INTERNATIONAL JOURNAL OF SYSTEMS APPLICATIONS, ENGINEERING & DEVELOPMENT
Issue 5, Volume 5, 2011

Is Big Brother watching you?

Tuomo Tuohimaa, Ilkka Tikanmäki, Jyri Rajamäki, Jouni Viitanen, Pasi Patama, Juha Knuuttila and Harri Ruoslahti

Abstract - People are increasingly worried about the developments in information technology, especially what concerns about their privacy. Nowadays, it can be proved that personal information is very difficult to protect - especially in the Internet. Scientific studies show that the key risk of security is people. There are people who develop computer systems, and those who use information technology. Privacy and security protection can be seen as a basic human right. Confidence to the Law Enforcement Agencies (LEAs) has always been high in Finland. Despite of this, there are people in society, who do not trust at all to LEAs - especially what comes for different kind of surveillance by the police.

Development and the speed of different kind of information are really fast, and one of the main problems is the law retardation. How many people are even thinking about what kind of a walking data bank they are with, for example mobile phones, bonus- and credit-cards? In fact in this society, there is always someone who knows who you are, how you live, who your friends are, wherever you are, what you do, what you buy, what are your hobbies and what kind of lifestyle you have. But the main concern in this matter is not how anyone other than the authority gets such information - but what LEA is doing with information they get.

However, people are willing to give more rights to authorities if, usage of these intrusive means, are more transparent and better informed to the public. Today there are technological possibilities to create more transparent and credible monitoring for surveillance activities and in this paper is given an example of that.

Keywords— Law enforcement, Legal audit, Oversight, Privacy, Public safety, Surveillance, Trust

Manuscript received April 23, 2011. This work was supported in part by Tekes – the Finnish Funding Agency for Technology and Innovation – as a part of the research project 940/08 SATERISK.

T. Tuohimaa and I. Tikanmäki are post-graduate students at Information Systems, Laurea University of Applied Sciences, Vanha Maantie 9, FI-02650 Espoo, Finland (phone: +358-9-8868 7400; e-mail: tuomo.tuohimaa@laurea.fi, ilkka.s.tikanmaki@laurea.fi).

I. Tikanmäki is with Laurea University of Applied Sciences, Vanha Maantie 9, FI-02650 Espoo, Finland (phone: +358-9-8868 7400; e-mail:

J. Rajamäki is Principal Lecturer and Scientific Supervisor of research projects at SIDlab Networks, Laurea University of Applied Sciences, Vanha Maantie 9, FI-02650 Espoo, Finland (phone: +358-9-8868 7400; e-mail: jyri.rajamaki@laurea.fi).

J. Viitanen and H. Ruoslahti are Lecturers of Security Management at Laurea University of Applied Sciences, Vanha Maantie 9, FI-02650 Espoo, Finland (phone: +358-9-8868 7400; e-mail: jouni.viitanen@laurea.fi, harri.ruoslahti@laurea.fi).

J. Knuuttila is Principal Lecturer of Security Management at Laurea University of Applied Sciences, Vanha Maantie 9, FI-02650 Espoo, Finland (phone: +358-9-8868 7400; e-mail: juha.knuuttila@laurea.fi).

P. Patama is with Laurea Trevoc Ltd. Teknobulevardi 3, FI-01530 Vantaa, Finland (phone: +358-50-030 3800; e-mail: pasi.patama@trevoc.com).

I. Introduction

THIS paper tries to look forward, how is possible to create law enforcement surveillance operation that can be approved by the citizens. This subject is a spinoff of the SATERISK project, which is e.g. looking to risks in GNSS-tracking [1].

A Finnish Ex- Minister and Member of Parliament wrote in his blog [2]:"I have always been somewhat suspicious about the drug police's demands to get more powerful eavesdropping systems. There is no use for these systems. If police has the right to listen in telephone conversations, no one will tell secrets on the telephone, and so on. And there will always be someone who will misuse those rights."

'Mike' McConnell, a former director of United States National Intelligence, has said [3]: "…we all want security, but won't give up our privacy … so we have to rethink intelligence, reshape it, and were not there yet … any bureaucracy can do evil … there must be oversight…"

The European Union anti-terrorism legislation required telecommunications operators to retain phone data and Internet logs for a minimum of six months in the case they are needed for criminal investigations [4].

German Law had then ordered that all data – except content – from phone calls and e-mail exchanges be retained for six months for possible use by LEAs who could probe who contacted whom, from where and for how long.

The Federal Constitutional Court of Germany ruled that this law violated Germans' constitutional right to private correspondence and failed to balance privacy rights against the need to provide security. It did not, however, rule out data retention in principle. "The disputed instructions neither provided a sufficient level of data security, nor sufficiently limited the possible uses of the data," the court said, adding that "such retention represents an especially grave intrusion." The court said, that because citizens did not notice the data was being retained it caused "a vague and threatening sense of being watched" [5].

In abovementioned cases, the bottom line is the trust. Terrorist attacks and other serious crimes are happening around the globe, Germany is not an exception. Despite of it, circa 35,000 Germans have appealed to overturn the law. People seem to be willing to take a chance with terrorists and criminals because they fear that a LEA is abusing its powers and intruding their privacy. These cases are not even as intrusive as technical tracking or eavesdropping. If police is utilizing the specific phone call or e-mail exchange data, the operator's system and log files will have marks that the copy of the data has been delivered to the LEA.

In cases when a LEA is using its own room audio recording or technical tracking systems, the trust building between citizens and LEAs is even more difficult. In cases of call detail records data utilizing, there will always be a log file mark in the operator's system and that leaves a trace. However, LEAs are still using some stand-alone systems, where no log marks are created.

In Finland, the oversight of police's coercive usages is based on a file system SALPA that the National Bureau of Investigation runs [6]. The SALPA system guides, how to make applications and notifications in the correct manner. But, could this system alone be a sufficient legality control system, if the information that police officers write down are not based on actual log files? These non-transparent systems might be handicaps to LEAs. The LEA may act so that everything is done according to the law. However, they cannot prove it because methods cannot be audited by an outsider. The LEA can only claim that they are doing the right thing. These claims are challenged periodically but always afterwards when the Ministry of Interior is conducting legality inspection to see how operations are conducted and documented. This is not a very efficient and transparent way of operating. With the lack of trust, there is a lack of new legislation that allows usages of new crime fighting tools. With this situation, everyone is losing something; security. We believe that there is a way to find balance between security and individual freedom and to find common ground between good will approach and taking advantage of advanced technology, resulting in a powerful law enforcement tool open to third-party review.

Finnish futurologist Mannermaa says that the society is presented as "soft surveillance, knowledge and non-forgetting history data". The important difference between 'Some Brother Society' and Orwell's 'Big Brother' is that in a 'Some Brother Society' surveillance is commonly agreed upon and transparency. An important point is that when information society's first stage deepens to 'ubiquitous network society', single-sided enforcement and surveillance is straining people. Within ubiquitous network society, it is possible to create multi directional surveillance and develop transparent authority power [7].

The remainder of this paper is organized as follows: Section II introduces theoretical framework. Section III describes what is wrong with surveillance society. Section IV introduces the ways in which we can be watched. Section V presents weak signals, for example a poll results from students at the Laurea University of Applied Sciences. Section VI reviews technical solution. Section VII describes conducting operations with the proof of concept system. Section VIII presents informatics crime. Section IX reviews framework for security; while section X presents strategy suggestions for security. Section XI provides conclusion of this paper.

II. Theoretical Framework

A. Resign Science Research

Task of design science is to produce knowledge to improve the activities of design and construction. The mission of design science is show, how to construct and evaluate innovations and artifacts. Design Research consists of activities concerned with the construction and evaluation of technological artifacts to meet organizational needs [8]. The principle of design-science research is the knowledge and understanding of a design problem and its solution are acquired in the building and application of an artifact [9].

The core mission, of a design science, is to develop knowledge that can be used by professionals in the field in question to design solutions to their field problems. Understanding causes of problems can be very helpful when professionals are designing solutions. It develops knowledge on the advantages and disadvantages of alternative solutions [10] and develops knowledge for the design to solve improvement problems [11].

Everlasting interesting research topic in the Information Systems (I)S field is how to effectively develop new systems. This is interesting because Information Technology (IT) is developing and technical knowledge is growing. In this process, new kinds of systems and development methods are created [12].

B. Big Brother Society

Professor Jaakko Talvitie wrote in his blog 11.3.2011 [13] that information about us is continuously gathered. Whenever we do something in the Internet, there will be a mark somewhere. Furthermore, we concede our information, either consciously (social media) or the extent unconsciously (bonus card purchases). Information will end up somewhere, but we really do not know where. We do not know who is in responsible for information, how to secure that information or who have access to all of that. All this creates a vague unease, but we are accustomed to state of affairs, no major disasters have occurred. We sleep soundly in our beds. There are, however, contradictory features. For example, I have noticed that the same people who, frankly, touted by the world about very personal information and insights, are allergic to the idea that some party monitors and records up their doings, shopping and mobility. [13]

Also, other examples of discrepancies can be found. Toll road debate has revealed major concern such as GPS-based systems, the ability to track people's location. Some people argue that in a free country the authority does not need to know where people are. Overall thinking, this is a good principle, but we remind that in Finland, almost every one carries a mobile phone. If not the authority, at least the mobile phone operator knows best every moment, where you are. [13]

Similarly, we are concerned about visions about digitalization of our health reports and moving that information to the Internet. We are wondering the relevant risks, and we are sceptical. At the same time, we pay our bills in the Internet applying e-bank systems by using money, which does not exist anywhere else than in bits online. [13]

After a little more of thinking about that resistance and scepticism, it seems to be so, that the negative force is surprisingly often the authority. Big Brother supervises in this case, that the other Big Brother cannot supervise. This is respectable, but Big Brother is a brake on development. Things are swirled, prepared and buried forever in endless rounds of working groups and consultation, instead of developing the legislation and practices that support the digitalization and make it a safe and clear from individual's legal point of view. At the same time a digital service offering - currently at the forefront of social media - develops faster and it is searching for new forms. [13]

For example, where stays the criminalization of identity theft? Where is the data protection law, which would contribute the safe and orderly digitalization instead of its prevention? At this rate, no-man's-land grows between the law and the reality. We are afraid that even in this case applies the old rule to public services: traffic lights will not come to a dangerous known road on way to school until the first child gets hit by a car. [13]

C. *Some Brother Society*

This article is going to explore already available technical possibilities to build surveillance operations according to the 'some brother' vision presented [7]. Scenario time lines are usually 10-20 years and since Mannermaa has stated his vision already two years ago and it is obvious that new reformation is going to take time. If we want to see results in the original 10 year timetable, we should see signs of implementation acceptance already now. Though commercial markets are not yet visible, we should see signs of acceptance in society and technology should provide possibilities to support this ubiquitous realization already.

In this study we looked at the citizens' willingness to give more power to authorities if the usage of these intrusive means is more transparent and better monitored. This is conducted by questionnaire. Concerning design research, we look at possibilities to create transparent and plausible monitoring of surveillance activities on both levels of technology and processes used by authorities in this field.

How would it be possible to credibly show people, that power is used according the rights and in ways benefiting people? In this part we describe theory what systems evolving in this direction would be like and look at what is possible to achieve and what kind of difficulties there might be. As part of this surveillance authoring process, we could also see methods of open acceptance processes in technology which are used to conduct these intrusive operations.

By opening this process of technological development to publicly accepted review processes we could reach levels of assurance in a wider scope. In LEAs' surveillance, security is important and security through obscurity is not enough.

Security risk identification is a systematic attempt to define well-known risks, or to predict new risks, which lead to threats and vulnerabilities. It also includes the identification of each risk impact and sensitivity studies. System is surrounded by risks and those risks should be identified and analyzed by management or risk management of the organization [14].

III. What is Wrong with Surveillance Society?

In big cities, we already live in a ubiquitous surveillance society. In all developed countries, the cities suffused with surveillance encounters, not merely from dawn to dusk but 24/7. Massive social and technological advances have occurred in the last few decades and will continue in the years to come. Some think surveillance is as a malign plot hatched by evil powers and others think that it is the only way cut crime. Surveillance is always two-sided. Within both these sides, benefits and downside must be acknowledged. One guard looking a street view and people with two cameras is normally not apple to get much information. But a network with cellular phone triangulation, on line search queries, loyalty cards etcetera, you really can get in persons private life.

IV. The Ways in Which We Can Be Watched

There are safeguards against the abuse of surveillance by LEAs. The LEAs' use of surveillance is one of the most regulated operation of any group in society. But still many people are particularly concerned about the unseen, and what as they think is uncontrolled or excessive surveillance. Here as an example a list from a BBC story how we can be watched [15]:

- 4.2m CCTV cameras
- 300 CCTV appearances a day
- Reg plate recognition cameras
- Shop RFID tags
- Mobile phone triangulation
- Store loyalty cards
- Credit card transactions
- London Oyster cards
- Satellites
- Electoral roll
- NHS patient records
- Personal video recorders
- Phone-tapping
- Hidden cameras/bugs
- Worker call monitoring
- Worker clocking-in
- Mobile phone cameras
- Internet cookies

With regard to keystroke recorder programmes, only LEAs can legally obtain information from these sources. Unfortunately, large-scale technological infrastructures are prone to large-scale problems, and we can read about data leakage almost daily from the newspapers. Fortunately, it is really difficult for a cracker to get all the information about one person.

There are allegations about LEAs abusing surveillance. Most LEA officers are answering, that they are not abusing surveillance. Unfortunately, they cannot prove the case otherwise, because the case and material are confidential and publicly not available to use as argument. LEAs are claiming that any of the police surveillance that is unseen is in fact controlled and has to be proportionate otherwise it would never get authorized. To faultlessly control something like this means that you must have faultless control of the surveillance equipment all the time. How is this possible and how you can prove it to the public?

Unfortunately, people do not realize that when they give their personal information, they can not control it any more. People have lost their data ownership, when they released their personal information. They no longer have the privacy of personal information. When more personal information has been released then less privacy they have. Data protection and privacy practices become more increasingly important role. The main point here is that people have less control over what kind of information about them is and have been collected, used, stored and released by various agencies; both private and public sectors [16].

In Web-based environment, personal information is released by the data owner, and it is used in the organizations. Organizations collect store and process information to meet their own needs. Information privacy can protect against different kind of misuse of data.

Information will play an important role in privacy domain when they are collected, manipulated, stored, and disclosed according their needs [16].

We are living in a fast-growing information technology age. The Information and Communication Technology (ICT) is involving in our daily life every day, and it is expected that it will be much more deeply blended with our life. The Internet makes us living in a global village. Everyone could meet anyone who is online at anywhere, and at any time [17].

Currently, information such as credit card numbers, passwords, e-mail account fingerprints, digital photos, cell phone number and although the CV document should be private. The concept of privacy has become more complex and has been expanded. However, as the ICT continues further development, threats to privacy personal data and other information keep growing too. Widespread use of ICT in itself threatens personal information safety. For example, Radio Frequency Identification (RFID), a database of information mining, and wireless network at home cause a significant risk that sensitive information can be leaked to others or to the public. We can say the more advanced ICT becomes, the more there is a risk for the security of your personal information [17].

People can talk about using webcams, headsets and chat, and you can send instant messages and e-mails each other. Personal information can be spread quickly around the world through these Web technologies. It is very easy to copy information from the Web and send it back to another website again, and so information can be sent directly all over the world. Therefore, it can be very difficult to control your personal information in this information age. New information methods and tools for personal information are more vulnerable to privacy violation. Privacy is no longer a local problem: it has now a global focus. Therefore, all the privacy and security issues should be extended become an international project that will benefit from such diversification. Theories of privacy should develop worldwide to the general solution, especially the philosophy of IS security. Central to this focus should be on people. There are people who have different views on privacy, fundamental values of society, influence of different cultures, which develops information and that dominates the way in which IT is used.

Another feature of the personal information in the information age is that it is keeping expanding and variety; and difficult to handle. It is so easy to copy data from the Web and pass it again to another site. At the same time, new ICT achievements make people have more personal facts and ICT tools violating someone's privacy [17].

V. Weak Signals

So with regard to this study, we went to look for weak signals, which we have already three:

1. The Member of Parliament writing, that in any case LEAs' are prone to abuse these systems.
2. The judgement of the German constitutional court.
3. The professor Jaakko Talvitie`s writing in his blog 11.3.2011.

Then, there are a growing number of con intelligence organizations like Privacy International, Surveillance- Studies Network and Civil Liberties Union. Does this mean that people are plainly just against surveillance? On the other hand, are common people willing to exchange privacy to security and are they more willing to do so if the systems are more transparent. To find out this, we made a poll of 80 people answered reported in [18]. There we can see the need for transparency because without it there might not be new legislation that meets LEAs' needs. The poll was focused to students at the Laurea University of Applied Sciences. There were two basic groups, business management students and security management students. Tough the number of answers was only 80, it was enough for the purpose of finding out if weak signals existed, not yet in this phase to get to the bottom of it.

In Fig. 1, the red columns presents those who want to give more jurisdiction based rights to LEAs in current circumstances; there only 17.3% fully agreed. The green columns presents those who are willing to give more jurisdiction based rights when given assurance that LEAs are not abusing their powers; there 27.5% fully agreed. This was our first small (n=80) poll just to find, if the phenomenon existed. We did find that there is a remarkable shift. From these columns, a shift can be seen to pro more powers to LEAs, if people can be sure that LEAs are not abusing them. The fact which makes it even more noteworthy is that in the 2007 Police barometer (n=989), 48% of Finns fully trusted the police and 46% trusted for most part [19]. So, only 6% had no trust in police. In Finland, police is by far the biggest law enforcement agency. So, even when there is wide and good trust base, there is still a need for more transparency. What we

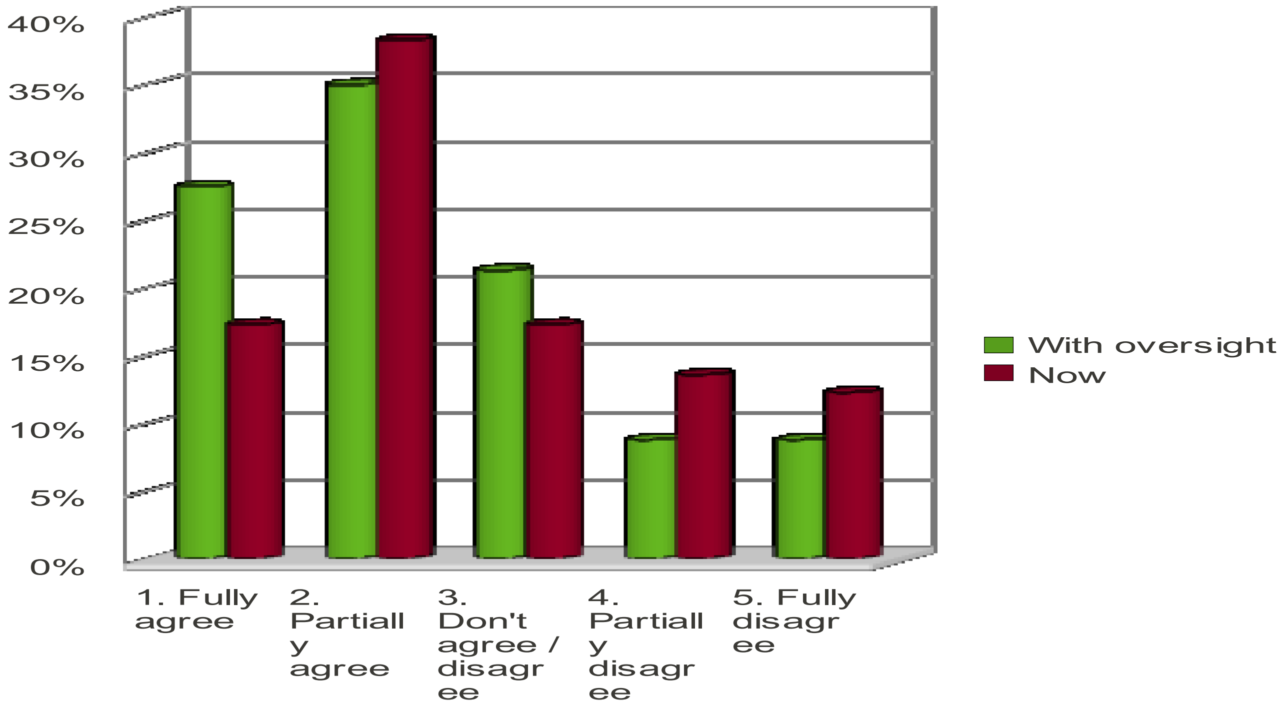

Fig. 1. Poll on willingness of conceding more powers for LEA

can see from our poll is that citizens are more willing to give more jurisdiction based rights, if they have more trust to the system. This is the fact why we think that a growing number might say yes to more jurisdiction based rights to LEA, if they are more certain that LEA is not abusing its powers. The trend is there, so in that sense of Mannermaa's vision of the future development might be possible.

VI. Technical Solution

For this paper, we have made a Proof of Concept (PoC) system which is described in Fig. 2.

- The 'surveillance data' is consumed by the police (blue line in Fig.2).
- Surveillance data is also delivered simultaneously to the oversight officer (blue line). When the oversight officer (or party) wants to audit conducted operations, he calls the police officer to visit him and bring accessing key for data (green line + key),
- REQ(uest) and Court order (black line between the police and court).
- When Court issues mathematical token (red line + key), surveillance equipment accepts court issued token and sets parameters to operation as ordered (from court order) (red line + key).
- From surveillance target, equipment collects data (blue area) - "substance".
- So, all data is stored by the police and the oversight officer, but permitting to audit data contents can only happen with operation decryption key from the police and no leakage is possible without police presented decryption key.

Nowadays, it is possible to use publicly accepted and reviewed authentication and cryptography functions to authorize and control deeply privacy invading equipments and data they produce. And to gain publicly accepted operation schemes in these surveillance operations. However, this requires commonly agreed ground, where device manufacturers and surveillance power projectors (police, intelligence) are authorized to obtain technology to fulfil this principle.

The technology and procedure to be used in the given scenario consist from several parts. Notably, the biggest difference compared to current situation is that the proof of concept system is centralized and parts are only working together and no ad-hoc usage is possible. The process parts are the Court (instance of permissions), the Police (instance of cases and operations), the Legal audit (monitoring, auditing and inspections of coercive means) and the Target (surveillance operation target).

For this paper, we implemented a proof of concept system which brings transparency and trust to shady surveillance operations without disclosing any confidential parts of operations to any unauthorized party.

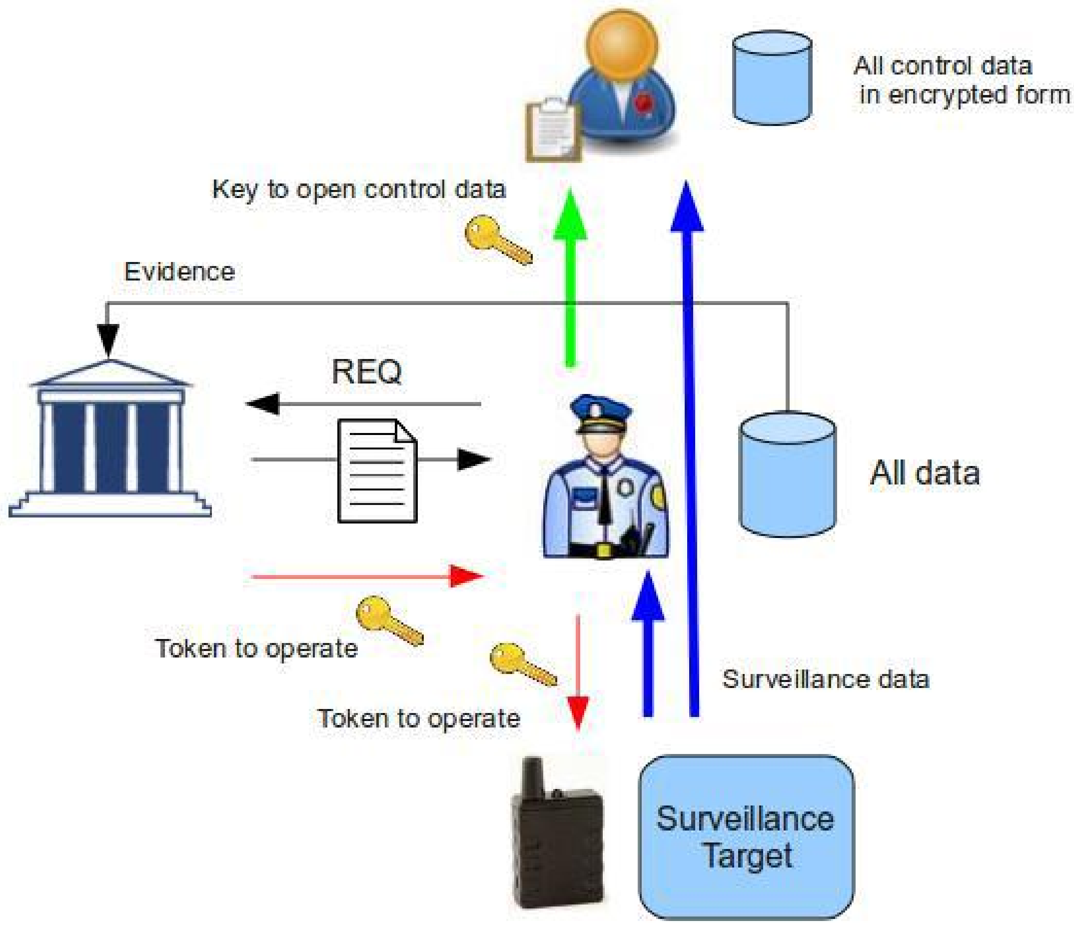

Fig. 2. System for transparent surveillance.

For this approach, we identified most intrusive parts used in these operations and data they produce. These are surveillance equipment and data which they produce. As long as these pieces of equipment are capable to operate without authenticated permission token, there is no means to control their usage. No process or instance is able to present publicly accepted proof of correct use of these pieces of equipment as long as there are no publicly proven technical control methods involved in the chain. The same applies to the data they produce. There are some recognized evidence authentication needs and schemes in both legalization and technology, but it is not capable to fully expose when, where and by whom data is produced and is surveillance data obtained under permission granted.

When coercive means are used, acting authority should be challenged with these questions:

- Is equipment capable to operate without technical authentication token?
- If equipment is used, who gains awareness of operation?
- Is there a possibility to 'try' to do operation with surveillance equipment and if it succeeds, do the permission paperwork later? If there is produced data, can we identify amount of produced data?
- If equipment is run over period of time, could we assure that control of technology has been under acting party control all that time?

VII. Conducting Operations with the Proof of Concept System

Opposite to traditional surveillance operations, where equipment is taken to the case, used and material is extracted - our implementation includes chain of trust between the process parties. Making it possible to create a transparent and yet secure surveillance operation base. Transparency is based on technology which supports operations legal processes firmly, making it possible only to obtain surveillance material with technology authenticated to operation. For oversight, all the data from the source is sent in encrypted form to a trusted third party (ombudsman etc.), a trustee of the public. This trusted third party can not see the actual data until the representative of the LEA is present with the decryption key. This is the way how secrets stay as a secret, and "black" operations are impossible.

VIII. Informatics Crime

The technological achievement and the rapid accession of informatics networks have lead to better communication systems, developing contacts around the world and the computers have become instruments for carrying out various activities on daily life.

The development of the Internet facilitated by computers and different techniques has changed the communication and informational exchange modality. Legislation and international cooperation in this field did not keep up with the technological changes.

Informatics crime is nowadays frequently reflected in mass-media. Stronger fear has emerged regarding informatics attacks and other ordinary frauds. Informatics crimes become more and more difficult to solve and Informational crimes are familiar only to a small group of law enforcement agencies.

Growing access to data bases offers the possibility to use them abusively or for illicit purposes, attacking via computers or producing remarkable damages to informatics systems and to data.

Advanced technique offers the possibilities easily exercise illicit activities outside the borders. Informatics crimes are an international problem.

Lack of spectacular results in the fight against informatics crime consists in a series of objective and subjective causes, out of which we mention:

- Advanced technology used in crime;
- Lack of education of the officers in the law enforcement agencies;
- Lack of a reaction plan in case of circumstances may determine the impossibility to identify the damages;
- Reluctance to report to the law enforcement agencies.

The informativeness of social life and usage by offenders of modern technologies have determined the gradual abandonment of traditionalist crime elements, the accent being placed on hiding the complex traces or consequences after perpetration of the deed.

Ongoing developments in the field of informatics have lead to growing risks and to the permanent change in the sociological profile of the informatics crimes [20].

IX. Framework and Suggestions for Security

Personal information should only be maintained by owner or control to ensure its privacy. In Web-based applications, this information should be disclosed in order to fulfill transaction.

There are three main issues that need to be taken into consideration [16]:

1. Personal information shouldn't be access by unauthorized users.
2. Only required personal information will be shown.
3. Personal information can't be passed by outsiders.

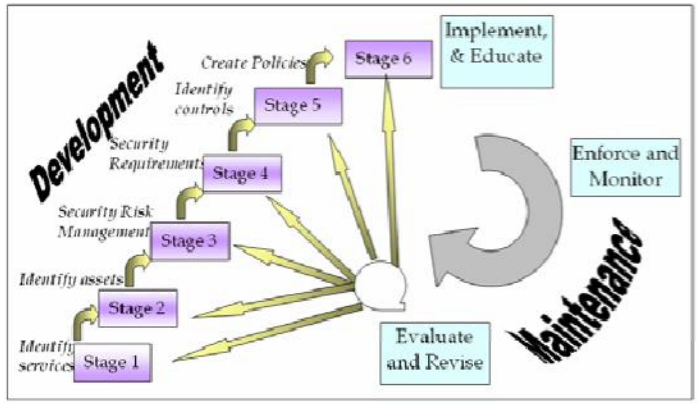

Fig. 3 The development and maintenance stages of the security framework [14].

The proposed framework for developing and maintaining system security allows well structured approach for security. Those stages are properly described and their implementation leads to effective implementation of the whole system security. This security framework allows organizations to understand existing security postures and surrounded risks [14].

One of the goals is to develop ICT to make life safer and help to create a healthier and more harmonious world. Our attention is not only to develop new technologies, but also to the needs of human beings and natural environment in which we live. It is interesting to consider more privacy issues if we have more security technology that can be used. Although we have an infinite number of high-tech, but where is the quality of our life? [17]

To implement a telecommunication secure system it is necessary to consider [21]:

1. Security Features seen as a meaningful system;
2. Security objectives concern in the system design;
3. Any threat to the system;
4. Methods and resources to implement/put the security system.

Security attacks can be either illegal outside nodes or legal inside. The latter nodes are called malicious nodes and attacks from them are harder to detect than from outside attackers [22].

X. Conclusions

The public economy will still be weak for some years. This means that many parties suggest saving money in law enforcement by using less manpower and more surveillance technology. In some points that leads for the need of new legislation for LEAs. We believe that people are willing to give new powers if they can be sure, that LEAs are not abusing their powers. What LEA officers need to understand is that there might not be new legislation and further no use of new technology, if the systems are not linear and transparent.

As a part of the surveillance authoring process, we could also see methods of open acceptance process in technology, which are used to conduct these intrusive operations. By opening this process of technology development to publicly accepted review process we could reach level of assurance in wider scope. In surveillance operations, security is important and security through obscurity is not enough.

Technically, it is possible to generate real oversight for some LEA systems that already are in use. In this case, the computer systems and surveillance equipment in law enforcement will only be a little more complicated and only marginally more expensive. The foundation for a trip towards the 'some brother society' is there already.

Despite the recent developments in computer vision and other areas, there are still significant technical challenges to be overcome before for example the dream of reliable automatic surveillance comes true. Technical challenges are compounded by practical considerations. Progress continues more rapidly, and demanding for automated surveillance continues growing in many areas from crime prevention, public safety and home security to different industrial control and military intelligence [23].

REFERENCES

[1] http://www.saterisk.fi
[2] O. Soinivaara, web block. Narcotic Police under suspicion in Finnish, 10.12.2007.
[3] T. Shorrock, Spies for hire, Tantor Media, 2008, p. 55.
[4] Directive 2006/24/EC of the European Parliament and of the Council of 15 March 2006 on the retention of data generated or processed in connection with the provision of publicly available electronic communications services or of public communications networks and amending Directive 2002/58/EC.
[5] German constitutional court, Germany Federal Constitutional Court overturns data retention law, 2 March 2008.
[6] Finnish National Institute for Legal policy, Telecommunications surveillance and legal protection in Finland, 2009.
[7] M. Mannermaa, Jokuveli – Elämä ja vaikuttaminen ubiikkiyhteiskunnassa (Some brother society), WSOYpro, 2008 [in Finnish]
[8] R. Pirinen, Research Framework of Integrative Action. Americas Conference on Information Systems. 2009, 6. San Francisco, California August 6th-9th 2009.
[9] A. R. Hevner , S. T. March, J. Park and S. Ram, "Design Science in Information Systems Research," *MIS Quarterly*, Vol. 1, No. 28, 2004, pp. 75 - 105.
[10] J. E. van Aken, Management Research as a Design Science: Articulating the Research Products of Mode 2 Knowledge Production in Management. *British Journal of Management*, 2005.
[11] J. E. van Aken, Management research based on the paradigm of design sciences: The quest for field-tested and grounded technological rules, *Journal of Management Studies*, Vol. 2, No. 41, 2004, pp. 219 - 246.
[12] M. L. Markus, A. Majchrzak and L. Gasser, "A design theory for systems that support emergent knowledge processes", *MIS Quarterly*, Vol. 3, No. 26, 2002, pp. 179-212.
[13] J. Talvitie, Isoveli valvoo? (Big Brother watches?) Web block 11.3.2011. http://www.activityblog.fi/2011/03/isoveli-valvoo/
[14] K. Saleh and A. Al-Khaili," A Framework for Engineering Trustworthy Computer Systems", in *Proc. 5th WSEAS Int. Conference on Information Security and Privacy*, Venice, Italy, November 20-22, 2006, pp. 81 - 86.
[15] BBC news story,"How we can be watched?", BBC London, 2006/11/02
[16] N. A. Ghani and Z. M. Sidek, "Controlling Your Personal Information Disclosure", in *Proc.7th WSEAS International Conference on Information Security and Privacy*, 2008, pp. 23 - 27.
[17] J-X. Feng and J. Hughes, "Analyzing Privacy and Security Issues in the Information Age", in Proc. 3rd WSEAS International Conference on Computer Engineering and Applications, 2009, pp. 220 - 223.
[18] Jouni Viitannen, Pasi Patama, Jyri Rajamaki, Juha Knuuttila, Harri Ruoslahti, Tuomo Tuohimaa & Ilkka Tikanmaki, "How to Create Oversight in Intelligence Surveillance" *in Proc. 9th WSEAS International Conference on Applied Electromagnetics, Wireless and Optical Communications (ELECTROSCIENCE '11)*, Meloneras, Gran Canaria, Canary Islands Spain, March 24-26, 2011. ISBN: 978-960-474-286-8. pp.52-56.
[19] Finnish ministry of interior, Police barometer 2008.
[20] C-S. Duse, D-M. Duse and M. I. Rusu, "Informatics Crime", in Proc. 8th WSEAS Int. Conf. on Electronics, Hardware, Wireless and Optical Communications, pp. 783-786.
[21] F. Hartescu and S-V. Nicolaescu, "Information and Network System Security", in Proc. 9th WSEAS Int. Conference on Data Networks, Communications, Computers, Trinidad and Tobago, November 5-7, 2007, pp. 441-446.
[22] Y-C Shim, "Secure Efficient Geocast Protocol for Sensor Networks with Malicious Nodes", in Proc. 8th WSEAS Int. Conf. on Electronics, Hardware, Wireless and Optical Communications, pp. 179-184.
[23] B. Anandampilai and K. Krishnamoorthy, "Automated Visual Surveillance in computer vision", in Proc.10th WSEAS International Conference on Acoustics & Music: Theory & Applications, pp. 36-44.