A One Day Big Brother Diary

Marc Peter, Macskási Csaba

Abstract. This paper describes a day of a member of our society. That day happens to be the worst case scenario considering privacy and freedom. This paper should make people realize how mass surveillance works, which technologies are being used and what you can do to protect yourself. It demonstrates the amazing amount of data which can be collected from individuals.

Keywords: mass surveillance, big brother, privacy

1. Introduction

The amount of stored personal data which invades the users privacy is rising continuously. This paper tries to summarize the most common or interesting risks, technologies and how they are being exploited. It tries to present the enormous amount of data on a diary entry of an average person. Moreover it contains also some advice on how to prevent data extrusion and save your privacy.

2. The Day

Our test person gets up and instantly switches on the television (see section 3.1), which gets the signal over Ip-TV. While laying on the couch he orders an espresso from his coffee-machine which is connected and can be controlled by Ethernet. Of course all actions are logged on the home-server and – as an additional security feature – also at a backup-provider. During breakfast he checks the weather prognosis. While doing that his MUA automatically checks his e-mails (see section 3.2) via wireless LAN (see section 3.3). Before leaving the house he activates the home security system which is connected to a security company and opens the garage door which is remote controlled by Bluetooth (see section 3.3). He gets caught on tape by three cameras around the block while leaving the area (see section 3.4). As he takes the highway his license plate number is being recognized automatically to check if he has paid the road toll (see section 3.6). After that he gets photographed by a radar, despite the speed limit warning from his GPS system (see section 3.5). Beside all these obstacles he reaches the office , where he can enter the parking lot with a chip card. All that separates him from his desk is the office door which must be elegantly opened by the RFID-chip on his split ring (see section 3.6). He takes a seat and boots his PC. In the lower left corner of the screen, right next to the clock a little logo with the letters “VNC” appears. The last time he checked his mails was more then an hour ago. That is awfully lot, so he has to check them again via the web interface of his e-mail provider (see section 3.2). Of course he does not use encryption and his browser is only allowed to communicate via the proxy server of the company. After some time he cannot resist the temptation to buy some new stuff so he visits a popular online auction platform and buys some accessories for his mobile phone. (see section 3.8) The payment is made via the web site of the bank where he has his account. After all this hard work he gets a coffee from the company's coffee machine which he can only pay for by QUICK. At the end of the day he gets photographed by Google-Earth while getting out of his car in front of his house (see section 3.7).

3.) Technoligy / Prevention

1. Ip-Tv

Is one of the newest technologies that are covered in this paper. The idea of sending TV pictures over the internet is an old one. The reason why this is such a new technology is that there are missing pre requirements. For TV over IP a bandwidth of 5 Mbit per second is necessary.[6]

A normal TV signal is sent via broadcast over a DVB-C/S/T infrastructure to the set top boxes. This means all customers can only see the same pictures to the same time. The intention for IPTV is this guidline:

“A different picture for each customer.”

To satisfy the customer’s needs different technologies can be used.

Unicast IPTV:

This solution sends all frames that are visualized on the TV over IP. Every set top box has his own connection to a server which delivers independent pictures for each customer.

Multicast IPTV:

This sort of IPTV uses also the IP layer as transport. The normal broadcast signal is sent via a multicast to the greater network nodes. When a customer likes to switch the program the set top box joins this multicast. The video on demand content is also sent via unicast.

Switched broadcast:

This is the only solution which uses a different transport layer than IP to send the pictures. As transport the “normal” DVB protocol is used for the broadcast and unicast signal. When a subscriber requests a video on demand a DVB channel own DVB channel is used to transfer the picture.

P2P IPTV:

A providers sends each channel to a few users which deliver the pictures again to the other users. This technique is used to deliver the broadcast pictures. When a two or more subscriber requests the same video on demand stream quite at the same time this stream is also delivered via P2P.[7]

What all this solution have together is the ability to send data back to the service provider. Basically your TV provider can see what you are watching in the TV. They can send you customized advertisements and make a suggestion what you want to see. Like “other people who watched this film also watched that one”.

The solutions number 2 and 3 that are listed above can only be provided by your local internet provider because of technical controls. The technique described in point 4 is the most dangerous out of the view of data security. Many people that are using the P2P client can see what you are watching.

2. E-Mail

E-Mail has almost completely replaced regular mail. As technology is improved, privacy issues become bigger and bigger. Some decades ago mail could only be read and censored by the government or employees of the post office. This has changed. Mail is not being delivered by one organization any more. It runs through several different networks as backbones and local providers. As conclusion the possibility of someone eavesdropping has increased dramatically.

As anyone can observe in public, unencrypted WIFI-networks pop3 is still a very popular protocol to check E-Mails. Considering the encryption of this protocol – which is none – it can be said that pop3 is a huge security issue. But people use it anyways as it is easy to set up and most of them do not even know about the risks. The SMTP protocol which is being used to send E-Mails is also unencrypted and does not feature sender validation which makes is very easy to forge mail and eavesdrop as messages are being delivered. An other problem is that there is almost no evidence if someone reads an other person's mail. There is no envelope which is gets destroyed while opening a letter. If the files where mails are stored are read on file system level not even the reading notification is sent.

Privacy problems do not only exist in form of private letters. Public mail can also be an issue. Imagine that you post something on a mailing list. Are you sure that you will agree with the posted content in ten years? Do you really want your employer to be able to read everything you have ever posted online? Because that is what we get thanks to mailing lists and search engine caches even if we manage to remove the data from the original source.

To reduce the risk of data extrusion you can use cyphered protocols and tunnels. Do not use pop3. If you must use it try to tunnel it over VPN or SSH. Use PGP to encrypt messages.

3. Wireless LAN / Bluetooth

During the past few years wireless LAN has become very popular due to it's simplicity from the user's point of view. Its great for home users because they don't have to drill holes in their walls and they have internet access in every room. However, there are two major problems with WIFI: It is insecure by design and most people (especially home users) who set up wireless connections don't have the knowledge to build a secure network. Many home users don't use encryption like WEP or WPA at all which allow attackers to capture network traffic immediately. There are also security issues beyond the user: " *Wireless networks often are cited for their lack of physical security. Unlike a wired network, an attacker could be in an unsecured location such as a parking lot or a passing car.*" [3] Furthermore there are security flaws in WEP and WPA encryption. With proper attacks like ARP replay or station deauthentication the WEP key can be found in minutes allowing the attacker to decrypt network traffic. Basically this means that any script kiddie with a laptop and a car can eavesdrop on people in their homes.

The only possibility to increase privacy in wireless networks dramatically is to use higher level encryption. This can be done for example by setting up a VPN connection or an SSH-tunnel. However these methods are usually unusable for home users, because they don't have a VPN or SSH server to connect to.

It is said that Bluetooth is the most vulnerable communication technology which is being used. CITATION NEEDED! One reason for this are the default settings of cellular phones and other devices. Many people do no know this and do not disable Bluetooth. As a result data can be read and written to these devices.

4. Cameras / Biometric identification

Nowadays you can find cameras on the most public places. They are used to protect railway stations, shopping malls and our streets. In the most scenarios they are not only used to bring the pictures to monitor. All these pictures are analyzed via a biometric analyzer. These analyzers are based on different specific software modules that can identify different types of geometric structures.

A person can be identified by the face, the fingerprint, the hand geometry, the Iris, the signature and the voice.[4] Analyzing a face can be divided in 4 steps:[5]

Picture recording:

The picture can be made with a normal camera. The limitation for a good picture is the light conditions and a resolution of 100 x 100 pixels. The system also determines if a face can be localized.

Normalizing, modification:

The picture is cut to get the detail of the face. It's also converted into the black/white format.

Extraction of attributes:

After standardizing the picture all characteristic face attributes are measured. Including cheekbones, corner of the mouth, outline of the nose and the circumorbital rings. Out of these data a sample picture is created and stored as a template.

Matching:

There are two different methods to compare such templates. The first method compares only sections of the template. A sample for this is the "Elastic Bunch Graph Matching". The second one compares the whole face and is called "Template Matching". In practice a combination of these two variants is used.

The precursor in video observation is Great Britain. In the cities of GB you can find more than 4.5 million cameras. When you take a walk through London you are filmed approximately 300 times a day. It's not beside the point that your whole daily routine can be tracked.

5. GPS

The Global Positioning System is a satellite based positioning system. It uses 24 satellites which circuit on 6 orbits the earth. This system was invented in the 60th and 70th from the U.S. Department of Defense (DoD). GPS implements a time-difference-of-arrival concept using precise satellite position and on-board atomic clocks to generate navigation messages that are continuously broadcast from each of the GPS satellites. [Neff] In former times the equipment was too big to integrate the technique in smaller devices. Nowadays it is integrated in new telephones, cars, bike computers and so on. Often these devices have a so called buddy system integrated in the device. This means that the telephone sends your exact position to another phone which displays the distance between the devices. This solution is also used by transport companies to track their drivers. These applications are as save as the transmission between the sender and receiver is implemented.

One other major problems are the so called GPS Jammers. These devices sends their own GPS to signal to jam the signal or the manipulate the signal. Manipulating the signal is the worst case that can happen. To avoid this the newer, more expensive receiver implemented techniques. But up to now it's possible to break the connection between a receiver and the GPS satellites. These GPS jammers are often used by car hijackers to prevent the using of car tracking systems.

6. RFID

Radio Frequency Identification (RFID) is a technology which is designed to transfer information over a short distance. In the most scenarios where RFID is used the maximum distance is about 5 to 10 meters. The range of application starts from parking tickets, access systems, time management systems over personal identification and ends with car toll systems.

RFID is the umbrella term for different transmission technologies. These technologies can be categorized in the frequency range, modulation profile and the encryption that they are using. All of these parameters are conducive to the security of RFID.

The manipulation methods of the RFID technology can be divided in two different sections. The first is the avoiding the transfer and the second is changing something in the data connection. The second one is the worse case of these two, because people can get unauthorized access, betray toll charge system and misuse all other applications that are using RFID.

The worst case scenario occurred in 2006 when the British government decided to use a RFID based mechanism to secure their peoples passports and it took only 48 hours to crack the used security mechanism. The Problem in this case was that the information on this chip was not stored encrypted. Only the connection was encrypted in this case.

RFID is an often well hidden, pervasive way to gather information. On one hand there are passive mode chips can be included in plastic cards, passes or even clothing. These chips cannot be detected visually but can only be read from a close range. *"Some passive tags operate in the low-frequency band (125–134.2 KHz), such as proximity cards and implantable glass-covered transponders. These devices have a typical read-range of less than two feet."* [1] On the other hand there are active devices which have an own power source and can actively transmit. Usually these devices are lager then passive ones because of the built-in power supply. However, they can be pervasive too: "*As a self-powered application example, a system had been built around the piezoelectric shoes that periodically broadcasts a digital RFID as the bearer walks."* [2] The danger of these devices lies in the traceability of the carrier. Without special equipment it is impossible to notice when such a chip is being read. This especially dangerous because RFID readers can also be very small devices. Some short distance readers can even be built into cellphones.

One can protect himself in two ways: Destroying the RFID chip or blocking it's signal. While the first possibility is bad because the device cannot be used ever again the second one is a good option. The blocking is done by a Faraday cage. The easiest way to achieve this is to wrap the chip in aluminum foil.

7. Web sites with registration / Google / Google-Earth

Google products and other websites are possibly the biggest "privacy hole" which can be exploited by anyone. As people browse the internet they leave data behind. Not just technical information like connection logs, but also forum posts, entries in mailing lists. This is especially bad because the internet does not forget. One can still find messages from mailing lists witch are more than 10 years old. The only tool which is needed is a search engine.

An other privacy issue are websites witch require registration. Many users just enter their names and personal information and send them – of course without encryption – to web servers. This is the point where other risks come in. This is not just a privacy problem. It is the risk of identity theft as many web sites still use clear text protocols to transport login data. Many people use only one or two different passwords for web sites. If someone manages to get the user name and password on server A there is a high risk that the same login data is also valid on server B, assuming that server B is also used by the same person whom the login data belongs to.

Google-Earth is a moderate, but growing risk. As the available resolution becomes higher and higher, many details become visible. In our opinion it invades one's privacy that everyone, regardless of his location can look for swimming pools in our back yards or determine how many doors our garage has.

8. Telephone

The technology to send voice over a cable is a quit old one. The first steps were made in 1837. From this former times up to now the most telephone port word wide are analog telephone ports. This means that the voice signal is only transformed in an electric signal without any encryption. To intercept a call between two people you only need a normal speaker that you connect to the cables and you can hear anything what they are speaking. Another problem here is that the distance between a phone customer and the telephone provider can be up to 8 kilometers. During the whole distance an attacker can connect to your cable if he wants.

Nowadays more and more phone users change their devices to digital ones. But in older codecs also the digital signal can be intercepted because there is no encryption. When we speak of digital telephones we often mean VOIP. To send voice calls over IP is a logical conclusion because today the IP ISO/OSI model is the most used transport. To give the most used standard a name we should have a look on H323. Because H323 is the oldest standard it is also the one with the weakest security.[8] The voice data are sent in an RTP (real time protocol) stream which you can intercept with an open source media player like VLC. The new protocols like SIP are able to encrypt their data, to make prevent the data form spying.

The most popular phones today are the mobile phones. It's the like the wired phones, in older editions there was no security/encryption included. But with mobile there comes another reason. When you have switched on your phone our position can be tracked by using triangulation.

4 Risk Analysis

The following table tries to summarize the risks which affect an average person every day. The amount of usage of each technology greatly affects the real risk it causes.

technology	Usage (low, medium, high)	Risk (low, medium, high)
Ip-TV	Low (for now)	low
E-Mail	high	high
Wireless LAN	high	high
Bluetooth	high	medium
Cameras / biometric identification	medium	medium
GPS	Medium	low
RFID	Medium	medium
Websites	High	high

telephones	high	medium

It follows that E-Mail, wireless LAN and web sites are the most used technologies from this list. All these technologies are based on networks (internet). As conclusion it can be said that the biggest risk of all is global networking.

5 Personal Opinion

We are concerned about the described privacy issues. In wrong hands these technologies could be fatal. Imagine what it would have been like if the KGB had such methods of mass surveillance. We advise everyone to use only encrypted protocols and not to leave any evidence regardless of what you do. It can be used against you. Big brother is watching you – This slogan is not made up. It is reality.

References

1. S. L. Garfinkel, A. Juels, R. Pappu: RFID Privacy: An Overview of Problems and Proposed Solutions, http://doi.ieeecomputersociety.org/10.1109/MSP.2005.78, (2005)

2. J. Kymissis, C. Kendall, J. Paradiso, N. Gershenfeld: Parasitic Power Harvesting in Shoes, http://doi.ieeecomputersociety.org/10.1109/ISWC.1998.729539, (1998)

3. B. Potter: Wireless Security's Future, http://doi.ieeecomputersociety.org/10.1109/MSECP.2003.1219074, (2003)

4. Anil K. Jain, Arun Ross, Sharath Pankanti: Biometrics: A Tool for Information Security http://www.gpa.etsmtl.ca/cours/sys863/References/C2/Jain_TIFS06.pdf, (2006)

5. Yasushi Tomii, Steffen Scheer: Gesichtserkennung http://www2.informatik.hu-berlin.de/Forschung_Lehre/algorithmenII/Lehre/SS2004/Biometrie/05Gesicht/gesichtserkennung.pdf , (2004)

6. Jean-Francois Fleury: IPTV – The need for standards http://www.isma.tv/technology/white-papers/Paper-IBC-FleuryJF_finalPROTECTED.pdf, (2005)

7. Thomas Silverston, Olivier Fourmaux: Measuring P2P IPTV Systems https://www-rp.lip6.fr/site_npa/site_rp/_publications/796-silverston-nossdav07.pdf, (2007)

8. D. Richard Kuhn, Thomas J. Walsh, Steffen Fries http://www.commserv.ucsb.edu/reference/background/VOIP_security_considerations.pdf, (2005)

9. Jörg Schwenk: Sicherheit und Kryptographie im Internet http://books.google.at/books?hl=de&lr=&id=PIRlRegShvYC&oi=fnd&pg=PA1&dq=email+sicherheit&ots=0DF2RzKgFg&sig=EyiydZsdnisISBdAKqaaBSIMVoA#PPP1,M1, Vieweg+Teubner Verlag, (2005)