



# openHPI – Internet Security Internet Surveillance

**Prof. Dr. Christoph Meinel**  
Hasso Plattner Institute, Potsdam, Germany

# Introduction

The Internet provides for today's society an integrative communication infrastructure and makes the world a global market place. We cannot imagine modern life without the Internet

However, the Internet also offers many ways to monitor people

- Everyone leaves traces on the Internet that others (also undesirable) can track down and evaluate, e.g. via

- emails
- social networks
- browser profiles/ cookies
- web beacons
- webcams
- IP addresses
- ...



Source: [naturalnewswatch.wordpress.com](http://naturalnewswatch.wordpress.com)

# Email Observation (1/2)

---

- Without special precautions, emails are sent and received in plain text
- Who has access to emails and could monitor them?
  - email providers, since they store and send emails
  - anyone who has access to the registered computer or to the email account
  - operators of Internet routers through which email traffic is handled
  - attackers who have taken over Internet routers
- Emails with sender and recipient in the same country can also be transferred via foreign routers (e.g. USA), if these enable a faster connection
  - allows access to emails, even from abroad ...

## Email Observation (2/2)

---

**Large-scale monitoring** does not read all emails

- Emails are searched for specific words or phrases, in order to find, select or filter relevant emails

**Precautions:**

- Encryption and signing of emails
- Some email providers include encryption with their service
  - But email providers themselves could still read along ...
- **Better:** Encrypt yourself, e.g. with PGP or GPG

# Observation in Social Networks

---

People can also be monitored with the help of social networks - Facebook, Twitter, Google+, etc.

- Many posts about everything happening to people every day
- Who can observe?
  - operators of the social network
  - "friends" or members of the network
- Also popular are offers of "Login with ..." for other Internet services, e.g. login with Facebook or Google
  - very convenient: Saves another registration or new password
  - **but**: The operator of the social network sees which other services you are using

# Browse Profiles and Cookies

---

Browsers can also be used to get information about people

- Browsers save all the websites visited (history/ chronicle) in order to allow users to retrieve them more quickly
- Even passwords are often stored in the browser
- By reading the history, you will know when the user has called which page, how often he/she does it, and where he/she has logged on (e.g. password manager)
  - opens up opportunities for attackers to log on under a false name and therefore obtain the passwords
  - requires browser access

## **Precautions:**

- Regular deletion of history and cookies removes browser traces

# Web Beacons (1/2)

---

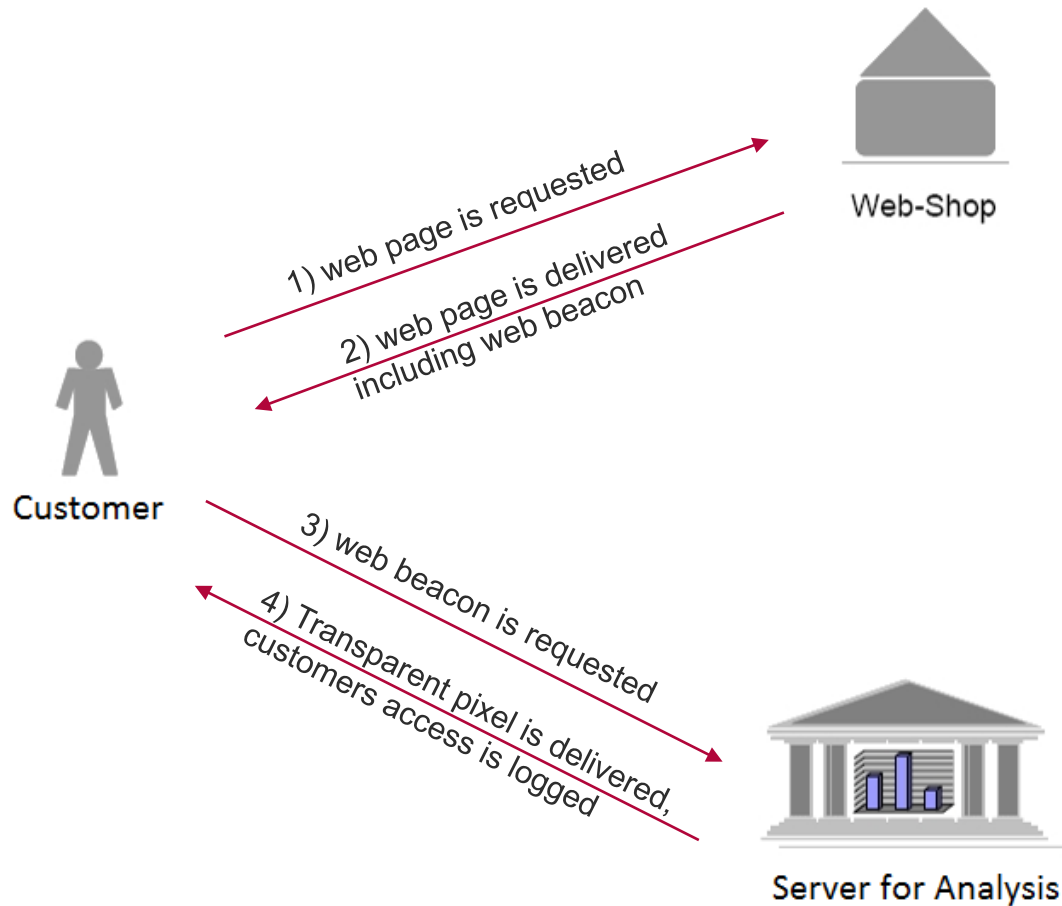
Counting pixels are tiny (thus “invisible”) 1x1 pixel large pictures, inserted on websites or in emails

- As soon as an email with a web beacon is opened, the image is loaded from the server and the sender of the email (or its server) knows that the email has been opened
  - web beacons are used in online marketing, for example, for newsletters
  - another form of reading confirmation
- Using web beacons on web pages, the number of visits can be determined

## **Precautions:**

- Email programs can block the loading of images/ HTML ...

## Web Beacons (2/2)



Source: Wikipedia

# Observation via Webcams

---

Webcams enable many useful functions

- Video chat
- Video calling
- monitoring own house, for example,
  - pets
  - to check if everything is fine

However, it also provides third parties with the means of hacking or using webcams for their own purposes, e.g. for spying on and monitoring

- people
- buildings, houses and apartments
- streets, traffic, ...

# IP Addresses (1/3)

---

Even without browsers and cookies, Internet movements can be tracked by means of IP addresses

- To access the computer or smartphone via the Internet, the domain name or IP address is used
- When visiting a website, your own IP address must be sent so that the answer can be sent to the correct computer
- IP addresses can be stored in this way
- Recurring visits are recognizable in this way, even without the user logging in or registering

## IP Addresses (2/3)

---

**When using IPv4**, for web sites, it is not easy to recognize such movements and assign them to a user because of the lack of addresses

- Different users from the same home network can use the same IP address outwardly
- Router redirects the response for this IP address to the "correct" user in the home network
- Users cannot be clearly identified to the outside world

Reason: IPv4 has only a limited number of IP addresses that are already exhausted

- This is why it is often used with dynamic IP addresses
  - Changes at specific time intervals, e.g. every 24h

# IP Addresses (3/3)

---

The current successor protocol to IPv4 is **IPv6**

- An inexhaustible supply of IP addresses (from  $2^{32}$  to  $2^{128}$ )
- Each device can have its own IP address
  - computers, laptops, smartphones, household appliances (refrigerator, washing machine, ...), sensor cords, etc.
- Enables more efficient routing (less computational effort)
- Home routers are no longer necessary
- Autoconfiguration, procedures such as DHCP are redundant
- Security aspects (IPSec) are permanently integrated in the protocol
- Mobile IP

**But:** Internet movements can be assigned directly to a device/user via their own IP address ...

# Internet Surveillance via PRISM (1/2)

---

## **PRISM** – US example of surveillance in a big way

- PRISM was launched in 2005 and is run by NSA
- PRISM has access to 9 of the largest Internet corporations and services including Microsoft, Google, Facebook, Yahoo, Apple
- So far, the largest form of Internet surveillance
- This affects not only Americans, but people around the world who use American services
- It was made public in 2013 by whistleblower Edward Snowden, who gave information about PRISM et al. via media like “The Guardian” and “The Washington Post”

# Internet Surveillance via PRISM (2/2)

---

**PRISM** – US example of surveillance in a big way

- PRISM allows NSA access to:
  - emails
  - videos
  - voice chats (also Voice-over-IP)
  - photos
  - data transfers
  - details from the social network
- Data are scanned for specific information
- Also live communication can be monitored