Security issues in the mobile internet literature review example

Law, Security

Introduction

With wireless services that are growing by the day, there is a need to have wireless networks. Wireless networks are becoming essential services for many people. With wireless networks comes security. Security is an important factor when connectivity is concerned. Important data is stored in devices that are connected. There is therefore a need to have secure network so that the data that is being stored is secure and safe from attacks. This paper will look at the wireless networks and their security issues. It will particularly look at the GPRS, 3G and 4G.

The advent of digital systems has given rise to wireless network development. There are various mobile phone developments that have been seen coming up, ranging from GPRS, 2G, 3G and now 4G. All these advancements have been realized as vendors and developers try sealing the loops they experience with the current networks. Security has played a key role in the development of mobile networks. This paper will analyze the three mobile networks, GPRS, 3G and 4G.

General Packet Radio System (GPRS)

This technology provides radio access to the mobile GSM (Global System for Mobile Communications). GPRS is developed on GSM network so that it enhances effective and reliable applications that use the internet. This way, it enables data to be transmitted to and from the mobile network which uses circuit switching. The GSM uses circuit switching while GPRS uses packet switching. This, therefore, requires some hardware and software so that upgrades can be made. GPRS is the first technology to be developed that is

meant to enable end-to-end infrastructure of wireless systems. The rationale for this technology is to enable subscribers of GSM who use circuit-switching to access data services because it means an increase in subscription speed. With GPRS, speeds are increased up to 172kbps; this is not possible with GSM/SMS. Packet switching is only used when users are only transmitting or receiving data. Instead of dedicating a particular radio channel to a specific user for a specific time, the whole radio channel is shared by many users. In addition, a mobile host can get allocations that go more than the 8 slots which are available in the TDMA frame. With the use of GPRS, peak time is improved for GSM, thus, supporting virtual connectivity and also aiding in transferring packets that was sent using circuit switching technology. In this process, it reduces the SMS center and loading of the signaling channel. There are two extensions introduced to the switching of the GSM system. They would be able to accommodate the packet switching process of GPRS. These extensions include Gateway GPRS support node (GGSN and Serving GPRS support node (SGSN). The functions that are performed by GGSN are equivalent to those that are performed by MSC and SGSN.

There are four channels that are defined in GPRS as coding schemes. These channels include CS1, CS2, CS3 and CS4. These channels have radio data rates in the 8-TDMA frames as 8. 8, 13. 3, 15. 6 and 21. 4kbps in that order. Normally, CS3 is used to give 124. 8kbps frequency in the frame of TDMA. The real speed that is used for accessing and browses to the internet is 40kb/s. GPRS facilitates immediate connection whenever information needs to be sent or received from the internet without the need to have modem dial-up connections. Users of mobile phones, which are capable of using

GPRS and use GSM networks that have GPRS features can, access the internet with ease.

Security issues of GPRS

The security issues of GPRS is like that of GSM where the most important aspects are identity authentication, identity confidentiality and confidentiality; these should be found in the signaling that occurs between GPRS serving node and that of the mobile device. An additional feature apart from the GSM is the GPRS backbone. The mobile station initiates security authentication by sending a request to the network as SGSN. After this, Home Location Register (HLR) and Authentication Center (AuC) generate random numbers (RAND), signed response (SRES and encryption key (GPRS-Kc. These are used to undertake the security process in GPRS. This has been the mechanism that has been used in GPRS. There is also the use of an algorithm to undertake the data integrity test.

Limitations of GPRS

One limitation of GPRS is that of cell capacity. Its operation depends on the time slots that are assigned by the mobile operator. It also has limited speed because the theoretical explanation that is can use 172. 2kbps is not real because this will mean only one user will have to be used the time slot. This technology also lacks the store and forward mechanism. Another limitation is delayed in transit. This is because the packets are sent in all directions and this can mean that some packets can be lost on the way.

Third generation (3G) wireless technology

The standard that is managing this technology is international mobile telecommunications (IMT) 2000. The main goal of 3G network is to reach speeds of up to 144kbps, 384kbps, and 2Mbps whose environments are high mobility, low mobility, and stationary in that order. This technology has the capacity to transmit data at high speeds and also is able to process applications that are multimedia in nature. They are also able to provide personalized internet services, and digitization convergence.

The main advantage that comes with 3G networks is that it is faster than previous 2G networks. Smart mobile devices have services which range from voice calls to data services. 3G network has the ability to provide data and voice services with speeds going up to 200 kbps. If it is only data that are being transmitted, then the speed will go up to several Mbps. There are many 3G networks which are in use currently and the most common are enhanced Data rates for GSM evolution (EDGE) that is from the family of SDMA technologies. One of these technologies includes EV-DO (Evolution-Data optimized); this technology uses Code Division Multiple Access of Time Division Multiple Access in regard to multiplexing. Another technology is HSPA (High Speed Packet Access).

Security of 3G

The security issues in 3G are due to the outcry that wireless systems were insecure. Due to mobility of mobile devices, and IP based technologies come with security vulnerabilities. There are several aspects that are considered in 3G security. These aspects include mobility, security threats that are

identified, and the types of information that are to be protected. There is also the issue of the complexity over the 2G network.

When 3G security architecture was being established, three factors were considered, which include network domain security, user domain security, application domain security and visibility and configurability of security. These aspects were considered when undertaking security assessments for 3G networks.

4G (Fourth Generation networks)

This technology comes with high data rates. In high mobility environments like trains and cars, the speed is 100Mbits/s while fixed accessing will give a speed of up to 1Gbps. Today, this is one major development that is seen in mobile technologies. It is the same as getting Gigabit or LAN network access in a mobile device. This technology gives IP communication that has high speeds to smart phones and laptops. Regarding speed, this technology can be said to have faster connections and speeds than cable or DSL technologies. After 4G is installed, one can download an application on their mobile device as though they are downloading it in a desktop computer. With this, one can run applications like YouTube, IT TVs and Video on Demand with very high speeds. If one has a VoIP client in their Smartphone, then they are able to make VoIP calls in their mobile phones. This is one thing that is going to eradicate and floor mobile voice business in the near future. Although this technology has been developed and used in most parts of Europe and America, it is still in the development stage. It has not been rolled out fully.

Difference between 3G and 4G networks

The main difference that is evident with these two technologies is with the data rate. In 4G, a user can go up to 100Mbps and in the case of 3G, download speed can go up to 14Mbps while upload is 5. 8Mbps. This is in theory. Another difference is that of infrastructure. In 4G, the network is all IP. 3G network, on the other hand, is a hybrid of between circuit network and packet network. By being all IP, 4G is bound to create and support faster web surfing and data connectivity. In 3G, there was a lot of work in trying to convert data transmission from the mobile device to traffic that is based on IP. This was a slow process. 4G has merely adopted technologies from 3G like Wi-Max and LTE. The definition of ITU is 3. 9G and not 4G. With 4G, there is a new standard, WIMAX. This technology has improved speeds of transmitting data. With it has come a new standard, the 802. 16m. With this technology, data transmission goes up to 100Mbps in high-mobility areas and up to 1Gbps in low or stationary environments. 4G also mobile devices to display high definition video (HD TV).

Security issues solved by 4G

4G promises to solve the mobile security issues that are associated with 3G and GPRS. It is a technology which incorporates quality of service (QoS) and mobility. Another issue that will enhance security is that of the use of IPV6 address scheme. With this scheme, each and every mobile device is likely to have its own IP address. The current security problems that are found in mobile devices are the use of multiple layers of encryption that are found in the protocol stack.

Conclusion

With the introduction of wireless technologies comes security concern. 4G wireless network is here to solve the security issues that were found in 3G and GPRS. Security vulnerabilities are a common thing for most networks. This paper has analyzed the security concern that has been taken into consideration by the wireless networks.

Works Cited

Ericsson. Basic Concepts of WCDMA Radio Access Network. NY: Routledge, 2002.

Fernandez, Eliot and Eliab Jossy. An Overview of the Security of Wireless Networks. Toronto: Articy Publishers, 2004.

Hartel, Moses. GSM Superphones. New York: McGraw-Hill, 2009.

Lauter, Kenneth. " The Advantages of Elliptic Curve Cryptography for Wireless Security." Wireless Communications, IEEE 11. 1 (2004): 62-67.

Mehotra, Anderson. GSM Systems Engineering. Norwood, MA: Artech House, 2007.

Scourias, Joseph. Overview of the Global System for Mobile Communication. New York: McGraw-Hill, 2007.