

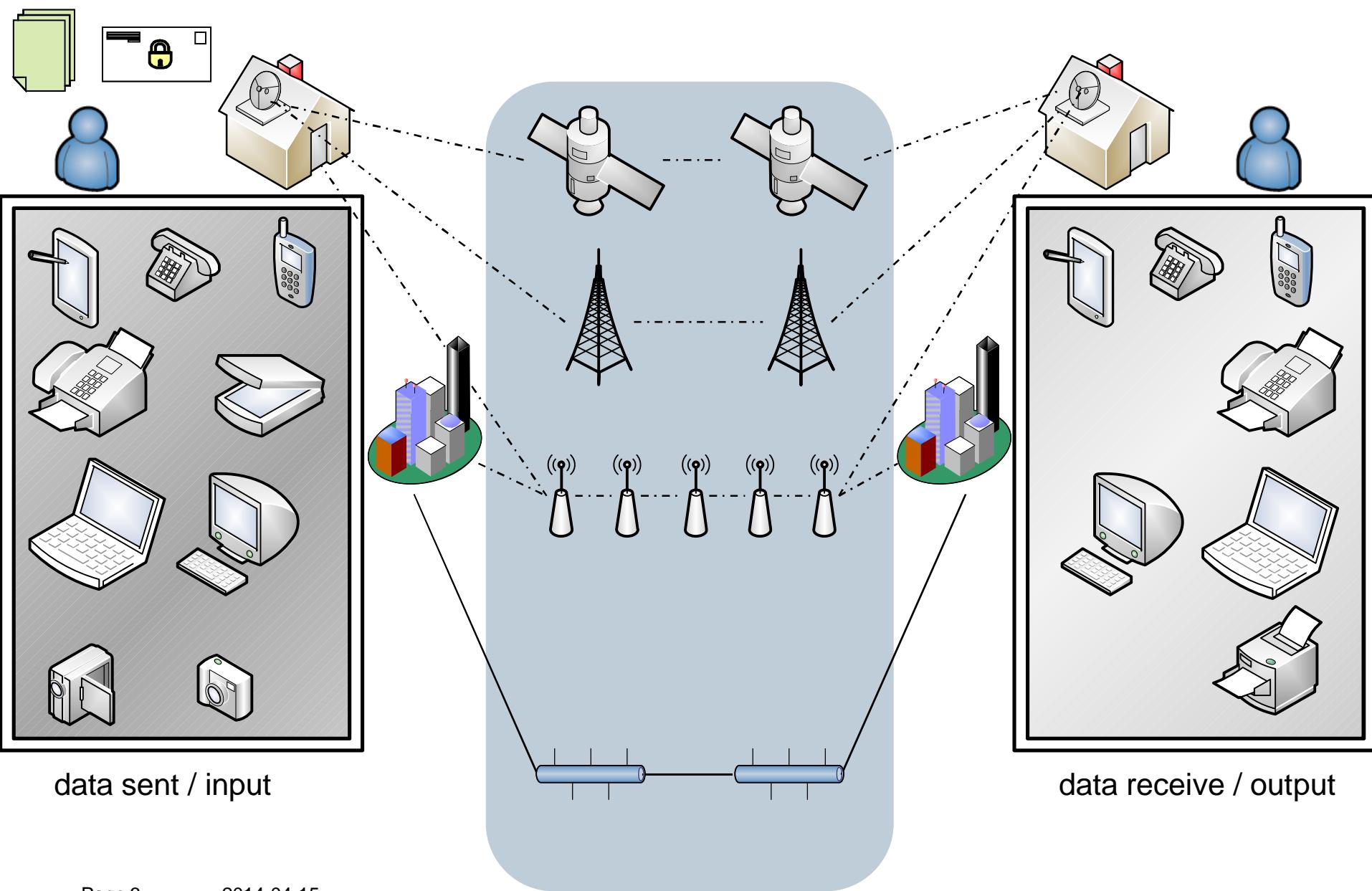
Dr. Gregor Kuznik, Version 1,0 English / April 2014

# **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 anybody's 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



## table of content

1. point of attack	2.2 threats posed to me	
1.1 infrastructure		
1.2 data transfer		
1.3 components / end user products	3. risk management	
	3.1 risk analysis	
	what is relevant for me?	
1.4 information gathering		
	3.2 risk mitigation	
	what I can change	
2. impact	3.3 risk acceptance	
2.1 threats concerning a company	what I cannot change	

# 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 compromises (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
  - „Built-in 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)



38.1%

29.1%

13.4%

10.0%

# **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 administration (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 concerning a company

targets

- espionage
  - intellectual property
  - strategy (portfolio, merger & acquisitions, carve outs, head counts)
  - marketing (offers, orders, suppliers, vendors, customers)
  - assets (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 concerning 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
- loneliness
- 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_Technology_Handbook)

- [http://docwiki.cisco.com/wiki/Internetworking\\_Basics](http://docwiki.cisco.com/wiki/Internetworking_Basics)
- [http://docwiki.cisco.com/wiki/Introduction\\_to\\_LAN\\_Proocols](http://docwiki.cisco.com/wiki/Introduction_to_LAN_Proocols)
- [http://docwiki.cisco.com/wiki/Introduction\\_to\\_WAN\\_Technologies](http://docwiki.cisco.com/wiki/Introduction_to_WAN_Technologies)
- [http://docwiki.cisco.com/wiki/Bridging\\_and\\_Switching\\_Basics](http://docwiki.cisco.com/wiki/Bridging_and_Switching_Basics)
- [http://docwiki.cisco.com/wiki/Routing\\_Basics](http://docwiki.cisco.com/wiki/Routing_Basics)

<https://en.wikipedia.org/>

- [https://en.wikipedia.org/wiki/Computer\\_network](https://en.wikipedia.org/wiki/Computer_network)
- [https://en.wikipedia.org/wiki/Osi\\_model](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

The screenshot shows the Firefox browser interface with the 'Options' dialog open. The main menu bar is visible at the top, and the 'Add-ons' section is expanded. A sub-menu item 'Options' is selected, which has opened the 'Options' dialog window. The 'General' tab is selected in the top navigation bar of the dialog. Below it, a sub-navigation bar includes tabs for 'General', 'Data Choices', 'Network', 'Update', and 'Certificates'. The 'Certificates' tab is highlighted. A question 'When a server requests my personal certificate:' is displayed, followed by two radio button options: 'Select one automatically' (unchecked) and 'Ask me every time' (checked). At the bottom of the dialog are three buttons: 'View Certificates' (highlighted with a mouse cursor), 'Validation', and 'Security Devices'.

# point of attack – data transfer certificate trusted chain

The image shows two windows from a Certificate Manager application.

**Left Window: Your Certificates**

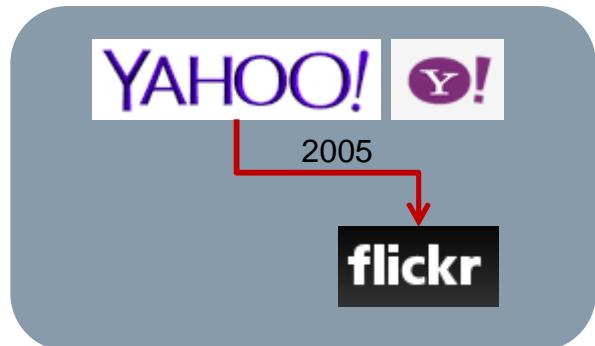
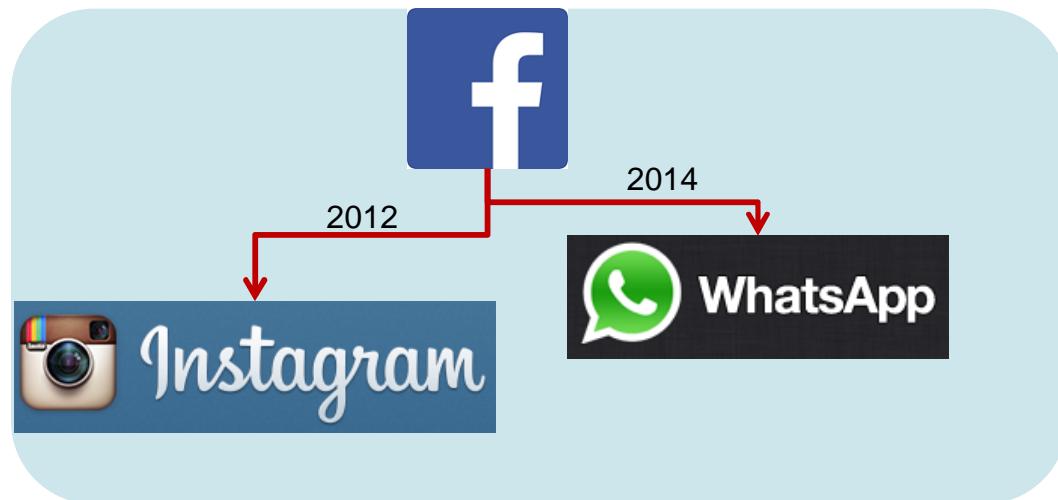
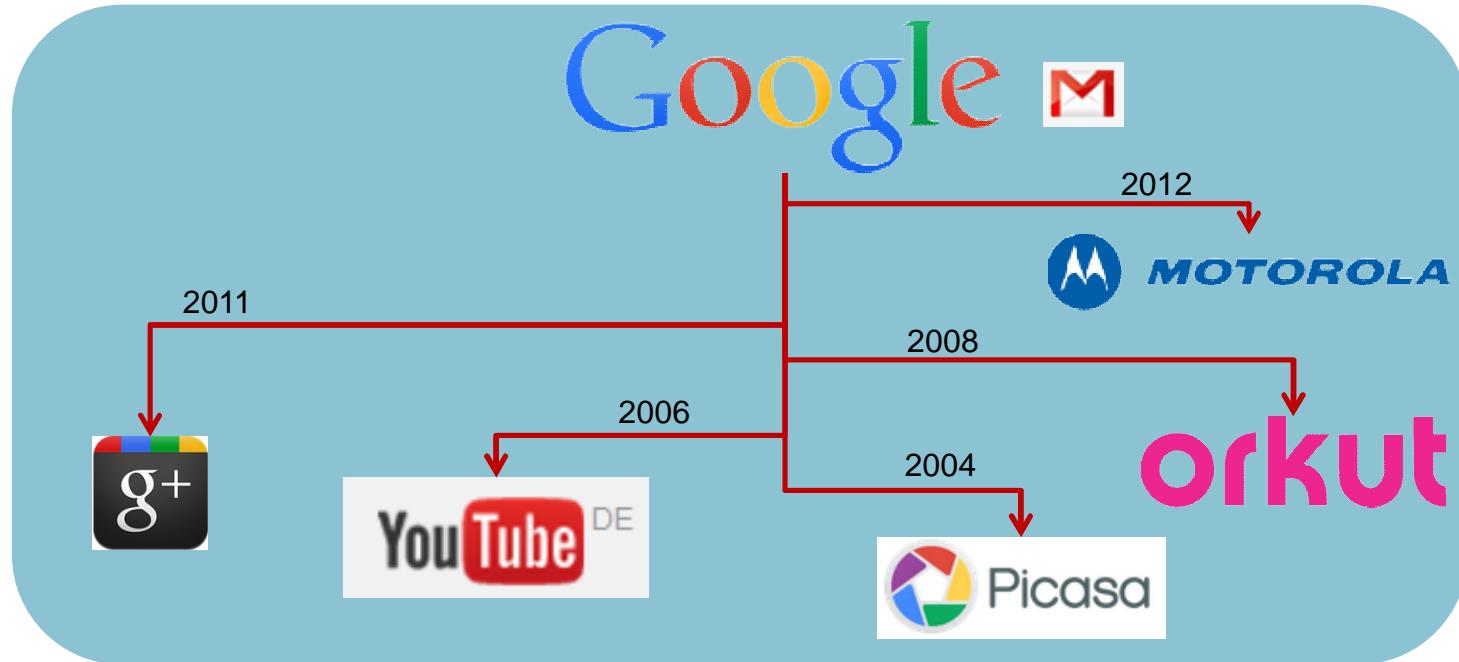
- Certificate Name: Siemens  
Security Device: Software Security Device
- Certificate Name: Sistema Nacional de Certificación Electrónica  
PSCProcert: Builtin Object Tokener
- Certificate Name: Sociedad Cameral de Certificación Digital - C...  
AC Raíz Certicámara S.A.: Builtin Object Tokener
- Certificate Name: Sonera  
Sonera Class1 CA: Builtin Object Tokener

**Right Window: Certificate Viewer for Siemens Issuing CA Class Internet Server 2011**

**General Tab:**

- Certificate Hierarchy:**
  - Baltimore CyberTrust Root
  - Siemens Internet CA V1.0
  - Siemens Issuing CA Class Internet Server 2011
- Certificate Fields:**
  - Siemens Issuing CA Class Internet Server 2011
    - Certificate:** Version, Serial Number, Certificate Signature Algorithm, Issuer
    - Validity:** Not Before

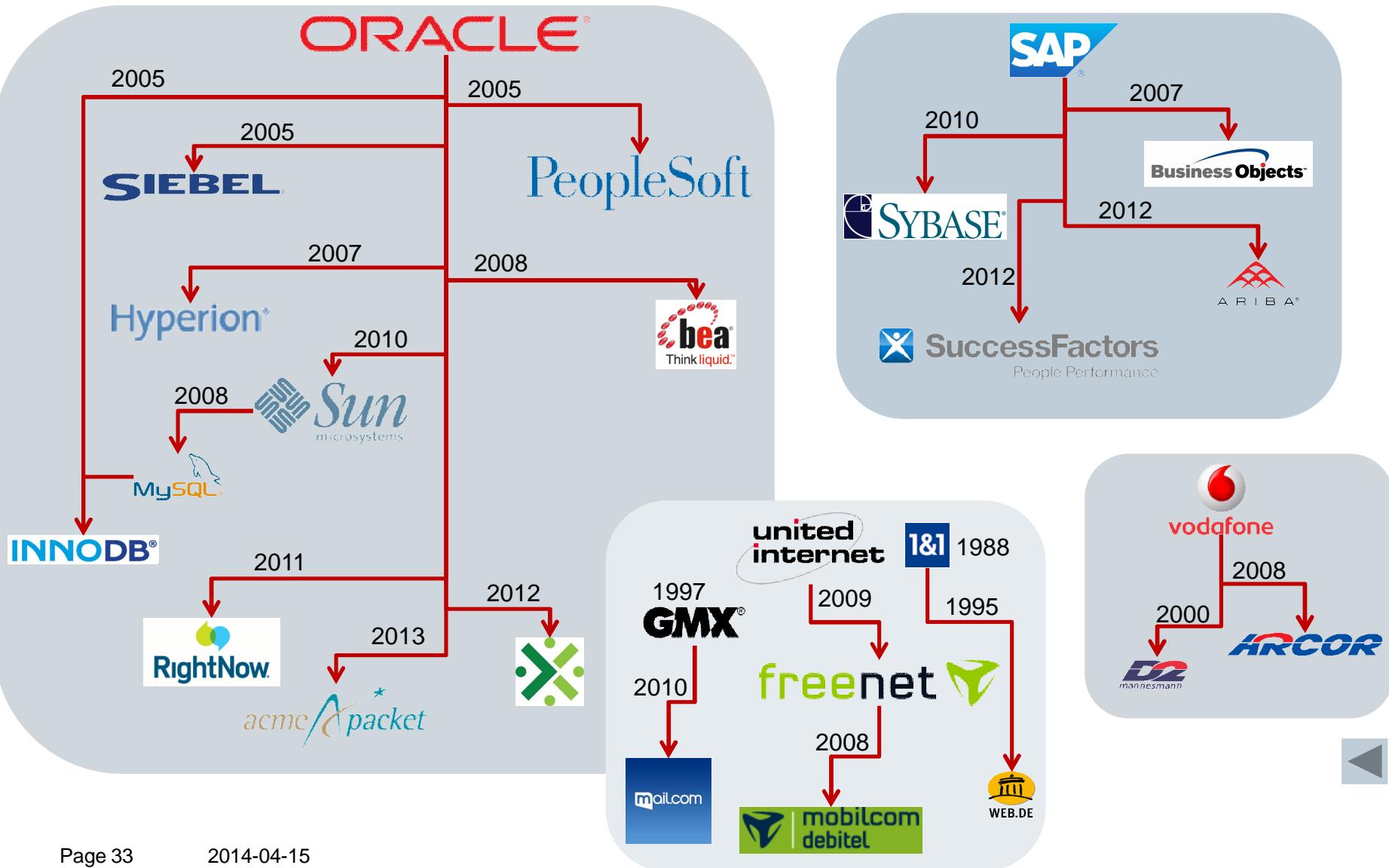
## point of attack – information gathering social platforms



## 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



## point of attack – information gathering search engines – sample google

URL	1st address	2nd address	3rd - nth address
<a href="http://www.google.de">www.google.de</a> 2a00:1450:400d:803::1017	173.194.39.119	173.194.39.120	173.194.39.127
<a href="http://www.google.at">www.google.at</a> 2a00:1450:400d:803::101f	173.194.39.119	173.194.39.120	173.194.39.127
<a href="http://www.google.fr">www.google.fr</a> 2a00:1450:400d:802::101f	173.194.39.127	173.194.39.119	173.194.39.120
<a href="http://www.google.ch">www.google.ch</a> 2a00:1450:400d:803::1018	173.194.39.120	173.194.39.119	173.194.39.127
<a href="http://www.google.com">www.google.com</a> 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

The screenshot shows a Firefox browser window with several tabs and extensions. The main content area displays geographical information for the IP address 173.194.39.191, which is associated with the domain www.google.de.

**Geotool Extension Information:**

Domain Name:	www.google.de
IP Address:	173.194.39.191
Server Location:	United States
Domain Nationality:	Germany

**Geotool Map and Data:**

A satellite map of the western United States is shown, with a red location pin placed near the San Francisco Bay Area. The map includes labels for Nevada, California, and Utah. A small inset map shows the location of the main map. The Geotool interface includes a zoom control (+/-) and orientation buttons (N, S, E, W).

**Geotool Summary Data:**

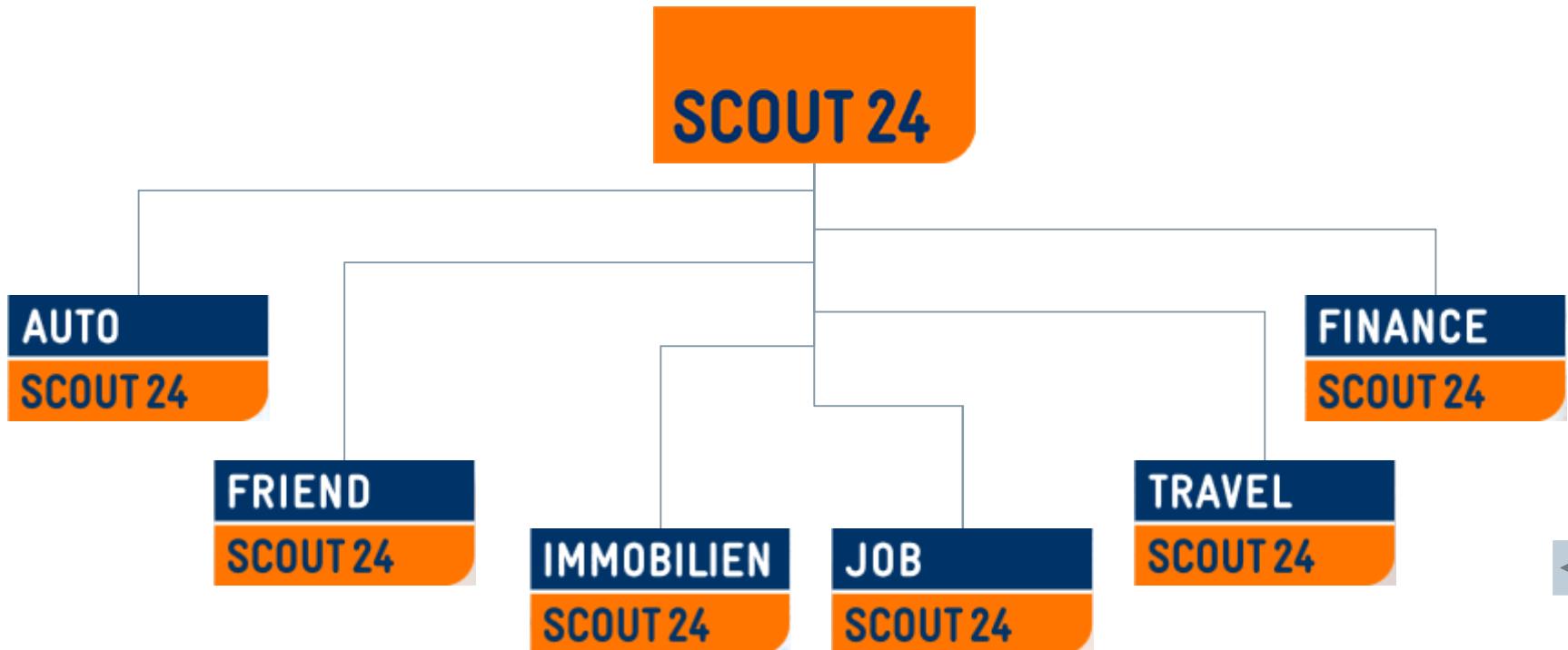
Parameter	Value
Hostname	<a href="#">www.google.de</a>
Continent	North America
Country	United States
Region	California
Metropolis*	San Francisco-Oakland-San Jose
City	Mountain View
IP Address	<a href="#">173.194.39.191</a>
ISP	Google Inc. (AS15169)
Flag	
Country Code	US (USA)
Local time	07 Feb 2014 04:24 PST
Postal Code	94043
Latitude	37.419
Longitude	-122.057

**Toolbar Buttons:** The toolbar includes icons for Stop, Back, Forward, Home, Refresh, and a search bar.

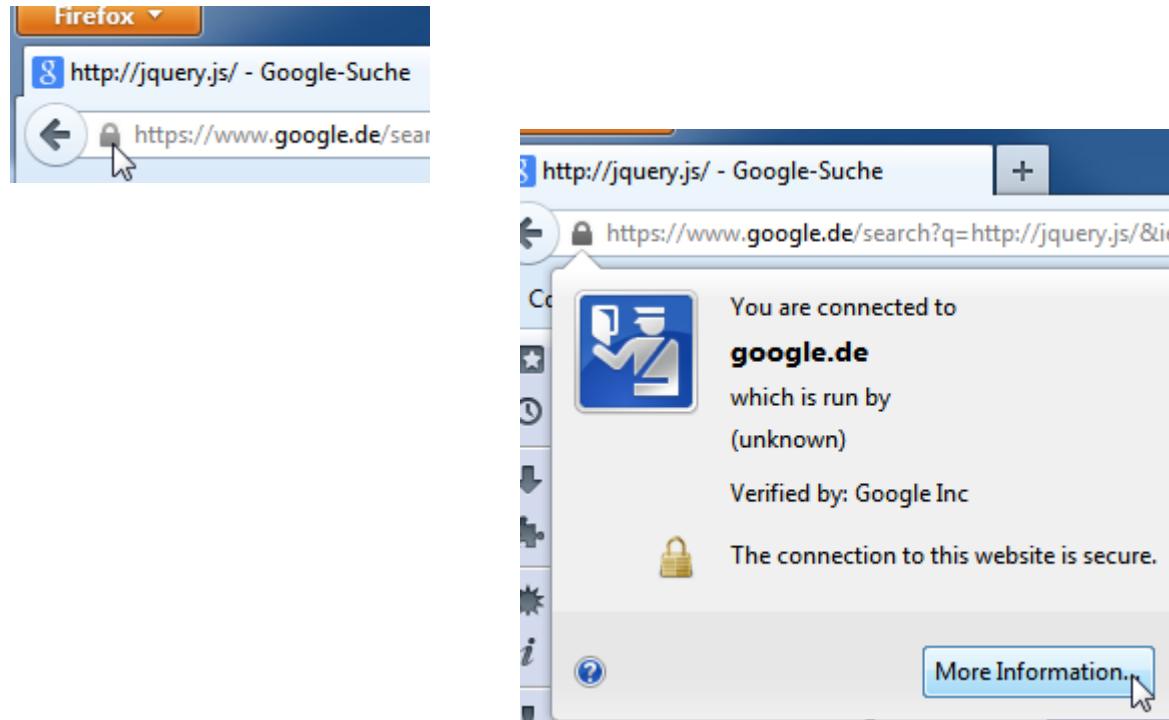
**Address Bar:** The address bar shows the URL <http://jquery.js/>.

**Geotool UI Elements:** The Geotool extension is identified by its logo and name in the top right. It also features a dropdown menu for language selection (English (US)).

# point of attack – information gathering trading platforms



# risk mitigate – what I can change certificate



# risk mitigate – what I can change certificate

The screenshot shows a certificate viewer interface for the website [www.google.de](https://www.google.de). The top bar displays "Page Info - https://www.google.de/search?q=http://jquery.js/&ie=utf-8&oe=utf-8&rls=org....". Below the bar are tabs for General, Media, Permissions, Security, and JSView. The Security tab is selected.

**Website Identity:**

- Website: [www.google.de](http://www.google.de)
- Owner: This website does not supply ownership information.
- Verified by: Google Inc

**Certificate Viewer:"www.google.de"**

**General Details**

**View Certificate**

**Certificate Hierarchy:**

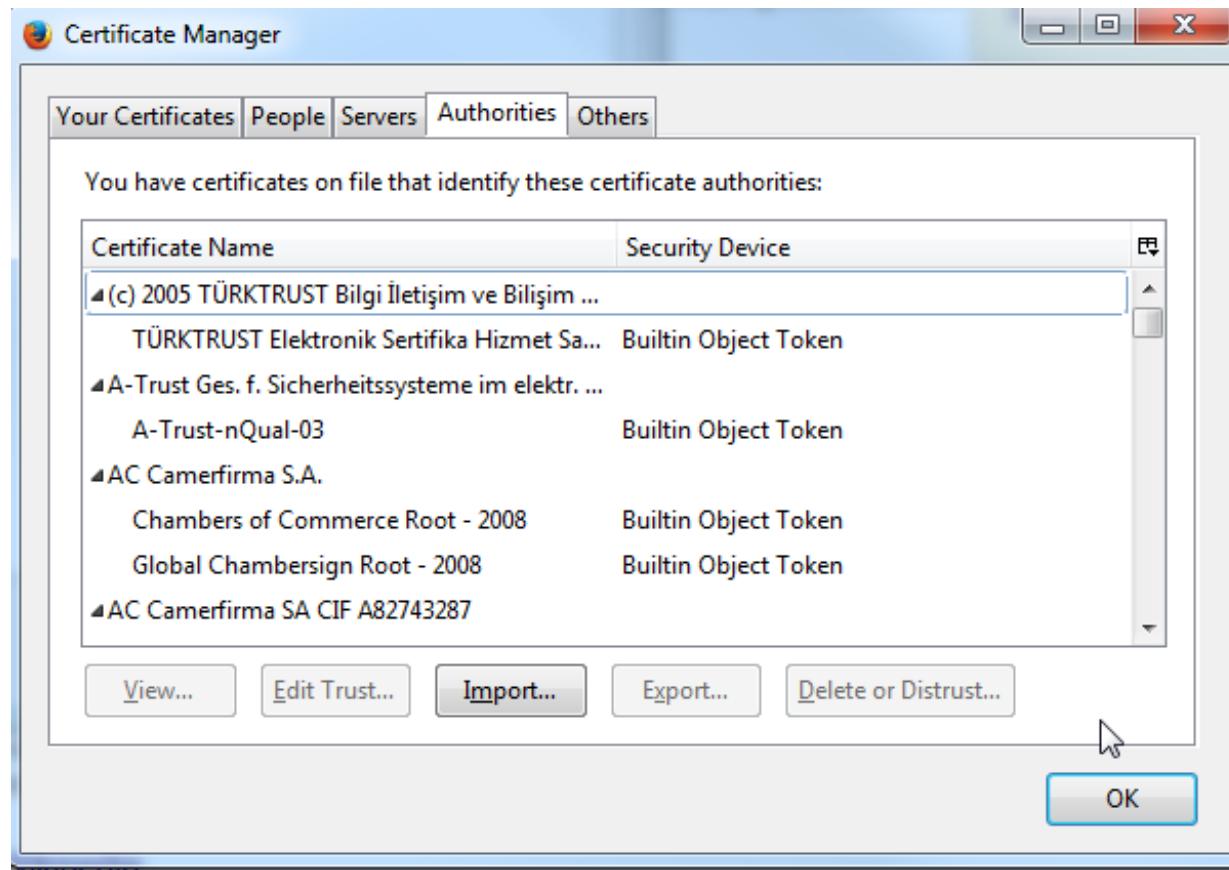
- GeoTrust Global CA
  - Google Internet Authority G2
    - [www.google.de](http://www.google.de)

**Certificate Fields:**

- www.google.de
  - Certificate**
    - Version
    - Serial Number
    - Certificate Signature Algorithm
  - Issuer
  - Validity**
    - Not Before

A vertical scroll bar is visible on the right side of the main content area.

# risk mitigate – what I can change certificate authorities



# **risks acceptance – what I cannot change laws / Patriot Act**

<b>Section</b>	<b>Section title</b>
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**

18 U.S.C. § 1030(a)(1)

### **Section title**

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

