Study of Wireless Network Security and Interworking

Bodduna Venkateshvarlu

Research Scholar, Manav Bharti University, H.P., INDIA

ABSTRACT: A variety of wireless technologies have been standardized and commercialized, but no single technology is considered the best because of different coverage and bandwidth limitations. Thus, interworking between heterogeneous wireless networks is extremely important for ubiquitous and high performance wireless communications. Security in interworking is a major challenge due to the vastly different security architectures used within each network. The goal of this article is two-fold.First, we provide a comprehensive discussion of security problems and current technologies in 3G and WLAN systems. Second, we provide introductory discussions about the security problems in interworking, the state of the art solutions, and open problems.

Index Terms—Wireless LAN, Land mobile radio cellular systems, Internetworking, Communication system security, Computer network security, Data security

----------♦----------

SECURITY IN CELLULAR SYSTEMS

The cellular phone industry has been experiencing revenue losses of more than U.S.$150 million per year due to illegal usage of their services [13]. As the cellular system evolved, newly employed security features reduced the feasibility of technical fraud. However, as third generation cellular systems become major components of ubiquitous wireless communication, the security of cellular systems faces new challenges.

Integration into packet switching networks (such as the Internet) will expose these systems to all kinds of attacks, and will demand a higher level of security. In this section, we discuss the security issues in analog and 2G cellular systems.

A. The First Generation (analog)

One of the biggest concerns of carriers is fraudulent access to services because it directly contributes to revenue loss. *Cloning* is a well-known fraud in which an attacker gains access by impersonating a legitimate user. Every cellular phone has an electronic serial number (ESN) and mobile identification number (MIN) programmed by the carrier. With no encryption employed, people can obtain a legitimate subscriber's ESN and MIN by monitoring radio transmissions.

When an attacker reprograms a phone with stolen ESN and MIN, the system cannot distinguish the cloned phone from the legal one. The countermeasure against cloning is authentication with a safe key distribution mechanism. *Channel hijacking* is another threat where the attacker takes over an on-going voice or data session. To mitigate such attacks, the signal messages also should be authenticated.

An inherent problem with wireless communication is that anyone with the appropriate equipment can eavesdrop without fear of detection. When AMPS (Advanced Mobile Phone Service) launched as the first commercial analog wireless phone system (Chicago, U.S. in 1983), the only security belief (rather than feature) was that the high cost of becoming a receiver constituted a legitimate form of access control.

However, the error of this belief became quite evident once receivers became affordable, and all wireless conversations lost their privacy. Realizing the limitation of legislative measures, providers turned to cryptography. The digitization of the voice and control channels in 2G systems made cryptographic measures more feasible.

B. The Second Generation (2G)

IS-41 (in the U.S.) and GSM (in Europe) are the major two 2G systems. Authentication in IS-41 uses the CAVE (Cellular Authentication and Voice Encryption) hashing algorithm. The network broadcasts a random number (RandSSD) and the mobile generates an 18-bit authentication signature by hashing A-Key (a 64-bit master key), ESN, and RandSSD using CAVE.

The signature authenticates the mobile to the network. However, an 18-bit authentication signature is too short to prevent random guessing attacks from succeeding. This renders the CAVE algorithm insecure [14]. Encryption algorithms such as CMEA (Cellular Message Encryption Algorithm) and ORYX (not an acronym) protect the signaling data and user data in IS-41, respectively. However, CMEA was broken in 1997 [15], as was ORYX in 1998 [16].

While originally launched as a pan-European cellular system, GSM (Global System for Mobile communications1) has grown to be the most popular mobile phone system in the world. GSM authenticates the subscriber through a challengeresponse method similar to the one in IS-41. However, GSM uses a longer master key (128 bits) stored in a removable SIM (Subscriber Identity Module), which enables flexible deployment.

At one point in time, the GSM MoU (Memorandum of Understanding Group) kept the security model and algorithms secret, hoping that *security through obscurity* would make the system secure. However, some of the specifications were leaked, and critical errors were found. An attacker could go through the security model or even around it, and attack other parts of a GSM network [17]. Also, the authentication

algorithms were so weak that a few million interactions with a SIM card disclosed the master key [18]. Furthermore, function A5, used for the encryption of voice, signal data and user data, was reverse engineered in 1999[19]. Publishing and peer reviewing cryptographic algorithms is a fundamental security principle, and eventually GSM when underwent the review process to address these flaws.

SECURITY IN 3G

Second-generation systems have successfully addressed the problems of first-generation (analog) systems: limited capacity, vulnerability to fraud, and susceptibility to eavesdropping, to name a few. However, 2G systems are still optimized for voice service, and not well suited to data communication [20].

The increasing demand for electronic commerce, multimedia communications, other Internet services, as well as simultaneous mobility, necessitated the

development of more advanced third-generation technology (3G)2. UMTS (Universal Mobile Telecommunication System) [3] and CDMA2000 phase 2 (3xRTT) [2] are the two major 3G platforms whose security features we will discuss for the remainder of this article.

A. Security Challenges in 3G

3G systems face new security challenges; new revenuerelated frauds will emerge in the context of a new billing model based on data volume and quality of service [21]. Moreover, because the 3G network is essentially an IP network, 3G networks and users are exposed to the full range of threats that ISPs (Internet Service Providers) and their consumers currently face on the Internet. A cell phone's limitation of storage and processing power implies that security features such as protection software may be excluded. Hence, mobile handsets in 3G should be treated as computing devices whose vulnerability to malicious access is higher than that of their fixed counterparts.

B. Access Security in CDMA2000

CDMA2000 [2] made a significant departure from the original CDMA's security scheme for the following reasons: _ Weakness of the CAVE, CMEA and ORYX algorithms.

- Weakness of the 64-bit keys.
- Lack of mutual authentication.

CDMA2000 adopted the AKA protocol with an optional extension. Hence, we briefly discuss the differences from UMTS. In CDMA2000, the user identity module (counterpart to GSM's SIM) is called UIM. The CDMA2000 extension to AKA defines new cryptographic functions f11 and UMAC [31]. f11 generates a UAK (UIM Authentication Key) to include in the AV, and UMAC is the message authentication function on UAK. Using the UAK protects the system from the rogue shell attack [32]. *Rogue shell* refers to a mobile that does not remove CK and IK after the UIM is removed. In a rogue shell attack, the mobile can make fraudulent calls using still-active CK/IK until the registration is revoked or a new AKA challenge is initiated. UMAC also provides an efficient reauthentication method.

CDMA2000 fully standardized the cryptographic functions used in AKA. SHA-1 [33] was specified as the core one-way function. For confidentiality, CDMA2000 chose the Advanced Encryption Standard (AES) [34]. Although there is no integrity protection of user voice and packet data in CDMA2000, MAC or UMAC functions protect the integrity of signaling data.

WI-FI PROTECTED ACCESS

Wi-Fi Protected Access (WPA) is the brand name given to the new security architecture for 802.11 by the industry trade group Wi-Fi Alliance. WPA was designed by task group I of the 802.11 working group. There are two parts to WPA. WPA I was an interim solution which required only firmware and operating system driver updates to eliminate most of the problems with 802.11 based security. WPA 2, on the other hand, is a complete redesign involving new algorithms and, unfortunately, new hardware as well. As of this time, WPA 2 is available from several vendors, so we will focus our attention on it for the rest of the section.

A. Confidentiality and Integrity

Confidentiality and integrity of messages within WPA 2 are provided by AES-CCM. The Advanced Encryption Standard (AES) is the underlying cipher [34]. Counter mode and CBC MAC (CCM) is the mode in which the cipher operates [42], [43]. AES was selected after a highly

competitive selection process, and cryptographers are comfortable with the robustness of the algorithm. Similarly, CCM is based on well understood primitives: counter mode and CBC MAC.

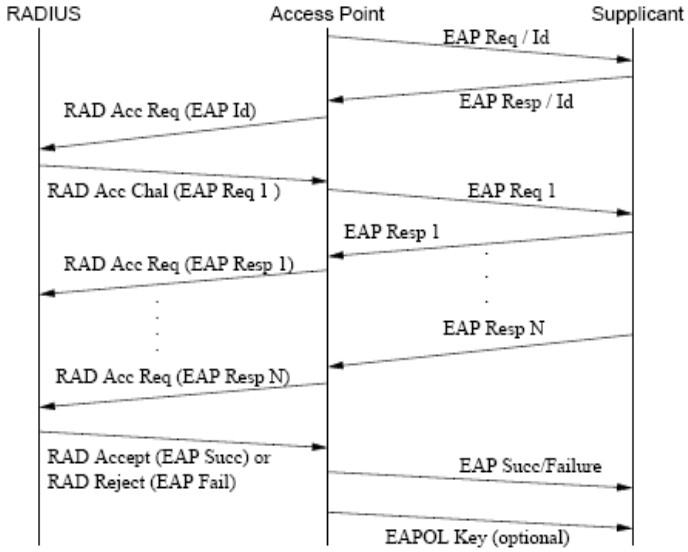

Fig. 3. *A complete 802.1X authentication session showing the EAP and*

RADIUS messages.

This article will not explore AES-CCM any further since it is well documented elsewhere, and has little interaction with interworking.

B. Authentication and Access Control

In a wireless environment, where network access cannot be restricted by physical perimeters, a security framework must provide *network access authentication*. WPA provides mechanisms to restrict network connectivity (at the MAC layer) to authorized entities only via 802.1X. Network connectivity is provided through the concept of a port, which depends on the particular context in which this mechanism is used. In IEEE 802.11, a network port is an *association* between a station and an access point.

The IEEE 802.1X standard provides an *architectural framework* on top of which one can use various authentication methods such as certificate-based authentication, smartcards, one-time passwords, etc. It provides *port-based* network access control for hybrid networking technologies, such as Token Ring, FDDI(802.5), IEEE 802.11 and 802.3 local area networks. WPA leverages the 802.1X mechanism for wireless 802.11 networks.

WPA provides a security framework by abstracting three entities as specified in the IEEE 802.1X standard [44]: the *supplicant*, the *authenticator* or network port, and the *authentication server*.

A *supplicant* is an entity that desires to use a service (MAC connectivity) offered via a port on the *authenticator* (switch, access point). Thus for a single network there would be many ports available (access points) through which the supplicant can authenticate the service. The supplicant authenticates via the authenticator to a central *authentication server* which directs the authenticator to provide the service after successful authentication. Here it is assumed that all the authenticators communicate with the same backend server. In practice this duty might be distributed over many servers for load-balancing or other concerns, but for all practical purposes, we can regard them as a single logical authentication server without loss of generality.

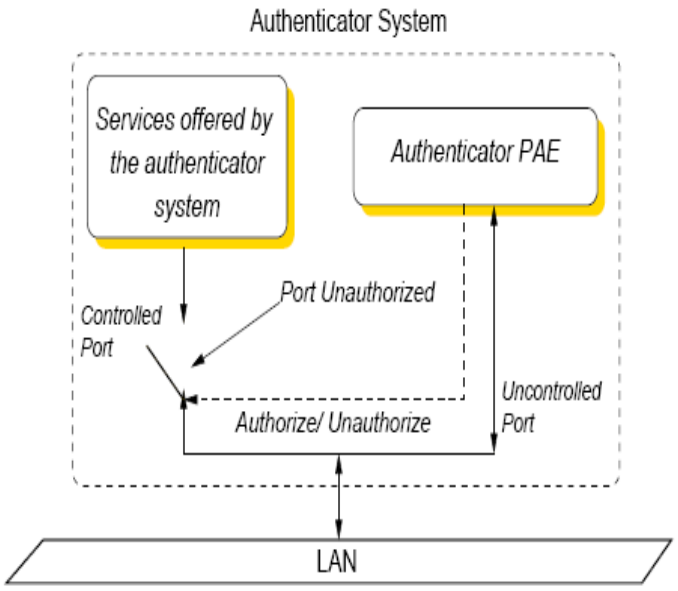

Fig. 4. *The Uncontrolled and Controlled ports in the authenticator*

The IEEE 802.1X standard employs the *Extensible Authentication Protocol* (EAP [45]) to permit a wide variety of authentication mechanisms. EAP is built around the *challengeresponse* communication paradigm. There are four types of messages: EAP *Request*, EAP *Response*, EAP *Success* and EAP *Failure*. Figure 3 shows a typical authentication session using EAP. The EAP Request message is sent to the supplicant indicating a challenge, and the supplicant replies using the EAP Response message. The other two messages notify the supplicant of the outcome. The protocol is 'extensible', i.e. any authentication mechanism can be encapsulated within the EAP *request/response* messages. EAP gains flexibility by operating at the network layer rather than the link layer. Thus, EAP can route messages to a centralized server (an EAP server such as RADIUS) rather than have each network port (access point) make the authentication decisions.

The access point must permit EAP traffic before the authentication succeeds. In order to accommodate this, a *dualport* model is used. Figure 4 shows the dual-port concept employed in IEEE 802.1X. The authenticator system has two ports of access to the network: the *Uncontrolled port* and the *Controlled* port. The *Uncontrolled* port filters all network traffic and allows only EAP packets to pass. This model also enables *backward compatibility* with clients incapable of supporting the new security measure: an administrative decision could allow their traffic through the *Uncontrolled* port.

The EAP messages are themselves encapsulated. The *EAP Over LAN*(EAPOL) protocol carries the EAP packets between the authenticator and the supplicant. It primarily [44] provides EAP-encapsulation, and also has session *start*, session *logoff* notifications. An EAPOL *key* message provides a way of communicating a higher-layer (e.g. TLS) negotiated session key. The EAP and EAPOL protocols do not contain any measures for integrity or privacy protection.

The authentication server and the authenticator communicate using the *Remote Authentication Dial-In User Service* (RADIUS) protocol [46]. The EAP message is carried as an attribute in the RADIUS protocol. The RADIUS protocol contains mechanisms for per-packet authenticity and integrity verification between the AP and the RADIUS server.

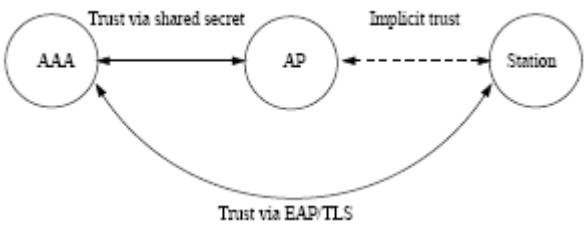

Fig. 5. *The Trust relations in TGi.*

CONCLUSIONS

As our lives depend more and more on wireless communication, security has become a pivotal concern of service providers, engineers, and protocol designers who have learned that obscurity does not guarantee security and that ad-hoc remedies only complicate matters. Instead, good security is developed in an open environment with the collaboration of experts. However, increased interest in the interworking of cellphone and WLAN systems introduces new challenges.

Centralized interworking authentication schemes have been proposed, but face scalability issues. Context transfer schemes are designed to address these scalability issues and are a promising area of future research.

REFERENCES

[1] "Bluetooth specification," http://www.bluetooth.org/spec/, 2001.

[2] Third Generation Partnership Project 2 (3GPP2), "Wireless IP Network Standard, P.S0001-B v1.0," *3GPP2 Techinical Specifications*, Oct. 2002.

[3] Third Generation Partnership Project, "General Packet Radio Service (GPRS); Service description (Stage 2), TS 23.060 v6.4.0," *3GPP2 Techinical Specifications*, Jan. 2004.

[4] Salkintzis, Ke. et al., "WLAN-GPRS Integration for Next-Generation Mobile Data Networks," *IEEE Wireless Communications*, Oct. 2002.

[5] J. Ala-Laurila, J. Mikkonen, and J. Rinnemaa, "Wireless LAN Access Network Architecture for Mobile Operators," *IEEE Communications Magazine*, pp. 82–89, Nov. 2001.

[6] Pahlavan, K. et al., "Handoff in Hybrid Mobile Data Networks," *IEEE Personal Communications*, Apr. 2000.

[7] M. Buddhikot, G. Chandranmenon G., S. Han, Y. W. Lee, S. Miller S., and L.Salgarelli, "Integration of 802.11 and Third Generation Wireless Data Networks," *IEEE INFOCOM 2003*, Apr. 2003.

[8] M. Buddhikot and G. Chandranmenon and Seungjae Han and Yui-Wah Lee and S. Miller and L. Salgarelli, "Design and Implementation of a WLAN/CDMA2000 Interworking Architecture," *IEEE Communications Magazine*, Nov. 2003.

[9] Third Generation Partnership Project, "3GPP system to Wireles Local Area Network (WLAN) interworking; System description, TS 23.234, v6.0.0," *3GPP2 Techinical Specifications*, Apr. 2004.

[10] IEEE, "Draft Amendment to STANDARD FOR Telecommunications

and Information Exchange Between Systems-LAN/MAN Specific Requirements. Part 11: Wireless Medium Access Control and Physical Layer(PHY) Specifications: Medium Access Control (MAC) Security Enhancements," *IEEE Standard 802.11i*, May 2003.

[11] Third Generation Partnership Project, "Digital cellular telecommunications system (Phase 2+);

Performance Requirements on Mobile Radio Interface, TS 44.013 v5.0.0, R5," *3GPP Techinical Specifications*, June 2002.

[12] A. Mishra, M. Shin, J. Nick L. Petroni, T. C. Clancy, and W. A. Arbaugh, "Pro-active Key Distribution using Neighbor Graphs," *IEEE Wireless Communications Magazine*, Feb. 2004.

[13] "FCC." [Online]. Available: http:// wireless.fcc.gov / services / cellular/ operations/fraud.html

[14] W. Millan, "Cryptanalysis of the alleged CAVE algorithm," in *Proceedings of International Conference on Information Security and Cryptology (ICISC 1998)*, Dec. 1998.

[15] B. Schneier, J. Kelsey, and D. Wagner, "Cryptoanalysis of the Cellular Message Encryption Algorithm," in *Proceedings of Crypto'97*, Aug. 1997.

[16] D. Wagner, B. Schneier, and J. Kelsey, "Cryptanalysis of ORYX," in *Fifth Annual Workshop on Selected Areas in Cryptography (WSK)*, Aug. 1998.

[17] L. Pesonen, "Gsm interception." [Online]. Available: http: //www.dia.unisa.it/professori/ads/corso-security/www/CORSO- 900/ a5%/Netsec/netsec.html

[18] Greg Rose, "Authentication and Security in Mobile Phones," *Australian Unix User's Group conference AUUG99*, Sept. 1999.

[19] P. Ekdahl and T. Johansson, "Another Attack on A5/1," in *IEEE International Symposium on Information Theory(ISIT) 2001, Washington D.C.*, June 2001.

[20] Clint Smith et. al, Ed., *3G Wireless Networks*. McGraw-Hill Telecom, 2002.

[21] Mark Johnson, "Revenue Assurance, Fraud and Security in 3G Telecom Services," *Journal of Economic Crime management, JECM Fall 2002*, vol. 1, no. 2, 2002.

[22] G. Koien, "An Introduction To Access Security in UMTS," *IEEE Wireless Communications Magazine*, pp. 8–18, Feb. 2004.

[23] Third Generation Partnership Project, "3G Security; Security architecture (Release 6), 3GPP TS 33.102 v6.0.0," *3GPP Techinical Specifications*, Sept. 2003.

[24] ——, "Technical Specification Group Terminals; UICC-terminal interface; Physical and logical characteristics (Release 6), 3GPP TS 31.101 v6.2.0," *3GPP Techinical Specifications*, June 2003.

[25] ——, "Technical Specification Group Services and System Aspects; Personalisation of Mobile Equipment (ME); Mobile functionality specification (Release 5), 3GPP TS 22.022 v5.0.0," *3GPP Techinical Specifications*, Sept. 2002.