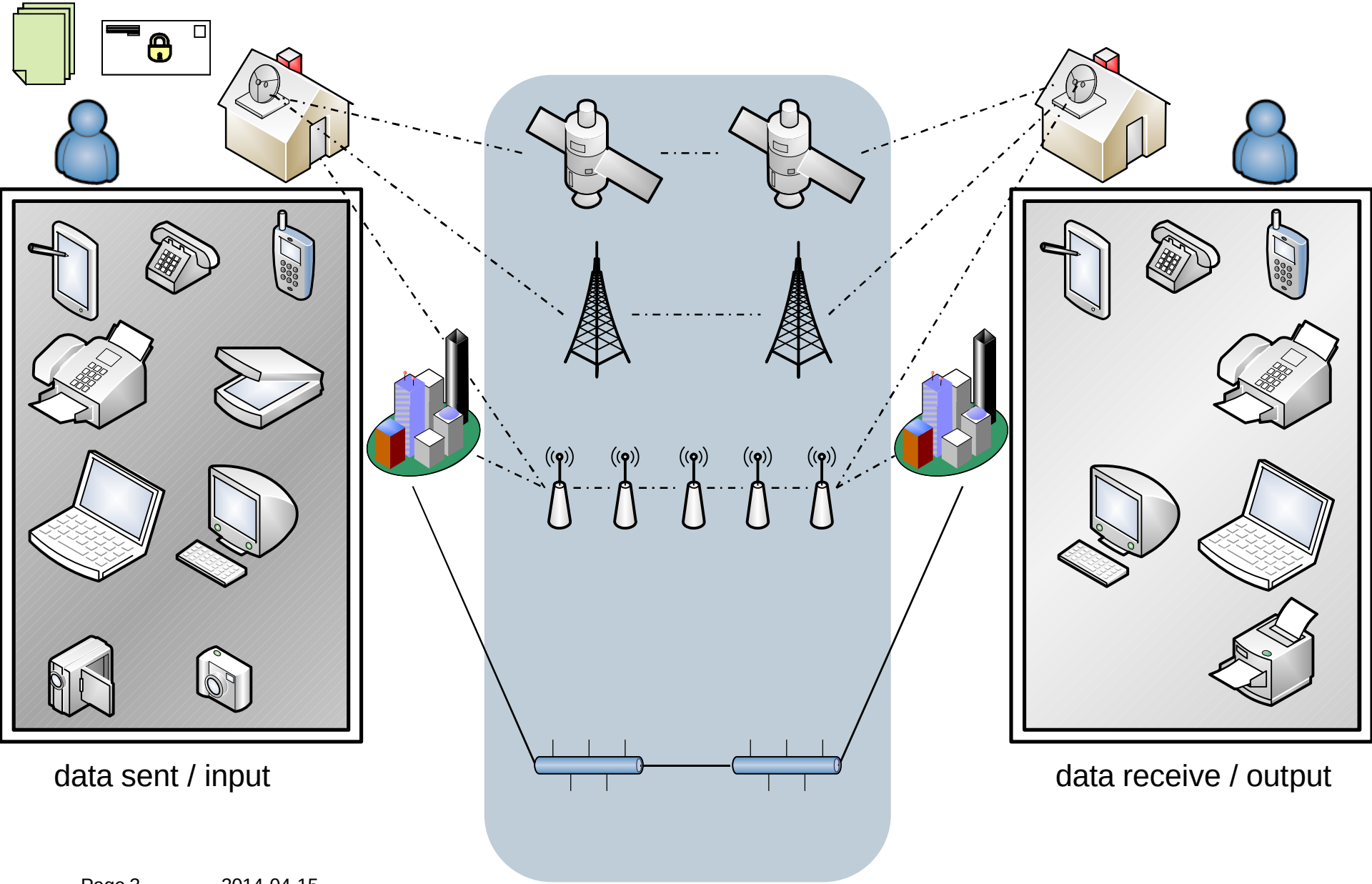
Dr. Gregor Kuznik, Version 1,0 English / April 2014

How the NSA activities affect our daily life.

abstract

"The past of the internet is the most important reason why weakness right from the design or planning stage keeps privacy and security at a low level and why there's neither governmental nor commercial interest to change state of things. The fundamental question is 'Does it impact anybodies life?' Let us suppose that you never use any electronic devices you don't need to think about. In my opinion nobody can ignore the threat caused by data collection and data mining."

basics of communication / data transmission



data sent / input

data receive / output

table of content

point of attack – infrastructure
DNS overview

Domain Name System (DNS)

- Internet company for Assigned Names and Numbers (ICANN)
  - ICANN accredited registrars
- Verisign
  - Verisign domain names - find a registrar

possible attacks

- DNS hijacking
- DNS spoofing / DNS cache poisoning

helpful links

- root DNSSEC
- Berkeley Internet Name Domain (BIND)

point of attack – infrastructure
IP addressing system overview

internet protocol (IP) addressing system

- Internet Assigned Numbers Authority (IANA), a department of ICANN
  - IP address numbers
- IP v4
  - IANA IPv4 address space registry
  - network address translation(NAT)
- IP v6

possible attacks

- IP spoofing
- ARP (Address Resolution Protocol) spoofing / ARP poisoning

helpful links

- Dynamic Host Configuration Protocol (DHCP)
- time server

point of attack – infrastructure
data transmission system

headwords

- network topology
- data bus
  - by cable
  - wireless / wireless LAN
  - via satellite

use cases

- digital subscriber line (DSL)
- local area network (LAN) / wide area network (WAN)
- voice over IP
- telecommunication
- navigation / global positioning system (GPS)
- broadcast

point of attack – data transfer basics

headwords

- OSI model
  - overview
  - layer details
- encryption / decryption / PKI
- plaintext / markup language (e.g. HTML, XML)
- socket layer / secure socket layer (SSL)

possible attacks

- distributed denial of service (dDoS) / denial of service (DoS)
- packet injection, content injection
- CA compromies (man in the middle)
- header spoofing, open redirect / content spoofing
- clickjacking, XSS, SQL injection

point of attack – data transfer advanced

certificate authority (CA)

- national or regional providers
- web browser contains around 50 root certificates
  - „Builtin Object Token“ versus „Software Security Device“
- significant barriers to entry (annual security audits such as Web Trust for CA)

SSL certificates

- less multinational companies dominate web site security market
  - Symantec (which bought VeriSign's SSL interests and owns Thawte and Geotrust) 38.1%
  - Comodo Group 29.1%
  - Go Daddy 13.4%
  - GlobalSign 10.0%
- subordinate root certificate allow transparent traffic management (mitm)

point of attack – components / end user products overview

scope

- internet / intranet
- house („Internet of Things“)
- wearables
- transportation systems (mobility)
- healthcare

point of attack – components / end user products details

internet / intranet

- personal computer, laptop / notebook, tablet PC
- router, switch, (cable) modem
- (wireless) mouse, keyboard
- (web) camera, headset, microphone, speaker
- smart tv / internet radio

house („Internet of Things“)

- heating units / smart thermostats
- smoke detector
- alarm system
- refrigerator
- smart grid

point of attack – components / end user products details

wearables

- glasses
- smart watches
- smart phones

transportation systems (mobility)

- elevator
- car
- train
- airplane

healthcare

- diagnostics
- prevention
- treatment

point of attack – information gathering overview

social media

- social network (facebook, Google+, Weibo, QZone, Habbo, Orkut, LinkedIn, XING)
- photosharing platforms (instagram, picasa, flickr, snapfish)
- videosharing platforms (YouTube, DailyMotion)
- virtual game-worlds (World of Warcraft)
- virtual social worlds (SecondLife)
- blogs (Twitter)

search engines

- Google, Yahoo, bing

trading platforms

- ebay, amazon, scout 24

point of attack – summary
weakness right from the design or planning stage

common measures

- commercial and governmental concern versus security and privacy
- less global player
  - DNS registration, IP adminstration (infrastructure)
  - GPS, satellite, transatlantic cable, telecommunication provider, broadcast, CA / SSL / PKI (data transmission system)
  - manufacturing elements, operating system, applications (components / end user products)
  - search, social media (information gathering)

additional features

- data transfer protocols
- undocumented backdoors (firmware, updates, open ports, encryption algorithm, random number generator, . . .)
- advertising, data collection, tracking

impact – threats concering a company

targets

- espionage
  - intellectual property
  - strategy (portfolio, merger & acquisitions, carve outs, head counts)
  - marketing (offers, orders, suppliers, vendors, customers)
  - assests (contacts, key player)

- sabotage
  - energy (power plant, power transmission, power distribution)
  - industry (engineering, design)
  - infrastructure and cities (railway, lightning, traffic lights, traffic control)
  - healthcare (diagnostic, prevention)

impact – threats concering a company

kind of attack

- social engineering
- phishing
- advanced persistent threats
- socialization

implications

- data leakage / data loss
- damage (image, health, safety)
- penalty / loss of money

impact – threats posed to me

job
- fire
- relocation / degradation
- income

justice
- prison
- penalty
- compensation

social
- isolation
- lonelyness
- malicious joy

risk analysis – what is relevant for me?

financial impact

- transactions / money transfer
- income
- credit assessment

identity theft

- social assurance number
- login data, accounts
- IP address, MAC address

visibility

- browser cache, search requests
- (web site) tracking, personalized advertisement
- positioning

risk mitigation – what I can change

compliance
- human rights
- German constitution
- laws
- policies

awareness
- transparency (social media, data protection settings, identity card)
- usability (don‘t share anything to anybody)
- visibility (geocaching, GPS, UMTS, bluetooth, wireless)

vendor / supplier
- service provider (mail, internet, telephone, cable television)
- producer (operating system, data base, browser, mail software)
- regular updates (patches, bug fixes)

risk mitigation – what I can change

tracking / data protection

- browser add-ons (gosthery, better privacy, flagfox, no script)
- browser cache (files, cookie, super cookies, flash cookies)
- encryption (email, encryption, forward secrecy, TSL, TrueCrypt)
- geolocation smartphone (Android app XPrivacy)

trust is good, control is better

- certificate (web site)
- certificate authorities (browser options)

inform about service provider

- read the end user (license) agreement /governance
- where‘s the service located?
- who‘s owner / responsible for the service?

risk acceptance – what I cannot change

laws

- Patriot Act
- Foreign Intelligence Surveillance Act
- Computer Fraud and Abuse Act
- EU retention of data

components infrastructure

- cable (ethernet, USB, display)
- router, switch, hub

components end user products

- car (ABS, airbag, cruise control, GPS, immobiliser)
- smartphone, iPhone (camera, microphone)
- (smart)TV / (internet)radio

references

http://docwiki.cisco.com/wiki/Internetworking_Technology_Handbook

- http://docwiki.cisco.com/wiki/Internetworking_Basics
- http://docwiki.cisco.com/wiki/Introduction_to_LAN_Protocols
- http://docwiki.cisco.com/wiki/Introduction_to_WAN_Technologies
- http://docwiki.cisco.com/wiki/Bridging_and_Switching_Basics
- http://docwiki.cisco.com/wiki/Routing_Basics

https://en.wikipedia.org/

- https://en.wikipedia.org/wiki/Computer_network
- https://en.wikipedia.org/wiki/Osi_model

http://heise.de/security

- http://www.heise.de/security/meldung/Ein-Drittel-aller-Zertifikats-Herausgeber-nur-Security-Ballast-2139451.html

thanks

thanks for your attention

backup
hidden slides with details

point of attack – data transfer
layer details (OSI model)

layer		standards / protocols
7.	application	NNTP, SIP, SSI, DNS, FTP, Gopher, HTTP, NFS, NTP, SMPP, SMTP, SNMP, Telnet, DHCP, Netconf, (more)
6.	presentation	MIME, XDR
5.	session	Named pipe, NetBIOS, SAP, PPTP, RTP, SOCKS, SPDY
4.	transport	TCP, UDP, SCTP, DCCP, SPX
3.	network	IP, IPv4, IPv6, ICMP, IPsec, IGMP, IPX, AppleTalk, X.25 PLP
2.	data link	ATM, ARP, SDLC, HDLC, CSLIP, SLIP, GFP, PLIP, IEEE 802.2, LLC, L2TP, IEEE 802.3, Frame Relay, ITU-T G.hn DLL, PPP, X.25 LAPB, Q.921 LAPD, Q.922 LAPF
1.	physical	EIA/TIA-232, EIA/TIA-449, ITU-T V-Series, I.430, I.431, PDH, SONET/SDH, PON, OTN, DSL, IEEE 802.3, IEEE 802.11, IEEE 802.15, IEEE 802.16, IEEE 1394, ITU-T G.hn PHY, USB, Bluetooth, RS-232, RS-449

point of attack – components / end user products transmitter house

- [Belkin] Mini Bluetooth 4.0 Adapter 
- [Microsoft] Xbox 360 Wireless Network Adapter  
- [Logitec] UE Smart Radio 
- [LG] Smart TV 
- [Vaillant] heating units 
- [Nest (Google)] smart thermostats 
- refrigerator (as part of a botnet)

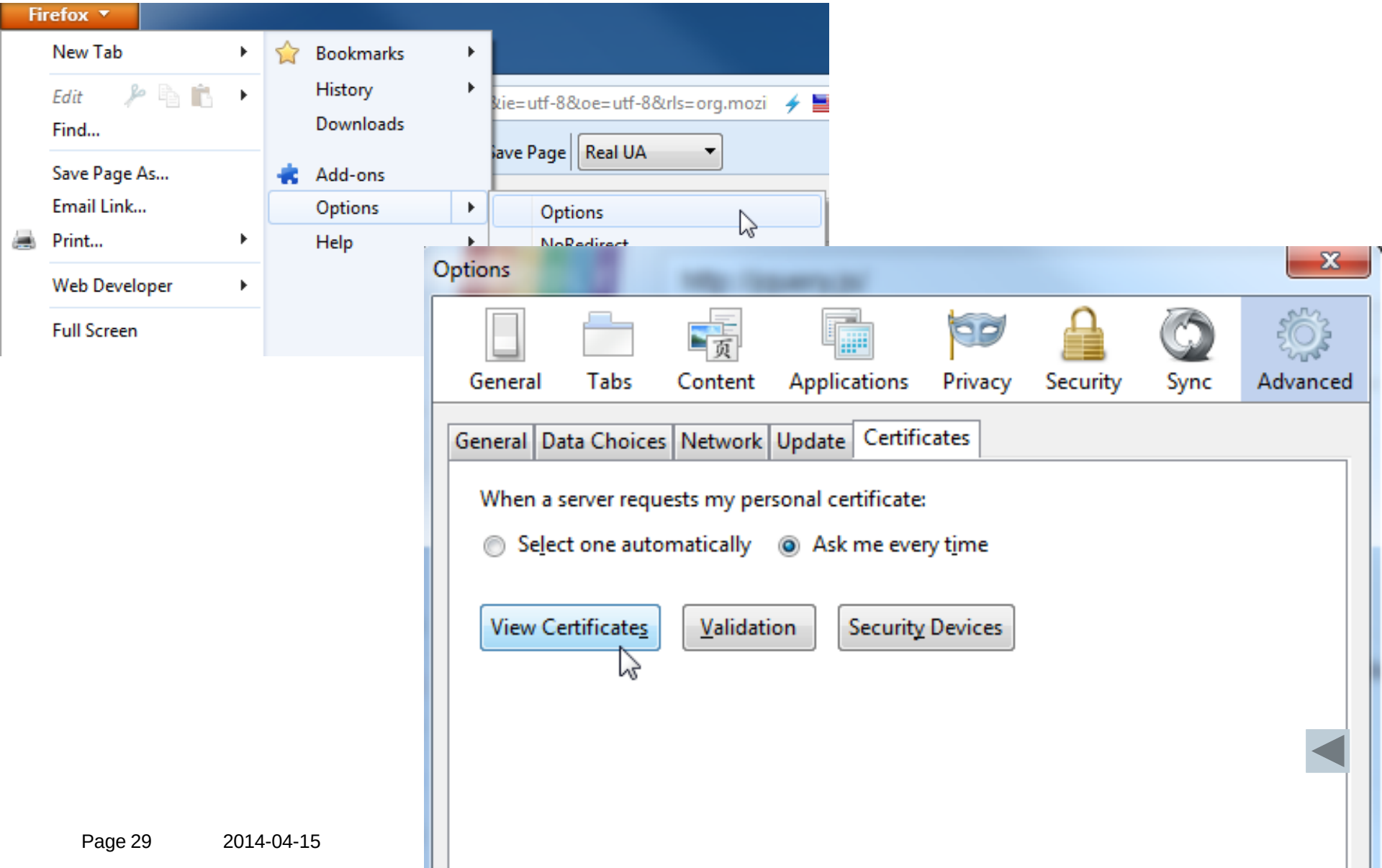
point of attack – components / end user products transmitter car

- ABS
- airbag
- brake power assist unit
- cruise control
- GPS
- immobiliser
- power-assisted steering

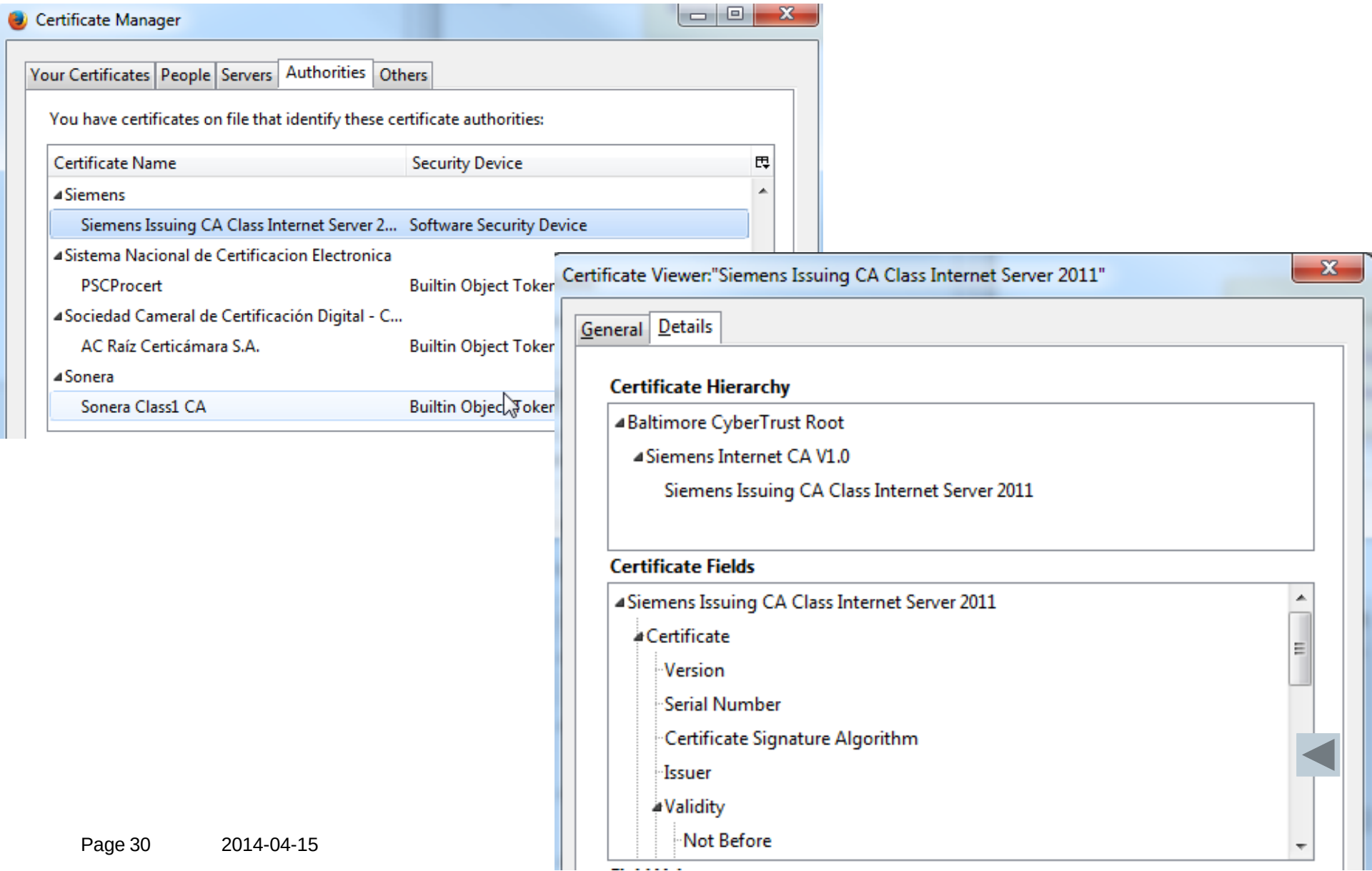
point of attack – components / end user products transmitter wearables

- [google] glass
- smart watches
- smart phones
- (web) camera

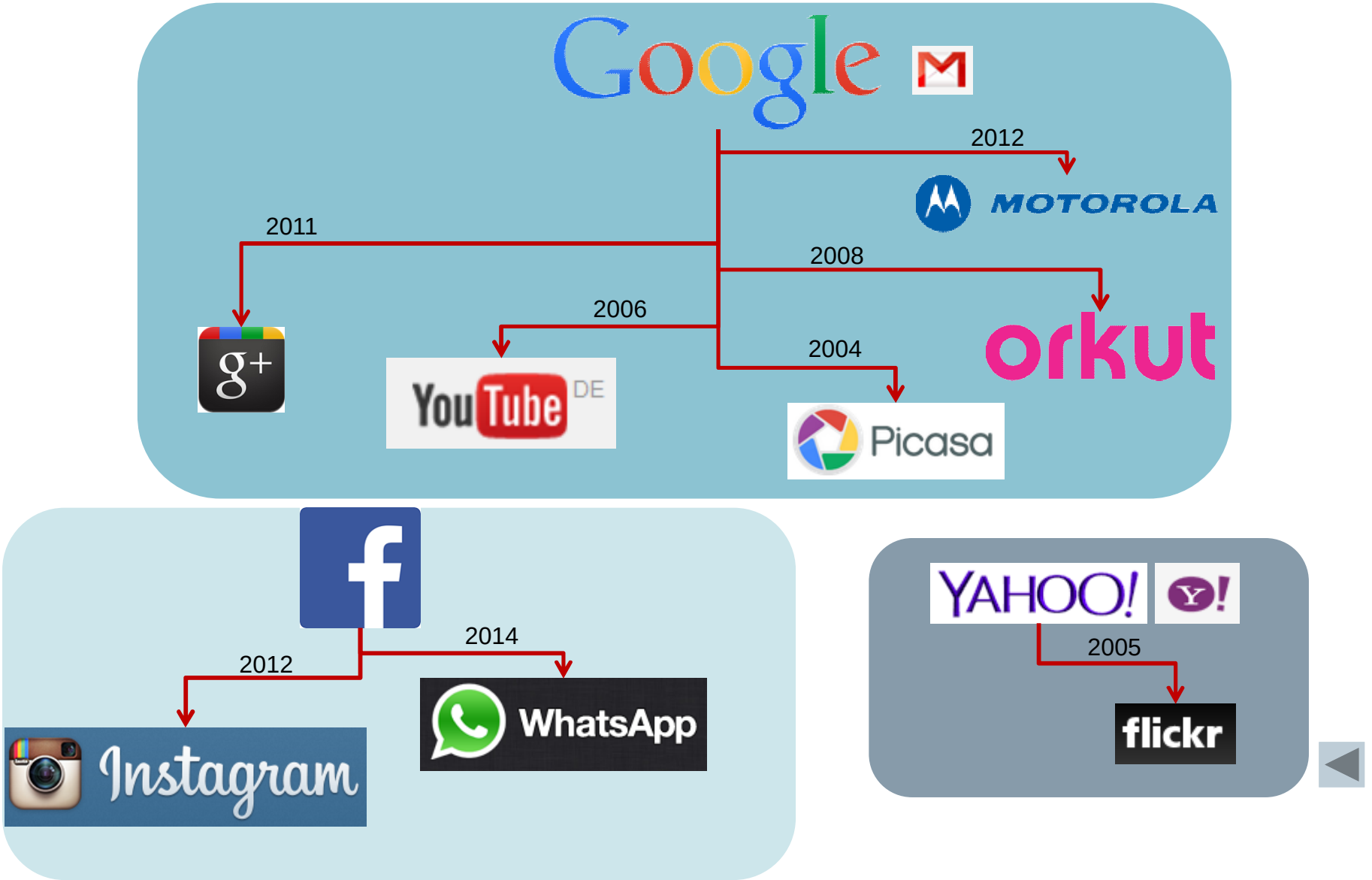
point of attack – data transfer
browser embedded



point of attack – data transfer
certificate trusted chain

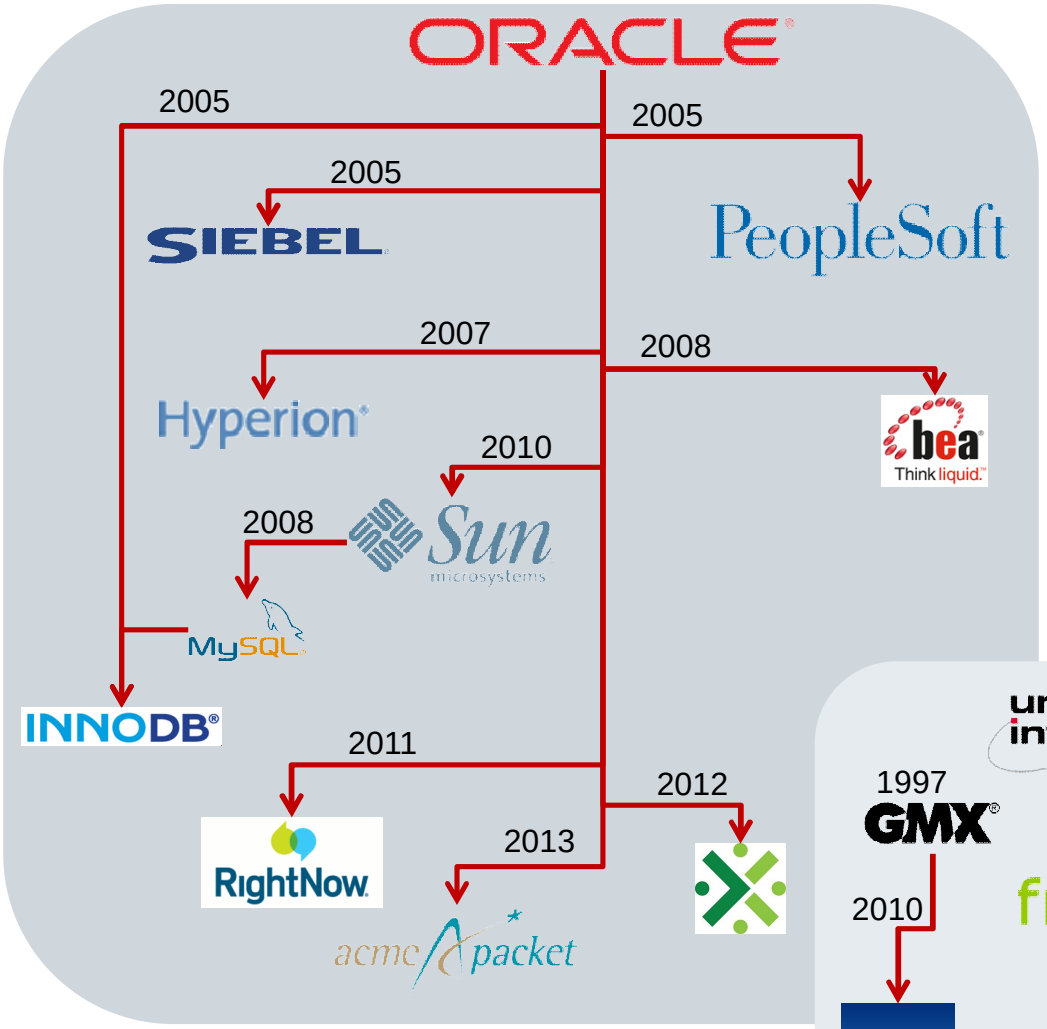


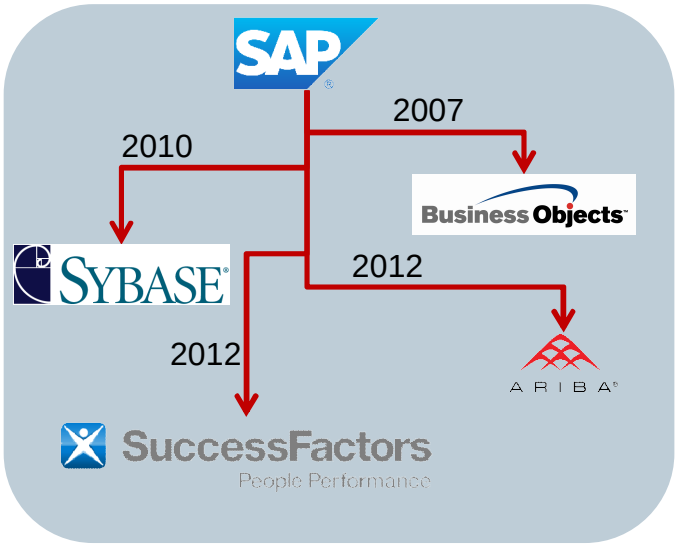
point of attack – information gathering
social platforms

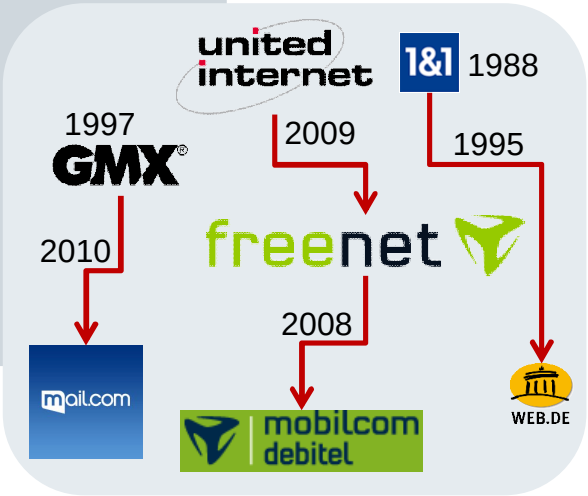


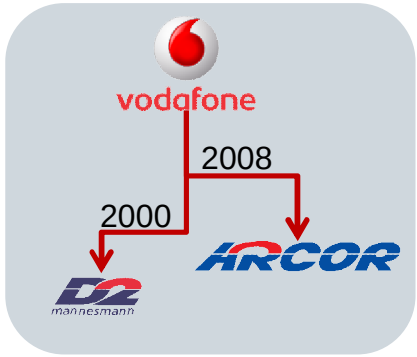
point of attack – information gathering
social platforms

point of attack – information gathering
merger and acquisitions









point of attack – information gathering
search engines

Google

YAHOO!

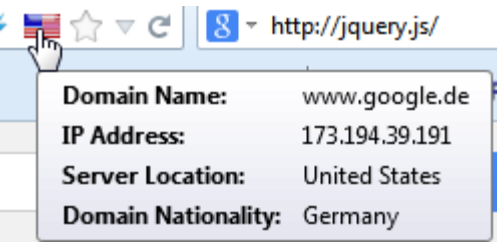
bing

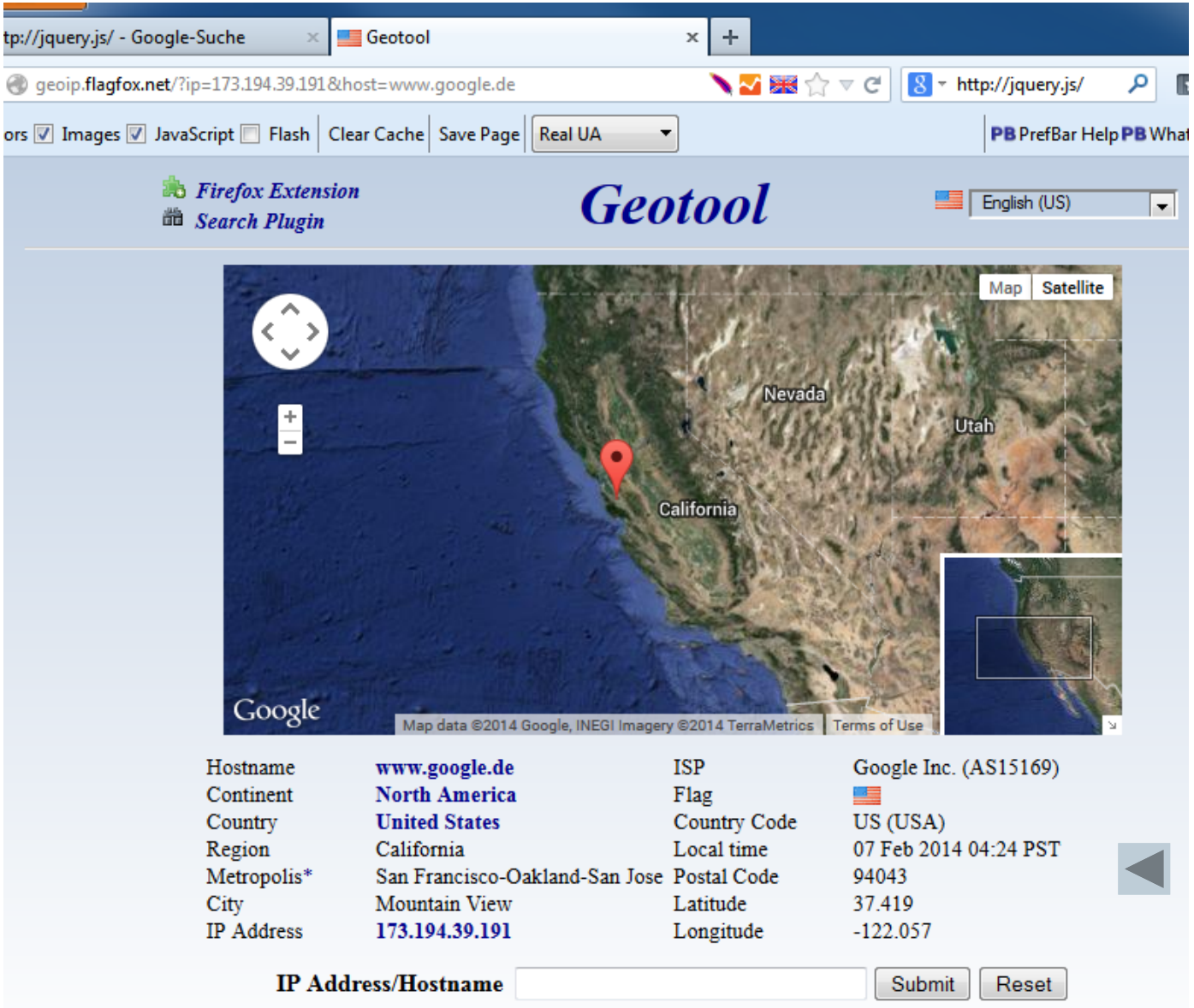
bing

point of attack – information gathering
search engines – sample google

URL	1st address	2nd address	3rd - nth address
www.google.de 2a00:1450:400d:803::1017	173.194.39.119	173.194.39.120	173.194.39.127
www.google.at 2a00:1450:400d:803::101f	173.194.39.119	173.194.39.120	173.194.39.127
www.google.fr 2a00:1450:400d:802::101f	173.194.39.127	173.194.39.119	173.194.39.120
www.google.ch 2a00:1450:400d:803::1018	173.194.39.120	173.194.39.119	173.194.39.127
www.google.com 2a00:1450:400d:803::1011	173.194.39.114	173.194.39.116	173.194.39.113 173.194.39.112 173.194.39.115

point of attack – information gathering
search engines – sample google





point of attack – information gathering
trading platforms

amazon

SCOUT 24

AUTO SCOUT 24

FRIEND SCOUT 24

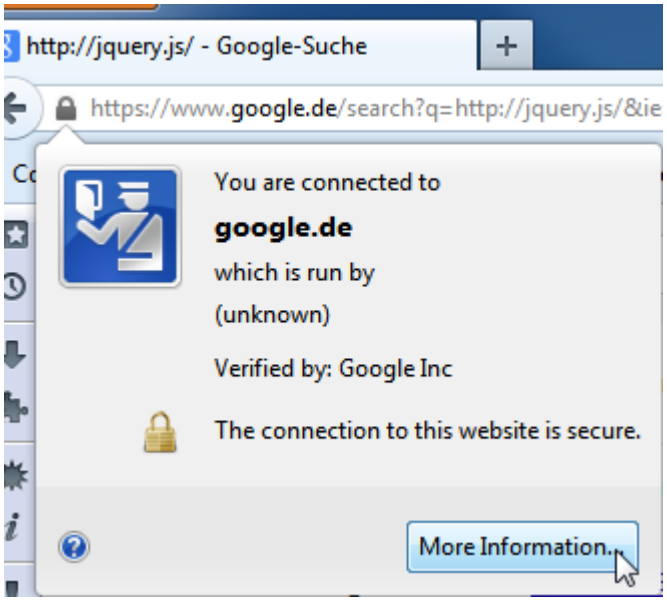
IMMOBILIEN SCOUT 24

JOB SCOUT 24

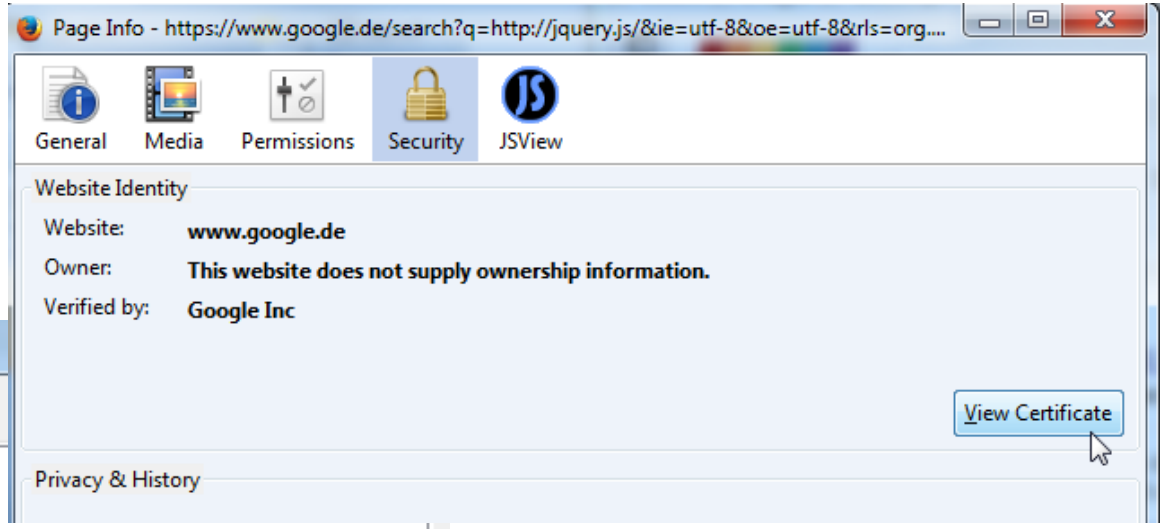
TRAVEL SCOUT 24

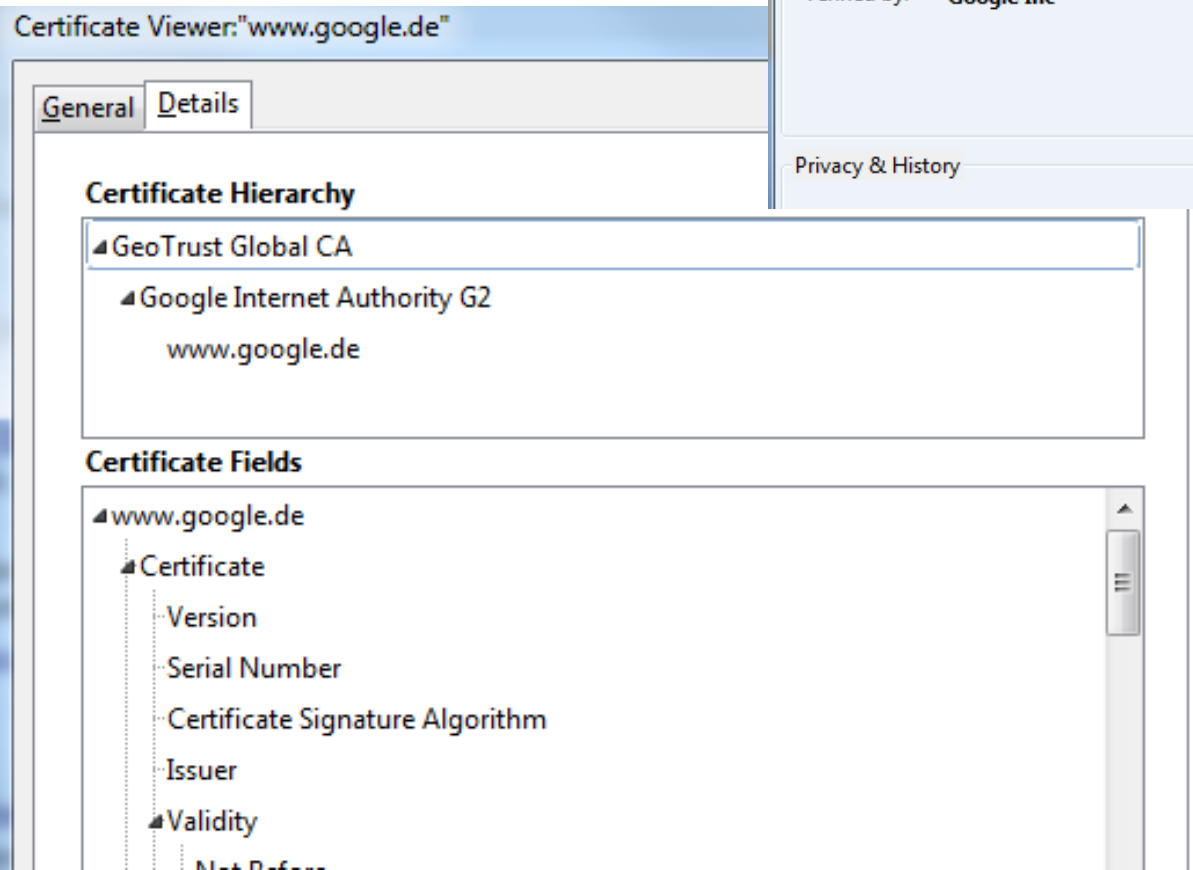
FINANCE SCOUT 24

risk mitigate – what I can change certificate

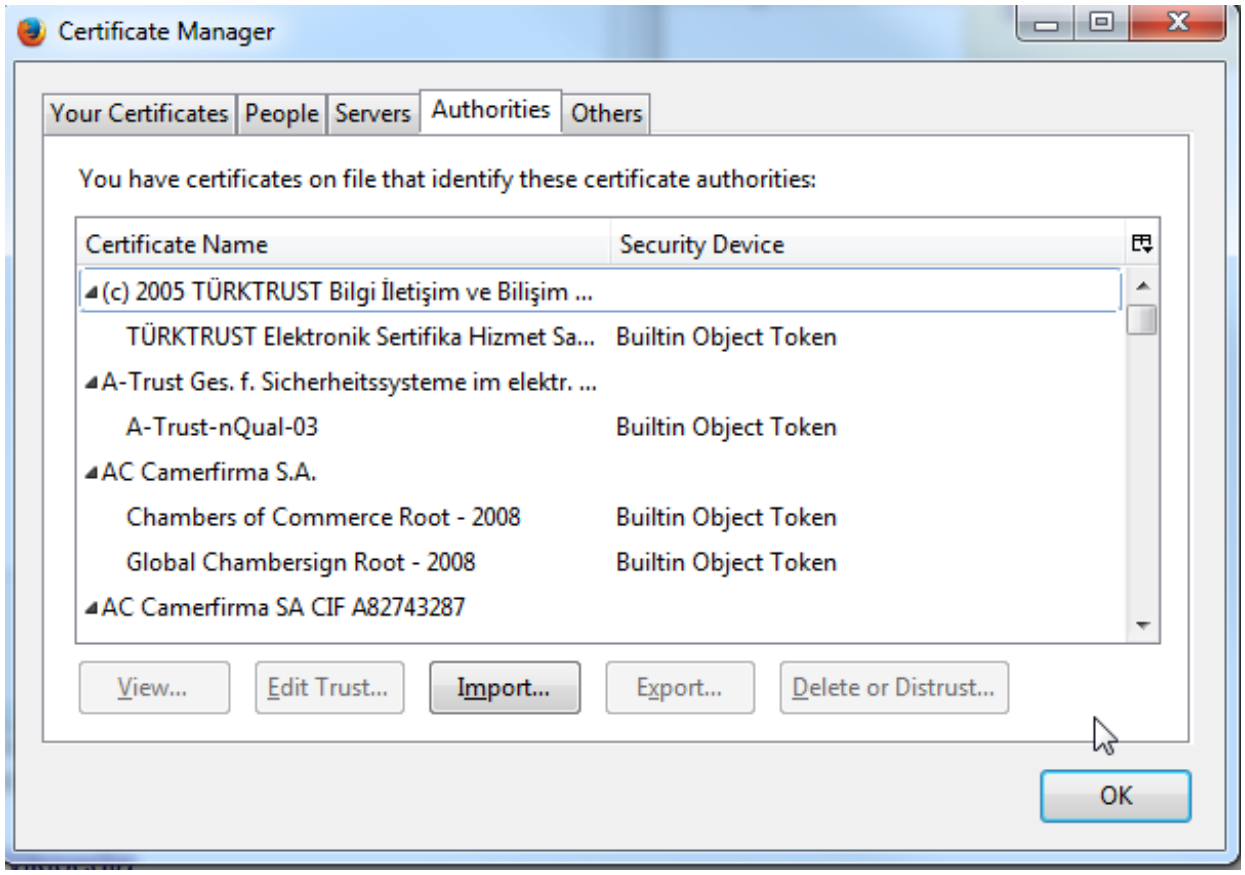


risk mitigate – what I can change certificate





risk mitigate – what I can change certificate authorities



risks acceptance – what I cannot change
laws / Patriot Act

Section	Section title
201	Authority to intercept wire, oral, and electronic communications relating to terrorism
202	Authority to intercept wire, oral, and electronic communications relating to computer fraud and abuse offenses
203(b)	Authority to share electronic, wire and oral interception information
204	Clarification of intelligence exceptions from limitations on interception and disclosure of wire, oral, and electronic communications
206	Roving surveillance authority under the Foreign Intelligence Surveillance Act of 1978.
207	Duration of FISA surveillance of non-United States persons who are agents of a foreign power
209	Seizure of voice-mail messages pursuant to warrants
212	Emergency disclosure of electronic communications to protect life and limb
214	Pen register and trap and trace authority under FISA
215	Access to records and other items under the Foreign Intelligence Surveillance Act.
217	Interception of computer trespasser communications
218	Foreign intelligence information
220	Nationwide service of search warrants for electronic evidence
223	Civil liability for certain unauthorized disclosures
225	Immunity for compliance with FISA wiretap

risks acceptance – what I cannot change
laws / Computer Fraud and Abuse Act

Section	Section title
18 U.S.C. § 1030(a)(1)	Computer Espionage. This section takes much of its language from the Espionage Act of 1917, with the notable addition being that it also covers information related to "Foreign Relations", not simply "National Defense" like the Espionage Act.
18 U.S.C. § 1030(a)(2)	Computer trespassing, and taking government, financial, or commerce info
18 U.S.C. § 1030(a)(3)	Computer trespassing in a government computer
18 U.S.C. § 1030(a)(4)	Committing fraud with a protected computer
18 U.S.C. § 1030(a)(5)	Damaging a protected computer (including viruses, worms)
18 U.S.C. § 1030(a)(6)	Trafficking in passwords of a government or commerce computer
18 U.S.C. § 1030(a)(7)	Threatening to damage a protected computer
18 U.S.C. § 1030(b)	Conspiracy to violate (a)
18 U.S.C. § 1030(c)	Penalties
18 U.S.C. through h § 1030(d through h)	Miscellany