3GTSM: A NOVEL 3G TERMINALS SECURITY MODEL

Liangyin Chen[1], Zhishu Li[1], Baolin Li[1], Jianchuan Xing[1], Jiancheng Ni[1], Qing Li[1], Liangwei Chen[2]

[1]School of Computer Science, Sichuan University, Chengdu 610065, China
[2]The First Middle School of Tongliang, Chongqing, 625000, China

ABSTRACT

With the widespread application of 3G terminals, the security issue of it becomes a paramount issue. This paper proposes a novel 3G terminals security model (3GTSM) to provide efficient support for security. A brief review of the security architecture of 3G communication system is given first, and then the security model, which proposes integration of biometric engine and selectable security module to the 3G terminals, is described in detail. The priority of the model provides a good solution for 3G terminals security finally.

1. Introduction

Currently, mobile equipment and mobile communication system are in such a poor security state that they do not withstand basic reverse engineering weaponry. Moreover, their security mechanisms are poorly designed and rely on obscurity rather than strong cryptographic protocols. Breaking these mechanisms does not yet require use of advanced attack techniques such as hardware attacks. Fortunately, people have to paid attention to this issue. The mobile equipment and chipset manufacturers are working hard to improve the overall security level of them.

In order to ensure the security of 3G system, which is the third communication system, the third generation partnership project (3GPP) added new authentication, authorization, accounting (AAA) and other integrity mechanism to protect critical signaling information on the system. It enhanced authentication protocol to provide mutual authentication and freshness of cipher/integrity key, and provided enhanced encryption, stronger algorithm, longer key, etc, which made the 3G system to be more credible than the global system for mobile communications (GSM). Therefore, 3G systems strengthened its security, and which relies on the security of 3G terminals largely.

As far as the 3G terminals security is considered, in order to meet the requirements of the 3G systems, we must make it to be scalable, be able to be configured expediently and be selectable for security module. In this paper, we focus on the selectable security module of 3G terminals.

Three facets about 3G terminals security has to be considered. The first one is related to the hardware that is the basis of 3G terminals. The second is related to software, which is much accounted for the security factor. In paper [1], security primitives and protocols are used to guarantee privacy and integrity of data, and the security methods are mainly defined through standards. The third is related to attacks, by which malicious users aim to defeat the security methods of the system [1].

First, from the view of hardware, the battery and the monitor controls gaps must be considered. The battery gap emphasizes that the current energy consumption overheads of supporting security on battery-constrained 3G terminals are very high [1]. The monitor controls gap highlights that the 3G terminals needs power monitor and bus monitor at any moment.

Second, from the view of performance, the processing and the flexibility gaps have to be taken into account. The processing gap emphasizes that current 3G terminals architectures are not capable of keeping up with the computational demands of security processing. The flexibility gap shows that 3G terminals are often required to execute multiple and diverse security protocols and standards [1].

Third, as far as the attack is considered, the tamper resistance and the assurance gaps have to be mentioned [1]. The tamper resistance gap emphasizes that secure 3G terminals are facing an increasing number of attacks from physical to software attacks, and the assurance gap is related to reliability and stresses, the fact that secure systems must continue to operate reliably despite attacks [1]. So, the 3G systems need a reliable authentication, access control, account and auditing systems, which are based on security hardware.

The remainder of the paper is organized as flow: Section 2 summarized the 3G communication system security architecture. The section 3.1 summarized the general 3G terminals pyramid. And the section 3.2 presents a novel 3G terminals security model (3GTSM). Finally, section 4 concludes the paper and draws some perspectives.

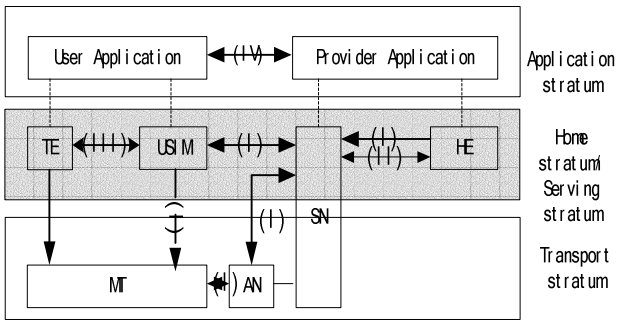

Figure 1: Overview of the security architecture of 3G
TE: (Terminal Equipment), MT: (Mobile Terminals), HE: (Home Environment), SN: (Serving Network), USIM: (Universal Subscriber Identity Module), AN: (Access Network).

2. The Security Architecture of 3G Communication System

According to the 3G security specification, the security architecture is made up of a set of security features and security mechanisms (see Figure 1 [7]).
A security feature is a service capability that meets one or several security requirements. A security mechanism is an element or process that is used to carry out a security feature. Figure 1 shows five different sets of features, each one facing a specific threat and accomplishing certain security objectives [6].
The following is the description of these groups of features [6]:
(I): Network access security provides users with secure access to 3G services and protects against attacks on the (radio) access link;
(II): Network domain security enables nodes in the provider domain to exchange signaling data securely and protects against attacks on the wire line network;
(III): User domain security allows users to have secure access to mobile stations;
(IV): Application domain security enables applications in the user and in the provider domain to exchange messages securely;
(V): Visibility and configurability of security informs the user if a security feature is in operation or not, allowing appropriate use of the service.
As far as 3G terminals are considered, it belongs to the TE or MT in Figure 1.

3. 3GTSM: A Novel 3G terminals Security Model

The security methods of 3G system in section 2 increase the security of the 3G communication. Yet the security of 3G terminals needs to be paid much attention to, to be strengthened, otherwise the security of system can not be ensured. In this section, we mainly investigate a novel 3G terminals security model.

3.1 General 3G terminals pyramid: Security Layer

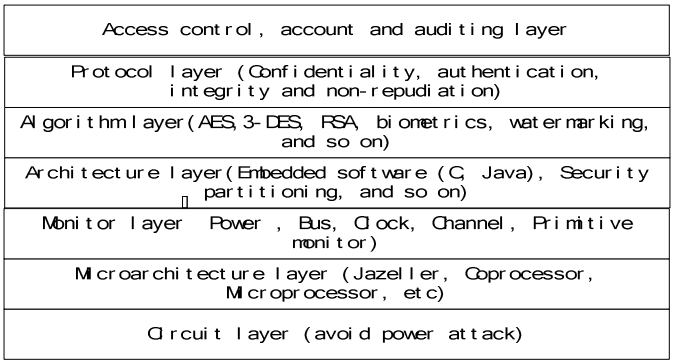

Figure 2: 3G terminals pyramid [3]

3G terminals are typical embedded system. We can't solve the security of embedded system at one single level of abstraction layers that are used to analyze the system, and 3G terminals are increasing their complexity and performance increasingly. So, 3G terminals security is a system problem, including the 3G communication system security. To ensure the security of 3G terminals system, we must address the problem in all abstraction layers (see Figure 2) [3], including the circuit layer.
Figure 2 illustrates seven primary abstraction layers in 3G terminals, each layer be responsible for special security function, which are:
• access control, account and auditing layer, in which includes AO (Account Object or Access Object) dispatch and associate, etc. This layer is closest to application program.
•protocol layer, in which includes the design of protocols to be performed on embedded devices to achieve such security goals as confidentiality, identification, data integrity, data origin authentication, and non-repudiation, and so on; [3]
•algorithm layer, consisting of the design of cryptographic primitives (such as block ciphers and hash functions, etc.) and application-specific algorithms used at the protocol layer; [3]
•architecture layer, consisting of secure hardware/software partitioning and embedded software techniques to prevent software attacks; [3]
•monitor layer, monitoring the power consumption of the embedded system, especially the smart card, to prevent from differential power analysis (DPA) attack [3], which mostly aim at smartcard. And the monitor layer should monitor the system bus also.
•microarchitecture layer, which deals with the hardware design of the modules (the processors and coprocessors)

required and specified at the architecture layer; [3]
•circuit layer, which requires implementing transistor level and package-level techniques to thwart various physical-layer attacks. [3]
The 3G terminals are divided into seven layers according to their different functions. And the up layer is based on its direct down layer which is thin-granularity. For example, monitor layer may be made up of several components, and each component may include several microarchitecture parts which are composed by a lot of circuit units. And those circuit units belong to circuit layer. For a 3G terminals security, every layer must be secure. For example, a smart card can possess an advanced protocol applying a strong cipher; however, if the circuit design allows for side-channel attacks that can extract the key, the smart card's security is broken [3]. If there isn't any method to avoid DPA attack, the attacker can deduce an encryption circuit's secret key by analyzing the power traces' statistical properties of the 3G terminals easily [3]. So, we must take over system security of 3G terminals.

3.2 3GTSM: A Novel 3G Terminals Security Model

3G system supports authentication, authorization and accounting (AAA) security features, and all of its secure features are realized by 3G Authentication and Key Agreement (AKA) procedure. The AKA procedure is a challenge-response protocol, which supports mutual authentication between the users and the system, and also provides cipher and integrity keys generating algorithms for the user equipment and the network.
The AKA mechanism provides highly security, however there are still the same security leak. For example, the user's authentication vectors can be attacked easily, and the cryptographic algorithm and encrypt key should translate in encrypted channel.
Furthermore, we designed a new security model based on 3G terminals themselves, which is scalable, selectable and configurable. In the model, we take account of both the hardware and the software synchronously. Indeed, sole software or sole hardware solutions have their limits when used in 3G terminals [2]. Therefore, we build 3G terminals systems that take benefit of both architectures and hardware monitors to increase security by detecting abnormal behaviors and by reacting appropriately [1]. In addition, a hardware design is necessary to achieve some of the security requirements. Since hardware/software co-design is a common practice in 3G terminals designs, such as using Field Programmable Gate Array (FPGA) design or adding new instructions. As far as 3G terminals be considered, the CPU should be designed specially and be safe.
In the basis of the 3G terminals pyramid from [3] and the fruits of many researchers, we advanced a novel security model, including several hardware and software layer according to 3G terminals pyramid (see Figure 2), which is showed in Figure 3. In the model, we mainly extended the architecture layer and the algorithm layer to make the security method is selectable. The biosensor, which is used to tamper physical attack, is integrated to the 3G terminals system.

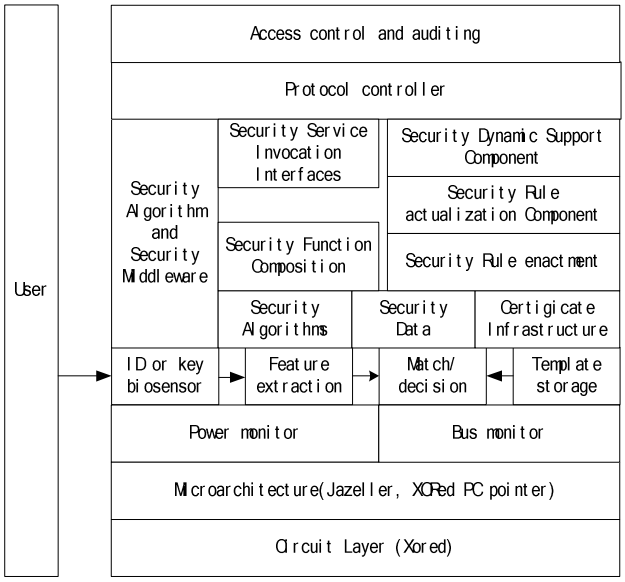

Figure 3: 3G Terminals Security Model: 3GTSM

Figure 3 includes seven parts. Each part has its own function. In microarchitecture part, the java processor, which is designed specially for 3G terminals, is advised to be used in 3G terminals. Compared with other methods, the proposed Java processors appear to be more suitable for 3G terminals. Java is more robust, secure and portable in addition to its inherited common advantages of object-oriented programming languages such as encapsulation, polymorphism, dynamic binding and inheritance. And Java processor's increasing robustness and security can be attributed to automatic garbage collection, static and run-time type checking, exception handling mechanism, array boundary checking and restrictive object reference management while its enhanced portability is realized through the compilation and execution of Java machine instructions called bytecodes instead of the particular processor binaries [4]. It potentially delivers much better performance than a general-purpose processor for Java applications by tailoring hardware support for some Java special features such as security, multithreading and garbage collection. Compared with other methods, Java processors appear to be more suitable for 3G terminals devices [4]. For 3G terminals, added-service based on 3G network will increase fast, and most of the service is related to Java. For example, ARM Jazeller is a well-known Java processor. In

this layer, we should block out the debug port, because they (such as Joint Test Action Group (JTAG)) may direct to physical attack.

It is known that buffer overflow attacks have been causing serious security problems for decades and at least 50% of today's widely exploited vulnerabilities are caused by buffer overflow and the ratio is increasing over time [2]. Since the source code of most components is not available to system integrations, so it is hard to use a pure language-based approach to solve the buffer overflow for a system designer of 3G terminals [2]. We believe that an effective solution to protect 3G terminals against buffer overflow attacks should make use of the combination of hardware and compiler. Thus, we include Jazeller and XORed [2] technology in our model.

In XORed system, if a hacker changes a function pointer and makes it point to the attack code, the attack code can not be activated because the real address that the program jumps to is the XORed address with a key. Since the key is randomly generated for each process, it is extremely hard for a hacker to guess the key. The key itself is stored in a special register of Java CPU, therefore, the key value cannot be overwritten by buffer overflow attacks [2]. For the above security with XORed, WPKI (Wireless PKI) and SSL to be realized in the wireless encrypt module in USIM card or 3G terminals, we should make a special design for the CPU core of the 3G terminals, and add several special registers and hardware algorithm module to it.

The function of access control, auditing, protocol controller, crypto algorithm, and monitor parts, etc, is same as the general embedded system. The auditing and account system is a source monitoring and restriction system that has the purpose of improving the system's reliability and security. The accounting system is the most important part because it can offer various services, such as security improvement, overload control, and class-based accounting, which require CPU resource control [5] . And it can also prevent the excessive use of the CPU capacity of a process or a group of processes, though source monitoring and restriction [5].

Moreover, the basic security consists of security algorithms, security data and certificate infrastructure. The security algorithms involve various basic information security algorithms such as encryption/decryption algorithms, private key generation algorithms, digital signature algorithms, certificate generation services, and so on. The security data are various and are used to achieve security functions, such as symmetric secret keys, public keys, private keys, pseudo-random numbers and certificates. Certificate infrastructure is the PKI system.

Security middleware is based on the basic security constitute elements, and provides static services and dynamic services. The static services are the ones which can be directly used in applications by users. They consist of two parts: invocation interfaces of security services and security function composition. The component of security functions composition can integrate different security functions so that it can provide more security support for users. Dynamic services are to automatically provide the services of common security safeguard. The support of dynamic security services in running is provided by the dynamic security support components [11].

Our approach of 3G terminals security is to provide a widely architectural support for the prevention, detection and remediation of attacks, and support for access control, auditing and monitor. Most of 3G terminals are implemented as system-on-a-chip devices, where all important system components (processor, memory, I/O) are implemented on a single chip [1]. Since the main function of most 3G terminals is collected in one SOC, the SOC is primarily a security-related factor. Therefore, the circuit layer needs to be designed as well connected.

For 3G terminals, there are USIM to identify the user, but the USIM is easily be stolen, so the model is integrated a biosensor module, which is used to discriminate the real user. This made the security feature to be selectable, telephone using USIM and data service using both USIM and biosensor module.

If all the above aspects are considered in a 3G terminals, the security of the system will increase greatly, thus meeting the specific performance and constraints issues.

4. An Example

In the project of 07GGYB361GX, we have realized the security model of the 3G terminals. This model integrates some advanced hardware and software mobile security technologies, which can support the content protection, secure transactions, secure network access, secure flashing and booting, terminal identity protection and network lock protection, and so on.

5. Summary

We propose a model prototype by using FPGA design and adding new instructions to the CPU that integrates Java instruction sets and XORed address technology. The defending against buffer-overflow attack, the extensibility of dynamical security support and security management of the new system are enhanced in comparison with general 3G terminals system.

In order to build a secure 3G terminals, we must take over the security of 3G system, and pay attention to both hardware and software. If we co-design our 3G terminals with hardware and software, we'll achieve the security of 3G terminals easier.

5. Reference

[1]. Gogniat, G.; Wolf, T.; Burleson, W.; Reconfigurable Security Support for Embedded Systems, System Sciences, 2006. HICSS '06. Proceedings of the 39th Annual Hawaii International Conference on, Volume 10, 04-07 Jan. 2006 Page(s):250a - 256a.

[2]. Shao, Z.; Zhuge, Q.; He, Y.; Sha, E.H.-M.; Defending embedded systems against dynamical security support via hardware/software, Computer Security Applications Conference, 2003. Proceedings. 19th Annual, 2003 Page(s):352 – 360.

[3]. Hwang, D.D.; Schaumont, P.; Tiri, K.; Verbauwhede, I.; Securing embedded systems, Security & Privacy Magazine, IEEE, Volume 4, Issue 2, March-April 2006 Page(s):40 – 49.

[4]. Tan, Y.Y.; Yau, C.H.; Lo, K.M.; Yu, W.S.; Mok, P.L.; Fong, A.S.; Design and implementation of a Java processor, Computers and Digital Techniques, IEE Proceedings-Volume 153, Issue 1, 10 Jan. 2006 Page(s):20 – 30.

[5]. Sugaya, M.; Oikawa, S.; Nakajima, T.; Accounting system: a fine-grained CPU resource protection mechanism for embedded system, Object and Component-Oriented Real-Time Distributed Computing, 2006. ISORC 2006. Ninth IEEE International Symposium on, 24-26 April 2006 Page(s):10 pp.

[6].Tomás Balderas-Contreras René A. Cumplido-Parra. Security Architecture in UMTS Third Generation Cellular Networks.

[7]. 3rd Generation Partnership Program. Security Architecture. Technical Specification 33.102. Release 5. Version 5.2.0.

[8]. Ray-Guang Cheng, Shiao-Li Tsao. 3G-based Access Control for 3GPP-WLAN Interworking. IEEE 2004, pages(s):2967-2971.

[9]. Geir M. Køien and Thomas Haslestad, Telenor R&D, Norway. Security aspects of 3GPP-WLAN interworking. IEEE Communications Magazine. November 2003. page(s): 82-89.

[10].H.Honkasalo, k.Pehkonen, M.T.Niemi, and A.T.Leino,"WCDMA WLAN for 3G and beyond." IEEE Wireless Communications Magazine, vol.9.Page(s):14-18, April 2002.

[11]. MingChu Li, Yongrui Cui, Yuan Tian, Dong Wang, Songyuan Yan. A New Architecture of Grid Security System Construction. Proceedings of the 2006 International Conference on Parallel Processing Workshops (ICPPW'06). Page(s): 1-6.

[12]. FAN Chun-xiao,ZHANG Hong-yu, GU Zi. A Study Implementation of PKI in 3G Security Architecture (Chinese). CHINA RAILWAY SCIENCE, November, 2005, Vol, 26. No.6, page(s):126-130.