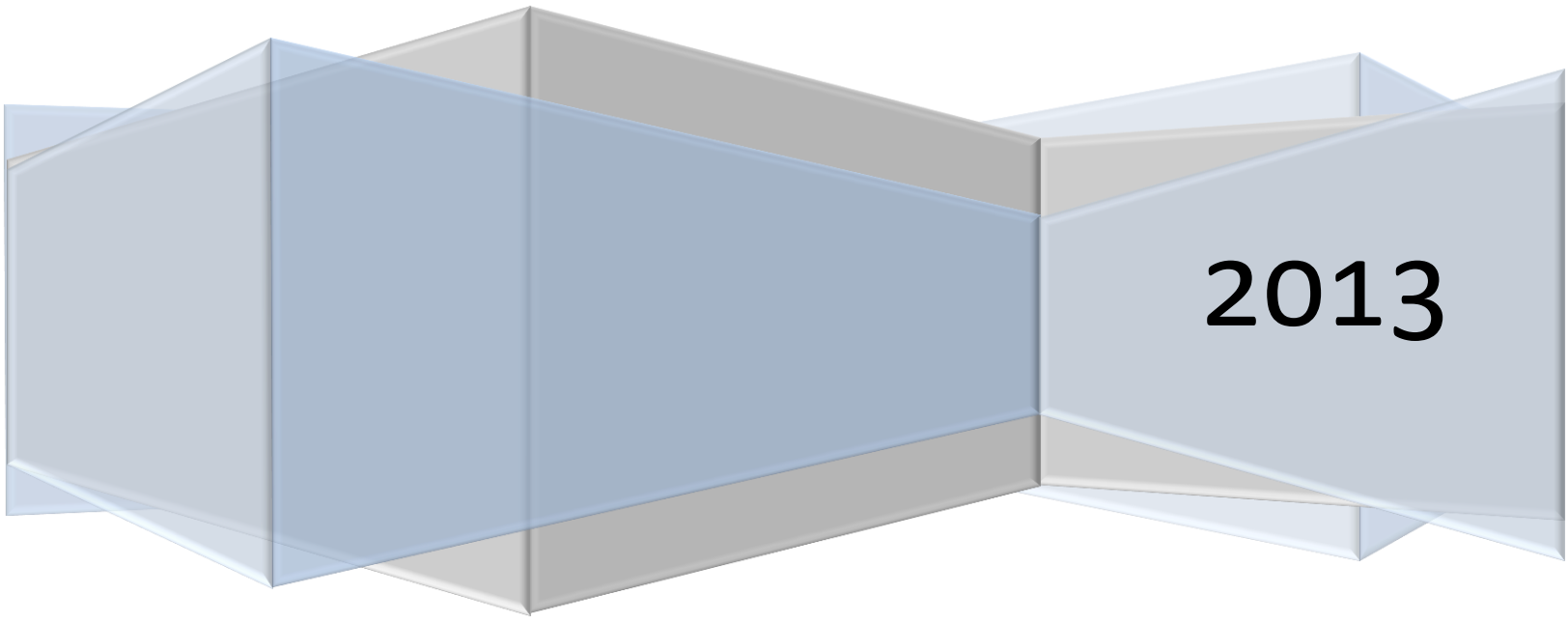
Computer Science Dept. (UCT)

Cry-Help Literature Review:

Secure Mobile Communication Protocols

By: Nina Otsweleng (OTSNIN001)



Abstract

Mobile phones can be used in crime reporting. However, due to the sensitivity of the data that is transmitted from the mobile phone to the relevant authorities, the security of mobile networks must be considered. There needs to be confidentiality, integrity, authenticity and non-repudiation of the data that is transmitted from one end to another. Mobile network architectures affect the security of data transmission. In this paper we take a look at these architectures and how they affect security. We also explore the issue of privacy and unlinkability in these networks. We then look at ways people have used protocols used to aid security in these architectures. Conclusions show that more literature is needed on unlinkability on mobile network architectures.

Crime Reporting

Most crime reports come to the attention of authorities through citizen reporting networks (Lasley & Palombo, 1995) . Lasley & Palombo (1995) explain in their article that the main crime reporting mode that has been used in the past has been spoken word. Crime reports are needed in society to help police and governments with crime mapping, tracking crime trends, victim characteristics and times and locations when crime is most prevalent (Advice: content.met.police.uk). This information is needed to help reduce crime in urban areas.

Mobile Crime reporting

Lasley & Palombo (1995) state that most victims and third parties do not report crime because of fear. Some of these fears are said to include not sounding credible enough to the authorities and the costs of being involved. They go on to mention that reporting crime could cost third parties time and money. In the case of victims they say that sometimes the perpetrator is a friend or lover which makes it hard for them to report a crime. Lasley & Palombo (1995) show us in their article, that the use of technology in crime reporting will increase the number of reports gained significantly.

In his study, Blom et al. (2010) talks about women who feel their mobile devices provide a comforting diversion from the immediate physical environment. These women are said love the idea of being able to text or call someone if they are in need of help. Among many suggestions, many of the women talk about how it would be ideal for them to use their phones to send silent signals to the authorities if they were in trouble (Blom, Viswanathan, Spasojevic, Go, Acharya, & Ahonius, 2010).

The above cases show that mobile devices could be used for crime reporting. However, there are underlying security and privacy concerns to be considered especially in the context of crime reporting. Data transferred from the mobile phone to the authorities needs to be secure and private due to its level of sensitivity. In the next section we review the underlying technology that aid secure mobile communication to ensure user security and privacy.

Mobile Communication Security

Mobile devices and phones have gained a wide spread popularity. Over the last years a number of communication systems have been developed and are being brought forward to the public by numerous vendors. Behind these systems are underlying technologies that define the limitations and capabilities of mobile communication networks. These technologies are mobile communication networks which affect communication security.

Jøsang & Sanderud (2003) describe communication security in terms of confidentiality, integrity, authentication and non-repudiation of transmitted data. They also add confidentiality of traffic (whether communication is taking place or not), location and the parties address for privacy concerns. Arapinis et al. (2012) affirms this view on the importance of privacy by giving an example of how phone users accept that network operators can track their geographical movements but would be happy if a random third party could do the same. He maintains this view in his paper as he speaks about issues on untraceability/unlinkability in mobile network architectures. We discuss this in later sections of this literature review. Jøsang & Sanderud (2003) explain that this type of security is usually implemented with cryptographic mechanisms. These cryptographic mechanisms are said to only be necessary when the information being transferred to other devices is extremely sensitive because they can affect the way an application runs. Misra & Wickamasinghe (2004) speak of two categories of security challenges a device must account for. These are content security and channel security. Content security is said to refer to protecting data stored on the device while channel security refers to preventing unauthorized users from gaining the content.

Mobile communication security is not only dependent on cryptographic algorithms but also on the network architectures where it happens and their protocols. An example of such network protocols are GSM (Global System for Mobile Communication), 2G and 3G. Misra & Wickamasinghe (2004) describe GSM to aid in the description of 2G (second generation) technologies. GSM is a standard used to

describe the protocols for 2G cellular networks. He then states that GSM uses two strategies to secure its radio path. These are encryption of data in the radio path and using temporary identification. He then goes on to describe how GSM works by stating the following: When an initial connection between the mobile device and base station is created, the mobile device sends its true identity to the base station. The base station then sends the device a temporary ID which it will use for the rest of the session activities. The temporary ID is used to help in keeping the user anonymous. Encryption is said to be used for protecting confidentiality of the data in the radio path. Misra & Wickamasinghe (2004) also state an important fact that affects security which is GSM encryption was only designed to establish security in the radio path between the mobile device and fixed network. Other authors such as Kayayurt & Tuglular (2006) point this out. GSM does not support end-to-end security of data. This could stand out as a big issue for a mobile application for crime reporting where crime information is very sensitive and needs to be kept secure at all times. Other authors bring to attention the lack of mutual authentication and weak encryption in GSM which attackers can use to their advantage.

GSM technologies have evolved from 2G to 2.5G (GPRS) to what most people use now which is 3G (third generation telecommunication systems). Though these variations come as improvements to their predecessors none provide end-to-end security of data transmitted over the mobile network (Misra & Wickamasinghe, 2004). Some improvements are based on the speed at which processing is done in them. Arapinis et al. (2012) gives a description of 3G in their article. 3G is a standard upheld by the third generation partnership project (3GPP) which was introduced in 1999. It is set up to support mobile data applications and to lower the costs of mobile data communications. Arapinis et al. (2012) lists the following as the aims of 3G;

- To provide authentication
- To provide confidentiality of data and voice communication
- To provide user privacy

Arapinis et al. (2012) then expands on the third goal of 3G which is provision of privacy by explaining the goals that fall within the privacy goals. These goals are said to be the following

- User identity confidentiality – through the use of temporary IDs as mentioned by Arapinis et al. (2012)
- User untraceability – an intruder should not be able to figure out whether different services are being delivered to the same user by eavesdropping.

Arapinis et al. (2012) looks specifically into the privacy goals of 3G to reveal attacks that could be done to the 3G protocol and compromise users' privacy and security. He explains that some of these attacks are only possible because attackers are now able to implement cheap fake base stations. He reveals the following known 3G vulnerabilities

1. IMSI catcher – the IMSI is the mobile device's true identity. This attack happens when a mobile phone is forced to reveal its identity by triggering an identification procedure from a fake base station.
2. 3G/GSM Interoperability – these attacks exploit vulnerabilities which 3G gets from 3G. These include the weak encryption and lack of mutual authentication in the GSM key agreement protocol.

Though they mention these attacks they focus on unlinkability and anonymity properties of 3G. Unlinkability describes the inability of an observer to decide whether certain items of interest are related or not (Tsai, Lo, & Wu, 2012). Arapinis et al. (2012) have an interesting article in that many other papers look at issues of linkability in mobile networks that connect to the internet such as (Tsai, Lo, & Wu, 2012) , (Huang, 2006) and (Bauer, McCoy, Greenstein, Grunwald, & Sicker, 2009) but they look at linkability in the context of mobile network architectures without internet connection. In their paper, they introduce a linkability attack on 3G's AKA protocol. The 3G AKA protocol is said to be a threat to unlinkability for 3G subscribers because the error message sent in case of authentication failure leak information about the subscriber's identity. They went on further to conduct tests to see how it performs. In their tests results they found that the anonymity property held while the unlinkability property verification failed. Active attackers are said to need only rely on paging procedures to break both anonymity and unlinkability.

Without delving into details, new privacy proposes fixes to the protocol. These include the use of a lightweight public key infrastructure in the protocol and encrypting a page request with a shared session key to protect against the paging request attack. They also propose a method to fix leaking of identity information by error messages which uses basic encryption. In their conclusion they state that their fixes to the protocols are friendly and can be used in the implementation of the next generation of mobile telephony standards.

Other articles describe completely different approaches to enhancing security in mobile communications. One of these is by Kayayurt & Tuglular (2006) who proposes implementing end-to-end security on a mobile network using Transport Layer Security (TSL) along with Secure Socket Layer (SSL). He gives a few advantages to why these protocols should be implemented in mobile communications. His reasons are as follows

- TLS and SSL have been use for a long time and therefore provide security that is well known and trustworthy. They have been accepted widely and are even in use in financial applications.
- They are common on the internet. If we use them on mobile devices integration between mobile applications and the internet will be made easier.
- They have open specifications and many implementations so can easily be tailored for mobile devices

Kayayurt & Tuglular (2006) do acknowledge in their paper that TLS and SSL are known for their resource consumption which is unsuitable for mobile devices. They go on to state that the solution that they present is based on a java platform and efficient for mobile phones. In their article they defined the specifics in which the end-to-end security would take place. Their protocol was designed to run on J2ME platforms including cellular phones. The application would need to have client/server architecture. The protocol was implemented using Java in order to support J2ME and JSE. In this protocol, the mobile device ran the client version of TLS and the back-end server ran the server version of TLS. The protocol was also designed to work with the GPRS standard (2.5G).

The authors then conducted an experiment to test out the protocol. In the experiment they tested the handshake procedure of TLS and the application level object transmission and reception. According to their experiment results everything went as expected. They did not run into trouble and so they believe that this protocol could be used to secure mobile communication data.

Mynttinen, J (2000) takes on a similar approach as Kayayurt & Tuglular (2006). He discusses of end-to-end security on a GSM using WAP. In his article he shows that WAP transactions over GSM are completely insecure unless extra security mechanisms are used.

Conclusion

Unlinkability of information was an interesting aspect of security for mobile crime reporting but was brought up in only one paper in the aspect of mobile network architectures. One would want to be able

to report a crime anonymously. Most papers that focused on unlinkability spoke on unlinkability in the internet situation. End-to-end security implementations over network architectures were interesting.

References

Jøsang, A., & Sanderud, G. (2003, January). Security in mobile communications: challenges and opportunities. In *Proceedings of the Australasian information security workshop conference on ACSW frontiers 2003-Volume 21* (pp. 43-48). Australian Computer Society, Inc.

Arapinis, M., Mancini, L., Ritter, E., Ryan, M., Golde, N., Redon, K., & Borgaonkar, R. (2012, October). New privacy issues in mobile telephony: fix and verification. In *Proceedings of the 2012 ACM conference on Computer and communications security* (pp. 205-216). ACM.

Misra, S. K., & Wickamasinghe, N. (2004). Security of a mobile transaction: a trust model. *Electronic Commerce Research*, *4*(4), 359-372.

Kayayurt, B., & Tuglular, T. (2006). End-to-end security implementation for mobile devices using TLS protocol. *Journal in Computer Virology*, *2*(1), 87-97.

Mynttinen, J. (2000, November). End-to-end security of mobile data in GSM. In*Tik-110.501 Seminar on Network Security. Helsinki University of Technology*.

Advice: content.met.police.uk. (n.d.). Retrieved April 4, 2013, from content.met.police.uk: http://content.met.police.uk/Article/Why-should-I-report-crime/1400006932847/1400006932847

Bauer, K., McCoy, D., Greenstein, B., Grunwald, D., & Sicker, D. (2009). Physical Layer Attacks on Unlinkability. *Privacy Enhancing Technologies*, 108-127.

Blom, J., Viswanathan, D., Spasojevic, M., Go, J., Acharya, K., & Ahonius, R. (2010). Fear and the City – Role of Mobile Services in Harnessing Safety and Security in Urban Use Contexts. *Proceedings of the 28th international conference on Human factors in computing systems*, 1841-1850.

Huang, D. (2006). Traffic Analysis-based Unlinkability Measure for IEEE 802.11b-based Communication Systems. *Proceedings of the 5th ACM workshop on Wireless Security*, 65-74.

Lasley, J. R., & Palombo, B. J. (1995). When crime reporting goes high-tech: An experimental test of computerized citizen response to crime. *Journal of Criminal Justice*, 519-529.

Tsai, J.-L., Lo, N.-W., & Wu, T.-C. (2012). Secure Anonymous Authentication Protocol with Unlinkability for Mobile Wireless Environment. *Tsai, Jia-Lun, Nai-Wei Lo, and Tzong-Chen Wu. "Secure anonymous authentication protocol with unlinkabili Anti-Counterfeiting, Security and Identification (ASID)*, 1-5.