EBERHARD KARLS
UNIVERSITÄT
TÜBINGEN

FACULTY OF
SCIENCE
Communication Networks

xRAC: Execution and Access Control for Restricted Application Containers on Managed Hosts

Frederik Hauser, Mark Schmidt, Michael Menth

http://kn.inf.uni-tuebingen.de

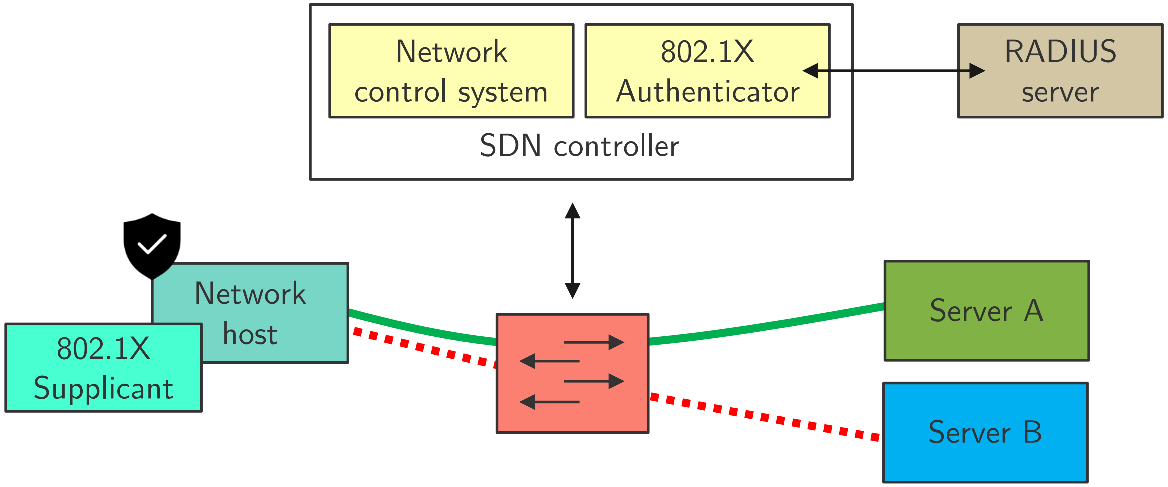
Publication

- Full paper accepted at NOMS 2020 (main session)
  - https://atlas.informatik.uni-tuebingen.de/~menth/papers/Menth20a.pdf

- Demo paper accepted at NOMS 2020
  - https://atlas.informatik.uni-tuebingen.de/~menth/papers/Menth20b.pdf

- Outline
  - Motivation
  - Concept
  - Prototypical implementation

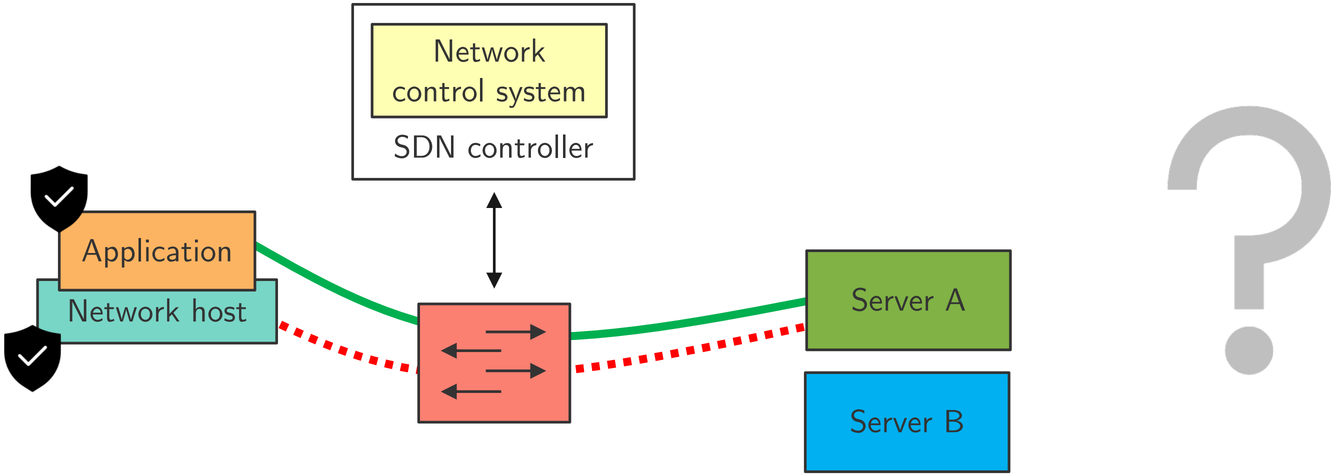
Motivation for xRAC (1/3)



- **Previous work**: 802.1X in SDN
  - Authentication of user / network host
  - Fine-granular network control of host traffic

Motivation for xRAC (2/3)

- **Desirable**: Fine-granular network control of application traffic

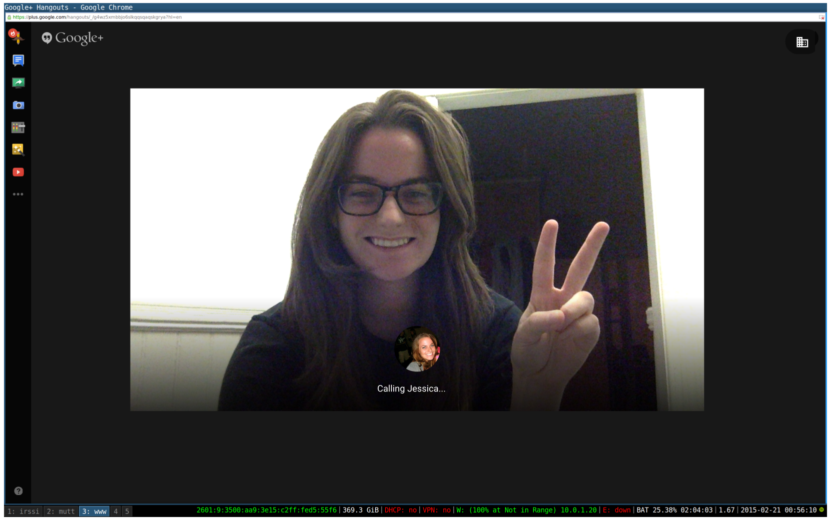


- Status quo: end-to-end encryption (TLS)
- How to solve it?
  - Traffic identification via ML
  - Traffic identification via host agent (control channel)
  - Authentication and authorization on application layer

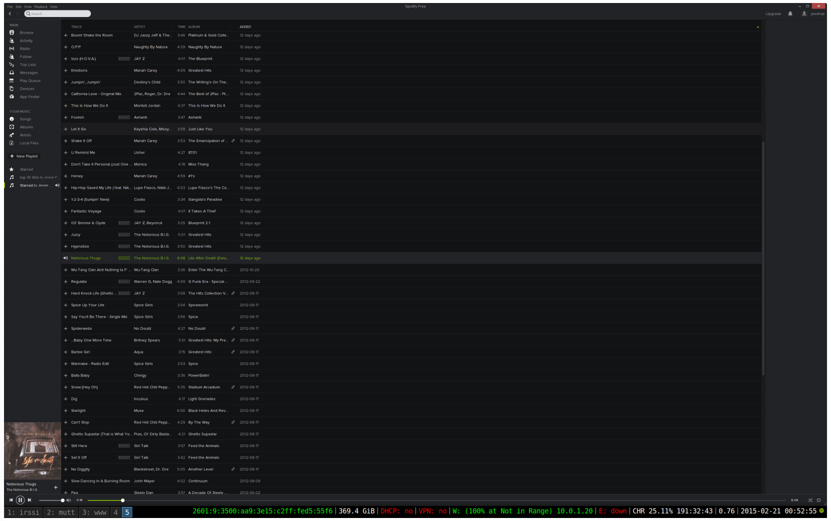
Motivation for xRAC (3/3)

„Most people use Docker for containing applications to deploy into production or for building their applications in a contained environment. This is all fine & dandy, and saves developers & ops engineers huge headaches, but I like to use Docker in a not-so-typical way.
I use Docker to run all the desktop apps on my computers.“

https://blog.jessfraz.com/post/docker-containers-on-the-desktop/


Google+ Hangouts - Google Chrome
https://plus.google.com/hangouts/_/g4wz5xmbbjo6slkqqsqaqskgrya?hl=en
Google+
Calling Jessica...

```
1: irssi  2: mutt  3: www  4  5   2601:9:3500:aa9:3e15:c2ff:fed5:55f6 | 369.3 GiB | DHCP: no | VPN: no | W: (100% at Not in Range) 10.0.1.20 | E: down | BAT 25.38% 02:04:03 | 1.67 | 2015-02-21 00:56:10
```



TRACK	ARTIST	TIME	ALBUM	ADDED
Boom! Shake the Room	DJ Jazzy Jeff & The...	3:46	Platinum & Gold Colle...	12 days ago
O.P.P	Naughty By Nature	4:29	Naughty By Nature	12 days ago
Izzo (H.O.V.A.)	JAY Z	4:01	The Blueprint	12 days ago
Emotions	Mariah Carey	4:09	Greatest Hits	12 days ago
Jumpin', Jumpin'	Destiny's Child	3:50	The Writing's On The...	12 days ago
California Love - Original Mix	2Pac, Roger, Dr. Dre	4:44	The Best of 2Pac - Pt....	12 days ago
This Is How We Do It	Montell Jordan	4:37	This Is How We Do It	12 days ago
Foolish	Ashanti	3:47	Ashanti	12 days ago
Let It Go	Keyshia Cole, Missy...	3:58	Just Like You	12 days ago
Shake It Off	Mariah Carey	3:53	The Emancipation of ...	12 days ago
U Remind Me	Usher	4:27	8701	12 days ago
Don't Take It Personal (Just One ...	Monica	4:18	Miss Thang	12 days ago
Honey	Mariah Carey	4:59	#1's	12 days ago
Hip-Hop Saved My Life (feat. Nik...	Lupe Fiasco, Nikki J...	4:03	Lupe Fiasco's The Co...	12 days ago
1-2-3-4 (Sumpin' New)	Coolio	3:34	Gangsta's Paradise	12 days ago
Fantastic Voyage	Coolio	4:01	It Takes A Thief	12 days ago
03' Bonnie & Clyde	JAY Z, Beyoncé	3:25	Blueprint 2.1	12 days ago
Juicy	The Notorious B.I.G.	5:01	Greatest Hits	12 days ago
Hypnotize	The Notorious B.I.G.	3:50	Greatest Hits	12 days ago
Notorious Thugs	The Notorious B.I.G.	6:08	Life After Death (Delu...	12 days ago
Wu-Tang Clan Aint Nuthing ta F' ...	Wu-Tang Clan	3:36	Enter The Wu-Tang C...	2012-10-20
Regulate	Warren G, Nate Dogg	4:09	G Funk Era - Special ...	2012-09-22
Hard Knock Life (Ghetto ...	JAY Z	3:58	The Hits Collection V...	2012-08-17
Spice Up Your Life	Spice Girls	2:54	Spiceworld	2012-08-17
Say You'll Be There - Single Mix	Spice Girls	3:56	Spice	2012-08-17
Spiderwebs	No Doubt	4:27	No Doubt	2012-08-17
...Baby One More Time	Britney Spears	3:31	Greatest Hits: My Pre...	2012-08-17
Barbie Girl	Aqua	3:15	Greatest Hits	2012-08-17
Wannabe - Radio Edit	Spice Girls	2:53	Spice	2012-08-17
Balla Baby	Chingy	3:36	PowerBallin'	2012-08-17
Snow [Hey Oh]	Red Hot Chili Pepp...	5:35	Stadium Arcadium	2012-08-17
Dig	Incubus	4:17	Light Grenades	2012-08-17
Starlight	Muse	4:00	Black Holes And Rev...	2012-08-17
Can't Stop	Red Hot Chili Pepp...	4:29	By The Way	2012-08-17
Ghetto Supastar (That is What Yo...	Pras, Ol' Dirty Basta...	4:21	Ghetto Supastar	2012-08-17
Still Here	Girl Talk	3:57	Feed the Animals	2012-08-17
Set It Off	Girl Talk	3:42	Feed the Animals	2012-08-17
No Diggity	Blackstreet, Dr. Dre	5:05	Another Level	2012-08-17
Slow Dancing In A Burning Room	John Mayer	4:02	Continuum	2012-08-09
Peg	Steely Dan	3:57	A Decade Of Steely ...	2012-06-02

```
1: irssi  2: mutt  3: www  4  5   2601:9:3500:aa9:3e15:c2ff:fed5:55f6 | 369.4 GiB | DHCP: no | VPN: no | W: (100% at Not in Range) 10.0.1.20 | E: down | CHR 25.11% 191:32:43 | 0.76 | 2015-02-21 00:52:55
```

Ramblings from Jessie

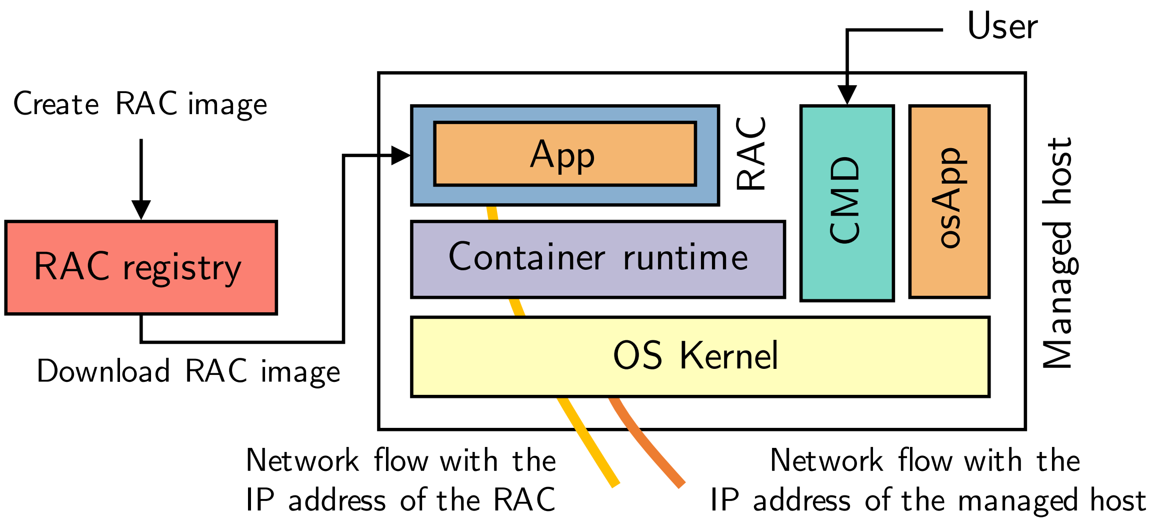
Docker Containers on the Desktop

Saturday, February 21, 2015

Hello!

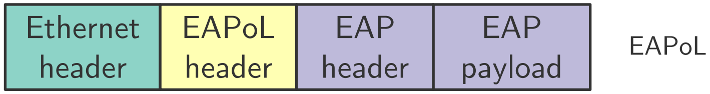
RACs

- Restricted Application Containers (RACs)
  - Docker container (application, dependencies, configuration)
  - Networking: unique IPv6 address
  - Execution: managed host



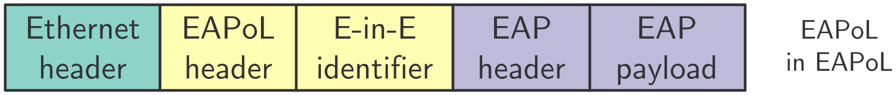
802.1X for AA of Applications

- FlowNAC (*Matias et al., 2014*)
  - SDN-based NAC for applications
  - EAPoL-over-EAPoL



Ethernet header	EAPoL header	EAP header	EAP payload

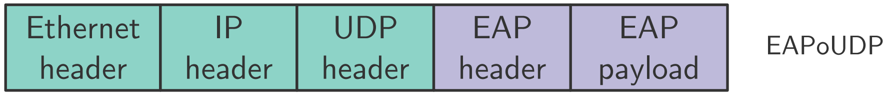
EAPoL



Ethernet header	EAPoL header	E-in-E identifier	EAP header	EAP payload

EAPoL in EAPoL

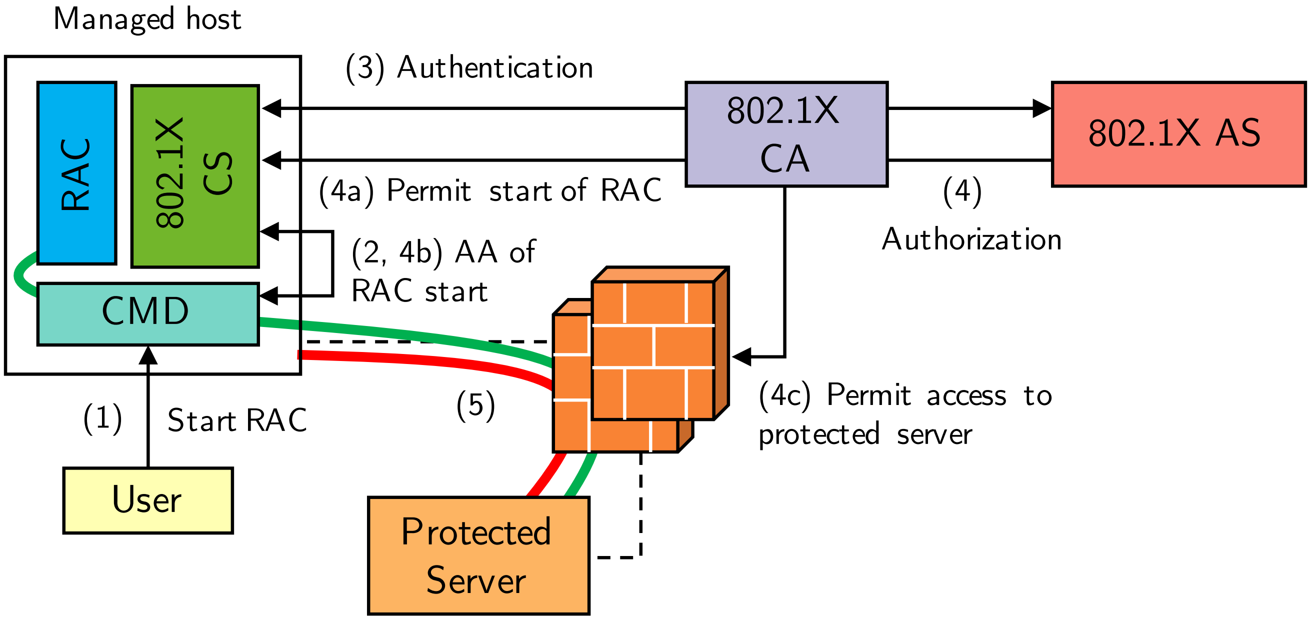
- EAPoUDP
  - Expired draft from PANA WG
  - Adopted by Cisco Trust Agent (deprecated)



Ethernet header	IP header	UDP header	EAP header	EAP payload

EAPoUDP

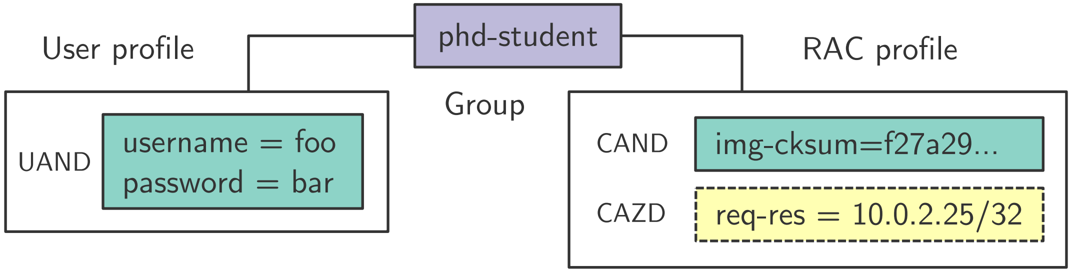
xRAC Architecture & Mechanism



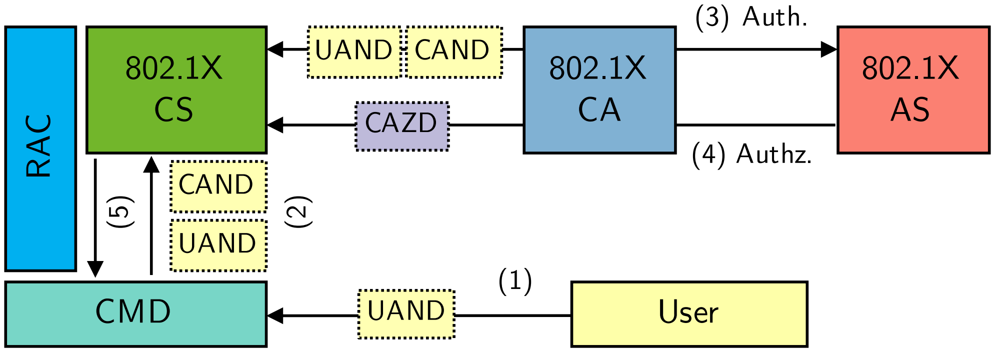
Idea: Adopt 802.1X AA for RACs

AA of Applications with xRAC (1/2)

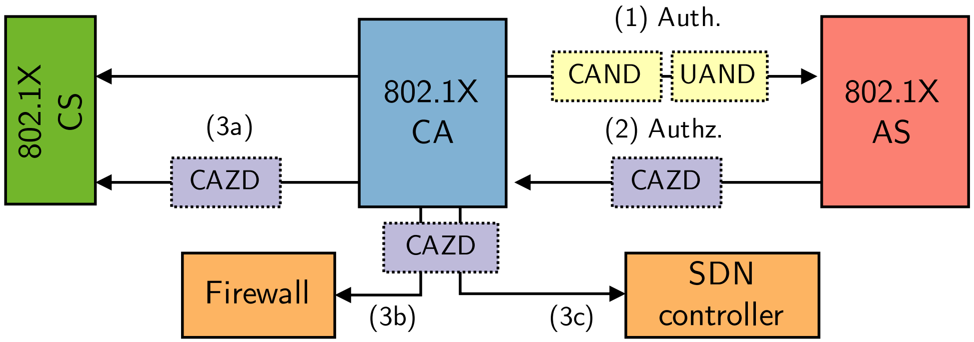
- **802.1X Authentication Server (802.1X AS)**
  - Task I: authenticate user
    - User Authentication Data (UAND)
  - Task II: authenticate RAC
    - Container Authentication Data (CAND)
  - Task III: perform authorization decision for user + RAC
    - Container Authorization Data (CAZD)



AA of Applications with xRAC (2/2)



Perspective of the 802.1X Container Supplicant (802.1X CS)

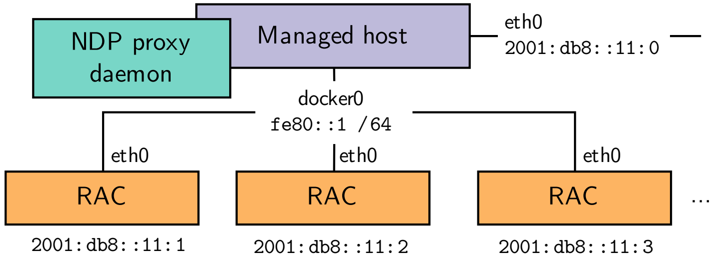


Perspective of the 802.1X Container Authenticator (802.1X CA)

Prototypical Implementation

- Prototypical implementation (Linux hosts + OpenFlow SDN)

- RAC networking
  - IPv6 subnet for managed host
  - Dedicated IPv6 global unicast address for every RAC



- 802.1X components
  - **802.1X CS:** Python plugin for Docker authorization (AuthZ) framework
  - **802.1X CA:** SDN application for Ryu SDN controller
  - **802.1X AS:** Vendor-specific attributes on FreeRADIUS server

- Sourcecode available on GitHub

https://github.com/uni-tue-kn/xrac