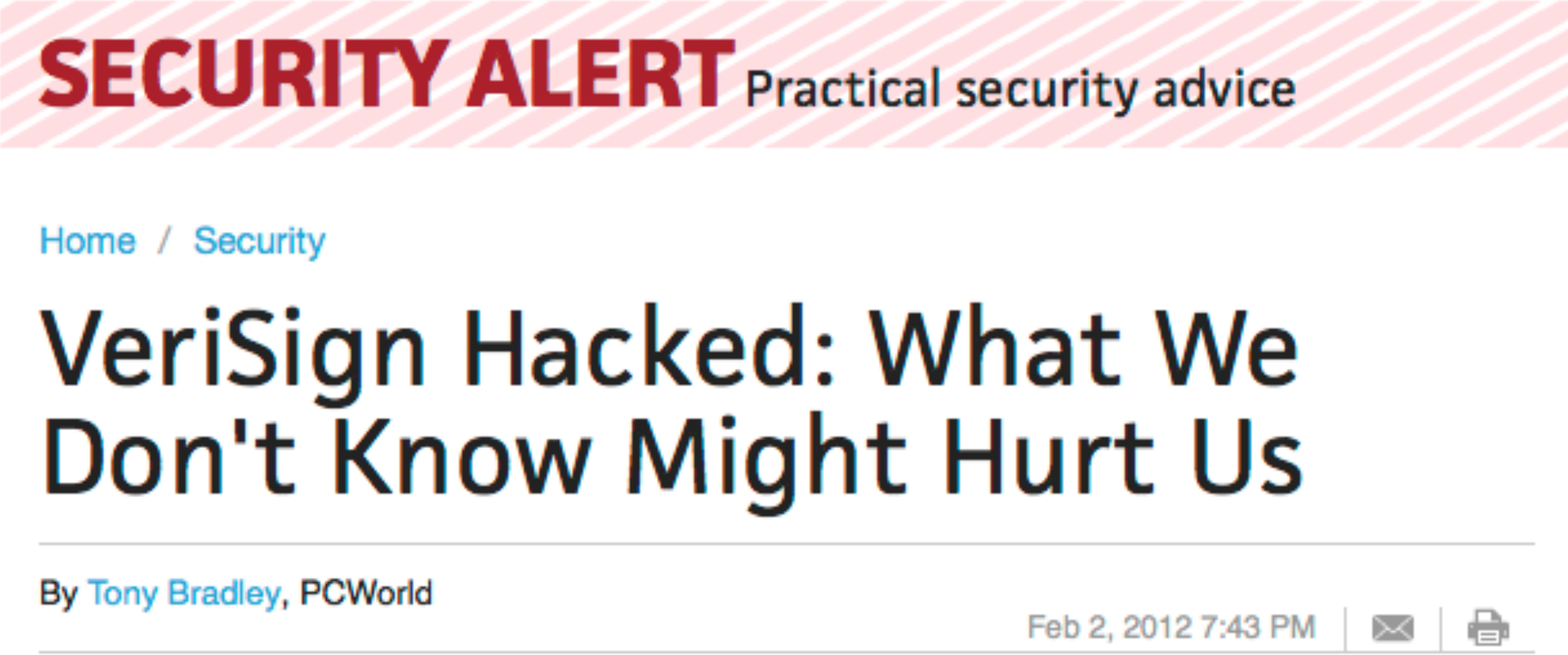
Intermediate certificate authority

Expires: Tuesday, 12 February 2019 01:00:00 Central European Standard Time

✓ This certificate is valid

Name	Kind	Expires
Zertifizierungsstelle der TUM	certificate	12 Feb 2019 01:00:00
VeriSign Class 2 Public Primary Certification Authority - G3	certificate	17 Jul 2036 01:59:59
UTN-USERFirst-Hardware	certificate	30 May 2020 12:48:38
UTN-USERFirst-Hardware	certificate	9 Jul 2019 20:19:22
UTN-USERFirst-Client Authentication and Email	certificate	30 May 2020 12:48:38
uac.dur.ac.uk	certificate	23 Jul 2016 01:59:59
Trust Italia Class 2 Consumer Individual Subscriber CA - G2	certificate	8 Jul 2015 01:59:59
TERENA SSL CA	certificate	30 May 2020 12:48:38
SwissSign Silver CA - G2	certificate	25 Oct 2036 10:32:46

VeriSign looks better



SECURITY ALERT Practical security advice

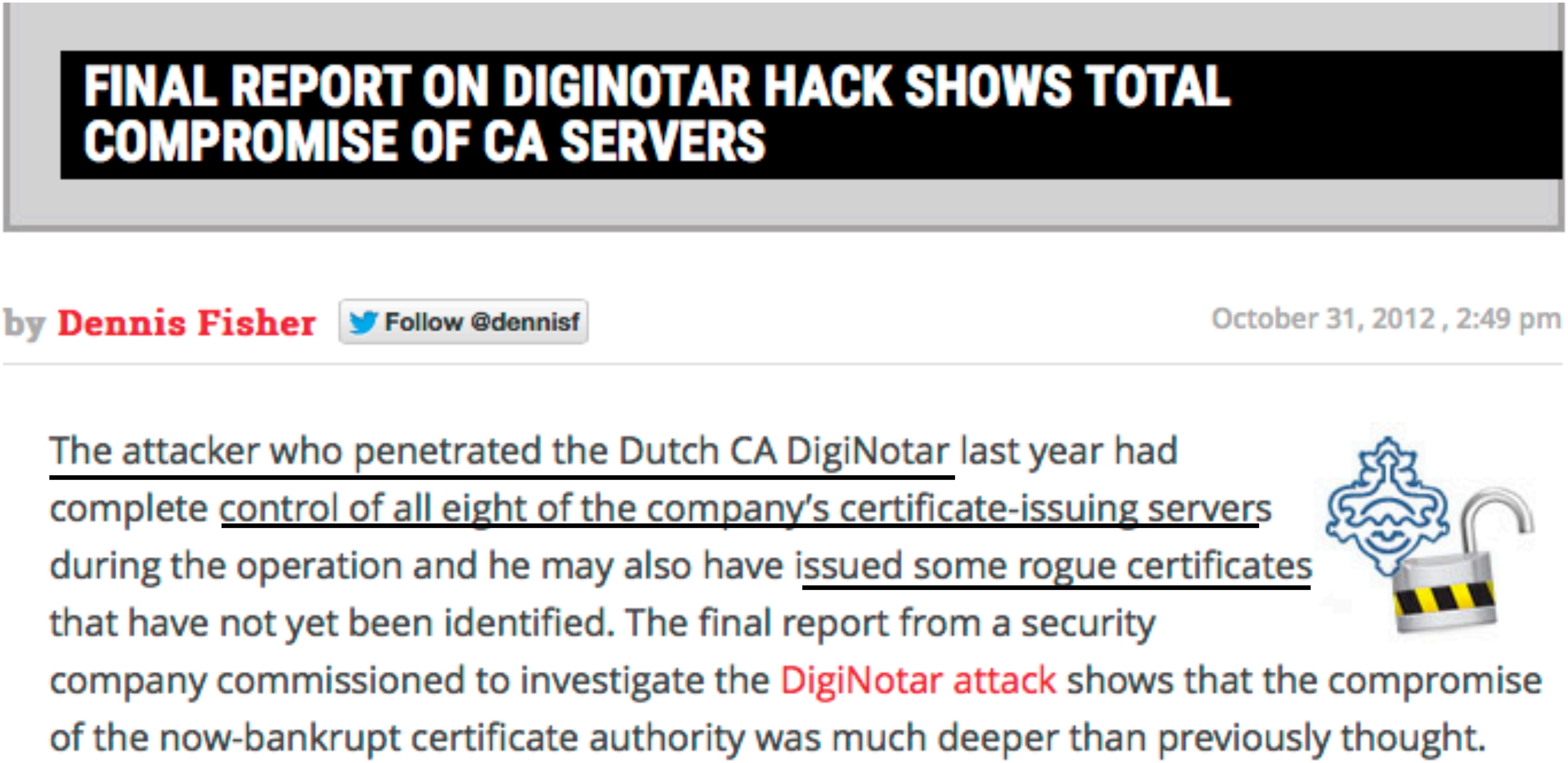
Home / Security

VeriSign Hacked: What We Don't Know Might Hurt Us

By Tony Bradley, PCWorld

Feb 2, 2012 7:43 PM

DigiNotar



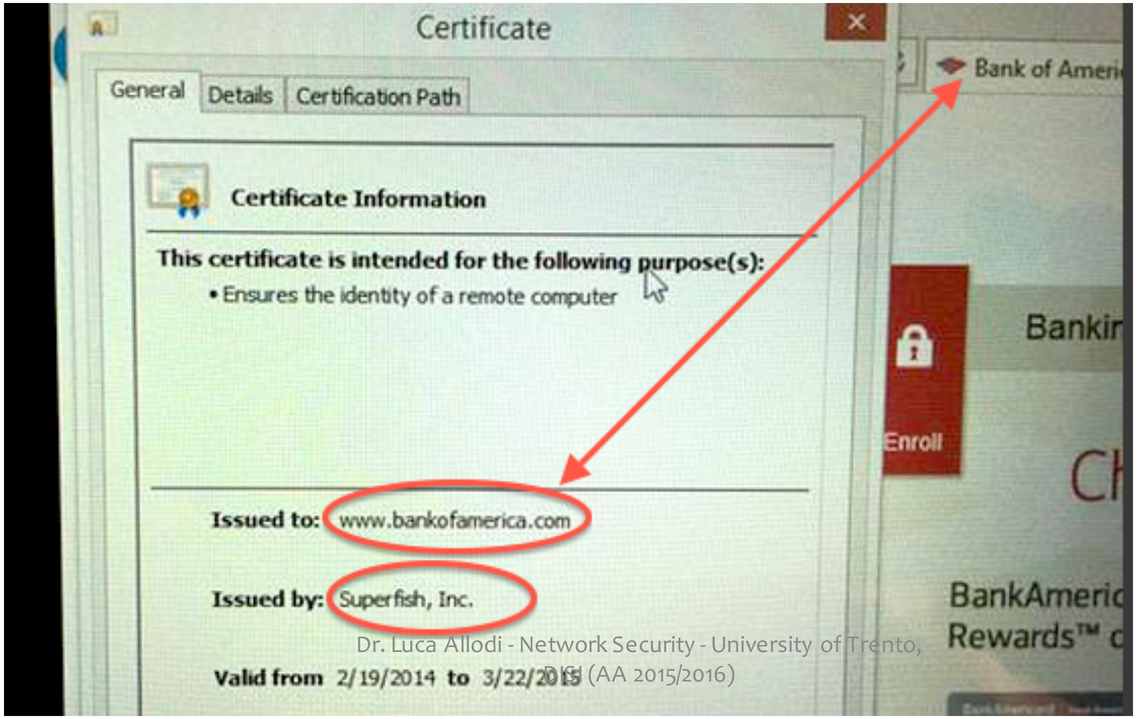
FINAL REPORT ON DIGINOTAR HACK SHOWS TOTAL COMPROMISE OF CA SERVERS

by Dennis Fisher Follow @dennisf October 31, 2012 , 2:49 pm

The attacker who penetrated the Dutch CA DigiNotar last year had complete control of all eight of the company's certificate-issuing servers during the operation and he may also have issued some rogue certificates that have not yet been identified. The final report from a security company commissioned to investigate the DigiNotar attack shows that the compromise of the now-bankrupt certificate authority was much deeper than previously thought.

Superfish

- Lenovo had a contract with advertisement network “superfish”
- User profiling to send personalised ads to Lenovo users
- Problem: can’t read HTTPS channels..
- Solution: Install a root certificate by default on the system!
  - Signs certificates, presents itself like original certificate
  - Same key for every affected Lenovo system (cracked and now public)



Certificate

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.bankofamerica.com

Issued by: Superfish, Inc.

Valid from 2/19/2014 to 3/22/2015

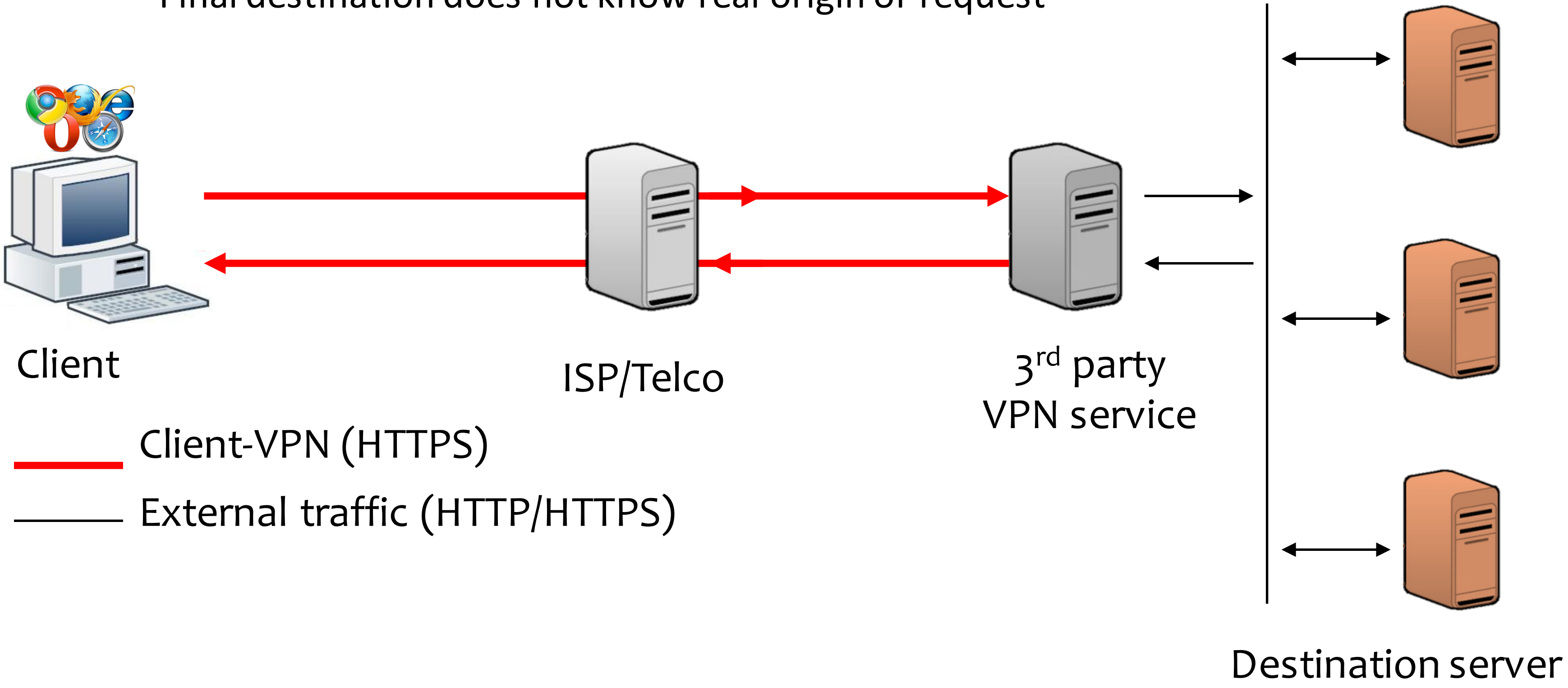
HTTPS: limitations

- Channel encryption is not full end-to-end encryption
  - Encrypted channel from user to server → server can forward traffic to 3rd parties (e.g. ad networks)
- HTTPS channel can be "downgraded" to HTTP → **sslstrip**
  - Server configuration is important
- HTTPS **shields the content of the traffic**
  - SSL/TLS act as wrappers around HTTP
  - Protects information such as
    - Payload (cookies, credentials, etc..)
    - Exact requested remote path
- **Routing** still happens in the clear over the classic TCP/IP stack
  - Traffic sniffing allows the attacker to reveal:
    - Source of traffic
    - Domain toward which request is directed
    - Timings (e.g. stayed on that domain x minutes between requests, on average new request every y minutes)

Confidentiality of data online

VPN services / Secure proxies

- User can decide to trust a proxy for his/her connection and send all traffic to it
  - ISP / destination server not fully trusted
- ISP sees only traffic toward VPN, does not know final destination
  - Final destination does not know real origin of request



Client

ISP/Telco

3rd party
VPN service

Destination server

🟥 Client-VPN (HTTPS)

— External traffic (HTTP/HTTPS)

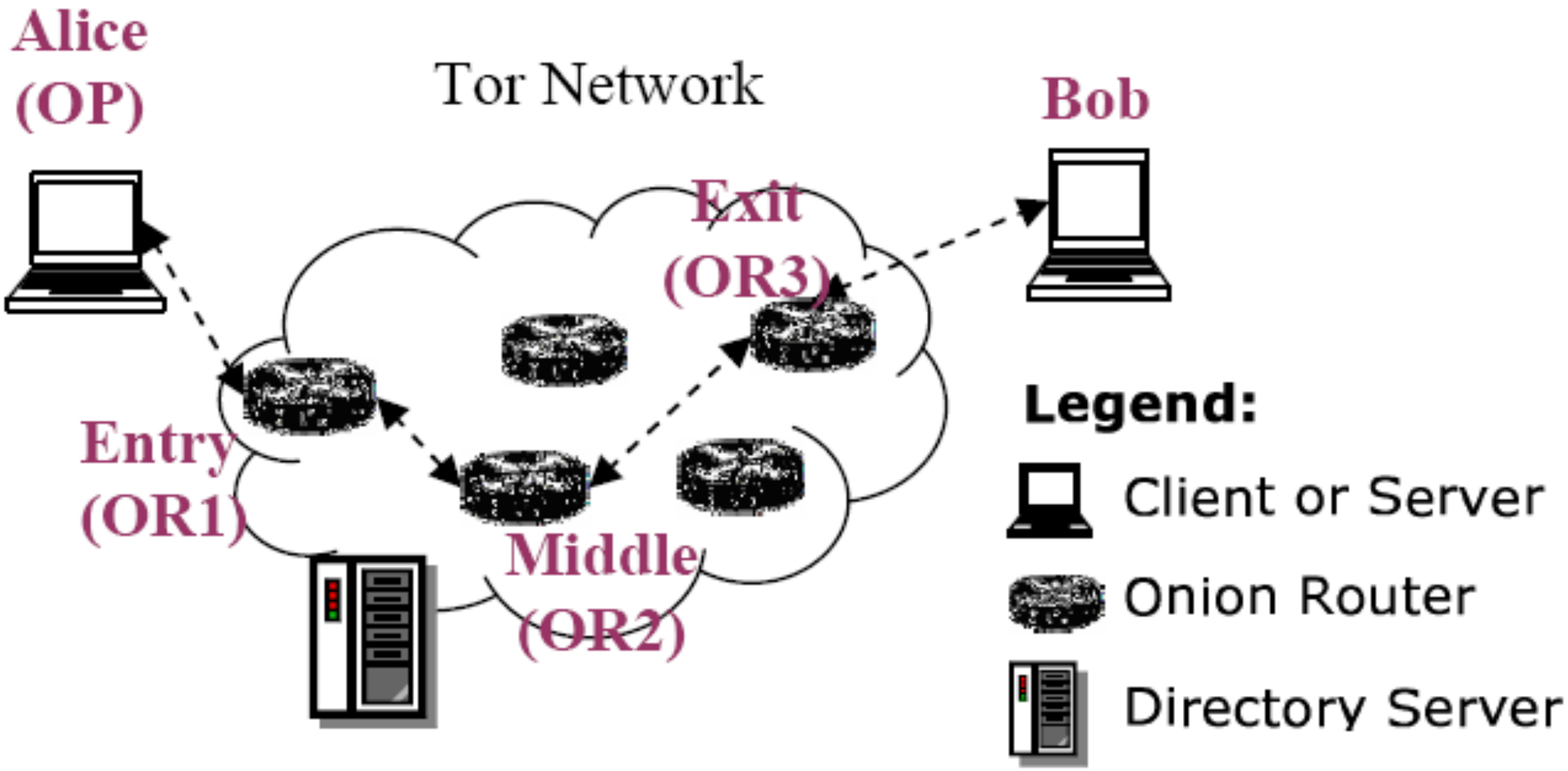
Onion routing

- What to do if you can’t trust a VPN server (or if it is blocked by the ISP)?
- → Onion Routing puts multiple layers of encryption (as in an onion) around the protocol
- Layers are removed at subsequent hops
  - No hop can know **both whom** sent the packet and **what** is in the packet

TOR

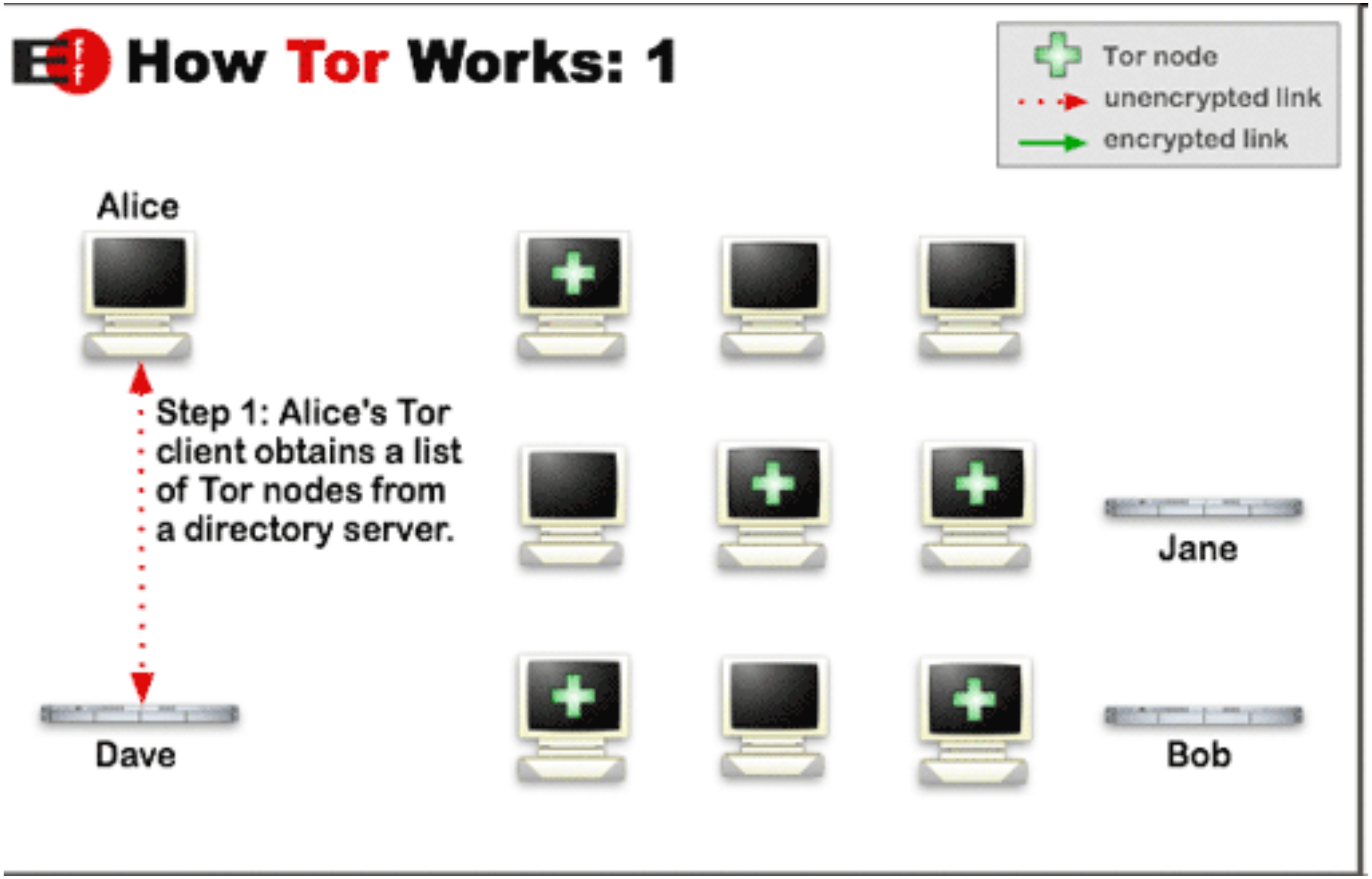
- Tor is a virtual distributed network that allows the user to achieve high privacy levels thanks to Onion routing
- Allows the user to connect to a certain service with intermediary infrastructural nodes knowing (e.g. ISP, proxy)
- Even the final destination never knows who really sent the request
- Creates a virtual network with known nodes
  - Onion Routers (OR) → route the traffic
  - Onion Proxy (OP) → creates the virtual circuit (OR_1 → OR_5 → OR_2 → OR_{EXIT}) to route the traffic
  - Traffic sent through TLS

TOR: structure

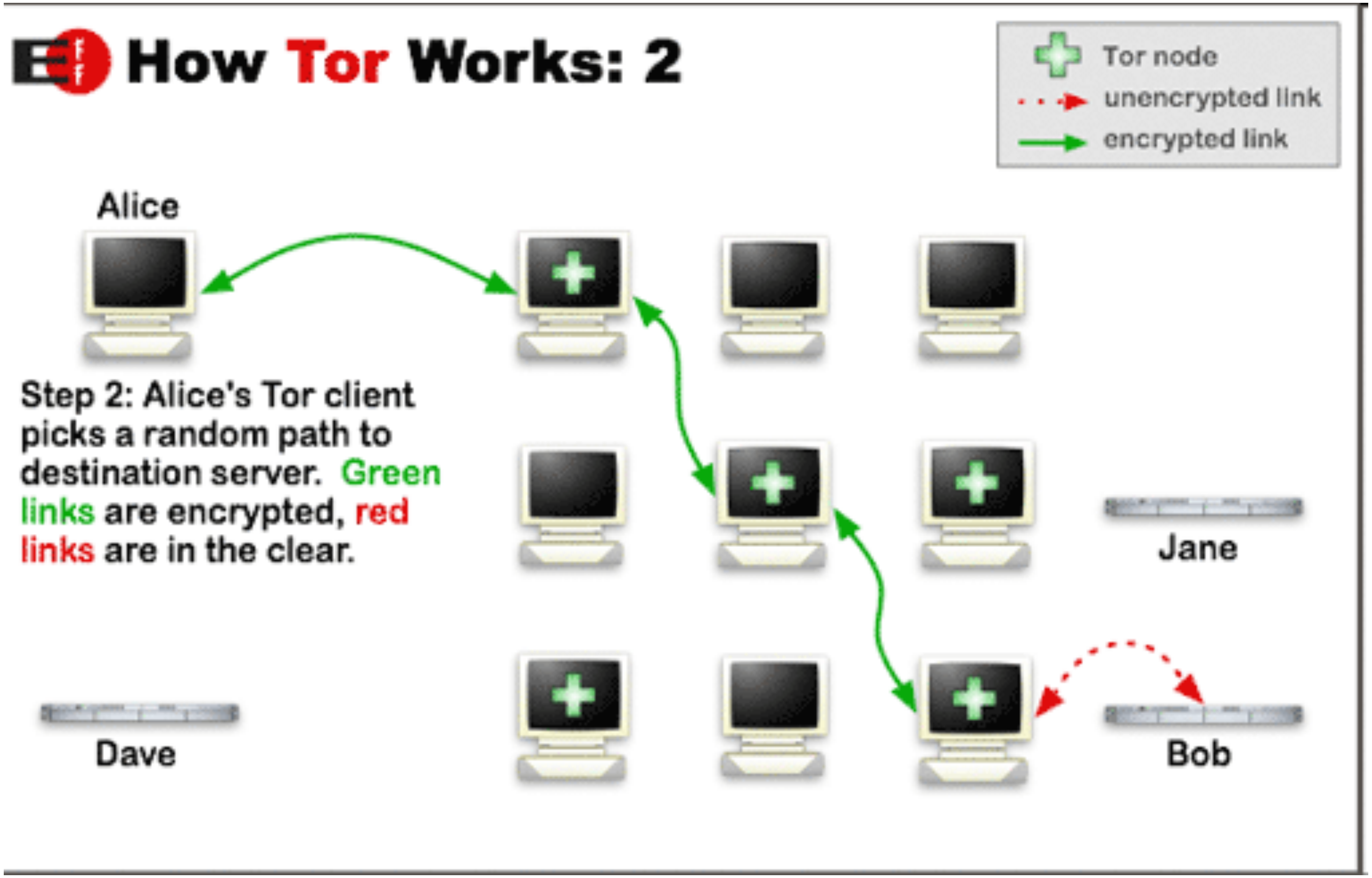


Chris Zachor "Anonymizing Network Technologies"

TOR in action (1)

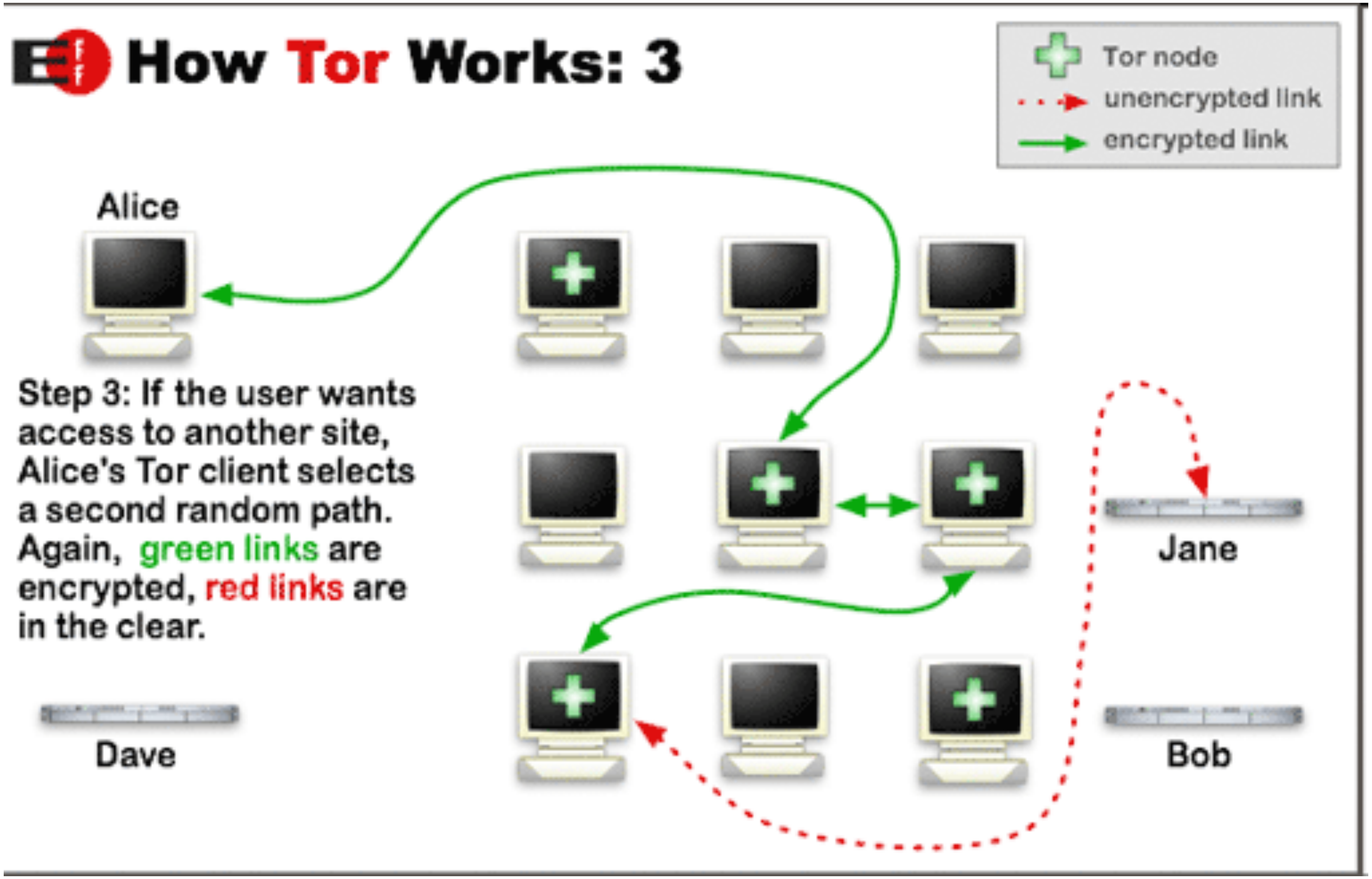

How Tor Works: 1
Tor node
unencrypted link
encrypted link
Alice
Step 1: Alice's Tor client obtains a list of Tor nodes from a directory server.
Jane
Dave
Bob

TOR in action (2)



Step 2: Alice's Tor client picks a random path to destination server. Green links are encrypted, red links are in the clear.

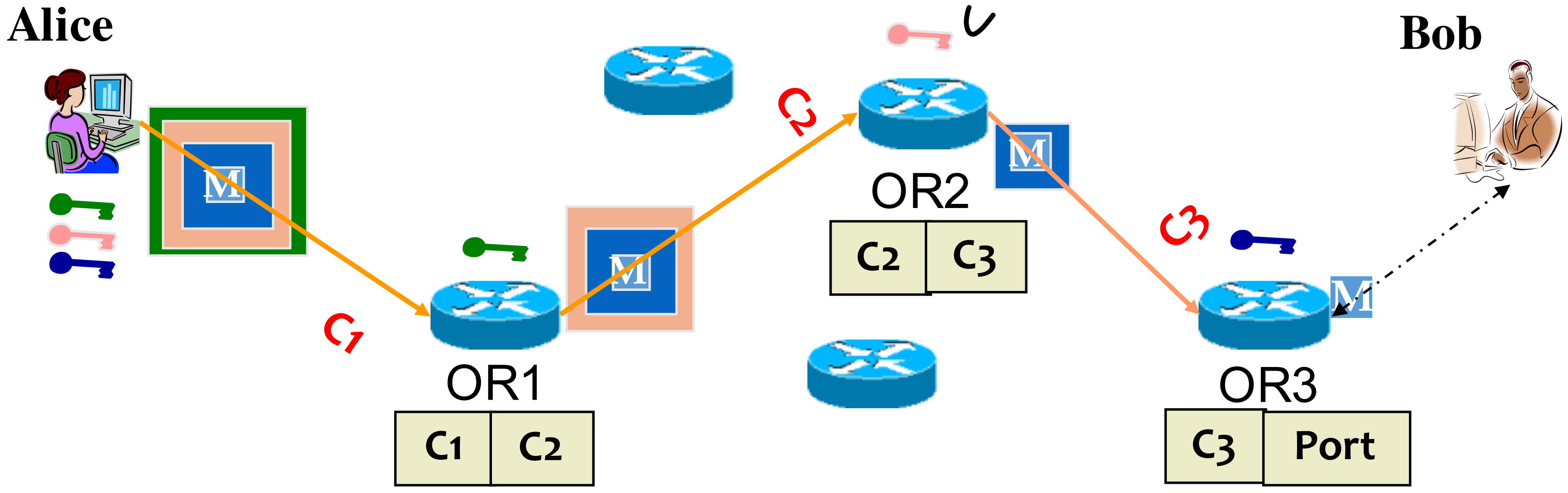
TOR in action (3)



Step 3: If the user wants access to another site, Alice's Tor client selects a second random path. Again, green links are encrypted, red links are in the clear.

TOR in detail

- Alice (OP) negotiate a key with every OR
- Every OR only knows who is before and after it
    - OR3 knows that the message is for Bob but does not know Alice sent it



Xinwen Fu@UMass Lowell

Attacks on TOR

- Exit node sees original traffic
  - If username and password in the clear, we start all over again..
- Timing-channel attacks
  - It is possible to infer who’s Alice by measuring how much time it passes between subsequent requests toward Bob
- **Not all the traffic generated from the system necessarily passes through TOR**
  - DNS requests (e.g. made by browser plugins) may reveal IP address
  - Javascript/browser extensions can reveal IP too
    - Apparently the FBI was able to find the owner of Silk Road (the infamous “darkweb” market) using this attack
- Limitations: https://www.torproject.org/download/download-easy.html.en#warning