Information security in satellite tracking systems

Pasi Kämppi, Jyri Rajamäki, Robert Guinness

Abstract—Satellite tracking is one of the most rapidly growing business areas in the world, and there are already many commercial applications available. Benefits for the customer are advertised, but there is no mention of information security. Modern satellite tracking systems contain communication 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 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. 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 as 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. Research on the technical risks of satellite tracking systems continued in 2009, and this paper describes one part of this larger research work.

This 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.

II. SATELLITE TRACKING SYSTEMS

Modern satellite tracking systems consist of many technical segments: the satellite 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. 1.

![Fig 1 Principle of a satellite tracking system](image)

A. Satellite segment

The satellite segment contains techniques to calculate the device’s position from satellite signals.

1) GPS

The most commonly used satellite positioning system is the Global Positioning System (GPS) [1]. It has been developed by the U.S. military, but service is also available for civilian usage. The system consists of 24-32 active satellites, and it covers whole world. Since the U.S. government stopped intentionally degrading the signal in 2000, the position data provided by GPS is quite accurate.

2) GLONASS

GLONASS (Global’naya Navigatsionnaya Sputnikowaya Sistema, Global Navigation Satellite System) [1] is developed and used by Russia. The system is like GPS, and 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 as accurate as GPS. The satellite constellation is optimized so that usability is best behind Russian borders.

3) GALILEO

GALILEO [1] 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 service 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.

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) [2] and Short Message Service (SMS) [3]. 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. End-users can access their services via the internet, so systems have to be connected to internet safely and reliably.

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

III. MOBILE NETWORK USER PLANE SECURITY

A. History
Originally GSM (Global System for Mobile communications) [4] 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) [5] that offered four times faster access rate compared to CSD. Common for these services is that they use communication channels based on Time-Slot Leasing (TSL) scheme.

General Packet Radio Service (GPRS) was the first packet-switched mobile network service that offered 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) [6], and it offered faster user data rate and smaller Round Trip Time (RTT).

Universal Mobile Telecommunications System (UMTS) [7] offers end-user data rates that make as real mobile internet experience as possible. Modern systems are upgraded with High Speed Downlink Packet Access (HSDPA) [8], 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.

B. 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. Logical architecture of GPRS network is described in 3GPP TS 23.060 V9.2.0, as shown in Fig 2.

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 GPRS Encryption Algorithm (GEA) and UTRAN supports 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.
C. Short Message Service

Short message service (SMS) provides a method to send short messages via mobile networks [3]. 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 Center (SMSC).

Globally networks of different operators are connected with Signaling System Seven (SS7) [10], 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 for 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.

D. 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 is. The most common technique is IP Secure Architecture (IPsec).

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.

IV. DATA CENTER 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 [11] 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 [12] 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”.

5) Cross site scripting
Cross site scripting (XSS) [13] 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 network, for example, RFC2196 Site Security Handbook [14] and Standard of Good Practice for Information Security [15].

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 all disabled.

V. CLIENT SECURITY

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.

Dedicated devices for satellite tracking are available, but their security vulnerabilities have not been investigated here.

A. Symbian OS
Symbian [16] is probably the most widely-used smart phone operating system in the world. Because it is like a computer, it has many vulnerable interfaces.

Threats can occur via downloadable applications, GPRS, SMS, web browser, or email. In theory, it is possible that a mobile can be hijacked and managed remotely to direct positioning data to a place available to the attacker.

B. iPhone
The iPhone [17] is the newcomer in the mobile world, and there has already been a few severe security threats reported. It has been possible to capture iPhone data via SMS [18], and the first worms [19] have also been spread among iPhones.

C. Other operating systems
Recently new smart phone operating systems like Android [20] and Bada [21] have been released. Nobody knows yet how vulnerable they are going be.

D. 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.
VI. END-USER SECURITY

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.

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 [22] is a method in which 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 [23] contains good instructions for end-users.

VII. 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.

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. Securing the satellite tracking system data path is especially important if the system is used to deliver sensitive positioning data.

REFERENCES

[2] 3GPP General Packet Radio Service (GPRS) Service description Stage 2, 3GPP TS 23.060 v9.2.0
[3] 3GPP Technical realization of the Short Message Service (SMS), 3GPP TS 23.040 v8.6.0
[5] 3GPP High Speed Circuit Switched Data (HSCSD) - Stage 2, 3GPP TS 23.034 v5.2.0
[10] SS7 Signaling Transport in Core Network, 3GPP TS 29.202 v5.2.0