SECURITY, PRIVACY, AND ACCOUNTABILITY IN WIRELESS ACCESS NETWORKS

This paper appears in: Wireless Communications, IEEE
Issue Date: Aug. 2009
Volume: 16 Issue:4
On page(s): 80 - 87
ISSN: 1536-1284
INSPEC Accession Number: 10915531
Digital Object Identifier: 10.1109/MWC.2009.5281259
Date of Current Version: 09 å£12009
Sponsored by: IEEE Communications Society

報告者:施惟詠
ABSTRACT

- The presence of ubiquitous connectivity provided by wireless communications and mobile computing has changed the way humans interact with information.

- In this article we address the security and privacy concerns in wireless access networks.
INTRODUCTION

In the context of wireless access networks, the main security goals include:

- Authentication
- Confidentiality
- Integrity
- Non-repudiation
- Access control
- Availability
Figure 1. *Typical challenge-response authentication: a) secret key cryptography-based; b) public key cryptography-based.*
In the context of wireless access networks, we deem the following privacy services/requirements indispensable:

- Anonymity
- Non-linkability
- Context privacy
- Confidentiality
- Integrity
Wireless mesh networks (WMNs) have been posed as the competitive rival to the future wireless cellular technologies and a promising technology for ubiquitous high-speed network access.

WMNs from everywhere within the community such as offices, homes, restaurants, hospitals, hotels, shopping malls, and even vehicles.
Figure 2. WMN network architecture [8].
**Figure 3.** The format of user identity information.
we present a sophisticated privacy-enhanced yet accountable security framework for metropolitan WMNs, termed PEACE, which aims to provide:

- Adequate user access control
- $k$-anonymity and non-linkability
- User accountability
Figure 4. PEACE trust model.
Figure 5. Construction of access credential: a) based on Boneh's group signature scheme; b) based on our modified group signature construction.
Figure 6. Illustration of key distribution.
CONCLUSION

• In this article we address security and privacy issues in wireless access networks.

• We discuss general approaches to achieving security and privacy and their effects on user accountability.