Journal of Network and Computer Applications 34 (2011) 432–442

Contents lists available at ScienceDirect

Journal of Network and Computer Applications

journal homepage: www.elsevier.com/locate/jnca

Security analysis of wireless mesh backhauls for mobile networks

Frank A. Zdarsky [a,*], Sebastian Robitzsch [b], Albert Banchs [c]

[a] NEC Network Laboratories, Kurfürsten-Anlage 36, 69115 Heidelberg, Germany
[b] University College Dublin, Performance Engineering Laboratory, Belfield, Dublin 4, Ireland
[c] Universidad Carlos III de Madrid, Dept. of Telematics Eng., Avda de la Universidad, 30, 28911 Leganés, Madrid, Spain

ARTICLE INFO

Article history:
Received 15 October 2009
Received in revised form
30 January 2010
Accepted 25 March 2010
Available online 9 April 2010

Keywords:
Security analysis
Wireless mesh backhauls
Mobile networks

ABSTRACT

Radio links are used to provide backhaul connectivity for base stations of mobile networks, in cases in which cable-based alternatives are not available and cannot be deployed in an economic or timely manner. While such wireless backhauls have been predominantly used in redundant tree and ring topologies in the past, mobile network operators have become increasingly interested in meshed topologies for carrier-grade wireless backhauls. However, wireless mesh backhauls are potentially more susceptible to security vulnerabilities, given that radio links are more exposed to tampering and given their higher system complexity.

This article extends prior security threat analyses of 3rd generation mobile network architectures for the case of wireless mesh backhauls. It presents a description of the security model for the considered architecture and provides a list of the basic assumptions, security objectives, assets to be protected and actors of the analysis. On this foundation, potential security threats are analyzed and discussed and then assessed for their corresponding risk. The result of this risk assessment is then used to define a set of security requirements. Finally, we give some recommendations for wireless mesh backhaul designs and implementations following these requirements.

© 2010 Elsevier Ltd. All rights reserved.

1. Introduction

Radio links are used to provide backhaul connectivity for base stations of mobile networks, in cases in which cable-based alternatives are not available and cannot be deployed in an economic or timely manner. To ensure high availability, such wireless backhauls have been predominantly used in redundant tree and ring topologies. Yet, following the success of WiFi-based wireless mesh networks in recent years, mobile network operators have become increasingly interested in meshed topologies for carrier-grade wireless backhauls as well.[1] Mesh topologies may provide availability levels comparable to redundant trees and rings, while being more flexible and using capacity more efficiently.

However, radio links are also more exposed, and thus easier to tap and to interfere with, than their wired counterparts. This makes wireless backhauls, and in particular multi-hop ones like in wireless meshes, potentially more susceptible to security vulnerabilities. For carrier-grade wireless mesh backhaul solutions security therefore becomes a high priority non-functional requirement.

Mobile network operators have high security demands in order to protect their business assets. Assets not only include the mobile network infrastructure and services, which must be protected from unauthorized use and from attacks on their availability or quality, but an important asset requiring protection is furthermore an operator's reputation with current and potential customers. They thus need to ensure that their customers' data that is transported via their networks is protected against misappropriation. In some legislation, this is even an obligation of carriers as part of their due diligence.

Architectural design issues can quickly compromise these security goals. A prominent example is GSM's security architecture that only requires user authentication towards the network. In contrast, the network itself is not authenticated to its users. This design flaw has subsequently been exploited to mount "false base station attacks": An attacker uses a device popularly called "IMSI-catcher", which pretends to be a legal base station with a superior signal quality. This causes mobile phones in the vicinity to associate themselves with the false base station, which then signals the mobile phones to switch off encryption, as investigated by Adoba et al. (2004). Similar attacks have been reported for Universal Mobile Telecommunication System (UMTS) networks by exploiting Global System for Mobile Communications (GSM) backward compatibility, as stated in Adoba et al. (2008).

* Corresponding author. Tel.: +49 6221 4342 142.
E-mail addresses: Frank.Zdarsky@neclab.eu (F.A. Zdarsky), Sebastian.Robitzsch@ucdconnect.ie (S. Robitzsch), banchs@it.uc3m.es (A. Banchs).

[1] The EU project CARMEN (2008) is designing a wireless mesh network architecture capable of supporting carrier-grade requirements over a diverse set of radio technologies.

1084-8045/$ - see front matter © 2010 Elsevier Ltd. All rights reserved.
doi:10.1016/j.jnca.2010.03.029

Although security attacks are well studied in 3G networks (the reader is referred e.g. to (*iGillott* Research, 2007) for a study of security in 3G networks including some statistics on attacks in the past), the multihop nature of Wireless Mesh Backhauls (WMBs) exposes the network to new security threats which require additional measures to counteract. This article therefore extends the security threat analysis of 3G network architectures by 3GPP (2001) for the case of WMBs.

The following section provides an overview of related work. Section 3 starts with a description of the security model for the considered architecture. It then provides a list of the basic assumptions made for the subsequent security analysis and introduces the security objectives, the assets to be protected and the actors of this analysis. On this foundation, potential security threats are analyzed and discussed in Section 4. They are classified both by the security objective under attack and the point of attack. Not all identified security threats are equally likely, as they require various levels of sophistication of an attacker. Also, the impact of a successful attack on the mobile network operator can vary. Thus, Section 5 performs a risk assessment of the identified security threats. The result of this risk assessment is then used to define a set of security requirements for wireless mesh backhauls. These requirements are outlined in Section 5.5. Section 6 then provides a list of general recommendations to meet these requirements for the design of wireless mesh backhaul architectures and protocols. Finally, Section 7 provides a short summary of the findings in this analysis.

2. Related work

Over the last years, a number of security architectures and mechanisms have been devised for Wireless Mesh Networks (WMNs).

Some of these works address user authentication in WMNs. For example, Zhang and Fang (2006) propose ARSA, a security architecture that allows users to access and roam between a multitude of WMNs belonging to different administrative domains based on a "pass" of a third-party provider. This is supposed to resolve the problem of establishing pair-wise trust relationships between the operators of the different WMNs. They also address the problem of user location privacy by providing the user with different alias identities. Similarly, Ren et al. (2010) describe PEACE, a security solution with authentication and key agreement protocols that provide protection against attacks on user privacy while providing a strict user access control.

Other papers address Denial of Service (DoS) attacks in WMNs. For example, Yan et al. (2009) study DoS attacks in which attackers generate a flood of high-rate data flows to deny service to other, legitimate traffic. They use a frequency analysis of incoming packets to detect such attacks and study different strategies of countering these attacks through selective random dropping.

Yet other papers address attacks on the control plane protocols of WMNs. For example, Naveed and Kanhere (2006) study attacks on dynamic channel assignment in 802.11-based WMNs, in which a compromised mesh node manipulates control messages of the channel assignment protocol to force mesh links to use heavily congested channels. Similarly, a number of attacks on routing protocols in WMNs and ad-hoc networks exist (see Hu and Perrig, 2004 for a survey of such attacks).

All of these works aim at addressing some security threats that according to the authors' intuition is relevant for WMNs. However, none of them contains a systematic approach to determine which security threats are really relevant and should require more efforts to prevent them. This question is particularly relevant if a wireless mesh network is used as backhaul for a mobile cellular network. In this case, many security features are already provided by the mobile network, for example the authentication framework with pair-wise trust relationships between operators, the handling of temporal identities and the policing of user data flows. Furthermore, all network entities are under a single administrative control, which facilitates protection of the control and data planes. In contrast to all these previous works, in this paper we conduct a complete analysis of security threats with focus on WMBs for mobile networks.

3. System model and security model

As stated in the introduction, before describing the potential security threats of a WMB a detailed system description is necessary to provide a reasonable understanding of the considered network architecture. Hence, this section presents the system model, the assumptions, the security objectives, the assets and the actors considered in the following threat analysis.

3.1. System description

Prior to going into the detailed analysis of the potential security issues, it is necessary to clearly delimit the system under test. When doing so, it is important to consider that a wireless mesh backhaul is supposed to provide a drop-in replacement for parts of the operator's wired backhaul. As such, it represents only a small sub-system within a complete mobile network architecture, e.g. a 3rd Generation Partnership Project (3GPP) architecture. It is valid to assume that this architecture provides its own security features, designed based on a separate security analysis. In case of 3GPP, the security analysis is documented in 3GPP (2001).

Fig. 1 shows the system security model of a traditional wireless access network with wired backhaul. It focuses on the transport stratum, i.e. all protocols required for the provisioning of a data transport between a user terminal (UT) and the core network. It further distinguishes between the management and control plane and the data plane of this stratum. The former divides into the user signaling part between the UT and its Point of Attachment (PoA) to the network, which in a mobile network is a wireless link, and the core network signaling part between the network elements of the access network and the core network, which is typically wired, but may use non-meshed wireless links for backhaul. The data plane transports data between the UT and the core network. This data traffic is typically end-to-end[2] encrypted. Note that the data plane from the point of view of the transport stratum may also carry management and control messages of the next higher stratum, i.e. the serving/home network stratum.

User signaling, core network signaling and user data form three "security domains", in the sense that if an attacker succeeds in overcoming the security features of one domain, all subsystems within this domain are compromised, but not necessarily those of other domains. The latter depends on how well domains are "firewalled" from each other. Fig. 2 shows the security domains of an access network using a WMB for backhaul. The figure also shows the security domains of the traditional access as grayed-out arrows, which are not covered in the present analysis, as it is assumed that proper security features to protect them are

[2] End-to-end in the sense of all the way between UT and the core network, so the content of data is not visible to the access network.

Download English Version:

https://daneshyari.com/en/article/460259

Download Persian Version:

https://daneshyari.com/article/460259

Daneshyari.com