Wireless Network Security and Interworking

MINHO SHIN, JUSTIN MA, ARUNESH MISHRA, AND WILLIAM A. ARBAUGH

Invited Paper

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 paper is twofold. 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.

Keywords*—Communication system security, computer network security, data security, internetworking, land mobile radio cellular systems, wireless LAN.*

I. INTRODUCTION

Wireless communication technologies cover a whole spectrum from wireless personal area networks (WPANs), such as Bluetooth [1], to third-generation (3G) cellular networks, such as CDMA2000 [2] and UMTS [3]. Despite such variety, opinions differ on which technology is optimal for satisfying all communication needs because of differing coverage and bandwidth limitations. For example, 3G networks provide widespread coverage with limited bandwidth (up to 2 Mb/s). However, wireless LANs (WLANs, IEEE Std. 802.11) provide high bandwidth (up to 54 Mb/s) with relatively smaller coverage area. For ubiquitous and high-performance wireless networking services, the *interworking* between wireless networks is extremely important. Most interworking studies have been dedicated to the integration of 3G and WLAN (see [4]–[9]).

Cellular and WLAN systems face distinct security challenges, and each has addressed security in unique (although not necessarily perfect) ways. Although fraudulent access has been reduced in 3G systems compared to previous generations, the major role of 3G in future packet-switched services introduces new challenges regarding security. And the weakness of WLAN's original security architecture, Wired Equivalent Privacy (WEP), spurred the creation of the Wi-Fi Protected Access (WPA) security architecture by the Wi-Fi Alliance and the IEEE 802.11i task group [10].

Security and performance are major challenges to the interworking of 3G and WLAN, especially for access control and privacy of mobile stations. The composition of two secure architectures may produce an insecure result. This occurs because of differing, possibly contradictory, security assumptions—e.g., the compromise of a session in a WLAN network may endanger subsequent sessions in 3G systems. Furthermore, support for high-bandwidth service with mobility demands a highly efficient authentication mechanism during handover. When a mobile station switches connectivity to a different network, the mobile station and the network have to authenticate each other. However, the authentication process required by each individual network tends to be complicated and costly. For example, the GSM technical specification on performance requirements [11] assumes that the mobile station responds to an authentication request from the network in *just under* 1 s. In WLAN, EAP-TLS authentication takes about 800 ms [12]. Long authentication delays during handover can cause a disruption of service that is perceivable by users.

We organize the rest of this paper as follows. We give historical perspective on the security of cellular systems in Section II and discuss current practice of 3G systems in Section III. Section IV provides background on WLAN security in the past, and Section V provides background on current WLAN security protocols. We describe interworking problems and the state of the art in Section VI and conclude in Section VII.

II. SECURITY IN CELLULAR SYSTEMS

The cellular phone industry has been experiencing revenue losses of more than US$150 million per year due to illegal usage of their services [13]. As the cellular system

Manuscript received September 23, 2004; revised January 5, 2005.

M. Shin, A. Mishra, and W. A. Arbaugh are with the Department of Computer Science, University of Maryland, College Park, MD 20742 USA (e-mail: mhshin@cs.umd.edu; arunesh@cs.umd.edu; waa@cs.umd.edu).

J. Ma is with the University of California, San Diego, La Jolla, CA 92093 USA (e-mail: jtma@cs.umd.edu).

Digital Object Identifier 10.1109/JPROC.2005.862322

evolved, newly employed security features reduced the feasibility of technical fraud. However, as 3G 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 ongoing 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 Advanced Mobile Phone Service (AMPS) was launched as the first commercial analog wireless phone system (Chicago, IL, 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 United States) and GSM (in Europe) are the major two 2G systems. Authentication in IS-41 uses the Cellular Authentication and Voice Encryption (CAVE) 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 Cellular Message Encryption Algorithm (CMEA) 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, Global System for Mobile Communications (GSM[1]) has grown to be the most popular mobile phone system in the world. GSM authenticates the subscriber through a challenge-response method similar to the one in IS-41. However, GSM uses a longer master key (128 bits) stored in a removable Subscriber Identity Module (SIM), which enables flexible deployment.

At one point in time, the GSM Memorandum of Understanding Group (MoU) 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 an 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 underwent the review process to address these flaws.

III. Security in 3G

2G systems have successfully addressed the problems of 1G (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 are not well suited to data communication [20]. The increasing demand for electronic commerce, multimedia communications, other Internet services necessitated the development of more advanced 3G technology.[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 paper.

A. *Security Challenges in 3G*

3G systems face new security challenges; new revenue-related frauds will emerge in the context of a new billing model based on data volume and quality of service [21]. Being an IP network, 3G and its users are exposed to the full range of threats that Internet service providers (ISPs) and their consumers currently face on the Internet. Due to limited storage and processing power of cellular phones, 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.

[1] Originally, GSM stood for Group Special Mobile.

[2] This paper does not discuss 2.5G systems, where limited packet data services are introduced. 2.5G systems include General Packet Radio Service (GPRS), Enhanced Data Rates for Global Evolution (EDGE), High-Speed Circuit Switched Data (HSCSD), and CDMA2000 phase 1. Refer to [20] for more details.

B. Security in UMTS

UMTS is an evolution of GSM in many aspects including security [22]. Security in UMTS includes enhancements such as mutual authentication and stronger encryption with 128-bit key lengths. The UMTS security architecture [23] defines the following security features. *Network access security*, the main focus of this paper, enforces access control of users and mobile stations, data confidentiality, data integrity, and user identity privacy. We elaborate on this security feature later on in the section. *Network domain security* enables nodes within the provider domain to securely exchange signaling data and protect against attacks on the wire-line network. The User Services Identity Module (USIM) is an application running on a removable smart card. *User domain security* secures the link between the user and the USIM and between the USIM and the terminal. The user-to-USIM link is protected by a shared secret stored securely in the USIM (e.g., a PIN) or provided interactively by the user [24]. The USIM-to-terminal link is also protected by a shared secret [25]. *Application domain security* enables applications in the user and provider domain to securely exchange messages [26]. *Visibility* ensures that security features are transparent to the user—so users are informed of security-related items such as access network encryption and level of security. *Configurability* allows the user to configure the security features in operation such as cipher algorithms. UMTS provides *user identity confidentiality*—in addition to *location confidentiality* and *user untraceability*—by using a temporary identity, a Temporary Mobile Station Identifier (TMSI).

C. AKA Protocol in UMTS

UMTS achieves network access security using the Authentication and Key Agreement (AKA) protocol [23]. Because CDMA2000 also adopted AKA with slight enhancement, the following description of AKA protocol also covers most of the security features in CDMA2000. The AKA protocol was developed by fixing and expanding the authentication method in GSM. Unlike GSM, where only the network verifies user's authenticity, AKA provides mutual authentication where both parties can verify one another's identity.

There are three entities involved in the authentication process: the user (MS or USIM), the serving network (VLR or SGSN), and the home environment (HLR/AuC). The serving network is the actual network to which the user connects. The Visitor Location Register (VLR) handles circuit-switched services and the Serving GPRS Support Node (SGSN) handles packet-switched services. The home environment is the network where the user is originally subscribed. The Home Location Register (HLR) contains the subscription database and it usually resides next to the Authentication Center (AuC)—thus we refer to them together as HLR/AuC. HLR/AuC plays a central role in the authentication process.

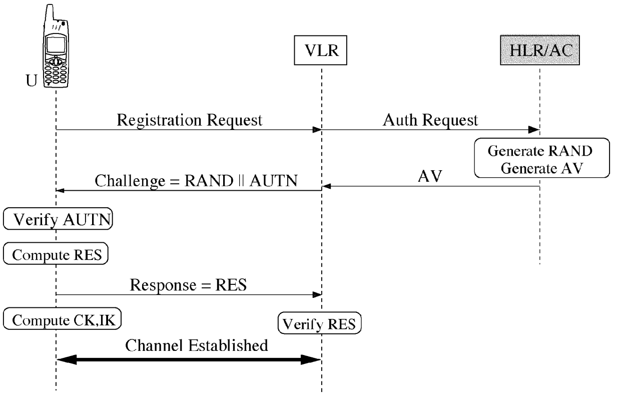

Fig. 1. AKA: Authentication in 3G (UMTS and CDMA2000).

AKA has three stages: initiation, transfer of credentials, and challenge–response exchange (see Fig. 1). During the initiation stage, the MS provides the network with its identity, either the IMSI or TMSI.[3] Based on the identity it receives, the network initiates the authentication procedure [22].

In the second stage, the HLR/AuC transfers security credentials of the specified user to VLR/SGSN. The establishment of a secure channel between HLR/AuC and VLR/SGSN may use a protocol such as Mobile Application Part (MAPsec) [27]. The *authentication vector* (AV) is the set of credentials transferred from HLR/AuC to SGSN/VLR in the form of a quintuple, $\langle$RAND, XRES, CK, IK, AUTN$\rangle$. The HLR/AuC may send multiple AVs to the SGSN/VLR for a specific user.

To generate an AV, the HLR/AuC begins by retrieving the user-specific 128-bit master key K from its subscriber database and generating RAND (the random challenge) using function $f0$ [28]:

$$\text{RAND} = f0(internal\ state).$$

From K and RAND, HLR/AuC generates XRES, CK, IK, AUTN as follows:

$$\begin{aligned}\text{XRES} &= f2(K, \text{RAND})\\ \text{CK} &= f3(K, \text{RAND})\\ \text{IK} &= f4(K, \text{RAND})\\ \text{AUTN} &= \text{SQN} \oplus \text{AK}||\text{AMF}||\text{MAC}\end{aligned}$$

where

$$\begin{aligned}\text{MAC} &= f1(K, \text{SQN}||\text{RAND}||\text{AMF})\\ AK &= f5(K, \text{RAND.})\end{aligned}$$

[3] To support fast handover between different VLR/SGSNs within the same serving network domain, the newly visited VLR/SGSN is allowed to request the IMSI and other confidential information from the previously visited VLR/SGSN. In this case, the mobile does not need to send its IMSI, which is normally transmitted in clear form without encryption.

XRES is the expected response corresponding to RAND—the USIM should be able to generate the same XRES to prove that it possesses the shared secret key K. The 128-bit CK and IK are the cipher key and integrity key for the resulting session. The AUTN, the authentication token, consists of SQN, AMF, and MAC. In AUTN, a sequence number SQN is protected against replay attack, and AK (anonymity key) is XORed with SQN to avoid identity tracking by observing a series of SQNs. AMF is an information field.[4]

In the last stage, the USIM and the VLR/SGSN authenticate each other through a challenge–response exchange. After VLR/SGSN receives AVs from HLR/AuC regarding the USIM, it chooses one AV and sends $\langle \text{RAND}, \text{ AUTN} \rangle$ to the USIM. With possession of master key K, RAND, AUTN, and the set of functions $f1, f2, \ldots, f5$, the USIM first computes SQN as

$$\text{SQN} = (\text{SQN} \oplus AK) \oplus f5(K, \text{RAND})$$

and detects possible replay attacks by checking if the retrieved SQN is within a certain range of its own SQN value. Then, the USIM verifies the VLR/SGSN's possession of the master key K by checking if the MAC is correct, i.e,

$$\text{MAC} = f1(K, \text{SQN}||\text{RAND}||\text{AMF}).$$

Once verified, the USIM calculates RES and transmits it to the VLR/SGSN

$$RES = f4(K, \text{RAND}).$$

Now the VLR/SGSN can verify if the USIM has the correct master key K by simply comparing RES from the USIM with XRES in the AV. After successful authentication, USIM can calculate CK and IK using $f3$ and $f4$, respectively, thus establishing a secure wireless channel. Fig. 2 summarizes the verification process.

The encryption and integrity functions are specified in [29]. They are based on the KASUMI block cipher [30], derived from Mitsubishi Electric Corporation's MISTY1 algorithm.

D. Access Security in CDMA2000

CDMA2000 [2] made a significant departure from the original CDMAs 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 UIM Authentication Key (UAK) 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.

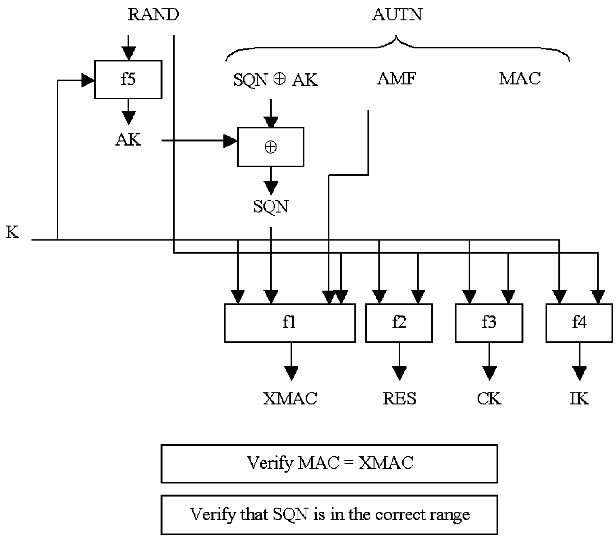

Fig. 2. AKA: Verification of network by the client.

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.

E. Security Issues in AKA

The separation of the AV generation and authentication procedures characterize AKA. In terms of performance, the distributed processing of AKA facilitates faster roaming, but requires a trust relationship between roaming partners.

In AKA, the network authenticates the user by a one-pass challenge–response mechanism, but the user only authenticates the network by verifying a MAC. AKA in its current form does not provide *full* mutual authentication. Full mutual authentication would be assured if the user authenticated the network by a challenge–response mechanism. However, the use of mutual challenge–responses was abandoned for performance reasons.

Despite the use of temporary identity, the user must transmit the permanent identity (IMSI) in plaintext when registering for the first time. The use of a trusted third party can resolve this concern.

[4] Example uses of AMF can be found in Annex F, 3G TS 33.102 [23].

IV. Overview of 802.11

Wireless data networks based on the IEEE 802.11 or Wi-Fi standard have seen tremendous growth in both the consumer and enterprise spaces, so security issues in this area have very broad impact. This section presents the basics of the original 802.11 security architecture.

A. Authentication

1) Open System Authentication: Open system authentication is the default authentication protocol for 802.11. As the name implies, open system authentication authenticates anyone who requests access.

2) Shared Key Authentication: Shared key authentication uses a standard challenge and response along with a shared secret key to provide authentication. The station wishing to authenticate, the *initiator*, sends an authentication request management frame indicating that it wishes to use "shared key" authentication. The recipient of the authentication request, the *responder*, responds by sending an authentication management frame containing 128 octets of challenge text to the *initiator*. The challenge text is generated by using the WEP pseudorandom number generator (PRNG) with the "shared secret" and a random initialization vector (IV). Once the *initiator* receives the management frame from the *responder*, it copies the contents of the challenge text into a new management frame body. This new management frame body is then encrypted with WEP using the "shared secret" along with a new IV selected by the initiator. The encrypted management frame is then sent to the *responder*. The *responder* decrypts the received frame and verifies that the 32-bit CRC integrity check value (ICV) is valid, and that the challenge text matches that sent in the first message. If they do, then authentication is successful. If the authentication is successful, then the initiator and the responder switch roles and repeat the process to ensure mutual authentication.

B. Access Control

1) Closed Network Access Control: Closed Network [35] is a proprietary access control mechanism. With this mechanism, a network manager can use either an *open* or a *closed* network. In an open network, anyone is permitted to join the network. In a closed network, only those clients with knowledge of the network name, or SSID, can join. In essence, the network name acts as a *shared secret*.

2) Access Control Lists: Another mechanism used by vendors (but not defined in the standard) to provide security is the use of access control lists based on the ethernet MAC address of the client. Each access point can limit the clients of the network to those using a listed MAC address. If a client's MAC address is listed, then they are permitted access to the network. If the address is not listed, then access to the network is prevented.

C. Security Problems

The security of 802.11 networks was completely decimated over a period of a few years beginning in 2000, and the protocol is used in some academic classes as an example of how *not* to design a security architecture.

First, Jesse Walker of Intel presented the IEEE with the problems during a meeting of the 802.11 standards body [36]. Next, Nikita Borisov, Ian Goldberg, and David Wagner at the University of California, Berkeley, independently found the same problems as well as new ones [37]. Arbaugh, Shankar, and Wan at the University of Maryland identified flaws in the access control and authentication methods in 2001 [38]. Fluhrer, Mantin, and Shamir broke the mode in which RC4 was being used in 802.11 [39], and finally Arbaugh and Petroni demonstrated that the mitigation technique to prevent the Fluhrer attack actually made the problem worse [40].

The problems with 802.11 security have been published in countless papers such as the ones cited above as well as others [41]. Rather than focus on the problems, we feel it is best to describe the solutions.

V. 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 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.

This paper 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, smart cards, one-time passwords, etc. It provides *port-based* network access control for hybrid networking technologies,

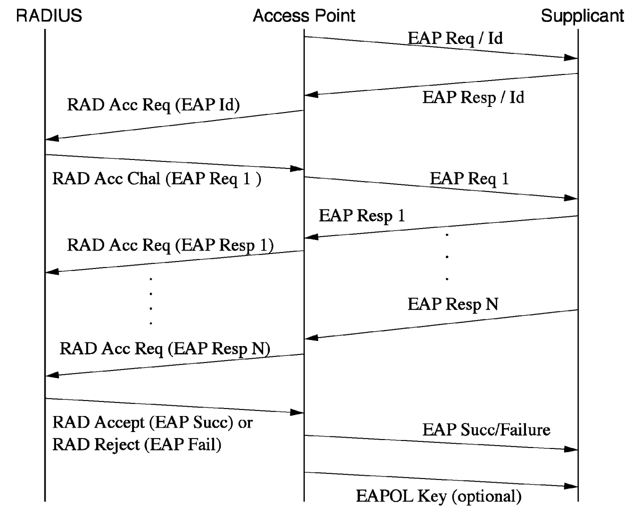

Fig. 3. A complete 802.1X authentication session showing the EAP and RADIUS messages.

such as Token Ring, FDDI(802.5), IEEE 802.11, and 802.3 LANs. 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.

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 *challenge–response* communication paradigm. There are four types of messages: EAP *Request*, EAP *Response*, EAP *Success*, and EAP *Failure*. Fig. 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.

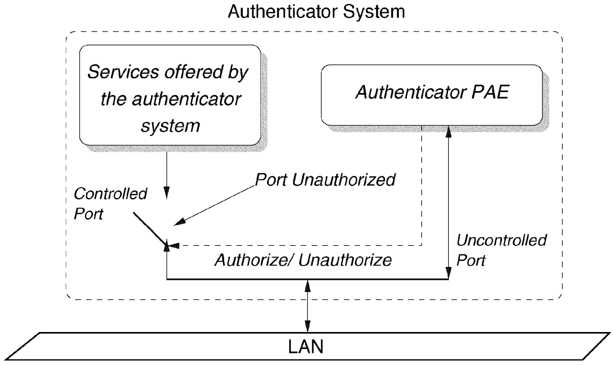

Fig. 4. The Uncontrolled and Controlled ports in the authenticator.

The access point must permit EAP traffic before the authentication succeeds. In order to accommodate this, a *dual-port* model is used. Fig. 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* and 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.

C. Known Security Problems

There are essentially three known security issues with WPA 2. The first is that the 802.11 medium access control protocol is ripe with denial of service attacks [47]–[49]. This is because the management frames within the protocol are not protected nor authenticated. As a result, anyone can *spoof* management messages providing the ability to disrupt user sessions [50]. The second, and a direct result of the first problem, is that sessions can be hijacked when encryption is not utilized [51]. Finally, the trust relationships within the WPA architecture are of concern. We will discuss this more, since it can potentially create significant problems with interworking.

Many people believe that the access point is a trusted party, but this belief is not completely correct. Fig. 5 depicts the trust relationships between entities. The solid arrows represent an explicit mutual trust relationship while the dotted line

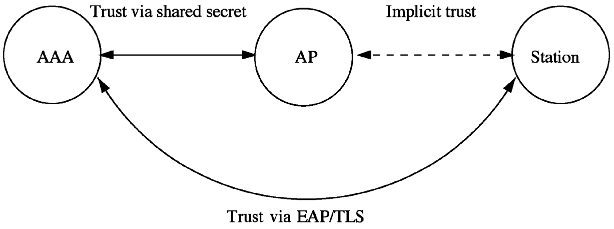

Fig. 5. The trust relations in TGi.

represents an implicit trust relationship that *must* be created in order to make security claims about the communications path. This trust relationship between the AP and the STA is transitive and derived from the fact that the station trusts the AAA server and the AAA server trusts the AP. This, unfortunately, is not ideal, since in many cases the trust relationship between the AAA server and the AP will not exist if shared keys, or better yet IPsec, are not used to protect the RADIUS traffic. However, the majority of the AP vendors in TGi had a strong desire for an inexpensive AP which was more of a relay than a participant in the communications.

VI. 3G/WLAN Interworking

In this section, we explore the security considerations of 3G/WLAN integration with emphasis on authentication and key distribution during handover.

A. Roaming Model and Scenario

In this paper, we focus on internetwork handovers[5] under loosely coupled architecture [7] where each system may provide different security features. We also assume that a mobile station (MN) has a security association (e.g., shared secret key) with its home network established out of band, but might not have security associations with foreign networks. Internetwork authentication can be especially challenging in this scenario. Let us proceed with an illustrative example to introduce the different methods of interworking.

A Chicago resident, Bill, is traveling to New York City by train. Bill's 3G service provider, IL-3G, is out of service in New York. However, when entering New York state, he comes in range of NY-3G (the local 3G provider who has a roaming agreement with IL-3G) and associates with it. Upon arriving at the Grand Central Terminal in Manhattan, Bill is in range of NY-WLAN (the local WLAN provider). Bill wants to use the WLAN for higher bandwidth, but his method of access depends on one of the following possible relationships among the three providers (IL-3G, NY-3G, NY-WLAN).

- (Case 1) NY-WLAN operates independently, and Bill already has an account with NY-WLAN.
- (Case 2) IL-3G, Bill's home network, has a roaming agreement with NY-WLAN.
- (Case 3) IL-3G and NY-WLAN do not have a roaming agreement, but NY-3G and NY-WLAN do.

Each case represents a typical authentication scenario as explained below.

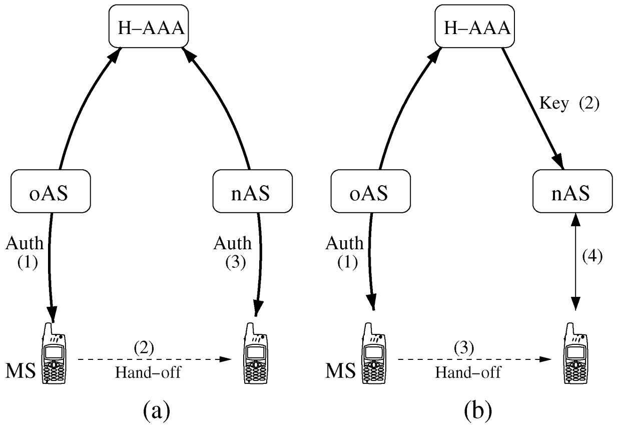

Fig. 6. Centralized authentication methods. The order of event is denoted in the parenthesis. (a) Centralized authentication. (b) Proactive key distribution.

B. Independent Internetwork Authentication

Independent internetwork authentication makes no effort at integration. Under Case 1, where the MN (Bill) already has a security association with the desired foreign network (NY-WLAN), the trivial solution is to authenticate by the new network's protocol (for example, EAP-TLS authentication in WLAN). This scheme does not require a trust relationship between networks. (A trust relationship between networks means there is a roaming agreement between them, and there exists a secure channel for confidential communication regarding subscribers.) Accounting and billing of each network should be independent.

C. Centralized Internetwork Authentication

If Bill's home network, IL-3G, has a roaming agreement with NY-WLAN (Case 2), then Bill can use NY-WLAN's service without registration. NY-WLAN authenticates Bill's account with help from IL-3G. Most research on internetwork authentication assumes that visiting networks collaborate with the home network [8], [52]–[56] [see Fig. 6(a)]. This approach requires the mobile station to authenticate itself to its home network through the visiting network. 3G wireless communication systems such as UMTS and CDMA2000 already have such authentication mechanisms in place (e.g., AKA protocol [23], [32]).

1) The State of the Art: Centralized internetwork authentication is the process by which the foreign network (NY-WLAN in the example) ensures that the client is a legitimate user of the home network (IL-3G). Authentication involves three entities: the MN, the foreign network AAA server (oAS and nAS in Fig. 6), and the home network AAA server (H-AAA in Fig. 6).

There are proposed protocols based on EAP, such as EAP-SIM [53] and EAP-AKA [54]. EAP provides a protocol framework for challenge–response based authentication and key distribution. Typically, the authenticator at the foreign network relays EAP traffic to the home network or retrieves authentication vectors (challenge–response pairs) from the home network. EAP-SIM [53] is based on the GSM authentication protocol. However, the original

[5] We use roam, handoff, and handover interchangeably.

GSM authentication has weaknesses such as the lack of mutual authentication and a weak 64-bit cipher key—these are problems that EAP-SIM tries to address. EAP-AKA [54] is an EAP version of the AKA protocol used by 3G systems. EAP-AKA is stateful and requires a synchronized sequence number between the MN and H-AAA. EAP-SKE is another authentication protocol over EAP [52]. The UMTS interworking security specification adopts the centralized approach for UMTS/WLAN integration [57]. However, EAP lacks support for identity protection, protected method negotiation, and protected termination, to name a few [58]. Recently, possible man-in-the-middle attacks on EAP-AKA and EAP-SIM were reported in [59]. By wrapping the EAP protocol within TLS,[6] protected EAP (PEAP) [58] addresses most of the deficiencies of EAP methods. The use of PEAP with EAP-AKA and EAP-SIM is currently under consideration [57].

Interdomain proactive key distribution is an extension of the existing intradomain fast handoff scheme by Mishra *et al.* [12]. The authors use *neighbor graphs* to capture handoff relationships between APs and predict the potential set of APs that a mobile node might associate with next. The AAA server, being aware of the neighbor graph, predistributes MKs to potential next APs, significantly reducing authentication latency. Bargh *et al.* [60] discusses the extension of intradomain proactive context distribution for interdomain handoffs. With the proposed scheme, typical message flow is as follows [see Fig. 6(b)].

1) oAS (old authentication server) detects MN's visit.
2) oAS requests H-AAA (home authentication server) for context distribution.
3) H-AAA calculates potential nASs (new authentication servers).
4) H-AAA predistributes context to nASs.

2) Discussion: For centralized authentication to work, the foreign network and home network should have roaming agreements or preconfigured security associations. With N networks, the overhead of roaming agreement is $O(N^2)$. Salgarelli *et al.* [52] attempt to address this problem by introducing a dedicated third party, an AAA-broker that maintains all required security associations between networks. This scheme reduces the total number of security associations to $O(N)$, i.e, between the broker and N networks. Thus, whenever a foreign network needs security associations with a home network, it only needs to request the broker to provide security association with the home network.

The inherent problem of centralized approaches is the high authentication latency caused by long geographic distances and the number of proxy/relay agents between the home network and foreign network. To address this concern, Kim *et al.* [61] adapt 3G-like mechanisms to WLAN security using EAP [45] under an AAA framework [46], [62]. The paper introduces an AAA-broker which behaves as a foreign network in GSM authentication by relaying authentication requests to the home network and verifying the client with authentication vectors. The scheme requires that the broker is located close to the client and is trustworthy, requiring a strong security association between the broker and the home network. However, the scheme works only with simple challenge–response authentication protocols. Reference [63] investigates AAA-broker selection algorithms that minimize authentication cost.

Proactive key distribution schemes solve the authentication latency problem, but require reasonably accurate handoff prediction systems to be effective.

D. *Context Transfer*

In Case 3, Bill is already authenticated by the NY-3G service, but NY-WLAN has no roaming contract with his home network, IL-3G. Since NY-3G and NY-WLAN trust each other enough to share the subscriber's confidential information, NY-3G can provide Bill's security context to NY-WLAN to allow Bill to access the WLAN. *Context* is information on the current state of a client required to reestablish the service in a new network without having to perform the entire protocol exchange from scratch [64].[7] Security context may include the following [65]:

1) authentication state: identifiers of the client and previous authentication result;
2) authorization state: services and functions authorized to the MN;
3) communication security parameters: encryption algorithms, session keys such as encryption and decryption keys, and message authentication keys.

Context transfer has been considered as a solution in intranetwork handoffs [60], [66]–[68]. In the remainder of this section, we consider interdomain context transfer to support and facilitate interdomain handoffs.

Context transfer can occur between entities on different levels: from old access point (oAP) to new access point (nAP),[8] from old access router (oAR) to new access router (oAR), and from old authentication server (oAS) to new authentication server (nAS). With context transfer, the communication delay between visiting network and home network is replaced by a relatively smaller internetwork communication delay between adjacent networks. However, interdomain context transfers require strong trust relationships between two networks.

1) Reactive Context Transfer: With a reactive context transfer, the context is delivered from the old network to the new network after the mobile node visits the new network. The typical message flow is the following.

1) MN visits new network.
2) nAS obtains the address of oAS.
3) nAS requests context transfer to oAS.
4) oAS transfers context of MN to nAS.
5) After verifying the context, nAS allows MN to attach.
6) After handoff, H-AAA may optionally verify MN's authenticity.

[6] Not to be confused with EAP-TLS, where TLS is wrapped within EAP.

[7] We only consider context regarding layer 2 security.

[8] Without loss of generality, we denote 3G base stations also as oAP or nAP.

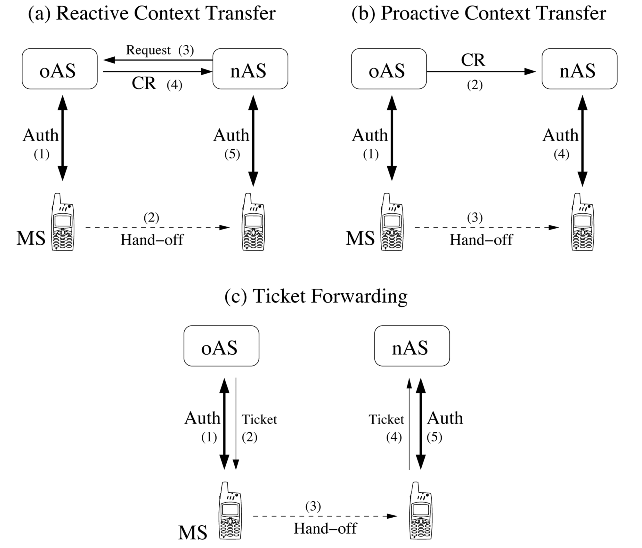

Fig. 7. Context transfer methods. The order of event is denoted in the parenthesis. (a) Proactive context transfer. (b) Reactive context transfer. (c) Ticket forwarding.

Fig. 7(a) illustrates the reactive context transfer with the order of event shown in parenthesis. There exist well-known solutions for intradomain reactive context transfer: Context Transfer Protocol (CTP, IETF [67]) and Inter Access Point Protocol (IAPP, IEEE Standard 802.11f [69]). The CTP is being defined by the Seamoby Working Group of IETF for layer 3 context transfer, from oAR to nAR. The layer 2 counterpart IAPP defines how nAP retrieves context from oAP, and the process involves a roaming server for reverse address mapping. Reference [60] describes how the combination of IAPP and CTP extends intradomain solutions to interdomain context transfer. Authors suggest encapsulating a L2 context in a L3 context to resolve addressing problems that prevent nAP from obtaining direct access to oAP.

Soltwisch *et al.* [70] describe a reactive context transfer protocol for seamless interdomain handovers, called IDKE (Inter Domain Key Exchange). The IDKE exploits CTP and IKE (Internet Key Exchange Protocol [71]) for the establishment of security associations and context transfer between access routers. To initiate a key establishment process between oAR and nAR, the MN issues nAR a token generated with a prior session key between MN and oAR. The token convinces oAR that MN has authorized the release of confidential information to nAR.

2) Proactive Context Transfer: With a proactive context transfer, the context transfer occurs before the mobile node visits the new network. There are two possibilities for proactive context transfer: soft handoff and prediction. With soft handoff, where the MN is connected to both old and new networks during the handoff period, the MN can notify oAS of the impending handoff and the destination network. In other cases, proactive context transfer requires a handoff prediction system. The following discussion considers prediction-based proactive context transfer schemes.

For intradomain handoffs, [68] exploits *neighbor graphs* to directly transfer context from oAP to potential nAPs. Reference [60] calls this *proactive context caching* and extends the method to interdomain handoff. The direct context transfer from oAS to nAS eliminates trust requirements between visiting and home networks, but requires trust relationships between old and new networks. In this case, trust between homeAS and nAS is implied by the transitivity of trust: trust between homeAS and oAS and between oAS and nAS. In contrast to proactive key distribution where the homeAS has a global view of neighbor graph, proactive context transfer only requires networks to have a local view of the neighbor graph. The following is the message flow of proactive context transfer.

1) oAS detects MN's visit.
2) oAS calculates potential nASs.
3) oAS predistributes context to nASs.

Fig. 7(b) illustrates the proactive context transfer.

3) Ticket Forwarding: Instead of sending context through the wired network, the oAS can issue a ticket (containing context) to the client and let the client provide nAS with the ticket upon visit. The nAS accepts the ticket only when it successfully verifies that oAS has issued the ticket. We include ticket forwarding among the other context transfer methods because homeAS is not involved during handoff.

The following illustrates typical process of ticket forwarding [see Fig. 7(c)].

1) oAS detects MN's visit.
2) oAS calculates potential nASs;
3) oAS issues tickets for each potential nAS;
4) oAS sends generated tickets to MN.
5) After handoff, MN provides nAS with corresponding ticket.
6) nAS verifies the ticket and accepts MN.

In step 2), oAS may need a handoff prediction system to determine the key to use for encrypting the ticket.

References [72] and [73] are good examples of ticket forwarding protocols. Kerberos [72] uses an *access grant ticket* for this purpose whereas [73] uses a *cookie*. Kerberos is a distributed authentication service that allows a client to prove its identity to a server, or verifier, without sending data across the network [74]. Rather than sending data directly to the verifier, an authentication server issues the client a ticket carrying an expiration time and a session key to be used in the next network. The authentication server signs the ticket itself and encrypts it with a secret key shared with the verifier. However, the weakness of the Kerberos password system was identified in [75]. Single sign-on (SSO) scheme [73] enables users to access multiple systems with a single authentication.

4) Discussion: Context transfer allows a new network to verify the authenticity of a MN without performing authentication from scratch. The main benefit of context transfer is performance, but it also allows for the flexible trust relationships: the visiting network and home network may not have explicit an trust relationship, but intervening networks might form a chain of trust between them. Accounting and billing at the visiting network is an open issue. Regarding security, context transfer has a very strong assumption that nAS believes that the security association between the MN and oAS is secure. However, the level of security differs from network to network, especially when they are heterogeneous. To impose its security level on the MN, the nAS can perform the full authentication process after the MN is allowed to access the network via context transfer. However, this *post hoc* authentication is not as secure as doing full authentication before the MN gains privileged access to the network.

To address the weakness of context transfer, the new network can perform full authentication or reauthentication of the MN with a master key delivered in the context. The previous network (oAS) and the mobile node (MN) calculate a new MK by hashing the current session key as

$$\mathrm{newMK} = \mathrm{PRF}(\mathbf{session\ key}, \mathrm{nAS})$$

where PRF is a pseudorandom function, and the oAS includes newMK along with the MN identifier in the context to nAS. At the time of handoff, nAS and MN share newMK, which is confidential if the previous session is secure and context transfer is properly protected. Then, nAS and MN can begin the full authentication process to ensure both share the same newMK and to establish strong session keys for further communications. Note that this method still excludes H-AAA from the process. It also resolves the *entropy mismatch problem*, where the new network requires higher entropy for encryption keys while the session key in old network has lower entropy. If the network is concerned about performance, it can perform reauthentication instead of full authentication. For example, EAP-TLS provides a reauthentication feature in which MN and nAS resume a previously established association and skip master key generation. To this end, oAS includes a new 48-byte MK and 32-byte session ID in the context, both generated by PRF.

VII. Conclusion

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" 2001 [Online]. Available: http://www.bluetooth.org/spec/

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

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

[4] K. Salkintzis *et al.*, "WLAN-GPRS integration for next-generation mobile data networks," *IEEE Wireless Commun.,* vol. 9, no. 5, pp. 112–124, Oct. 2002.

[5] J. Ala-Laurila, J. Mikkonen, and J. Rinnemaa, "Wireless LAN access network architecture for mobile operators," *IEEE Commun. Mag.,* vol. 39, no. 11, pp. 82–89, Nov. 2001.

[6] Pahlavan K. *et al.*, "Handoff in hybrid mobile data networks," *IEEE Pers. Commun.,* vol. 7, no. 2, pp. 34–47, Apr. 2000.

[7] M. Buddhikot, G. Chandranmenon, S. Han, Y. W. Lee, S. Miller, and L. Salgarelli, "Integration of 802.11 and third generation wireless data networks," in *Proc. IEEE INFOCOM 2003* vol. 1, pp. 503–512.

[8] M. Buddhikot, G. Chandranmenon, S. Han, Y.-W. Lee, S. Miller, and L. Salgarelli, "Design and implementation of a WLAN/CDMA2000 interworking architecture," *IEEE Commun. Mag.,* vol. 41, no. 11, pp. 90–100, Nov. 2003.

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

[10] *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] *3GPP Technical Specifications*, Digital cellular telecommunications system (Phase 2+); performance requirements on mobile radio interface, TS 44.013 v5.0.0, R5, Third Generation Partnership Project, Jun. 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 Commun.,* vol. 11, no. 1, pp. 26–36, 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 *Proc. Int. Conf. Information Security and Cryptology (ICISC 1998)* pp. 107–119.

[15] B. Schneier, J. Kelsey, and D. Wagner, "Cryptanalysis of the cellular message encryption algorithm," in *Proc. Crypto'97* pp. 526–537.

[16] D. Wagner, B. Schneier, and J. Kelsey, "Cryptanalysis of ORYX," in *Proc. 5th Annu. Workshop Selected Areas in Cryptography (WSK)* 1998, pp. 296–305.

[17] L. Pesonen, GSM interception [Online]. Available: http://www.dia.unisa.it/professori/ads/corso-security/www/CORSO-9900/a5%/Netsec/netsec.html

[18] G. Rose, "Authentication and security in mobile phones," presented at the Australian Unix User's Group Conf. (AUUG99), Melbourne, Australia.

[19] P. Ekdahl and T. Johansson, "Another attack on A5/1," presented at the IEEE Int. Symp. Information Theory (ISIT) 2001, Washington, DC.

[20] C. Smith, Ed. *et al., 3G Wireless Networks*. New York: McGraw-Hill Telecom, 2002.

[21] M. Johnson, "Revenue assurance, fraud and security in 3G telecom services," *J. Econom. Crime Mgmt.* vol. 1, no. 2, Fall, 2002 [Online]. Available: http://www.jecm.org/02_fall_art3.pdf

[22] G. Koien, "An introduction to access security in UMTS," *IEEE Wireless Commun,* vol. 11, no. 1, pp. 8–18, Feb. 2004.

[23] *3GPP Technical Specifications*, 3G security; security architecture (Release 6), 3GPP TS 33.102 v6.0.0, Third Generation Partnership Project, Sep. 2003.

[24] *3GPP Technical Specifications*, Technical specification group terminals; UICC-terminal interface; physical and logical characteristics (Release 6), 3GPP TS 31.101 v6.2.0, Third Generation Partnership Project, Jun. 2003.

[25] *3GPP Technical Specifications*, Technical specification group services and system aspects; personalization of Mobile Equipment (ME); mobile functionality specification (Release 5), 3GPP TS 22.022 v5.0.0, Third Generation Partnership Project, Sep. 2002.

[26] *3GPP Technical Specifications*, Technical specification group terminals; security mechanisms for the (U)SIM application toolkit; Stage 2 (Release 5), 3GPP TS 23.048 v5.8.0, Third Generation Partnership Project, Dec. 2003.

[27] *3GPP Technical Specifications*, 3G security; network domain security; MAP application layer security (Release 5), 3GPP TS 33.200 v5.1.0, Third Generation Partnership Project, Dec. 2002.

[28] *3GPP2 Technical Specifications*, 3gpp2 s.s0055 version 1.0, Enhanced Cryptographic Algorithms, 3GPP2, Jan. 2002.

[29] *3GPP Technical Specifications*, 3G security; specification of the 3GPP confidentiality and integrity algorithms; document 1: f8 and f9 specification (Release 5), 3GPP TS 35.201 v5.0.0, Third Generation Partnership Project, Jun. 2002.

[30] *3GPP Technical Specifications*, 3G security; specification of the 3GPP confidentiality and integrity algorithms; document 2: KASUMI specification (Release 5), 3GPP TS 35.202 v5.0.0, Third Generation Partnership Project, Jun. 2002.

[31] *3GPP2 Technical Specifications*, 3gpp2 s.s0078 version 1.0, common security algorithms, 3GPP2, Dec. 2002.

[32] G. Koien and G. Rose, "Access security in CDMA2000, including a comparison with UMTS access security," *IEEE Wireless Commun.,* vol. 11, no. 1, pp. 19–25, Feb. 2004.

[33] *Secure Hash Standard*, FIPS Pub. 180-1, National Institute of Standards and Technology (NIST), May 1993.

[34] *Advanced Encryption Standard*, FIPS Pub. 197, National Institute of Standards and Technology (NIST), Nov. 2001.

[35] Lucent Orinoco, "User's guide for the ORiNOCO Manager's Suite," Nov. 2000.

[36] J. Walker, "Unsafe at any key size: An analysis of the WEP encapsulation," IEEE 802.11 committee, Tech. Rep. 03628E, Mar. 2000 [Online]. Available: http://grouper.ieee.org/groups/802/11/Documents/DocumentHolder/0-362.zi%p

[37] N. Borisov, I. Goldberg, and D. Wagner, "Intercepting mobile communications: The insecurity of 802.11" [Online]. Available: http://www.isaac.cs.berkeley.edu/isaac/wep-faq.html

[38] W. A. Arbaugh, N. Shankar, and J. Wang, "Your 802.11 network has no clothes," in *Proc. 1st IEEE Int. Conf. Wireless LANs and Home Networks* 2001, pp. 131–144.

[39] S. Fluhrer, I. Mantin, and A. Shamir, "Weaknesses in the key scheduling algorithm of RC4," in *Proc. 8th Annu. Workshop Selected Areas in Cryptography* 2001, pp. 1–24.

[40] N. Petroni and W. Arbaugh, "The dangers of mitigating security design flaws: a wireless case study," *IEEE Security Privacy,* vol. 1, no. 1, pp. 28–36, Jan. 2003.

[41] R. Housley and W. A. Arbaugh, "WLAN problems and solutions," *Comm. ACM,* vol. 46, no. 5, pp. 31–34, May 2003.

[42] R. Housely, D. Whiting, and N. Ferguson, Counter with cbc-mac (ccm) [submission to NIST] 2002 [Online]. Available: http://csrc.nist.gov/encryption/modes/proposedmodes/ccm/ccm.pdf,

[43] B. Aboba, L. Blunk, J. Vollbrecht, J. Carlson, and H. Levkowetz, "Extensible Authentication Protocol (EAP)," RFC 3748, Jun. 2004.

[44] *Standards for Local and Metropolitan Area Networks: Standard for Port Based Network Access Control*, IEEE Draft P802.1X/D11, Mar. 2001.

[45] L. Blunk and J. Vollbrecht, "PPP Extensible Authentication Protocol (EAP)," RFC 2284, Mar. 1998.

[46] C. Rigney, S. Willens, A. Rubens, and W. Simpson, "Remote Authentication Dial In User Service (RADIUS)," RFC 2865, Jun. 2000.

[47] J. Bellardo and S. Savage, "802.11 denial-of-service attacks: real vulnerabilities and practical solutions," presented at the USENIX Security Symp., Washington, DC, 2003.

[48] D. B. Faria and D. R. Cheriton, "DoS and authentication in wireless public access networks," in *Proc. 1st ACM Workshop Wireless Security (WiSe'02)* pp. 47–56.

[49] M. L. Lough, "A taxonomy of computer attacks with applications to wireless," Ph.D thesis, Virginia Polytechnic Institute, Blacksburg, Apr. 2001.

[50] R. Baird and M. Lynn, Airjack driver. [Online]. Available: http://802.11ninja.net/airjack

[51] A. Mishra, N. L. Petroni, and W. A. Arbaugh, "Security issues in IEEE 802.11 wireless local-area networks: a survey," *Wireless Commun. Mobile Comput. J. (Invited Paper),* vol. 4, no. 8, pp. 821–833, 2004.

[52] L. Salgarelli, M. Buddhikot, J. Garay, S. Patel, and S. Miller, "Efficient authentication and key distribution in wireless IP networks," *IEEE Wireless Commun.,* vol. 10, no. 6, pp. 52–61, Dec. 2003.

[53] H. Haverinen, "EAP SIM authentication (work in progress)," Internet Draft, IETF, draft-arkko-pppext-eap-sim-03.txt, Feb. 2002.

[54] J. Arkko and H. Haverinen, "EAP AKA authentication (work in progress)," Internet Draft, IETF, draft-arkko-pppext-eap-aka-12.txt, Apr. 2004.

[55] P. Funk and S. Blake-Wilson, "," EAP tunneled TLS authentication protocol (EAP-TTLS) (work in progress) Internet Draft, IETF, draft-ietf-pppext-eap-ttls-03.txt, Aug. 2003.

[56] R. Molva, D. Samfat, and G. Tsudik, "Authentication of mobile users," *IEEE Network,* vol. 8, no. 2, pp. 26–34, Mar.–Apr. 1994.

[57] *3GPP Technical Specifications*, 3G Security; Wireless Local Area Network (WLAN) interworking security, TS33.234 v6.1.0, R6, Third Generation Partnership Project, Jun. 2004.

[58] A. Palekar, D. Simon, J. Salowey, H. Zhou, G. Zorn, and S. Josefsson, "Protected EAP Protocol (PEAP) version 2 (work in progress)," Internet Draft, IETF, draft-josefsson-pppext-eap-tls-eap-08.txt, Jul. 2004.

[59] N. Asokan, V. Niemi, and K. Nyber, "Man-in-the-middle in tunnelled authentication protocols," in *Proc. 11th Cambridge Int. Workshop Security Protocols* 2003, pp. 15–24.

[60] M. S. Bargh, R. J. Hulsebosch, E. H. Eertink, A. Prasad, H. Wang, and P. Schoo, "Fast authentication methods for handovers between IEEE 802.11 wireless LANs," in *Proc. 2nd ACM Int. Workshop Wireless Mobile Applications and Services on WLAN Hotspots (WMASH)* 2004, pp. 51–60.

[61] H. Kim and H. Afifi, "Improving mobile authentication with new AAA protocols," presented at the IEEE ICC (Int. Conf. Communications), Anchorage, AK, 2003.

[62] P. R. Calhoun, G. Zorn, P. Pan, and H. Akhtar, "Diameter framework document (work in progress)," Internet Draft, draft-ietf-aaa-diameter-framework-09.txt, Feb. 2001.

[63] H. Kim, W. Ben-Ameur, and H. Afifi, "Toward efficient mobile authentication in wireless inter-domain," presented at the IEEE Applications and Services in Wireless Networks Conf., Berne, Switzerland, 2003.

[64] J. Kempf, "Problem description: Reason for performaing context transfers between nodes in an IP access network," RFC 3374, Sep. 2002.

[65] H. Wang and A. R. Prasad, "Security context transfer in vertical handover," presented at the IEEE 14th Int. Symp. Personal, Indoor and Mobile Radio Communications (PIMRC 2003), Beijing, China.

[66] R. Koodli and C. Perkins, "Fast handover and context relocation in mobile networks," *ACM SIGCOMM Comput. Commun. Rev.,* vol. 31, no. 5, pp. 37–47, Oct. 2001.

[67] M. Nakhjiri, C. Perkins, and R. Koodli, Context Transfer Protocol Internet Draft: draft-ietf-seamoby-ctp-01.txt, Mar. 2003.

[68] A. Mishra, M. Shin, and W. A. Arbaugh, "Context caching using neighbor graphs for fast handoffs in a wireless network," in *Proc. IEEE INFOCOM 2004* pp. 351–361.

[69] *Trial-Use Recommended Practice for Multi-Vendor Access Point Interoperability via an Inter-Access Point Protocol Across Distribution Systems Supporting IEEE 802.11 Operation*, IEEE Standard 802.11f, Jul. 2003.

[70] R. Soltwisch, X. Fu, D. Hogrefe, and S. Narayanan, "A method for authentication and key exchange for seamless inter-domain handovers," presented at the Proc. IEEE 14th Int. Conf. Networks (ICON 2004), Singapore.

[71] D. Harkins and D. Carrel, "The Internet key exchange (IKE)," IETF, Nov. 1998.

[72] J. Kohl and C. Neuman, "The Kerberos Network Authentication Service (V5)," RFC 1510, Sep. 1993.

[73] Y. Matsunaga, A. S. Merino, T. Suzuki, and R. H. Katz, "Secure authentication system for public WLAN roaming," in *Proc. 1st ACM Int. Workshop Wireless Mobile Applications and Services on WLAN Hotspots (WMASH)* 2003, pp. 113–121.

[74] B. C. Neuman and T. Ts'o, "Kerberos: An authentication service for computer networks," *IEEE Commun.,* vol. 32, no. 9, pp. 33–38, Sep. 1994.

[75] T. Wu, "A real-world analysis of Kerberos password security," presented at the Network and Distributed System Security Symp. (NDSS), San Diego, CA, 2003.

Minho Shin received the B.S. degree in computer science and statistics from Seoul National University in 1998 and the M.S. degree in computer science from the University of Maryland, College Park, in 2003.

He is currently working toward the Ph.D. degree at the University of Maryland. He is a graduate research assistant with Maryland Information System Security Laboratory (MISSL). His current research interests include wireless networks, the security of wireless mesh networks, and 3G/WLAN integration security.

Justin Ma received the B.S. degree in computer science and mathematics from the University of Maryland, College Park, in 2004. He is currently working toward the Ph.D. degree at the University of California, San Diego.

His research interests include operating systems and networking, with an emphasis on network security.

Arunesh Mishra received the B.Tech. degree in computer science from the Indian Institute of Technology, Guwahati, India, and the M.S. degree in computer science from the University of Maryland, College Park. He is currently working toward the Ph.D. degree in the Department of Computer Science, University of Maryland.

His research areas include wireless networks and systems security.

William A. Arbaugh received the B.S. degree from the U.S. Military Academy, West Point, NY, the M.S. degree in computer science from Columbia University, New York, and the Ph.D. degree in computer science from the University of Pennsylvania, Philadelphia.

He is an Assistant Professor, Department of Computer Science, University of Maryland, College Park. His research interests include information systems security and privacy with a focus on wireless networking, embedded systems, and configuration management.

Dr. Arbaugh is on the editorial boards of the *IEEE Computer* and the *IEEE Security and Privacy* magazines.