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.

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