MESH TKT

Sébastien Raveau

June 30, 2023

.plan

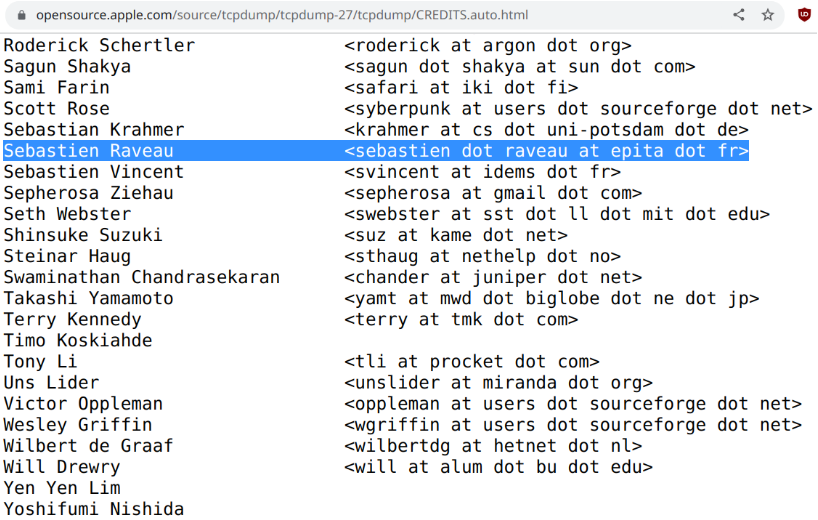
$ whoami

LSE

TII

WPA

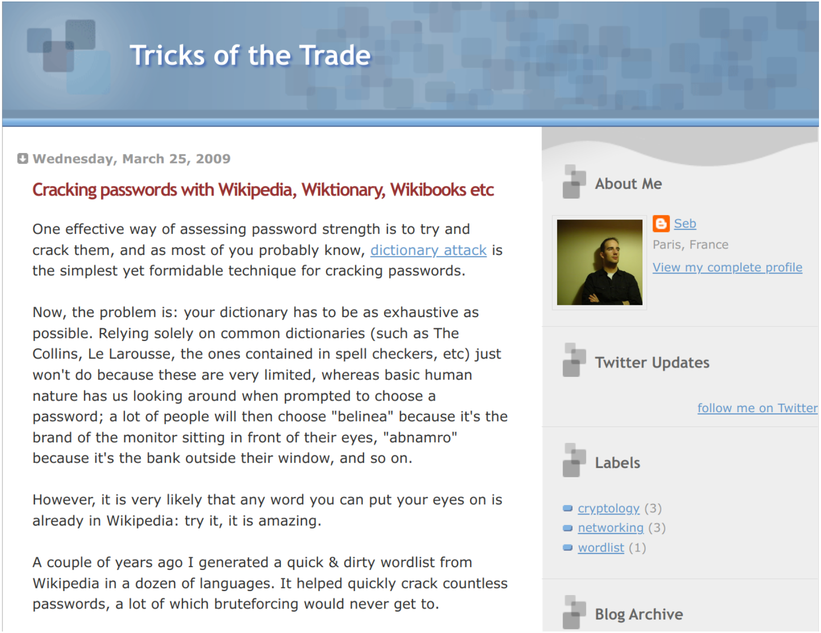
EPITA reprezent!



opensource.apple.com/source/tcpdump/tcpdump-27/tcpdump/CREDITS.auto.html

```
Roderick Schertler               <roderick at argon dot org>
Sagun Shakya                     <sagun dot shakya at sun dot com>
Sami Farin                       <safari at iki dot fi>
Scott Rose                       <syberpunk at users dot sourceforge dot net>
Sebastian Krahmer                <krahmer at cs dot uni-potsdam dot de>
Sebastien Raveau                 <sebastien dot raveau at epita dot fr>
Sebastien Vincent                <svincent at idems dot fr>
Sepherosa Ziehau                 <sepherosa at gmail dot com>
Seth Webster                     <swebster at sst dot ll dot mit dot edu>
Shinsuke Suzuki                  <suz at kame dot net>
Steinar Haug                     <sthaug at nethelp dot no>
Swaminathan Chandrasekaran       <chander at juniper dot net>
Takashi Yamamoto                 <yamt at mwd dot biglobe dot ne dot jp>
Terry Kennedy                    <terry at tmk dot com>
Timo Koskiahde
Tony Li                          <tli at procket dot com>
Uns Lider                        <unslider at miranda dot org>
Victor Oppleman                  <oppleman at users dot sourceforge dot net>
Wesley Griffin                   <wgriffin at users dot sourceforge dot net>
Wilbert de Graaf                 <wilbertdg at hetnet dot nl>
Will Drewry                      <will at alum dot bu dot edu>
Yen Yen Lim
Yoshifumi Nishida
```

Peut pas raconter sa vie tranquille



Tricks of the Trade

Wednesday, March 25, 2009

Cracking passwords with Wikipedia, Wiktionary, Wikibooks etc

One effective way of assessing password strength is to try and crack them, and as most of you probably know, dictionary attack is the simplest yet formidable technique for cracking passwords.

Now, the problem is: your dictionary has to be as exhaustive as possible. Relying solely on common dictionaries (such as The Collins, Le Larousse, the ones contained in spell checkers, etc) just won't do because these are very limited, whereas basic human nature has us looking around when prompted to choose a password; a lot of people will then choose "belinea" because it's the brand of the monitor sitting in front of their eyes, "abnamro" because it's the bank outside their window, and so on.

However, it is very likely that any word you can put your eyes on is already in Wikipedia: try it, it is amazing.

A couple of years ago I generated a quick & dirty wordlist from Wikipedia in a dozen of languages. It helped quickly crack countless passwords, a lot of which bruteforcing would never get to.

About Me

Seb

Paris, France

View my complete profile

Twitter Updates

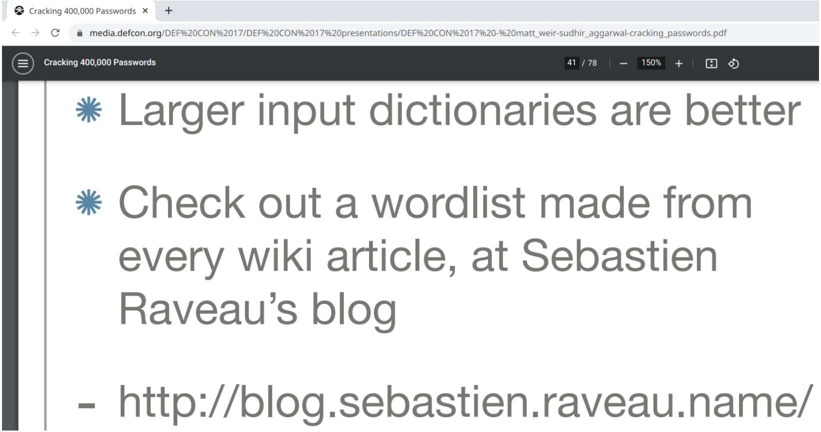
follow me on Twitter

Labels

- cryptology (3)
- networking (3)
- wordlist (1)

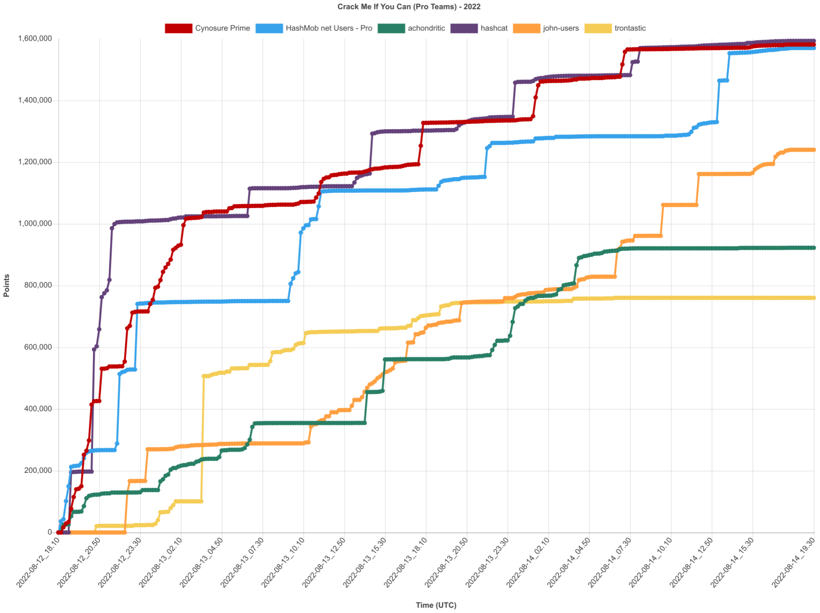
Blog Archive

DEF CON 2009: Cracking 400,000 Passwords


Cracking 400,000 Passwords
media.defcon.org/DEF%20CON%2017/DEF%20CON%2017%20presentations/DEF%20CON%2017%20-%20matt_weir-sudhir_aggarwal-cracking_passwords.pdf
Cracking 400,000 Passwords
41 / 78
150%

- Larger input dictionaries are better
- Check out a wordlist made from every wiki article, at Sebastien Raveau's blog
  - http://blog.sebastien.raveau.name/

Team Hashcat: DEF CON Crack Me If You Can



.plan

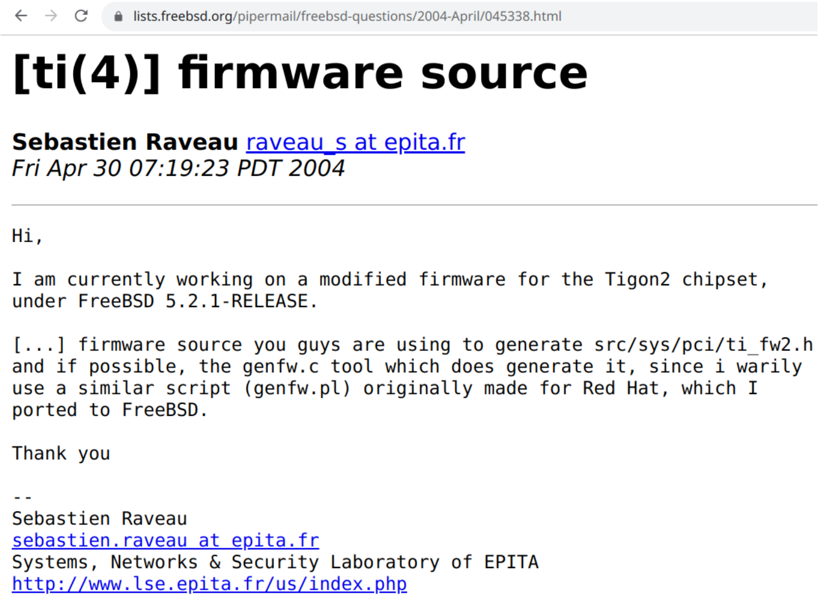
$ whoami

LSE

TII

WPA

LSE en 2004: Vianney, rootme, kaneton, NICEFw, etc



lists.freebsd.org/pipermail/freebsd-questions/2004-April/045338.html

[ti(4)] firmware source

Sebastien Raveau raveau_s at epita.fr
Fri Apr 30 07:19:23 PDT 2004

Hi,

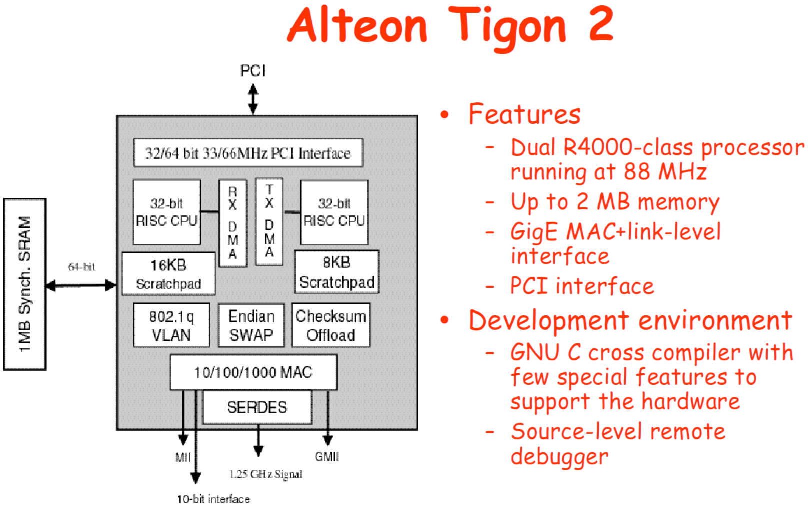
I am currently working on a modified firmware for the Tigon2 chipset, under FreeBSD 5.2.1-RELEASE.

[...] firmware source you guys are using to generate src/sys/pci/ti_fw2.h and if possible, the genfw.c tool which does generate it, since i warily use a similar script (genfw.pl) originally made for Red Hat, which I ported to FreeBSD.

Thank you

--
Sebastien Raveau
sebastien.raveau at epita.fr
Systems, Networks & Security Laboratory of EPITA
http://www.lse.epita.fr/us/index.php

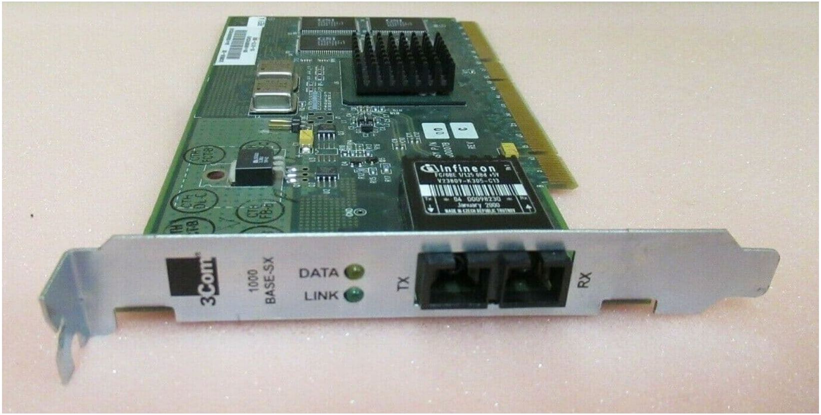
Tigon2 chipset: dual MIPS, opensource, bi-endian



Alteon Tigon 2

- Features
  - Dual R4000-class processor running at 88 MHz
  - Up to 2 MB memory
  - GigE MAC+link-level interface
  - PCI interface
- Development environment
  - GNU C cross compiler with few special features to support the hardware
  - Source-level remote debugger

3Com 3C985B-SX: ni 1000BASE-T, ni PCI-E



LSE@4am: debugging headless cross-compiled bi-endian

.plan

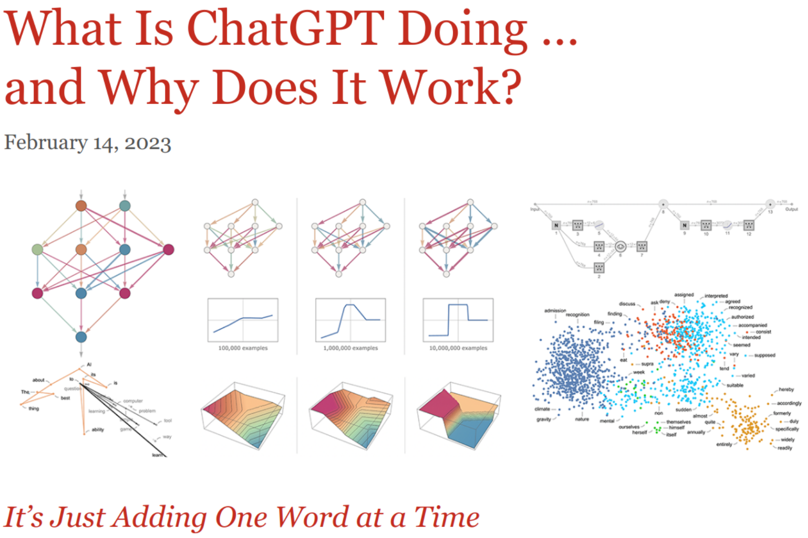
$ whoami

LSE

TII

WPA

Fin 2022: ChatGPT open access, everyone loses their mind



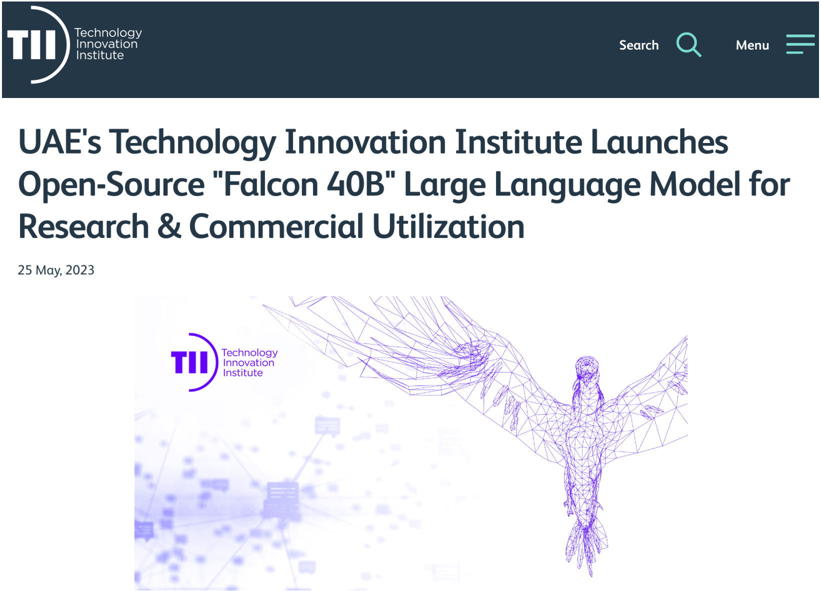
What Is ChatGPT Doing … and Why Does It Work?

February 14, 2023

It's Just Adding One Word at a Time

cf Stephen Wolfram Writings

Mai 2023: Falcon 40B opensource, no one bats an-

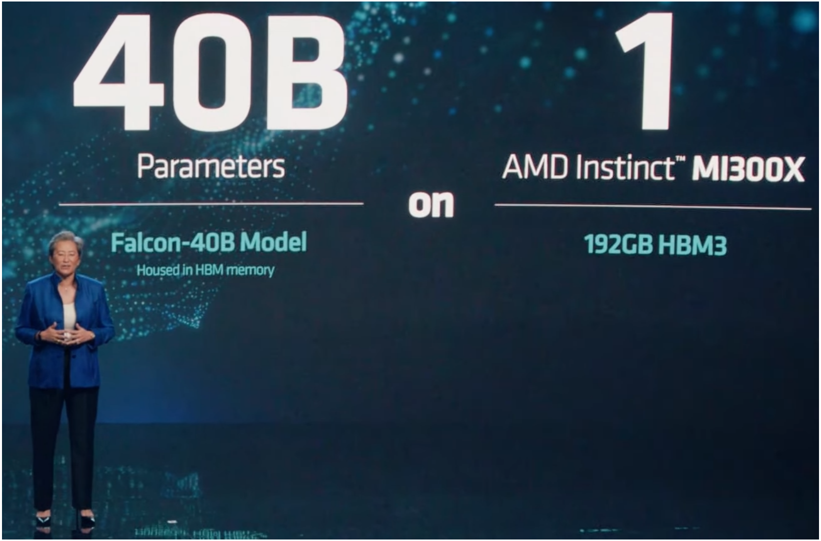


UAE's Technology Innovation Institute Launches Open-Source "Falcon 40B" Large Language Model for Research & Commercial Utilization

25 May, 2023

cf falconllm.tii.ae

Juin 2023: AMD Data Center & AI Technology Premiere



40B

Parameters

Falcon-40B Model

Housed in HBM memory

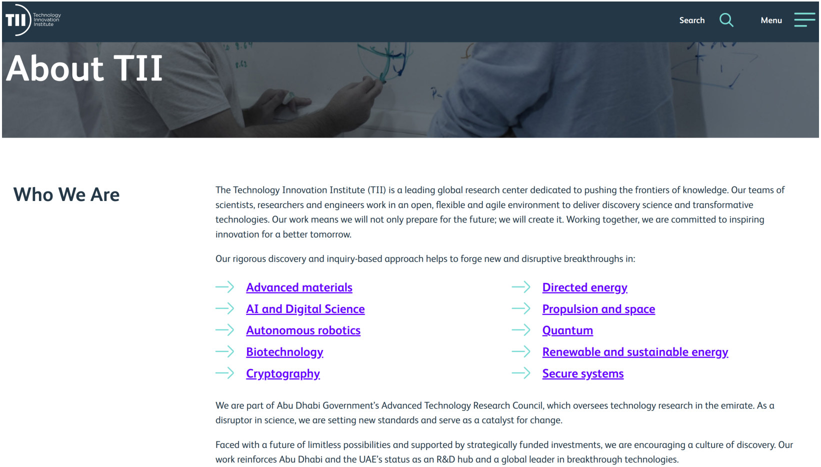
on

1

AMD Instinct™ MI300X

192GB HBM3

TLDR: $TII = (LSE + LRDE)^{awesome!}$



About TII

Who We Are

The Technology Innovation Institute (TII) is a leading global research center dedicated to pushing the frontiers of knowledge. Our teams of scientists, researchers and engineers work in an open, flexible and agile environment to deliver discovery science and transformative technologies. Our work means we will not only prepare for the future; we will create it. Working together, we are committed to inspiring innovation for a better tomorrow.

Our rigorous discovery and inquiry-based approach helps to forge new and disruptive breakthroughs in:

- Advanced materials
- AI and Digital Science
- Autonomous robotics
- Biotechnology
- Cryptography
- Directed energy
- Propulsion and space
- Quantum
- Renewable and sustainable energy
- Secure systems

We are part of Abu Dhabi Government's Advanced Technology Research Council, which oversees technology research in the emirate. As a disruptor in science, we are setting new standards and serve as a catalyst for change.

Faced with a future of limitless possibilities and supported by strategically funded investments, we are encouraging a culture of discovery. Our work reinforces Abu Dhabi and the UAE's status as an R&D hub and a global leader in breakthrough technologies.

cf youtube.com/@ATRCuae

.plan

$ whoami

LSE

TII

WPA

WPA 1/2/3 Personal: auth par mot de passe partagé

Avantages

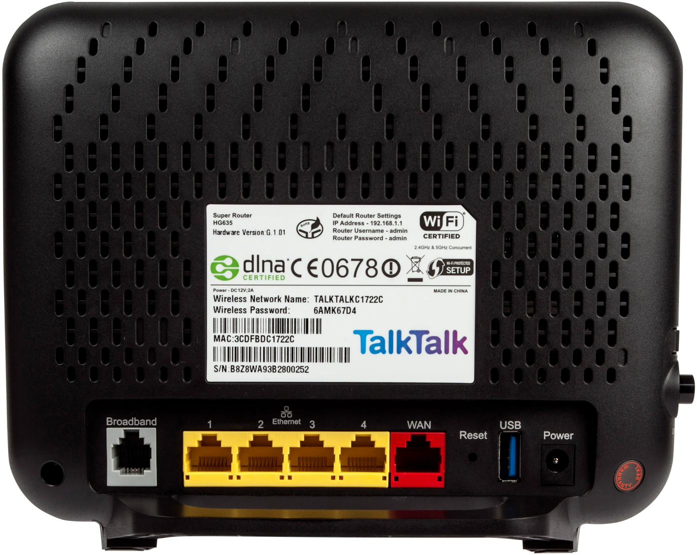
- On ne peut plus facile à configurer
- Supporté par tous les clients

Inconvénients

- Encourage de la sécurité faible
- Ne peut profiter de sécurité matérielle
- On ne sait jamais vraiment qui est qui
- Aucun contrôle sur le partage
- Impossible de bannir

cf Private/Identity/Dynamic PSK

Quasiment partout: Pre-Shared Key (PSK)



Super Router
HG635
Hardware Version:G.1.01

Default Router Settings
IP Address - 192.168.1.1
Router Username - admin
Router Password - admin

Power - DC12V;2A

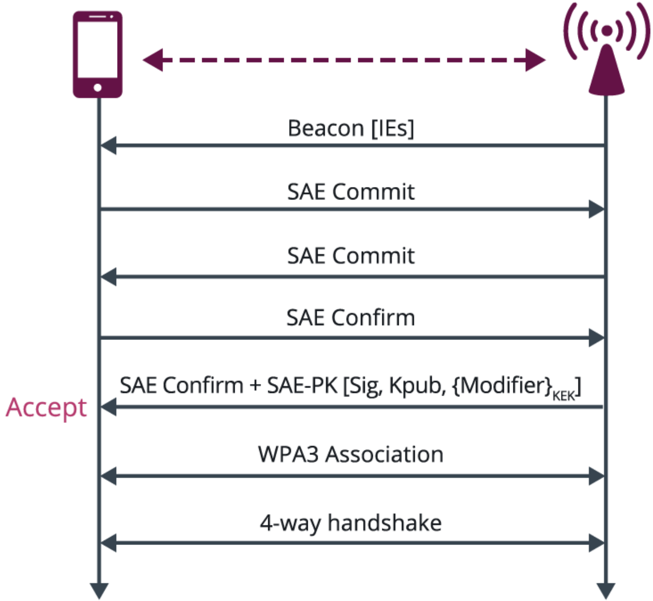
MADE IN CHINA

Wireless Network Name: TALKTALKC1722C
Wireless Password: 6AMK67D4

MAC:3CDFBDC1722C

S/N:B8Z8WA93B2800252

Un peu mieux: Simultaneous Auth of Equals (SAE)



WPA 1/2/3 Enterprise: auth par certificats, entre autres

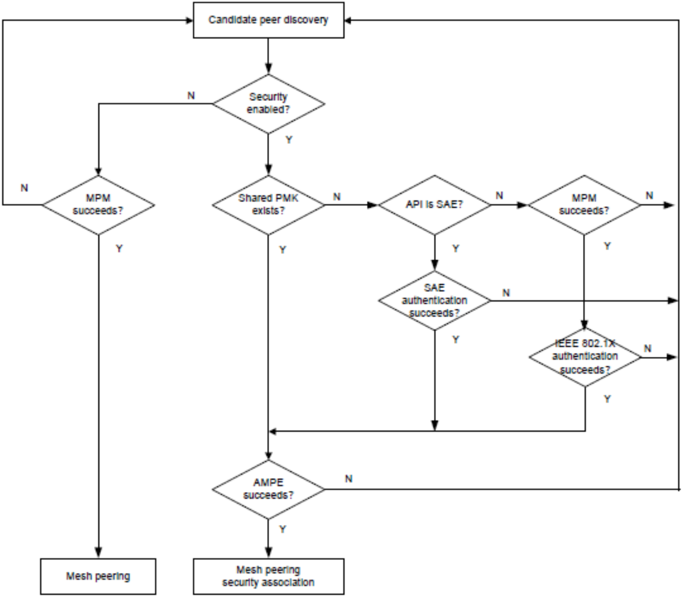
Avantages

- Identifiants très forts et individuels, surtout si HSM
- Difficile/impossible de partager/fuiter, surtout si HSM
- 2FA built-in et permet de protéger TLS avec e.g. GPSK
- Plus tous les avantages d'une gestion par PKI

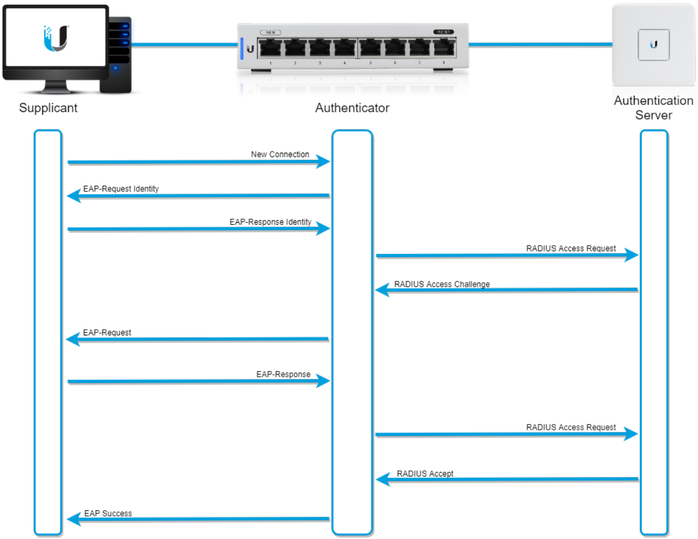
Inconvénients

- Standardisé pour le mesh mais pas encore implémenté

Mesh Peering Management, Authenticated MP Exchange



802.1x


Supplicant
Authenticator
Authentication Server
New Connection
EAP-Request Identity
EAP-Response Identity
RADIUS Access Request
RADIUS Access Challenge
EAP-Request
EAP-Response
RADIUS Access Request
RADIUS Accept
EAP Success

hostapd

Point d'accès WPA 1/2/3 Personal/Enterprise mais pas seulement:

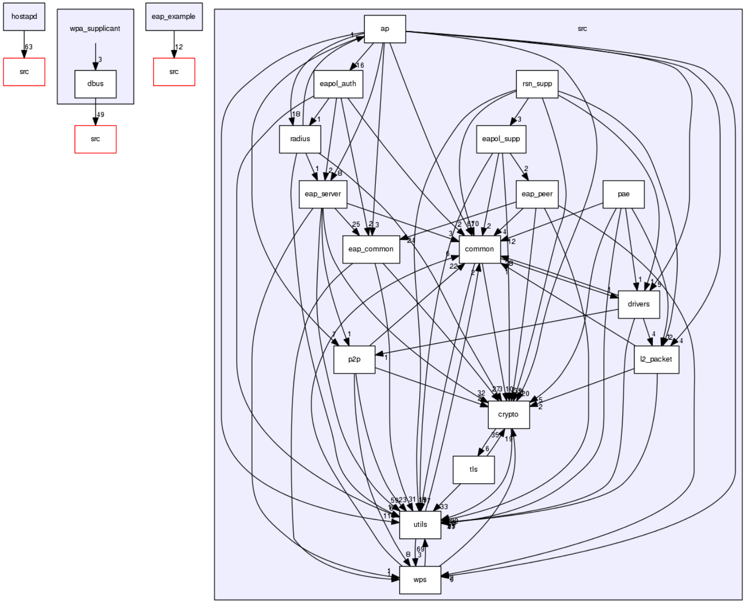
- Peer/Authenticator/AS 802.1x filaire (en plus du WiFi)
- Peer/Authenticator/AS MACsec

wpa_supplicant

Client WPA 1/2/3 Personal/Enterprise mais pas seulement:

- Supplicant 802.1x filaire (en plus du WiFi)
- Supplicant MACsec
- Point mesh WiFi
- Point d'accès WiFi?!

https://w1.fi/cgit/hostap/tree/



Contact

Par la ML du LSE ou bien:

- linkedin.com/in/sebastienraveau
- twitter.com/sraveau