Report on DIMACS* Workshop on Mobile and Wireless Security

Date of Workshop:
November 3 - 4, 2004

Workshop Organizer:

Bill Arbaugh
Computer Science Department
University of Maryland, College Park

Report Author:

Yuan Yuan
Computer Science Department
University of Maryland, College Park

Date of Report:
May 9, 2005

*DIMACS was founded as a National Science Foundation Science and Technology Center. It is a joint project of Rutgers University, Princeton University, AT&T Labs-Research, Bell Labs, NEC Laboratories America, and Telcordia Technologies, with affiliated partners Avaya Labs, HP Labs, IBM Research, Microsoft Research, and Stevens Institute of Technology.

1 Introduction

The DIMACS Workshop on Mobile and Wireless Security brought together researchers and practitioners in network security, cryptography, and other areas to address and discuss outstanding issues related to security in wireless cellular, wireless LAN, and mobile ad hoc networks. The workshop sessions were held on November 3rd and 4th, 2004. The technical program consisted of presentations, invited talks, and panel discussions. The discussion session invited all the participants to identify and explore research challenges that are critical to wireless network security, and to discuss directions for future research and collaboration.

The specific topics addressed and discussed in the workshop include:

- Wireless security and roaming: ensuring the same level of security and uninterrupted connectivity for roaming stations.
- Secure and efficient wireless network access schemes.
- Authorization and authentication frameworks and policies in wireless networks.
- Threshold cryptography and its impact on wireless roaming.
- Authentication and key management issues in wireless cellular network and IEEE 802.11-based wireless networks.

We summarize the workshop presentations in §2. Discussions about future research directions and challenges are summarized in §3.

2 Summary of Presentations

2.1 Wireless Authentication Overview

Speaker: William Arbaugh, University of Maryland

Dr. Arbaugh began his talk with the goal of this workshop, that is, identifying and addressing research problems in the wireless security domain and stimulating discussions and collaborations on related topics and areas. Then he described several technical trends in wireless networks:

- Wireless network access is becoming ubiquitous and broadband in nature.

- Users are more mobile and their roaming pattern changes from discrete mobility to continuous mobility.
- Devices are less expensive with less physical security functionalities.
- Most wireless technologies have different authentication and access control frameworks and attempt to provide easy interfaces.

Dr. Arbaugh further identified the security problems exacerbated by these technical trends. He pointed out that inter-networking allows attackers to find the "path of least resistance" and establish "man-in-the-middle attacks," and the existing solutions will either prohibit networks with weak security from joining or allow them to introduce security threats. Moreover, Dr. Arbaugh made several observations, including that there are questionable trust relationships that are transitively derived among multiple parties, there are limited security features at base stations, roaming and fast handoff create challenges, and there are complex authentications mechanisms. Finally, he concluded his talk in a call for discussions and efforts to address these research problems and challenges, to facilitate standardization and policy in order to provide protection and security in wireless networks.

Several questions were raised during the talk. Dr. Arbaugh and participants discussed about where security should be implemented from the point view of network layers and what the security mechanisms attempt to protect. The discussion pointed out that security requires cross-layer design and coordination among layers, and entities to be protected include service provider, users, and regulation agents (e.g., government).

2.2 Role of Authorization in Wireless Network Security

Speaker: Pasi Eronen, Nokia

In this talk, Mr. Eronen presented the role and problems of authorization in public wireless networks from the business and protocol points of view. He first described the current status of authorization, often considered as something that just happens at some step, and pointed out that this picture of authorization is both misleading and insufficient. Then he showed that there are multiple players involved in authorization, including Access Point(AP), access network, roaming broker, etc. These multi-party systems are often specified as sets of two-party protocols, each of which tries to be as independent as possible from the others. Even though these two-party protocols can simplify specification and offer certain flexibility, the boundaries between protocols can lead to difficulties. Therefore, a communication

channel is needed between the client and the authentication, authorization, and accounting (AAA) infrastructure (other than home AAA, which can also be utilized to build up roaming relationships and support handoffs).

He further observed that current authorization solutions are not sufficient since most of them are not secure, lead to limited amount of transferred information, and may break network uses other than browsing.

Finally, Mr. Eronen pointed out that handoffs and accounting also complicate the issue of authorization and session-related states in the network. In particular, the handoff can succeed only if the new AP is covered by the home network's promise to pay, and in the inter-operator case, the new AP accepts the promises of this home network. Currently, what is exactly covered by the implicit promise in RADIUS Access-Accept is not explicitly defined; and neither is this information communicated to the client. Regarding accounting, many existing systems also lack a channel for transmitting accounting-related information to the client.

He concluded his talk with a few suggestions on authorization design, including properly utilizing current components, avoiding hard-coding business model and policy, and providing communication channels between entities.

2.3 Network Access Control Schemes Vulnerable to Covert Channels

Speaker: Anne-Sophie Duserre

In this presentation, Ms. Duserre underlined a straightforward yet potentially harmful vulnerability of some network access control schemes, which allow an authentication server from a different administrative domain to be involved. She described the contexts of Network Access Control (NAC) and covert channel at the beginning. Network access control is about securely verifying the identity of a device/user that wants to connect to a network and checking whether this device/user is indeed authorized to do so. A covert channel is a communication channel that is used in an unintended and/or unauthorized way to transfer data in a manner that violates security policy. Then she presented several examples of access control schemes and compared the NAC adopted in wireless LAN in roaming scenarios to different techniques used in the cordless or the cellular telephony realms.

Ms. Duserre further talked about the impact of covert channels in signing roaming agreements and designing threat models. In the end, she suggested several different ways to mitigate the vulnerability in NAC, including reverting to more reliable NAC schemes, decreasing the potential attraction

of this channel, and monitoring the channel.

2.4 802.11 Authentication and Keying Requirements

Speaker: Jesse Walker, Intel

Dr. Walker examined some issues presented by 802.11i's use of Extensible Authentication Protocol (EAP), including freshness, binding, performance, and deployability issues. The goal of his talk was to help establish keying requirements for future standard development.

The talk started with a brief review of the current IEEE 802.11i standard, including 802.1X authentication and EAP authentication procedures. Then Dr. Walker analyzed the current standard and identified four related problems. The first problem was the lack of authentication and key-binding between the AP and the station (STA), which is caused by the fact that the AP never advertises its authenticated identity to the STA and its Basic Service Set Identifier (BSSID) is the only identifier exposed to the STA. On the other hand, the STA never advertises its authenticated identity to the AP and the Media Access Control (MAC) address is the only identifier the STA exposes to the AP. The second problem arises in the inconsistent contract caused by modern switched APs, since the pairwise master key (PMK), which is kept at the switch, does not cross crypto-boundaries if reused at different APs belonging to the same switch. Expiry timer available only inside an AP introduced the third problem, which may require STAs to equip with more predictable PMK usage to make caching work. The last problem considered the tradeoff between efficiency and security.

After identifying these four problems, Dr. Walker further explained the current keying and authentication procedures. He also pointed out the potential attacks to the existing procedures.

Then Dr.Walker talked about some prudent engineering practices for cryptographic protocols (Abadi and Needham, 1995) as design heuristics. Applying these practices to the current 802.11i standard, he suggested several practices to solve the identified problems including:

- 802.11 must advertise the AP's identity to the STA, otherwise the binding is not meaningful to the STA.
- Key usage should be identified by cryptographic boundary among devices, instead of by MAC addresses.
- AP should adopt cache timeout rules that can be conveyed to the STA.

Dr.Walker concluded his talk with a call for action on several challenging research topics. This talk also stimulated several interesting discussions on topics of key management/binding and trust relationship among APs and STAs.

2.5 Secure and Efficient Network Access

Speaker: Jari Arkko, Ericsson Research NomadicLab

In this talk, Mr. Arkko addressed the problems in network access, particularly with mobile nodes, and sketched a new architecture to deal with the different aspects of the network access problem. He first talked about the problems in the current network access approaches from the efficiency, security and functionality perspectives. Then he described several attempts currently being made to improve network access. These attempts include network access authentication mechanisms, fast handover mechanisms, IP layer attachment improvements, and other optimizations focusing on individual components. He further made several observations on current network access mechanisms, and pointed out that most work focused on a particular aspect of the problem and the state-of-the-art solutions lack system-level understanding of the security issues.

To address these problems, Mr.Arkko proposed some new ideas, attempting to deal with the problem as a whole rather than each single layer. Several potential solution components were suggested to form a new architecture, which includes addressing for each node, reduced messaging overhead, fast information retrieval, using delegation, avoiding Denial-of-Service, and protecting privacy.

Mr. Arrko further provided three examples of flows, variation with better mobility support, and handoffs, to illustrate the application of the proposed solution ingredients. He finally summarized the talk by suggesting that the network access problem should be handled as a whole at the system-level.

2.6 Extending the GSM/3G Key Infrastructure

Speaker: Scott Guthery, CTO Mobile-Mind, Inc., and Mary J. Cronin, Boston College

This presentation had two parts: Dr. Guthery provided a technical overview of the GSM/3G key infrastructure and the protocols with a focus on the role and security architecture of the Subscriber Identity Module (SIM), Dr. Cronin analyzed business models for SIM security extensions.

Specifically, Dr. Guthery focused his talk on SIM for mobile network authentication, Internet authentication, and local authentication. He first explained that SIM is an integral part of GSM security and holds a secret key K_i, another copy of which is held by the subscriber network. He described authentication procedures in the roaming scenario as a stepping off point for extending the GSM/3G key infrastructure in GSM/3G networks. Then he presented EAP-SIM, exploiting SIM, for Internet authentication, where the visited network is an EAP authenticator. The SIM toolkit was introduced to issue commands to the handset, such as displaying text, collecting keys, sending short messages, and blocking calls. In the end, Dr. Guthery discussed SIM for local authentication, authorization and cryptographic services.

Dr. Cronin continued the talk with a theory that outlines compelling business and revenue opportunities by leveraging SIM security. Then she introduced three potential business cases including:

- SIM-hosted and authenticated non-telephony m-commerce applications and services.
- SIM-enabled use of mobile handset for authenticated and authorized transactions via the wireless public network.
- Embedded SIMs for authorization of users or devices attached to any network, particularly WiFi.

She further discussed the business models and current status of the three potential business cases, and indicated the continuing efforts in searching for clear business cases for SIM extension.

2.7 Wireless Security and Roaming Overview

Speaker: Nidal Aboudagga UCL Crypto Group

Mr. Aboudagga gave an overview of the mechanisms and protocols for wireless security and roaming issues. Specifically, he talked about the Wired Equivalent Privacy (WEP) protocol based on the RC4 algorithm, which fails to provide a wired equivalent privacy to WLAN. The IEEE 802.1x combined with EAP is adapted to the wireless network to enable several kinds of user authentication. To solve the problem of data security over wireless networks, the Wi-Fi alliance created the Wi-Fi Protected Access (WPA) protocol based on earlier work by the IEEE 802.11i group. Now the IEEE 802.11i standard has been approved, and it uses strong security

features such as Temporal Key Integrity Protocol (TKIP) and Advanced Encryption Standard (AES).

After describing the current standards and protocols, Mr. Aboudagga discussed various problems and challenges of ensuring the same level of security and uninterrupted connectivity for roaming. The first problem was the large latency incurred by full authentication 802.1x/EAP or PSK in roaming. The other one was related to pre-authentication, which may enhance roaming performance but handoff latency time still limits the performance for multimedia applications. Moreover, pre-authentication can be only used in the same Extended Service Set (ESS) and is a computationally expensive mechanism.

In conclusion, Mr. Aboudagga made several observations on the current standardization activities and their insufficiency in supporting fast handoff and roaming in wireless networks. The participants discussed the working progress of multiple working groups, such as 802.11k ad 802.11f, and their limitations. One of the participants pointed out that some problems may be caused by current vendors' reluctance to change their products and adopted standards.

2.8 A Proposal for Next Generation Cellular Network Authentication and Authorization Architecture

Speaker: James Kempf, DoCoMo USA Labs

In this talk, Dr. Kempf presented a tentative architecture for cellular network authentication and authorization. He first described the two existing architectures that provide access authentication and authorization to wireless networks. The first one is the Pre-IP Layer-2.5 framework, in which the terminal and the network authenticate each other prior to establishing IP service typically through a Layer-2.5 flow between them. The second one is through restricted IP access and HTTP Web page login that provide authentication using a user name/password for account holders or a credit card number for one time access with no re-authentication on handover.

Dr. Kempf then explained the inherent problems in these two architectures and discussed an alternative architecture, i.e., hyperoperator, using certificates that could evolve from the IETF SEND router certification protocol, and possibly the Protocol for carrying Authentication for Network Access (PANA). He briefly reviewed SEcure Neighbor Discovery (SEND) and discussed prospects to extend it to handle network access authentication and authorization, and talked about PANA. He further pointed out that prospects for acceptance and actual deployment remain speculative due to

the deep embedding of traditional AAA architecture into existing wireless cellular and wireless standards.

2.9 Securing Wireless Localization

Speaker: Wade Trappe, Rutgers University

Dr. Trappe began this talk with some background on localization in wireless networks. Localization is important for facilitating local-based services and the goal is to determine the location of a wireless device through some forms of measurements. Several measurement methods have been proposed to utilize information, such as signal strength, time of flight, arrival angel, and neighbor location, to locate a wireless device. Dr. Trappe described the algorithms of several measurement methods and then presented the possible attacks on the localization algorithms.

Dr. Trappe first introduced localization background and possible attacks, and then discussed two proposed schemes to defend wireless localization. The first scheme is multimodal localization and its defense strategy is to make an adversary have to attack several properties at the same time. He then focused on the second method, Robust Statistical Method, of developing robust statistical estimation algorithms and data-cleaning methods to filter the collected data and discard invalid information. Furthermore, Dr. Trappe presented the performance of the proposed schemes.

3 Future Research Directions and Challenges

In the discussion session, the participants discussed several important issues and identified key problems. Such problems cover many aspects of key management/binding, trust relationship, privacy, roaming, mobility, and so on. A number of open problems and possible directions for future research were also proposed in the discussions. Some of them are listed below.

1. What is an identity, and how do you define and bind it within different layers?
2. How do you allow privacy or anonymity?
3. What are the potential applications of new cryptography methods, for example, threshold cryptography?
4. How do you make Public Key Infrastructure (PKI) or other public key semantics easier to manage?

5. How do you achieve realizable trust models with/without authentication and access control?

6. Key binding problem: design a well-defined key usage protocol for multiple-party agreement.

7. How do you optimize security mechanisms across layers and coordinate efforts among IEEE WG/IETF/IRTF?

8. How do you achieve Make before Break in roaming and mobility scenarios?

9. How do you effectively support Mobility and Internetworking, and address challenges of addressing, Denial-of-Service, Physical/MAC layer features, and consistent identity?

10. How do you mitigate compound Denial-of-Service attack mechanisms to provide Quality-of-Service?

11. How do you effectively achieve trust relationship initiation and management?

Acknowledgment

The author of this report would like to thank Dr. Brenda Latka, Associate Director of DIMACS, and Dr. Fred S. Roberts, Director of DIMACS, for valuable comments. The author also thanks the organizers and speakers of this workshop. The author and the DIMACS Center acknowledge the support of the National Science Foundation under grant CCR03-14161 to Rutgers University.