Accepted Manuscript

Title: Evil twins and WPA2 enterprise: A coming security disaster?

Author: Alberto Bartoli, Eric Medvet, Filippo Onesti

PII: S0167-4048(17)30280-8
DOI: https://doi.org/10.1016/j.cose.2017.12.011
Reference: COSE 1259

To appear in: *Computers & Security*

Received date: 11-10-2017
Revised date: 12-12-2017
Accepted date: 22-12-2017

Please cite this article as: Alberto Bartoli, Eric Medvet, Filippo Onesti, Evil twins and WPA2 enterprise: A coming security disaster?, *Computers & Security* (2018), https://doi.org/10.1016/j.cose.2017.12.011.

Evil Twins and WPA2 Enterprise: A Coming Security Disaster?

Alberto Bartoli[1], Eric Medvet, Filippo Onesti —— University of Trieste, Italy

Corresponding author
Alberto Bartoli
University of Trieste, TRIESTE, TS ITALY
bartoli.alberto@univ.trieste.it

Alberto Bartoli received the degree in Electrical Engineering in 1989 cum laude and the PhD degree in Computer Engineering in 1993, both from the University of Pisa, Italy.
Since 1998 he is an Associate Professor at the Department of Engineering and Architecture of University of Trieste, Italy, where he is the Director of the Machine Learning Lab.
His research interests include machine learning applications, evolutionary computing, and security.
Eric Medvet received the degree in Electronic Engineering cum laude in 2004 and the PhD degree in Computer Engineering in 2008, both from the University of Trieste, Italy.
He is currently an Assistant Professor in Computer Engineering at the Department of Engineering and Architecture of University of Trieste, Italy. His research interests include Genetic Programming, web and mobile security, and machine learning applications.
Filippo Onesti received the degree in Computer Engineering in 2017 from the University of Trieste, Italy.

Abstract

WPA2 Enterprise is a suite of protocols for secure communication in a wireless local network and has become an essential component of virtually every enterprise. In many practical deployments of this technology, a device that authenticates with username and password is at risk of leaking credentials to fraudulent access points claiming to be the enterprise network (*evil twins*) that may be placed virtually anywhere. While this kind of vulnerability is well known to practitioners, we believe these issues deserve a fresh look because the current technological landscape has magnified the corresponding risks. Convergence of organizations toward single sign-on architectures in which a single set of credentials unlock access to *all* services of the organizations, coupled with the huge diffusion of wifi-enabled personal devices which often contain enterprise credentials and that connect to wifi networks *automatically*, have made attacks aimed at stealing network credentials particularly attractive to attackers and hard to detect. In this paper we intend to draw the attention of the research and technological community on this important yet, in our opinion, widely underestimated risk. We also suggest a direction for investigating practical solutions able to offer stronger security without requiring any overhaul of existing protocols.

Keywords: authentication, wifi, smartphone, hacking, password

1 Introduction

WPA2 Enterprise is a suite of protocols for secure communication in a wireless local network and has become an essential component of virtually every enterprise. The framework is based on three different entities: user device that communicates via wireless link (Supplicant); wireless access point (Authenticator); server that stores user credentials (Authentication Server). Each user is

[1] Corresponding author: http://bartoli.inginf.units.it