Evil Twin And Beyond

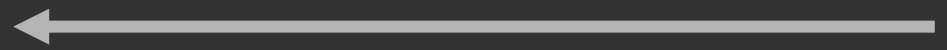
Sicherheit bei der Authentifizierung in WLANs

24. Januar 2024 – Aaron Schlitt – Hacken und Schnacken

WLAN

IEEE 802.11

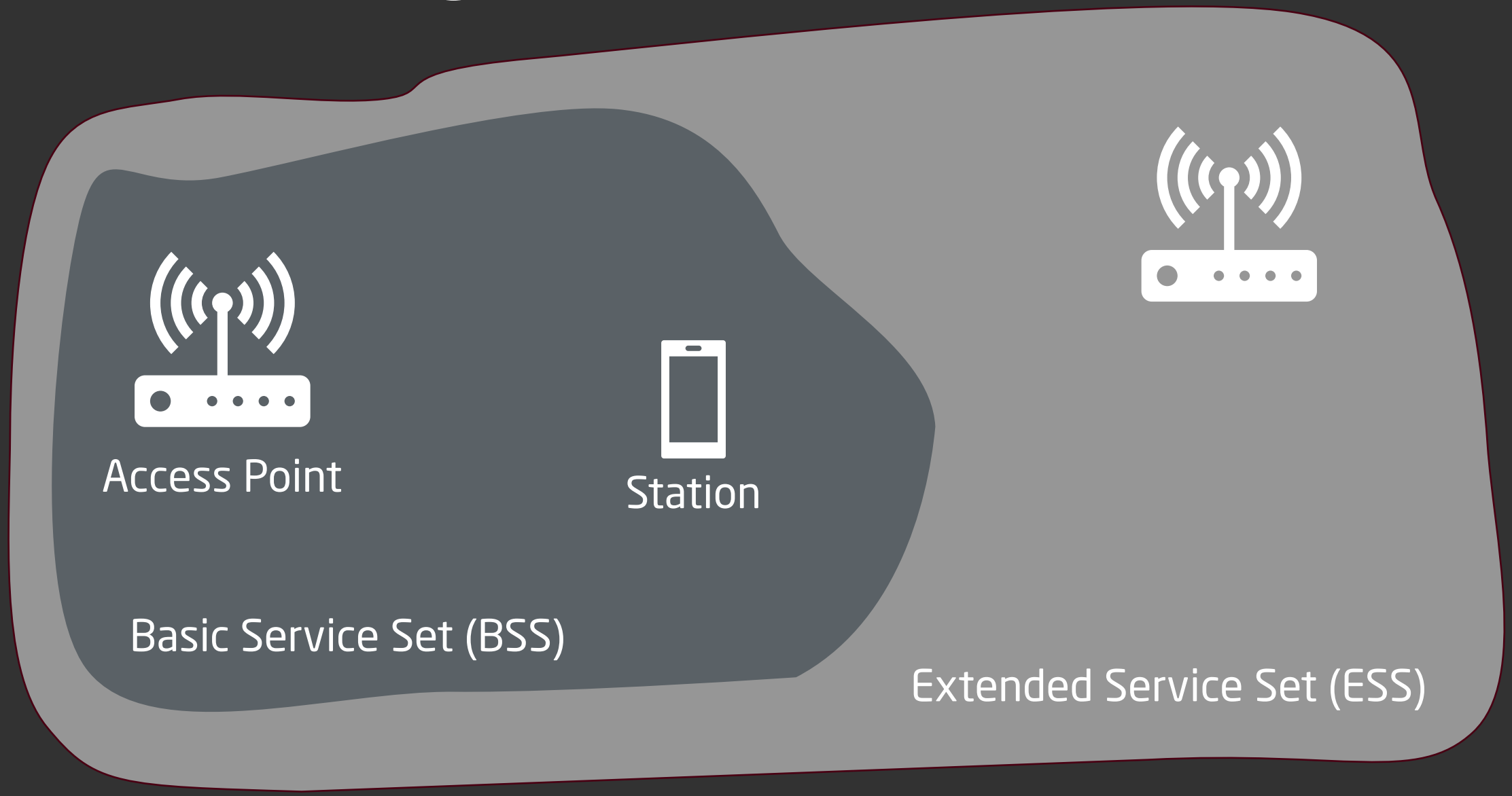
SAE



Wi-Fi Alliance

WPA3

Terminologie



Security: Der Verbindungsprozess

1. 802.11 Authentication and Association

2. PMK aus PSK generieren

3. 4-Way-Handshake

Security: Der Verbindungsprozess

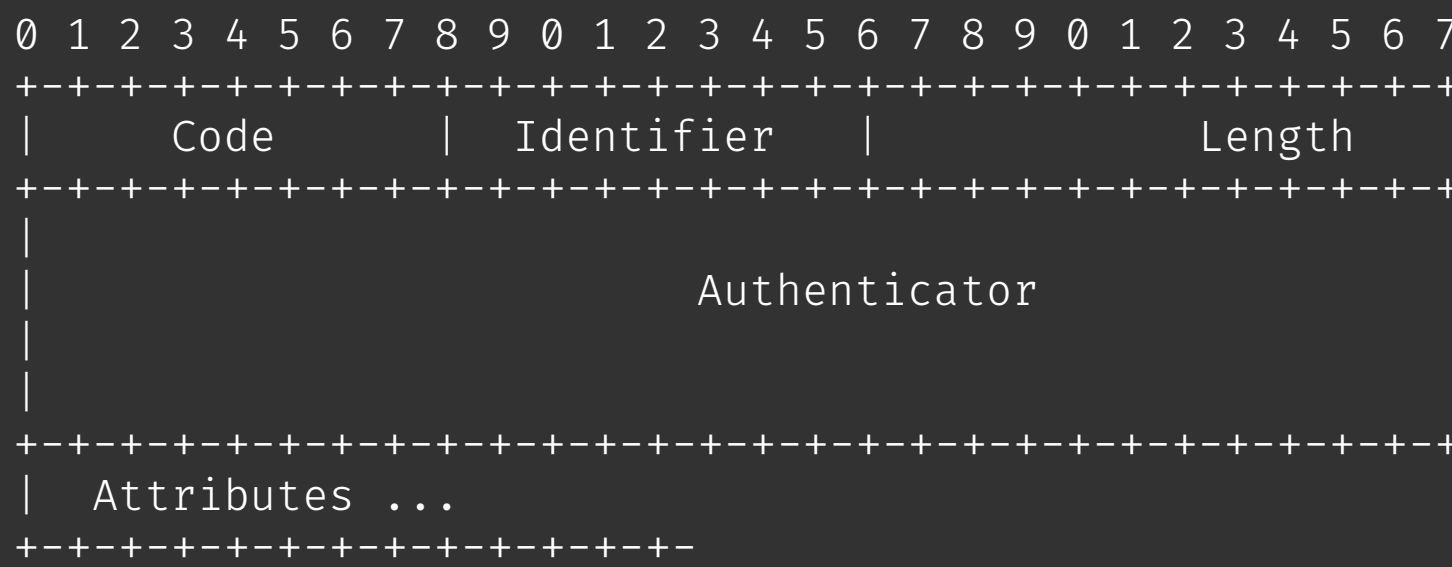
1. 802.11 Authentication and Association

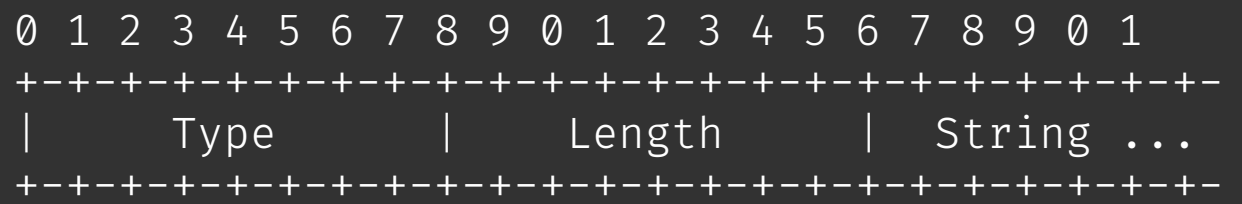
2. 802.1X Authentication

3. 4-Way-Handshake

802.1X-Komponenten

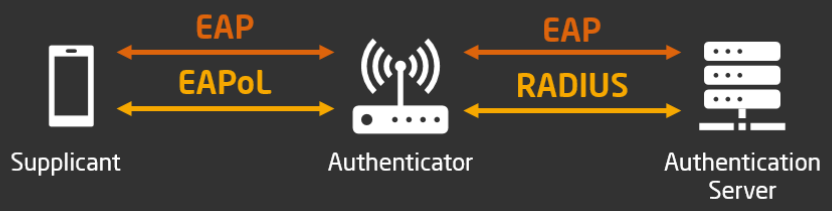
Remote Authentication Dial-In User Service





Security

802.1X-Komponenten

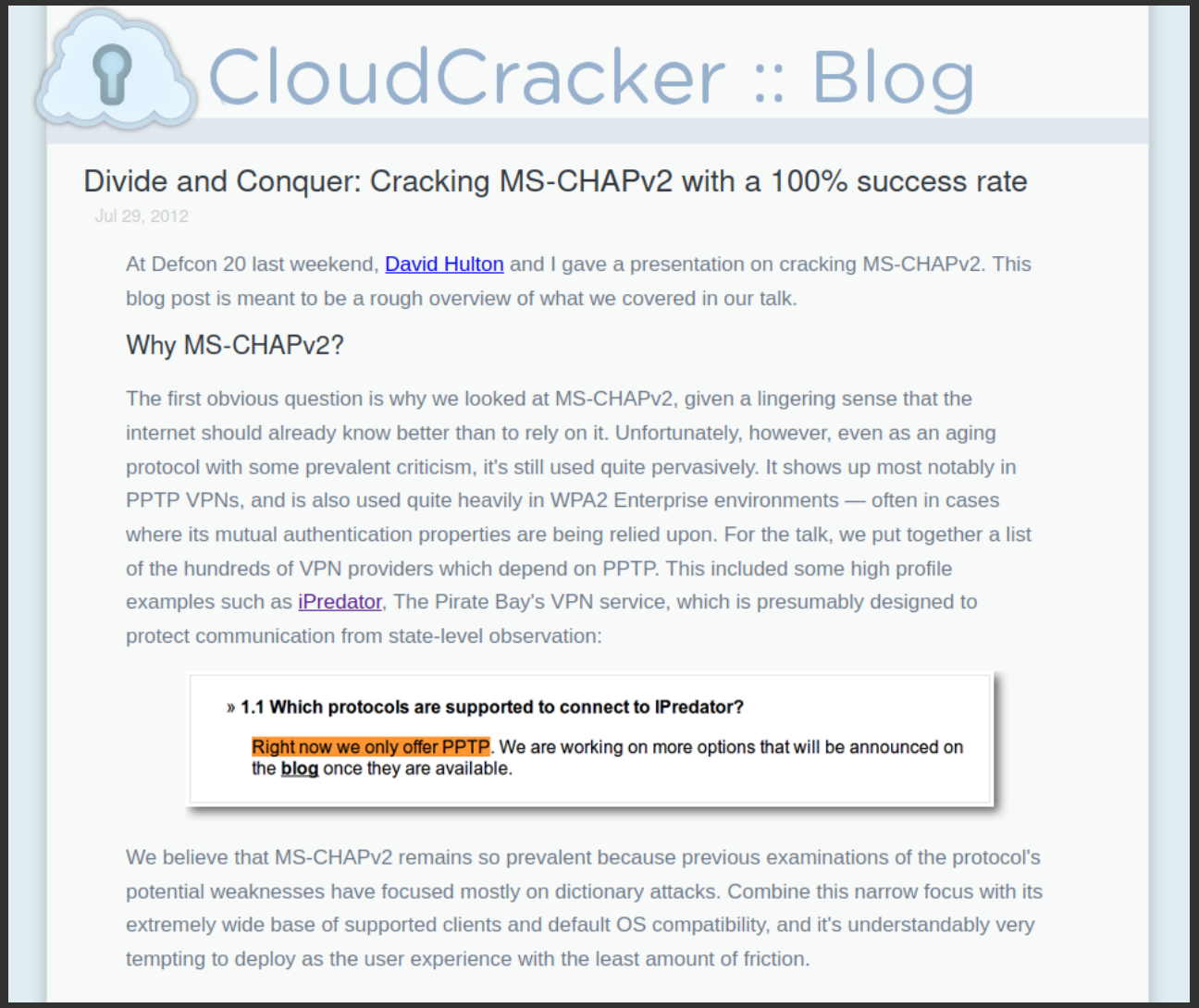


Connection name: hpi

General | Wi-Fi | Wi-Fi Security | Proxy | IPv4 Settings | IPv6 Settings

Security: WPA/WPA2 Enterprise
Authentication: Protected EAP (PEAP)
Anonymous identity:
Domain:
CA certificate: GEANT.crt
CA certificate password:
Show passwords
No CA certificate is required
PEAP version: Automatic
Inner authentication: MSCHAPv2
Username: aaron.schlitt
Password: [redacted]
Show password

Cancel | Save



CloudCracker :: Blog

Divide and Conquer: Cracking MS-CHAPv2 with a 100% success rate

Jul 29, 2012

At Defcon 20 last weekend, David Hulton and I gave a presentation on cracking MS-CHAPv2. This blog post is meant to be a rough overview of what we covered in our talk.

Why MS-CHAPv2?

The first obvious question is why we looked at MS-CHAPv2, given a lingering sense that the internet should already know better than to rely on it. Unfortunately, however, even as an aging protocol with some prevalent criticism, it's still used quite pervasively. It shows up most notably in PPTP VPNs, and is also used quite heavily in WPA2 Enterprise environments — often in cases where its mutual authentication properties are being relied upon. For the talk, we put together a list of the hundreds of VPN providers which depend on PPTP. This included some high profile examples such as iPredator, The Pirate Bay's VPN service, which is presumably designed to protect communication from state-level observation:

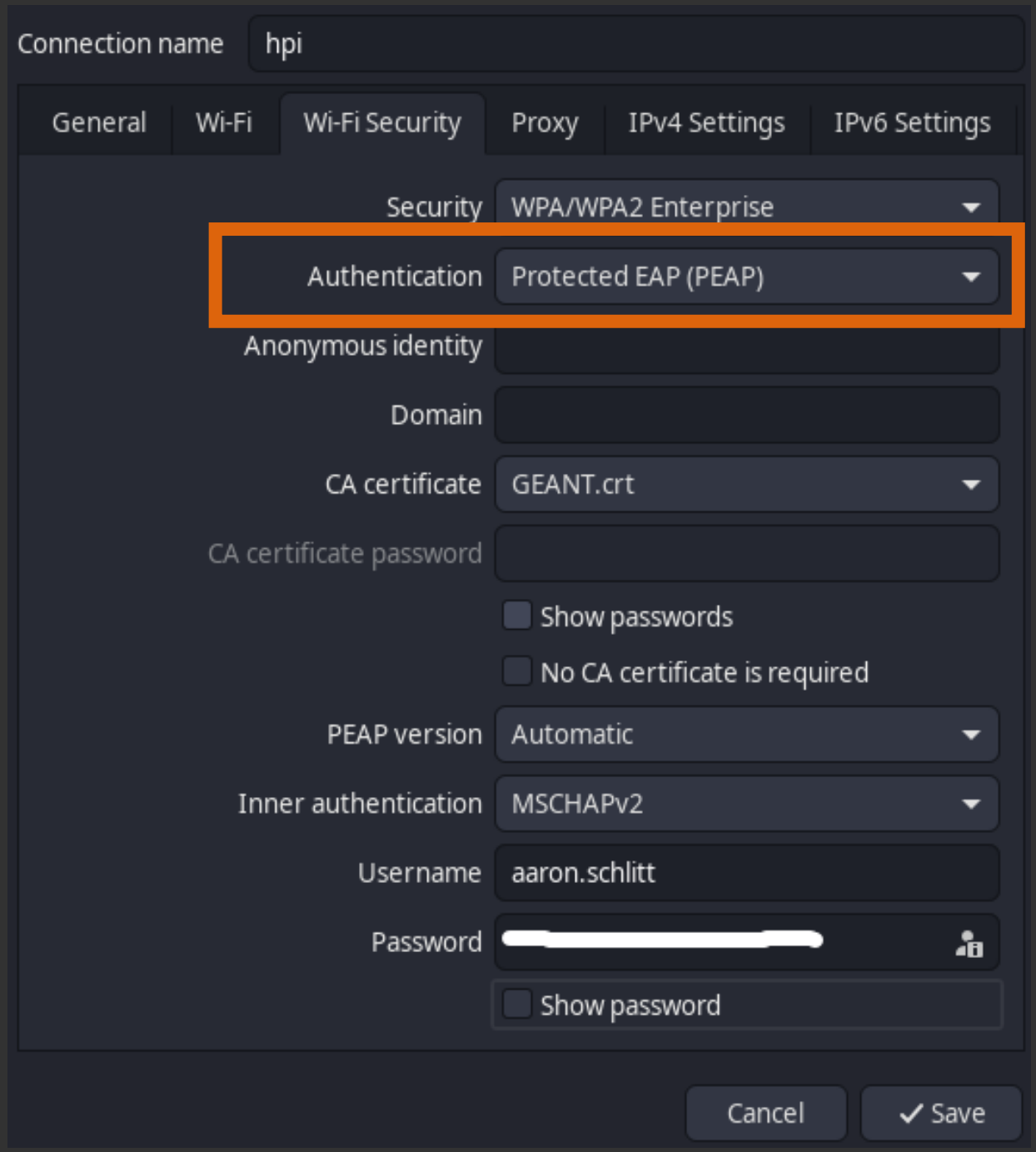
» 1.1 Which protocols are supported to connect to IPredator?

Right now we only offer PPTP. We are working on more options that will be announced on the blog once they are available.

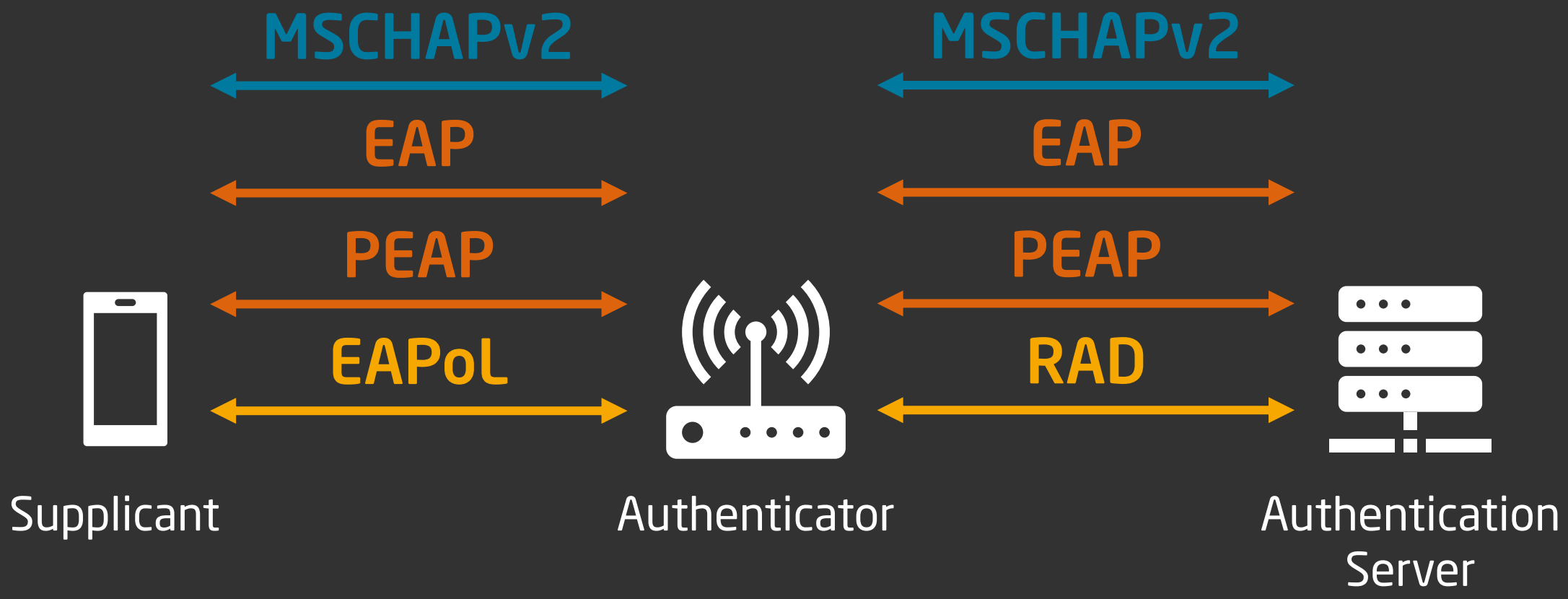
We believe that MS-CHAPv2 remains so prevalent because previous examinations of the protocol's potential weaknesses have focused mostly on dictionary attacks. Combine this narrow focus with its extremely wide base of supported clients and default OS compatibility, and it's understandably very tempting to deploy as the user experience with the least amount of friction.

→ MD4(Password)

TLS to the Rescue!



Alles zusammen



TOFU

source Docs GO TO CODE ↗

DOCUMENTATION

Getting Started | Security | Core Topics | Compatibility | Android Devices | Automotive | Reference

Filter

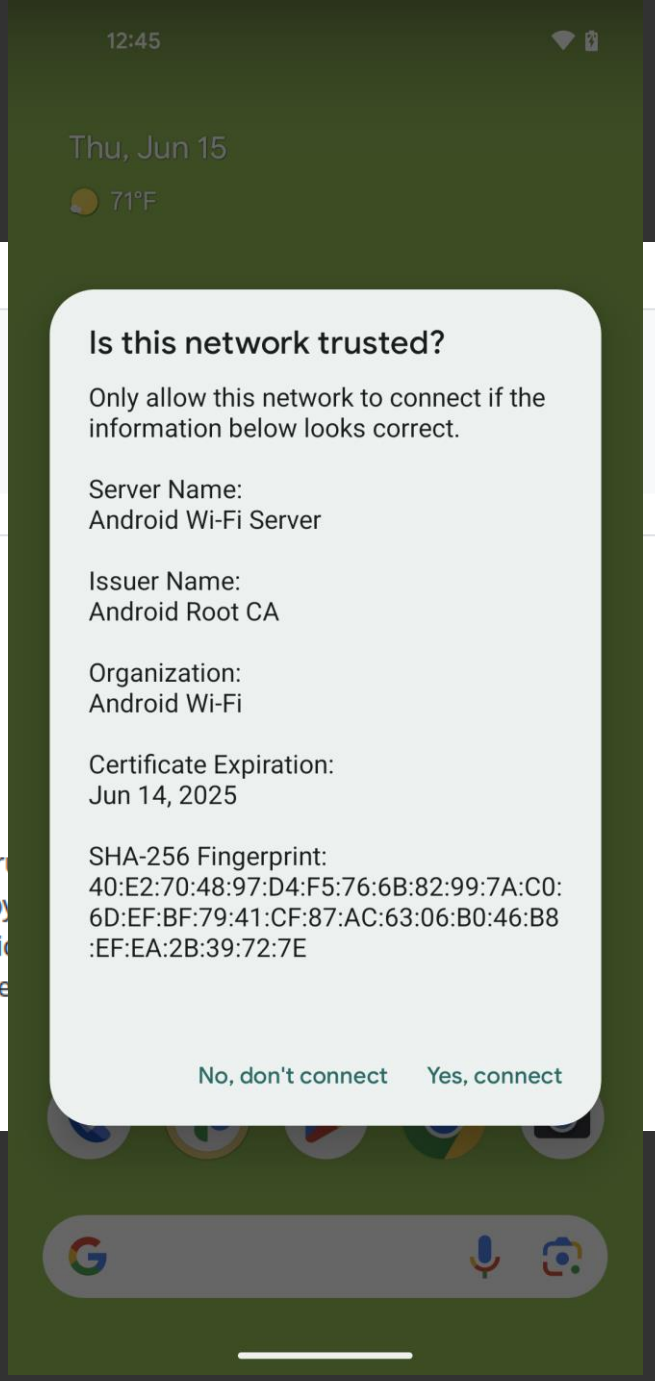
- Testing, Debugging, and Tuning Wi-Fi
- Android Packet Filter
- Carrier Wi-Fi
- MAC Randomization Behavior
- Implementing MAC Randomization
- Passpoint (Hotspot 2.0)
- STA/AP Concurrency
- STA/STA Concurrency

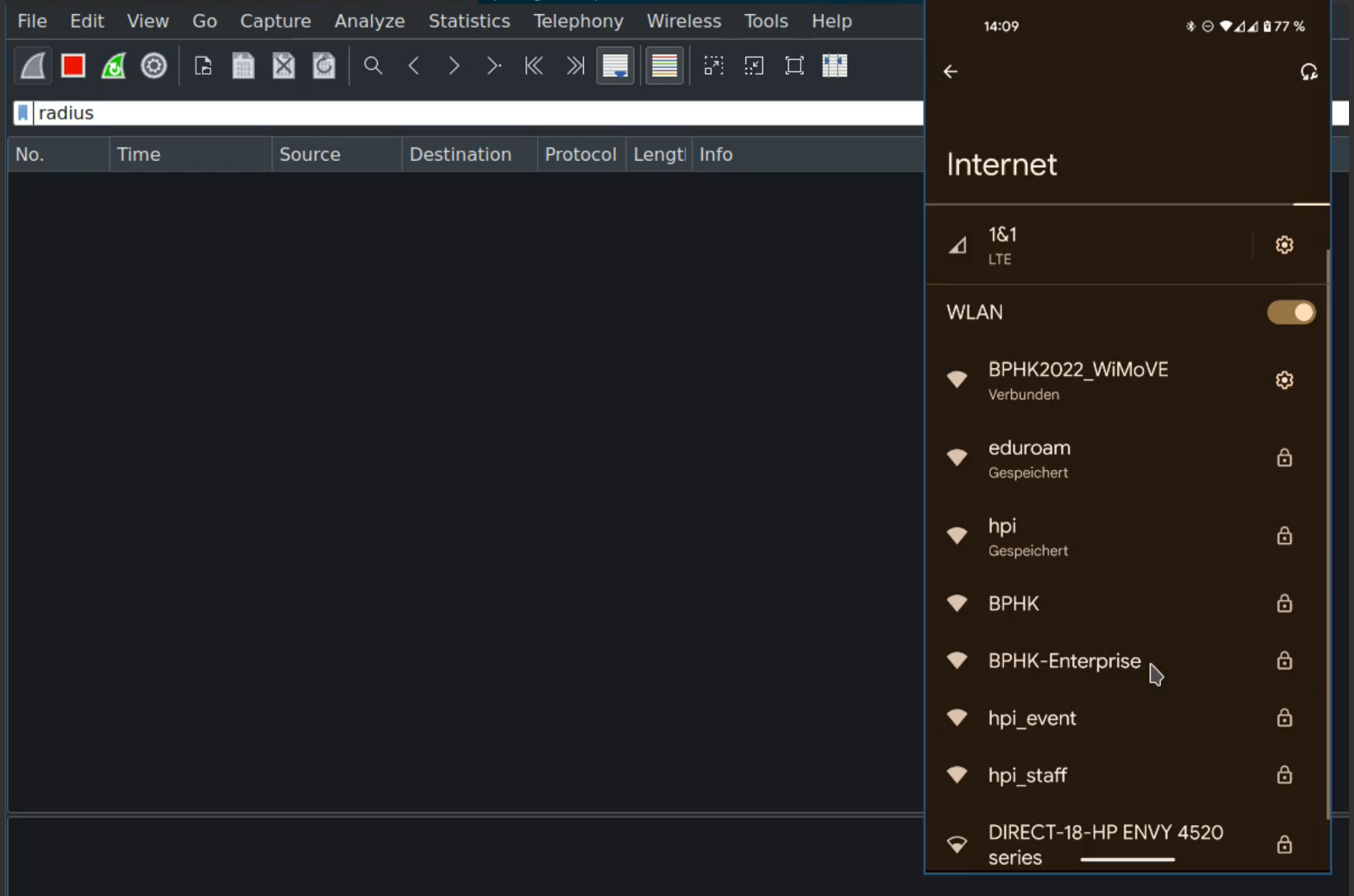
AOSP › Docs › Core Topics

Trust on First Use (TOFU)

For devices running Android 13 or higher, Android supports the Tr
(RFC7435), which lets users trust an enterprise (EAP) network by
setting its domain name in a saved network. TOFU allows the devi
when a user first connects to an enterprise network and retain the

Background




File Edit View Go Capture Analyze Statistics Telephony Wireless Tools Help
radius
No. Time Source Destination Protocol Lengt Info
14:09
77 %
Internet
1&1
LTE
WLAN
BPHK2022_WiMoVE
Verbunden
eduroam
Gespeichert
hpi
Gespeichert
BPHK
BPHK-Enterprise
hpi_event
hpi_staff
DIRECT-18-HP ENVY 4520 series

Bug Bounty? Well, too late...

DESCRIPTION bu...@google.com created issue on behalf of Aaron Schlitt #1

Report description

When using "Trust on first use" in Android 13, Android completes the MSCHAPv2 TLS authentication pro

CVE-2023-20965

https://dl.acm.org/doi/10.1145/3558482.3590199

28. Juni 2023

The Devil is in the Details: Hidden Problems of Client-Side Enterprise Wi-Fi Configurators

Ka Lok Wu
Department of Information Engineering
The Chinese University of Hong Kong
Sha Tin, Hong Kong
klwu@link.cuhk.edu.hk

Man Hong Hue*
Georgia Institute of Technology
Atlanta, GA, USA
hugohue@gatech.edu

Ka Fun Tang
Department of Information Engineering
The Chinese University of Hong Kong
Sha Tin, Hong Kong
1155126139@link.cuhk.edu.hk

Sze Yiu Chau
Department of Information Engineering
The Chinese University of Hong Kong
Sha Tin, Hong Kong
sychau@ie.cuhk.edu.hk

ABSTRACT

In the context of connecting to enterprise Wi-Fi, previous works show that relying on human users to manually configure or enforce server authentication often leads to insecure outcomes. Consequently, many user credentials can potentially be stolen by the so-called "Evil-Twin" (ET) attack. To ease the burden of human users, various easy-to-use Wi-Fi configurators have been released and deployed. In this work, we investigate whether such configurators can indeed protect users from variants of the ET attack. To our surprise, the results of our investigation show that all configurators considered in the study suffer from certain weaknesses due to their design, implementation, or deployment practices. Notable findings include a series of design flaws in the new trust-on-first-use (TOFU) configurator on Android (available since version 12), which can be exploited in tandem to achieve a stealthy ET attack. Moreover, we found that 2 open-source Android Wi-Fi configurators fail to properly enforce server authentication under specific situations. The cause of these could be partly attributed to the complexity stemmed from certificate name matching as well as the limitations of the Android API. Last but not least, we found that a commercial configurator not only allows insecure Wi-Fi configurations to be deployed, but also the covert injection of certificates on the user device to facilitate interception of other TLS traffic, posing yet another hidden security and privacy threat to its users. All in all, this study shows that despite years of research on the topic, developing a user-friendly yet reliable Wi-Fi configurator remains an elusive goal, and thus the threat of ET attacks continues to be relevant. As such, it is time to rethink whether the complexity of the standard certificate chain validation is actually good for enterprise Wi-Fi.

*Work done while the author was at The Chinese University of Hong Kong.

CCS CONCEPTS

• **Security and privacy** → **Mobile and wireless security**; **Software security engineering**; *Authentication.*

KEYWORDS

WPA Enterprise, Evil-Twin, Authentication, TLS, Trust-on-first-use

ACM Reference Format:
Ka Lok Wu, Man Hong Hue, Ka Fun Tang, and Sze Yiu Chau. 2023. The Devil is in the Details: Hidden Problems of Client-Side Enterprise Wi-Fi Configurators. In *Proceedings of the 16th ACM Conference on Security and Privacy in Wireless and Mobile Networks (WiSec '23), May 29-June 1, 2023, Guildford, United Kingdom.* ACM, New York, NY, USA, 11 pages. https://doi.org/10.1145/3558482.3590199

1 INTRODUCTION

Wi-Fi is a near-ubiquitous technology that enables Internet connectivity to countless devices. Depending on how the user gets authenticated, a Wi-Fi setup can be classified as the *personal* mode, where authentication is achieved using a pre-shared key (PSK), or the *enterprise* mode, where the authentication is done via the IEEE 802.1X standard. Comparatively, the enterprise mode enables a more fine-grained authorization and accounting, and is thus more commonly used by large companies and educational institutes. In fact, many organizations take advantage of IEEE 802.1X to reuse existing single sign-on (SSO) credentials for accessing their enterprise Wi-Fi. Unfortunately, this also makes enterprise Wi-Fi a high-value target for attackers, as stolen credentials can enable access to other resources of the victim organization.

Typical in such setups, the *client device*, also known as the *supplicant*, would establish a TLS tunnel with the *authentication server* to protect the password-based user authentication. Unfortunately, since the SSID itself is not cryptographically verifiable, an attacker can launch a Wi-Fi setup broadcasting the same SSID, known as an Evil Twin (ET), and trick nearby supplicants into connecting.

Danke!

Slides: https://aaronschlitt.de/hsv7