Information security risks for satellite tracking

Pasi Kämppi, Jyri Rajamäki, Robert Guinness

***Abstract*—**Satellite tracking is one of the most rapidly growing service business areas in the world, and there are already many commercial applications available. Benefits of the service for the customer are advertised, but very seldom there is any mention of information security of the system. Modern satellite tracking systems contain communication and data processing on many levels, so they are vulnerable to many risks of information security. This paper covers the main satellite tracking system information security vulnerabilities and gives guidelines on how to make systems and services more secure.

***Keywords*—**Information security, Internet, Mobile network, Satellite tracking

I. Introduction

Satellite tracking is one of the most rapidly growing business areas in the world [1]. Tracking devices have become quite cheap, and they are available to nearly everybody. Even smart phones can be used as tracking devices.

During the last decade, mobile network coverage has also grown, and internet has become a part of our everyday life. This evolution has enabled the innovation of new solutions, and one of them is the satellite tracking system.

Risks of satellite tracking have not been investigated widely, so a few students of Laurea University of Applied Sciences started to make preliminary research in 2008, which then gave rise to the SATERISK (SATEllite tracking RISKs) research project [2]; this paper is a part of this large research project.

Preliminary research revealed that information security in satellite tracking systems is not guaranteed, and this paper describes major vulnerabilities and gives some guidelines on how information security can be improved. Further research on the risks of satellite tracking is still needed; Chapter II presents the SATERISK research project; Chapter III describes the four segments (satellite, communications, data processing and end-user segment) of satellite tracking systems; the next four chapters, Chapters IV, V, VI and VII, discuss data security risks and solutions of these four segments, and these are followed by conclusions in Chapter VII and by references.

Manuscript received January 29, 2010. This work was supported in by Laurea University of Applied Sciences, by Tekes – the Finnish Funding Agency for Technology and Innovation and by some private and governmental organizations.

P. Kämppi is with Nokia Siemens Networks, Karaportti 3, Espoo, 02610 Espoo, Finland (phone: 358-50-5140823; e-mail: pasi.p.kamppi@ laurea.fi).

R. Guinness and J. Rajamäki are with the Laurea University of Applied Sciences, Vanha Maantie 9, Espoo, 02650 Finland.

II. SATERISK Project

SATERISK is a Finnish research project, which aims at a situation where devices and services, operations procedures, as well as laws and legislations on positioning and tracking, will allow the use of so-called m2m (machine to machine) tracking devices across state and union borders.

The project aims to bring new know-how on an international level to the European security field. The project will also create new methods and development paths for positioning and tracking systems. The widely-used US-based GPS (Global Positioning System) and Russian-based GLOSNASS (Global'naya Navigatsionnaya Sputnikowaya Sistema, Global Navigation Satellite System) satellite positioning systems will soon get an EU counterpart and rival from Galileo [3]. While most of the satellites are still on the ground, it is important that any problems and possibilities related to the new system are charted. The SATERISK project also aims to offer technological solutions to issues that arise while the project is ongoing.

SATERISK is a joint research project of universities, public organizations and private companies with regard to positioning, navigation and tracking systems on the whole tracking value chain, as shown in Fig. 1, founded by the participants and by Tekes – the Finnish Funding Agency for Technology and Innovation. The aim of the project is to evaluate the technical, operational and legislative needs and the associated risks for positioning and tracking, here and now, as well as in the future. Geographical examinations areas are (1) Finland, (2) EU / the Schengen Agreement Application Convention (SAAC) area and (4) Russia.

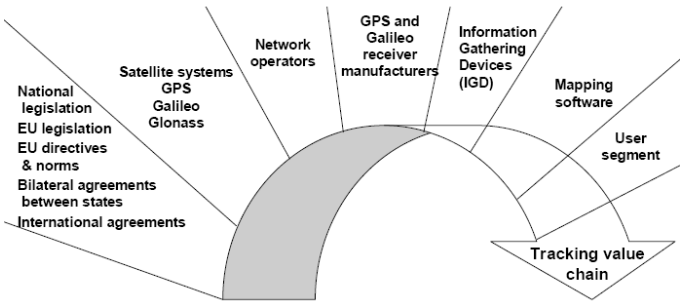

Fig. 1 Sectors of SATERISK project

Near-border and cross-border procedures for satellite tracking information, as well as the international co-

operability are studied in [4] and [5]. An example of a technical risk, jamming, is studied in [6]. This paper is one part of the research on the technical risks of satellite tracking systems, mainly studied by Laurea University of Applied Sciences.

III. Satellite Tracking Systems

Modern satellite tracking systems consist of four main technical segments: the satellite and tracking segment, communication segment, data processing segment, and end-user segment. The basic principle is that the tracked device is positioned by satellites, and the positioning data is delivered for post-processing via mobile networks and the internet. This principle is shown in Fig. 2. As an example, Fig. 3 describes the case of a remotely-tracked vehicle.

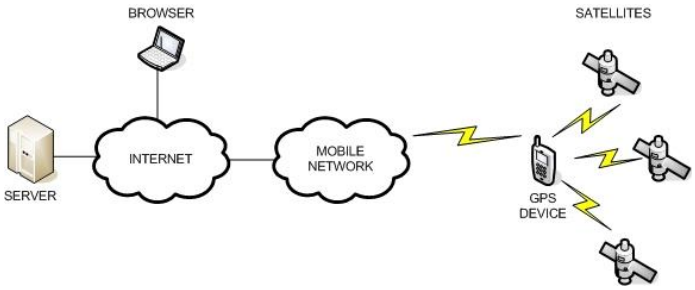

Fig. 2 Principle of a satellite tracking system [7]

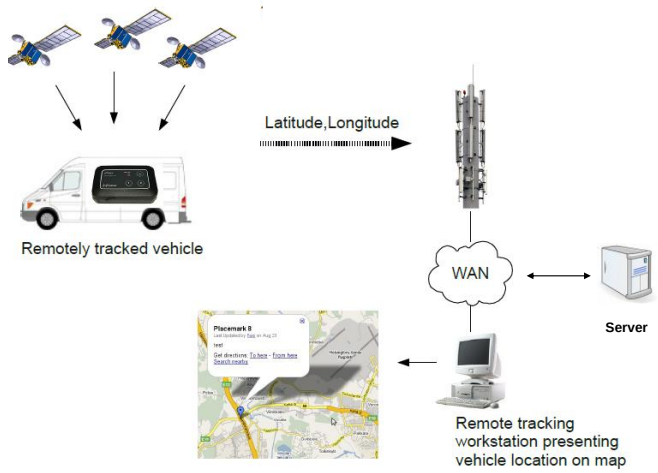

Fig. 3 Concept of remotely tracked vehicle

A. Satellite and tracking segment

The satellite and tracking segment contains satellites, radio path for satellite signals, signal receivers and techniques to calculate the device's position from satellite signals. With regard to this study, the following satellite systems are relevant.

1) GPS

The most commonly used satellite positioning system is the Global Positioning System (GPS). It has been developed by the U.S. military, but service is also available for civilian usage. The system consists of 26-28 active satellites, and it covers the whole world. Since the U.S. government stopped intentionally degrading the signal in 2000, the position data provided by GPS is quite accurate in Finland. [8]

2) GLONASS

GLONASS is developed and used by Russia. The system is like GPS, and in principle it should be able to offer as accurate as position service as GPS. In practice, the number of satellites operating in the GLONASS constellation has been quite low (8-12), so the service is not as accurate as GPS worldwide. The satellite constellation is optimized so that usability is best within Russian borders. [8]

3) GALILEO

GALILEO is under development by EGNOS (European Geostationary Navigation Overlay Service). EGNOS is a project that is sponsored by ESA (European Space Agency) and the European Commission. The goal of this project is to develop navigation services for civilian usage, independent of the military. GALILEO is technically like GPS and GLONASS, and some devices will be able to utilize all three systems. In this way, several techniques can be used simultaneously to guarantee better positioning accuracy and reliability. [8]

B. Communication segment

The communication segment contains techniques to deliver positioning data for post-processing and use by end-users. The most commonly used techniques are offered by mobile networks, namely the General Packet Radio System (GPRS) [9] and Short Message Service (SMS) [10]. The internet is used to route positioning data from mobile networks for post-processing, and this makes the system globally available. End-users can access their data via the internet as well.

C. Data processing segment

The data processing segment contains systems to process and store position data for end-users. These systems include servers and applications that make position data available. End-users can access their services via the internet, so systems have to be connected to the internet safely and reliably.

D. End-user segment

The end-user segment offers customer interfaces for their positioning data. Typically interfaces are offered via an internet connection and web browser.

IV. Satellite and Tracking Segment Security

Fig. 4 shows the satellite and tracking segment elements with the main technical challenges described in balloons. Commercial service providers and service users cannot contribute to the space constellation, data security of satellites

and the signals they are transmitting. Somehow, service providers and users could manage the radio path for satellite signals by operating procedures (e.g. avoid tunnels), by observations (e.g. checking possible jamming [6]) and by utilizing technical accessories (e.g. pseudolites [11], [12]). However, tracking devices are the main elements of satellite and tracking segment where service providers and user could contribute. Tracking devices might be dedicated devices or smart phones. The data security ability of dedicated tracking devices could vary significantly; some highly secure solutions are limited only to government agencies, e.g. [13]. On the other hand, data security of smart phones is highly dependent on the client software and the users' actions.

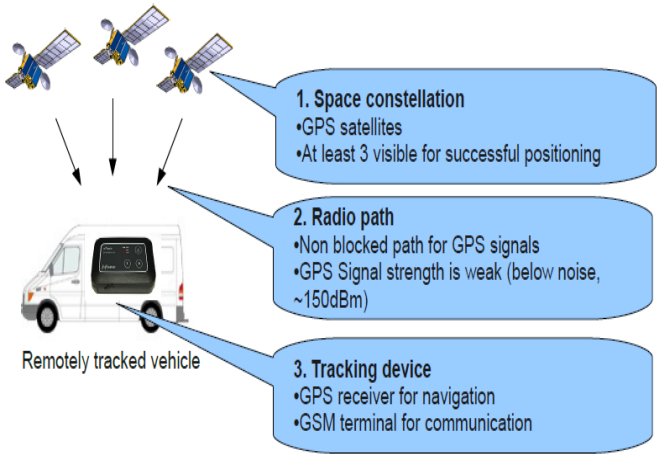

Fig. 4 Satellite and tracking segment elements

A. Client Security

Some commercial satellite tracking service providers have made matters easy by reusing smart phones as tracking devices. The user needs only to download a tracking application to turn his or her smart phone into a tracking device. Smart phones can be compared to computers in that they can have security vulnerabilities depending on the operating system used.

1) Symbian OS

Symbian is probably the most widely-used smart phone operating system in the world. Because it is like a computer operating system, it has many vulnerable interfaces [14]. Threats can occur via downloadable applications, GPRS, SMS, web browser, or email. In theory, it is possible that a mobile phone can be hijacked and managed remotely to direct positioning data to a place available to the attacker.

2) iPhone

The iPhone is a newcomer in the mobile world [15], however, there has already been a few severe security threats reported. It has been possible to capture iPhone data via SMS [16], and the first worms [17] have also been spread among iPhones.

3) Other operating systems

Recently new smart phone operating systems like Android [18] and Bada [19] have been released. Nobody knows yet how vulnerable they are going be.

B. Security solutions

Mobile devices can be protected by keeping the operating system up-to-date and by disabling interfaces that are not needed (e.g. Bluetooth). There are also a few commercial security applications available for extra protection.

V. Communication Segment Security

A. Overview of communication segment risks

The communication segment could be divided physically into mobile and fixed networks. Fig. 5 and Fig. 6 show the main technical challenges of these parts.

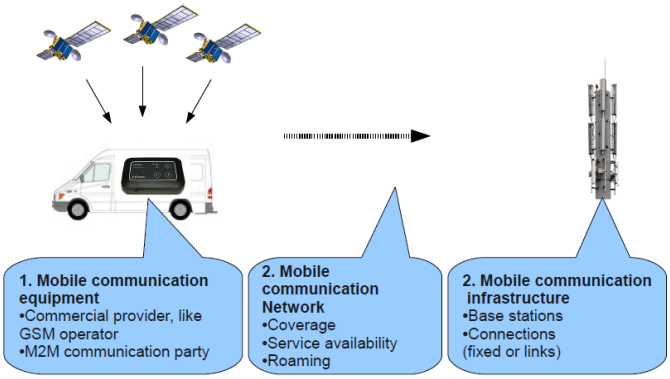

Fig. 5 Mobile communication elements

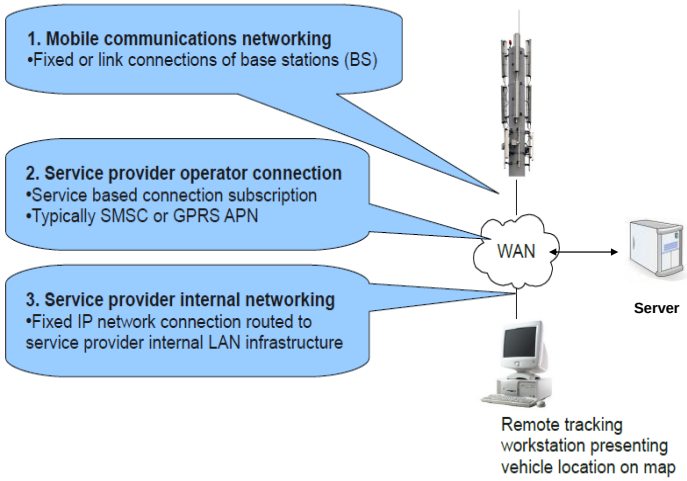

Fig. 6 Fixed network elements

B. History of mobile networks

Originally GSM (Global System for Mobile communications) [20] did not offer as advanced data services as they currently do. In the first phase, there was Circuit Switched Data (CSD), followed by High Speed Circuit Switched Data (HSCSD) [21] that offered four times faster

access rate compared to CSD. Common to these services is the use of communication channels based on a Time-Slot Leasing (TLS) sheme.

The General Packet Radio Service (GPRS) was the first packet-switched mobile network service that offered an internet-like end-user experience. In its first phase, GPRS was quite slow and network delay was large. GPRS was followed by Enhanced Data Rates for Global Evolution (EDGE) [22], and it offered faster user data rate and smaller Round Trip Time (RTT).

The Universal Mobile Telecommunications System (UMTS) [23] offers end-user data rates that make as real of a mobile internet experience as possible. Modern systems are upgraded with High Speed Downlink Packet Access (HSDPA) [24], and this type of mobile internet connection is comparable to a fixed connection in terms of data rate.

Common to all these development phases is a focus on developing faster networks, but mobile networks do not natively provide secure end-to-end user plane data transfer features.

C. GPRS

Originally GPRS was built on top of the GSM network infrastructure with a few additional network elements, and it reuses the majority of the existing network architecture. Later networks were upgraded with UMTS, and a few new network elements were introduced.

Fig 7 [9] presents the logical architecture of the modern GPRS network. Each of the boxes describes a single network element or the functional entity. The interfaces between network elements and functional entities are drawn with lines and each of the interfaces carries signaling and/or user plane data. In the user plane the most vulnerable interfaces are Gn-, Gp- and Gi-interfaces.

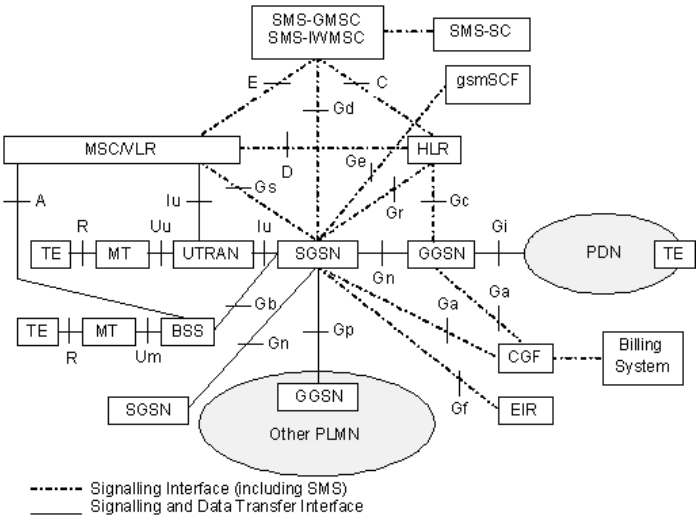

Fig. 7 GPRS Logical Architecture [9]

On the Base Sub System (BSS) and UMTS Terrestrial Radio Access Network (UTRAN), user plane data can be encrypted between Mobile Station (MS) and Service GPRS Support Node (SGSN). BSS supports the GPRS Encryption Algorithm (GEA) and UTRAN supports the UMTS Encryption Algorithm (UEA). Equipment is now available that can break ciphering from the air interface, so it is possible to capture data before it enters BSS or UTRAN.

When data continues towards a GPRS Gateway Support Node (GGSN), then data is encapsulated with GPRS Tunneling Protocol (GTP) [25] over IP. GTP does not support any encryption features. In practice, data is transferred as plain text, and it can be captured quite easily if the intruder has access to the backbone. GTP is used between operators as well, and it is quite vulnerable if traffic is routed via an insecure internet connection. From GGSN, data continues

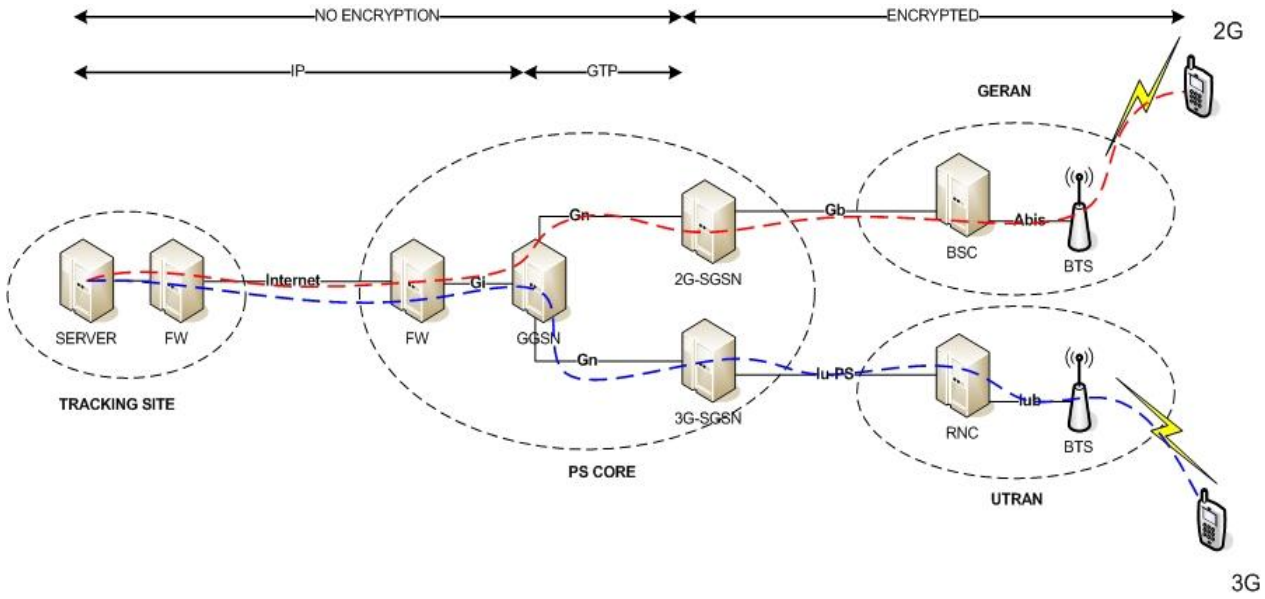

Fig. 8 Data flow in GPRS

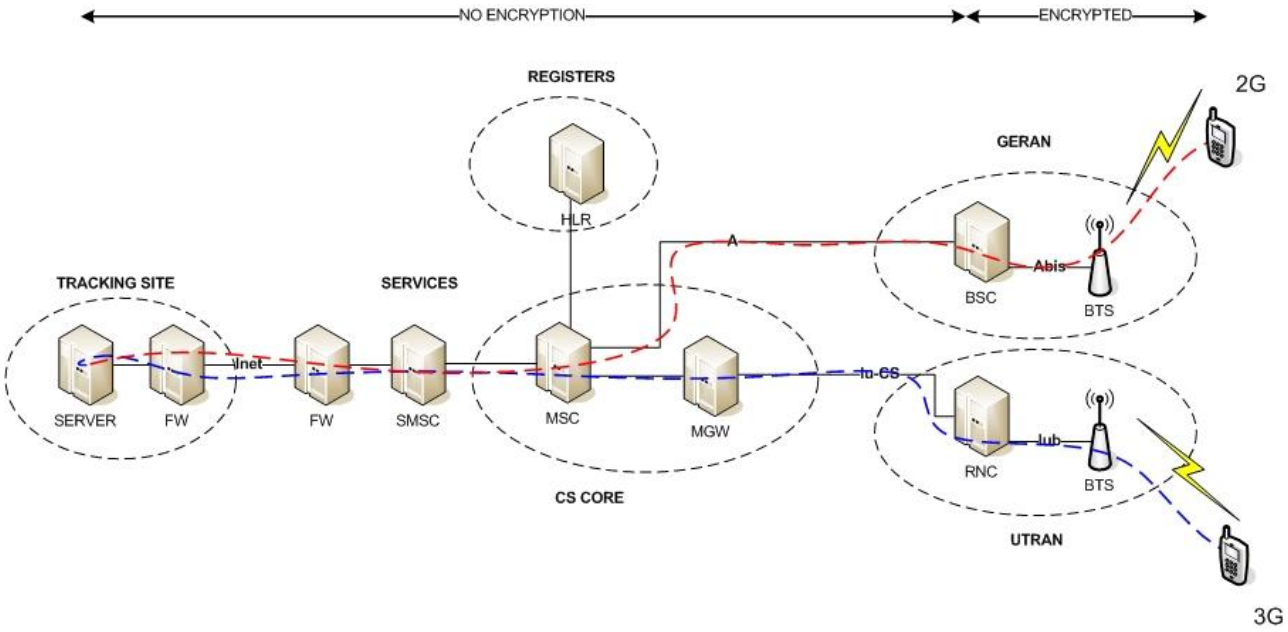

Fig. 9 Routing of SMS

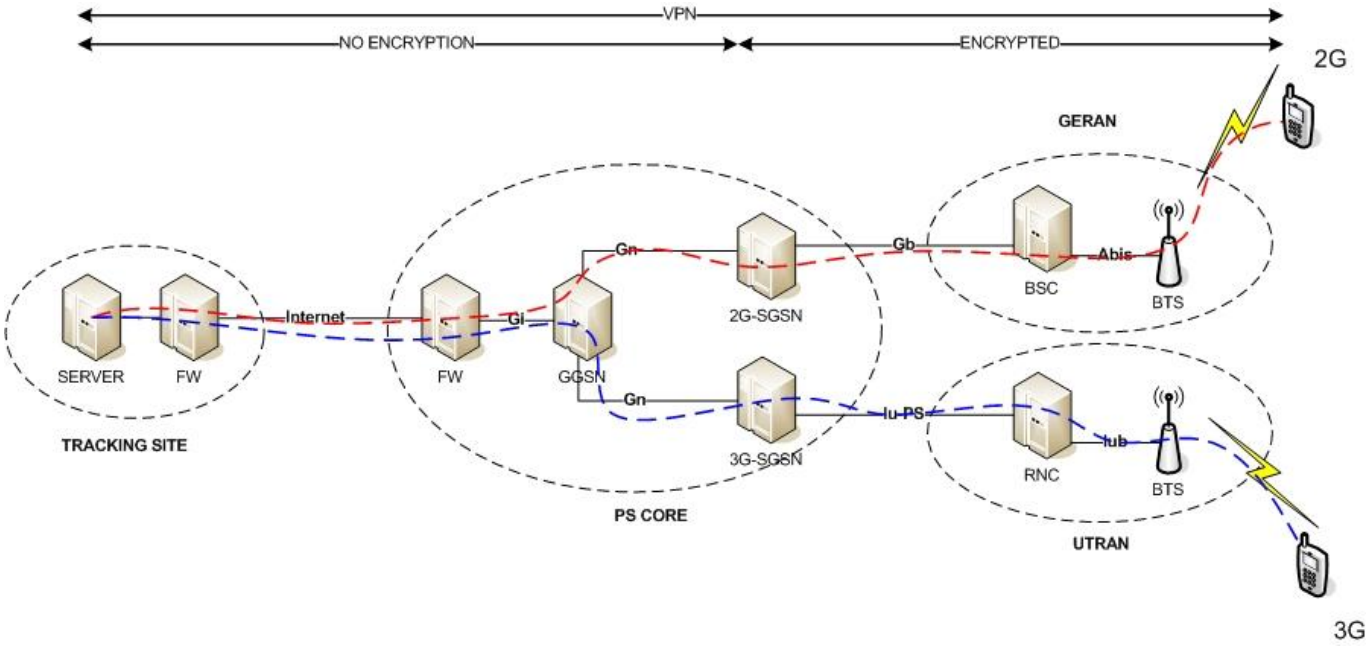

Fig. 10 GPRS security solution

towards the internet, and then data is available to anybody. Data flow is presented in Fig. 8.

D. Short Message Service

The Short Message Service (SMS) provides a method to send short messages via mobile networks [10]. Messages are delivered using signaling, and they are encrypted only in the air interface. After BSS and UTRAN they are transferred as plain text. From BSS and UTRAN the message continues towards the Mobile Switching Center (MSC) and Short Message Service Center (SMSC).

Networks of different operators are connected globally with Signaling System Seven (SS7) [26], so short messages are delivered between operators using SS7 as well. SS7 does not support any security functions, so it is possible to capture messages from the operator network if somebody is able to break in. Nowadays SS7 can be carried over IP, and this makes SS7 even more vulnerable if signaling between operators is routed via an insecure internet path. On the internet, signaling data is available to anybody.

In satellite tracking systems, positioning data is delivered for post-processing by a machine to machine (M2M) interface. Typically these interfaces (e.g. CIMD2) do not support any security functions, and data can be routed via an insecure internet path. Routing of SMS is presented in Fig. 9.

E. Security solutions

As discussed above, it is quite obvious that positioning data can not be carried safely via mobile networks. Globally there are many different operators with different information security practices, so the end-user can not rely on data being delivered safely. In the most blatant case, when data enters the internet, then it is available to anybody.

1) Data protection with GPRS

Data can be protected by establishing secure tunneling between the client and data processing center. By secure tunneling, we can make data transfer as secure as the chosen encryption method. The most common technique is IP Secure Architecture (IPsec). GPRS security solution is presented in Fig. 10.

2) Data protection with SMS

Due to the fact that SMS is delivered in mobile network signaling, it can not be secured by tunneling like GPRS data. SMS is plain text, so it can encrypted before sending by using Secure Hash Algorithms (SHA), such as SHA-256, SHA-384, or SHA-512. SMS security solution is presented in Fig. 11.

VI. Data Processing Segment Security

Position data is processed and stored in a place that can be compared to a small corporate data center from the security point of view. A data center is typically connected to the internet, so it is vulnerable for many threats like denial of service (DOS)-attacks, viruses, worms, pharming, cross scripting, and social engineering.

In some commercial satellite tracking solutions, the data center is hosted by the service provider, so the user can not be sure how positioning data is hosted. There are many open questions like: Where is the data center located, what kind of protection mechanisms are used, what is the professional level of the personnel, and is there any co-operation with government? Therefore, the user has to be aware of what service is chosen.

A. Security threats

1) Denial of service -attacks

The aim of denial of service attacks [27] is to make a website unavailable. A website can be overloaded by the attacker, and users will not be able to access their data.

2) Viruses

A computer virus is a small applet that needs a host program for spreading. Usually their purpose is to cause some harm to the infected system.

3) Worms

Worms are small applications that can spread independently in networks and execute code autonomously. Their goals are to cause disasters, open new security holes, and steal data.

4) Pharming

Pharming [28] is an attack in which a user is directed to a fake website instead of the real one. The user does not notice that they are at the fake website, so sensitive information like username and password can be stolen. Another term for this threat is “DNS cache poisoning”.

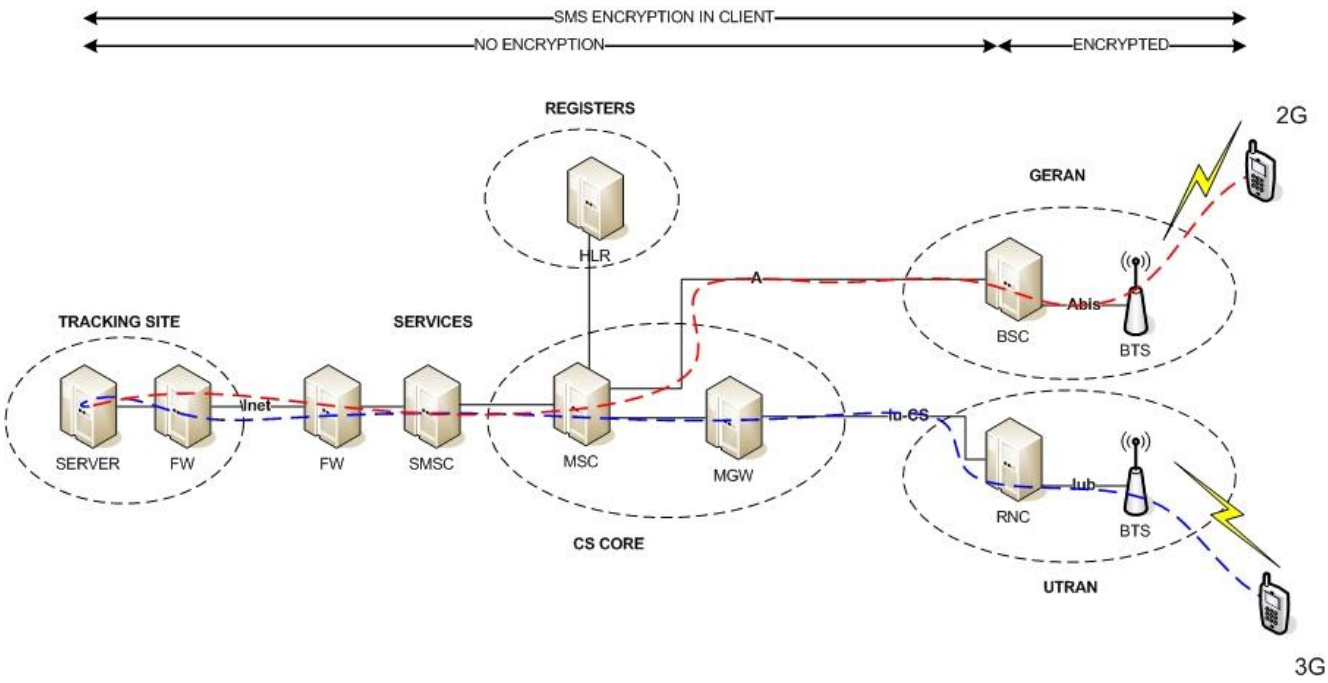

Fig. 11 SMS security solution

5) Cross site scripting

Cross site scripting (XSS) [29] is a WWW-server vulnerability where the attacker can execute code in the HTTP address or via an interactive webpage. The purpose can be to steal data or usernames.

6) Social engineering

Social engineering is a method in which somebody is tricked into giving sensitive information to the attacker. This is a very common way to discover data about a company.

B. Security solutions

There are many security threats when services are available via the internet and only a few have been introduced here. The main way service providers can protect their users is to be aware of these threats and make the system as secure as possible.

1) Best practices

There are many guides that include instructions on how to create secure networks, for example, *RFC2196 Site Security Handbook* [30] and *Standard of Good Practice for Information Security* [31].

2) Personnel

Information security is an area where knowledge has to be updated frequently. Personnel have to be aware about possible threats, which can be achieved by proper training.

3) Security equipment

Corporate networks can be secured with additional equipment like firewalls, Intrusion Detection System (IDS), and Intrusion Prevention System (IPS). A well-planned security solution is built by using all of them as needed.

4) Operating systems

It is important to keep operating system software updated. There are frequent new software releases, and maintenance personnel have to be aware of these updates. Operating systems can be "hardened," meaning that all unnecessary services are disabled.

VII. End-User Segment Security

Fig. 12 shows the main technical challenges of data processing and end-user segments. End-users can access their positioning data via the internet, and their computers are vulnerable for all the typical threats of the internet. How well their equipment is protected and maintained is fully dependent on the user. This can be a security risk for satellite tracking systems, if the attacker gains access to a hosting server using stolen user accounts.

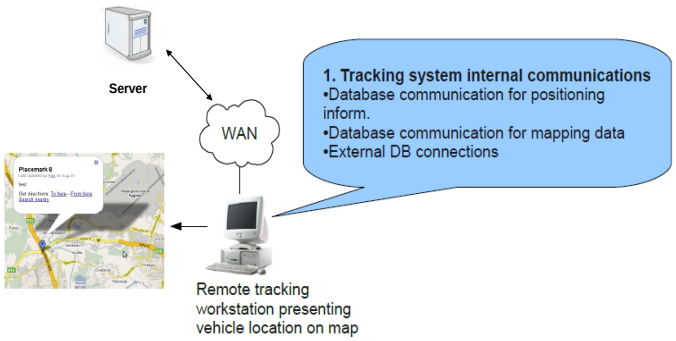

Fig. 12 Data processing and end-user segment elements

A. Security threats

1) Viruses, worms, adware, spyware

The most common security threats for end-user are viruses, worms, adware, and spyware. These threats can open ports to the system, or they can steal user accounts directly. Usually the user does not notice anything before it is too late.

2) Phishing

Phishing [32] is a method in which the attacker tries to request user accounts via email, phone, or faked web sites.

B. Security solutions

There are many commercial applications available for home users to protect their computer. Usually they are complete packages that include a firewall, virus scanner, and online protection against adware/spyware.

Being aware is a good way to be secure. Suspicious web sites and unknown download sources have to be avoided and account information has to be kept in a secure place. RFC2504 [33] contains good instructions for end-users.

VIII. Conclusion

As discussed in this paper, the satellite tracking system is quite a complicated system from the information security point of view. It contains parts of wireless and wired communication, and it is obvious that it contains information security risks if the system is not built properly. Many commercial satellite tracking applications are available, but normally no mention of their data security is given.

In any case, most security risks can be mitigated, and there are already effective security solutions available that can be applied to satellite tracking systems. Service providers and users are more likely to security precautions seriously is they are aware of the wide range of vulnerabilities. Securing the satellite tracking system data path is especially important if the system is used to deliver sensitive positioning data.

REFERENCES

[1] Viitanen, J., "Planning and requirement analysis of the SATERISK project", Master thesis, Laurea University of Applied Sciences, Espoo 2009. (In Finnish)

[2] SATERISK project, http://www.saterisk.com

[3] OPINION of the European Economic and Social Committee on the Green Paper on Satellite Navigation Applications COM(2006)769 final, Available: http://eescopinions.eesc.europa.eu/eescopiniondocument.aspx?language=en&docnr=989&year=2007

[4] Viitanen, J., Happonen, M., Patama, P. & Rajamäki, J. "International and Transorganizational Information Flow of Tracking Data", Proceedings of the 8th WSEAS International Conference on INFORMATION SECURITY and PRIVACY (ISP '09), Puerto De La Cruz, Canary Islands, Spain, December 14-16, 2009, pp. 111-115.

[5] Viitanen, J., Happonen, M., Patama, P. & Rajamäki, J. "Near Border Procedures for Tracking Information", WSEAS TRANSACTIONS ON SYSTEMS, In Press.

[6] Happonen, M., Kokkonen, P., Viitanen, J., Ojala, J. & Rajamäki, J., "Jamming Detection in the Future Navigation and Tracking Systems", in Proceedings of the 16th Saint Petersburg International Conference on Integrated Navigation Systems, 25 - 27 May, 2009 Saint Petersburg, Russia, pp. 314-317. ISBN 978-5-900780-69-6

[7] Kämppi, P., Rajamäki, J. & Guinness, R., "Information Security in Satellite Tracking Systems", Proceedings of the 3rd International Conference on Communications and Information Technology (CIT'09), Vouliagmeni Beach, Athens Greece, December 29-31, 2009, pp. 153-157.

[8] E. Airos, R. Korhonen, T. Pulkkinen, "Satelliittipaikannusjärjestelmät" [Satellite tracking systems], PVTT, Defense Forces Technical Research Centre, Publication 12, Riihimäki: 2007. Available: http://www.mil.fi/laitokset/pvtt/satelliittipaikannus.pdf

[9] 3GPP General Packet Radio Service (GPRS) Service description Stage 2, 3GPP TS 23.060 v9.2.0

[10] 3GPP Technical realization of the Short Message Service (SMS), 3GPP TS 23.040 v8.6.0

[11] B. W. Parkinson and K. T. Fitzgibbon, "Optimal Locations of Pseudolites for Differential GPS," Navigation: The Journal of the Institute of Navigation, Vol. 33, No. 4, Winter 1986 - 87, pp. 259 - 283.

[12] B. Elrod, K. Barltrop and A. J. Van Dierendonck, "Testing of GPS Augmented with Pseudolites for Precision Approach Applications," Proceedings of ION GPS-94, 7th International Technical Meeting of The Satellite Division of the Institute of Navigation, Salt Lake City, UT, September 20 - 23, 1994, pp. 1269 - 1278.

[13] Trevoc Ltd, http://www.trevoc.com

[14] The Symbian Foundation, http://www.symbian.org/

[15] Apple – iPhone – Mobile phone, http://www.apple.com/iphone/

[16] R. Mogull, "The iPhone's SMS vulnerability: What we learned", Macworld, 2009, Available: http://www.macworld.com/article/142179/2009/08/iphone_sms_security.html

[17] R. McMillan, "First IPhone Worm Spreads Rick Astley Wallpaper", PCWorld, 2009, Available: http://www.pcworld.com/businesscenter/article/181697/first_iphone_worm_spreads_rick_astley_wallpaper.html

[18] Androi Open Source Project, http://source.android.com/

[19] Samsung bada open platform, http://www.bada.com/

[20] GSM World – GSM, http://www.gsmworld.com/technology/gsm/index.htm

[21] 3GPP High Speed Circuit Switched Data (HSCSD) - Stage 2, 3GPP TS 23.034 v5.2.0

[22] GSM World - EDGE, http://www.gsmworld.com/technology/edge.htm

[23] 3GPP – UMTS, http://www.3gpp.org/article/umts

[24] 3GPP – HSPA, http://www.3gpp.org/HSPA

[25] GPRS Tunneling Protocol (GTP), 3GPP TS 29.060 v5.14.0

[26] SS7 Signaling Transport in Core Network, 3GPP TS 29.202 v5.2.0

[27] CERT/CC Denial of Service, http://www.cert.org/tech_tips/denial_of_service.html

[28] pharming.org, http://www.pharming.org/index.jsp

[29] Top 10 2007 - Cross Site Scripting – OWASP, http://www.owasp.org/index.php/Top_10_2007-A1

[30] Site Security Handbook, IETF RFC 2196,1997

[31] Standard of Good Practice for Information Security, ISF Standard, 2007

[32] APWG Internet Policy Committee, http://www.antiphishing.org/index.html

[33] Users´ Security Handbook, IETF RFC 2504,1999

Pasi P. Kämppi was born in Varkaus, Finland on 11th December 1973. Educational background is presented in chronological order: Upper secondary school, Varkaus, Finland, 1992; B.Sc. in telecommunications, University of Applied Sciences, Kotka, Finland, 1996; Specializing studies of data network designing, Laurea University of Applied Sciences, Espoo, Finland, 2009.

He performed his military service on 1996-1997 and he was ranked as sergeant in signal corps. He has been working with telecommunications since 1997. He started his career on 1997 in Nokia Networks as Testing Engineer and then he has been working as Senior Testing Engineer and System Specialist. Currently he is working as Senior System Specialist in Nokia Siemens Networks. His special interest is packet switched mobile networks including IP networks. He started his MBA program in Laurea University of Applied Sciences at the beginning of 2010 and this paper is part of his Master's Thesis.

Jyri K. Rajamäki was born in Punkalaidun, Finland 1963. He received his M.Sc. (Tech.) degree in electrical engineering from Helsinki University of Technology, Finland in 1991, and Lic.Sc. (Tech.) and D.Sc. (Tech.) degrees in electrical and communications engineering from Helsinki University of Technology in 2000 and 2002, respectively.

From 1986 to 1996 he works for Telecom Finland being Development Manager since 1995. From 1996 to 2006 he acted as Senior Safety Engineer and Chief Engineer for the Safety Technology Authority of Finland where his main assignment was to make the Finnish market ready for the European EMC Directive. Since 2006 he has been a Principal Lecturer at Laurea University of Applied Sciences, Espoo, Finland, where he also serves as a Head of Laurea's Data Networks Laboratory ´SIDLabs Networks´. His research interests are electromagnetic compatibility (EMC) as well as ICT systems for private and public safety and security services. He has authored more than 40 scientific publications.

Dr. Rajamäki has been an active actor in the field of electrotechnical standardization. He was 17 years the secretary or a member of Finnish national committee NC 77 on EMC, ten years a member of NC CISPR and he represented 15 years Finland at IEC, CISPR, CENELEC and ETSI EMC meetings. He was also the Chairman of Finnish Advisory Committee on EMC from 1996 to 2006. Dr. Rajamäki has been the scientist in charge for several research projects funded by Tekes – the Finnish Funding Agency for Technology and Innovation, industry and EURESCOM. He is currently the Scientific Manager of two Tekes projects.

Robert Guinness was born in St. Louis, Missouri, USA in 1981. He received his B.A. in physics from Washington University in St. Louis in 2004 and his M.Sc. in space studies from the International Space University (ISU) in Strasbourg, France in 2006. He conducted his thesis research at Johnson Space Center in Houston, Texas, where he completed a conceptual design of a crewed lunar lander.

In 1998 he completed a Missouri Space Grant Consortium internship in the Remote Sensing Laboratory at Washington University in St. Louis, conducting research on dust accumulation on Mars using data from the Mars Viking missions. From 2000 to 2004 he was a researcher in the Laboratory for Space Sciences at Washington University, conducting chemical and isotopic measurements of meteorite samples to study presolar grains. In 2001, he completed the NASA Academy at Goddard Space Flight Center, where he analyzed data from the Keck Observatory on circumstellar dust clouds. In 2002, he was a guest researcher at the Max Planck Institute for Chemistry in Mainz, Germany, where he conducted further research on presolar grains. From 2006 to 2008, he worked for Hamilton Sundstrand as a Mission Support Scientist and Lead Increment Scientist Representative for the International Space (ISS) program. Since 2008 he has worked for the Boeing Company and served as an Increment Payload Engineer for the ISS program, where he was responsible for the mission integration of 130 experiments conducted during Expeditions 19 and 20. Since 2009, he is also Director of Aerospace Systems for American Pioneer Ventures, a firm dedicated to helping early-stage startups and entrepreneurs achieve success. In December 2009, he came to Laurea University of Applied Sciences as a guest researcher, where he has participated in the SATERISK and Mayfly projects.

Mr. Guinness is a member of the Space Generation Advisory Council (SGAC) and served as the Regional Coordinator for the North and Central America and Caribbean region from 2006 to 2009.