Enabling Network access for IoT devices

draft-st-t2trg-nw-access-01
IETF 103
9 November, 2018
Bangkok

The Register®
Biting the hand that feeds IT

Emergent Tech ▸ Internet of Things

If you're serious about securing IoT gadgets, may as well start here

We're not here to fsck spiders – prove you care by getting busy with RADIUS and EAP

By Richard Chirgwin 25 Jul 2018 at 04:21 39 SHARE ▼

Can we overcome the SOHOpeless security of the Internet of Things at the home and small business level? An Internet-Draft from Ericsson engineer Mohit Sethi suggests so.

Sethi's ambitious proposal isn't destined for the hall of internet standards. Instead, it sets out a possible way to get IoT gadgets connected securely

Most read

A boss pinching pennies may have cost his firm many, many pounds

UK.gov went ahead with under-planned, under-funded IT upgrade? Sounds about right

Microsoft's next Windows 10 release creeps closer with a cluster of builds

Activists rattle tin to take UK's pr0n block to court

SpaceX dodges lightning while storms keep Japan earthbound

The Security Problem

The Security Problem

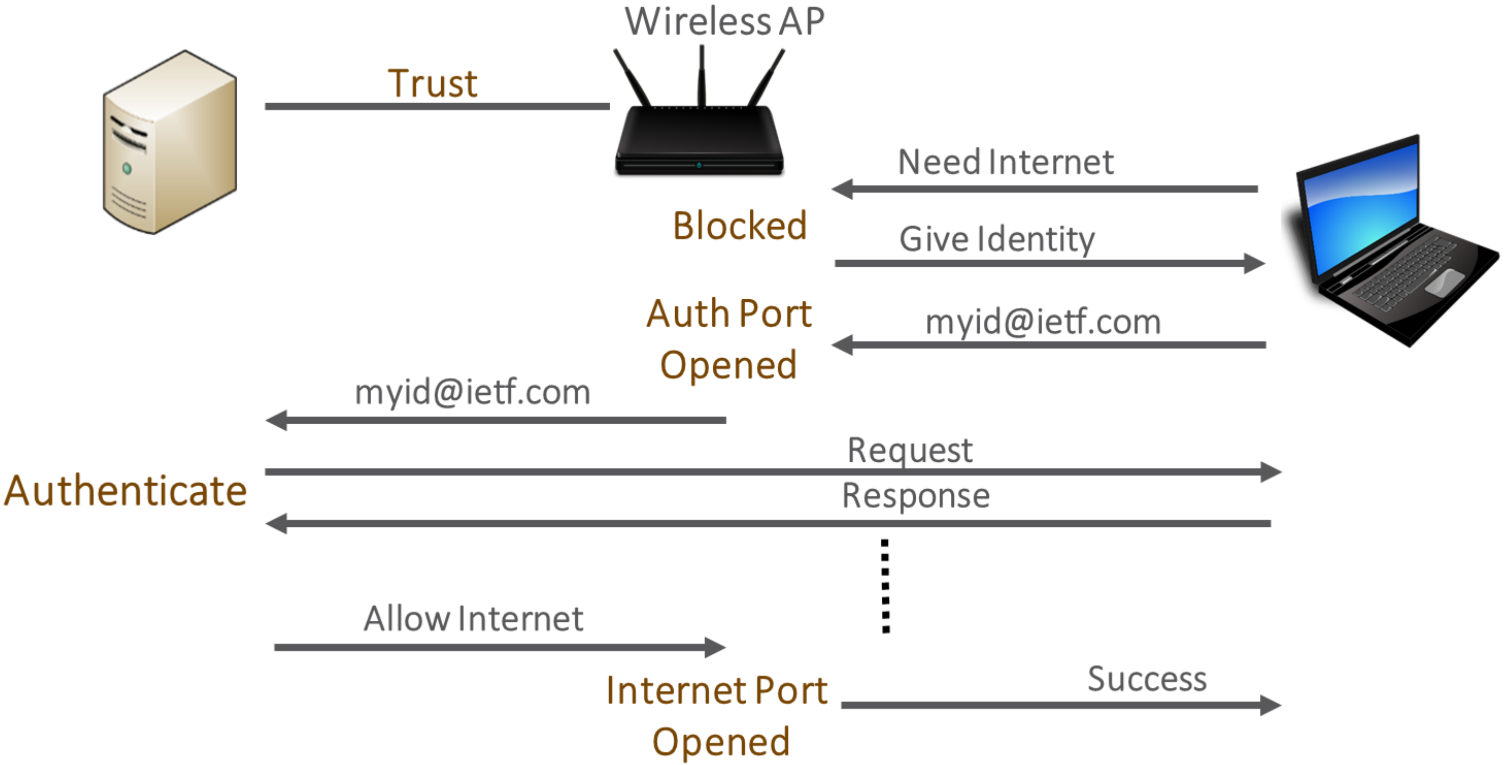
- Need to securely configure devices:
  - SSID and password for wireless Internet access
  - Secure association with a cloud service,
    e.g. with user account and password

- Need to securely manage devices:
  - Is my device misbehaving?
  - How do I perform a software update?

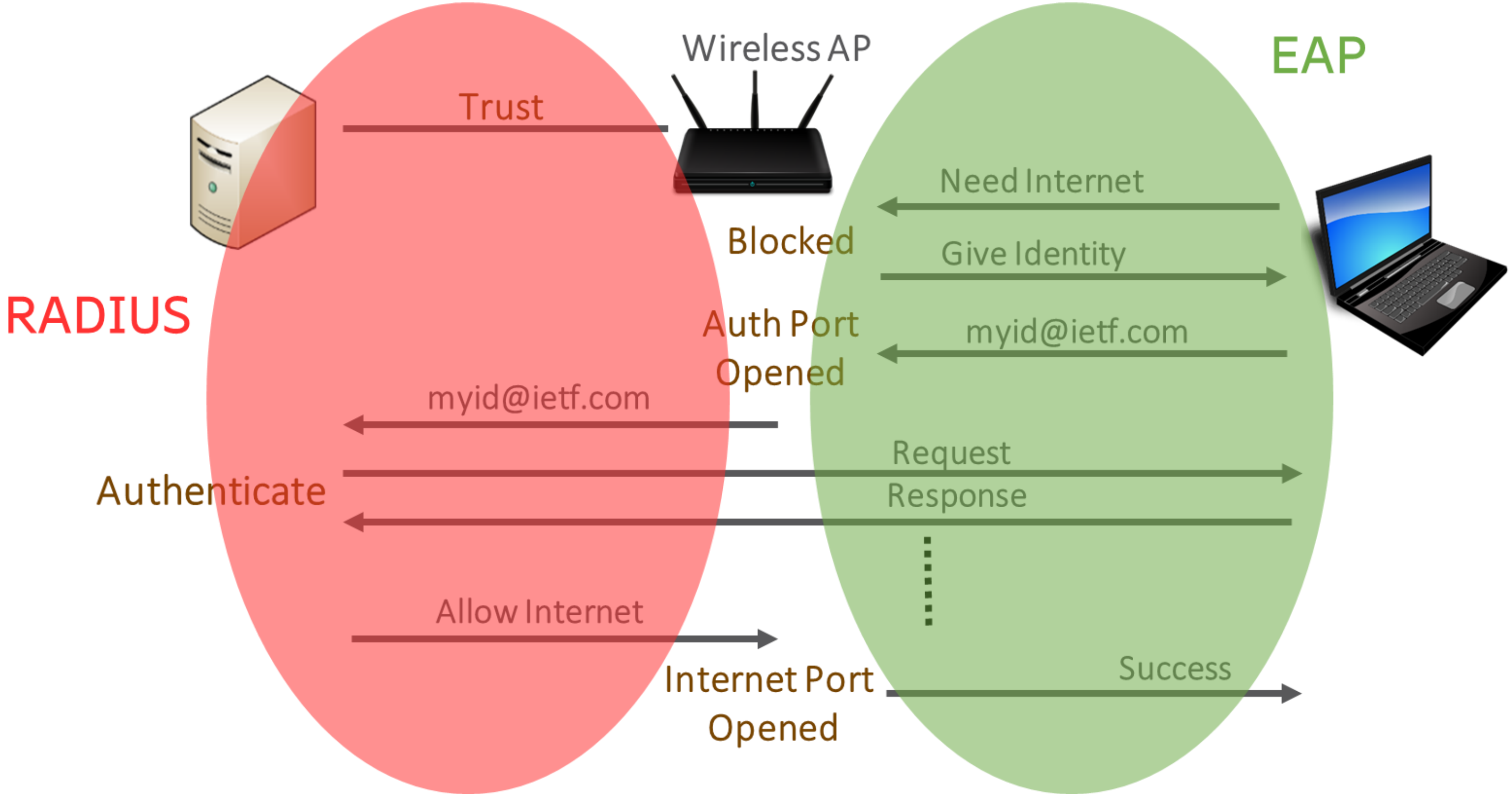
The Security Problem - Challenges

- Non-expert users
  - A typical home user does not have a computer science degree
  - Even enterprise IT administrators are only marginally better
- Scalability
  - How do I manage 2,3,4 to 100s of devices
- Minimal User Interface
  - How do I configure an Amazon dash button
- Lifecycle
  - What do I do when my Internet-connected toaster is no longer supported
    - (Revolv smart hub: http://revolv.com/)

802.1x Enterprise Security

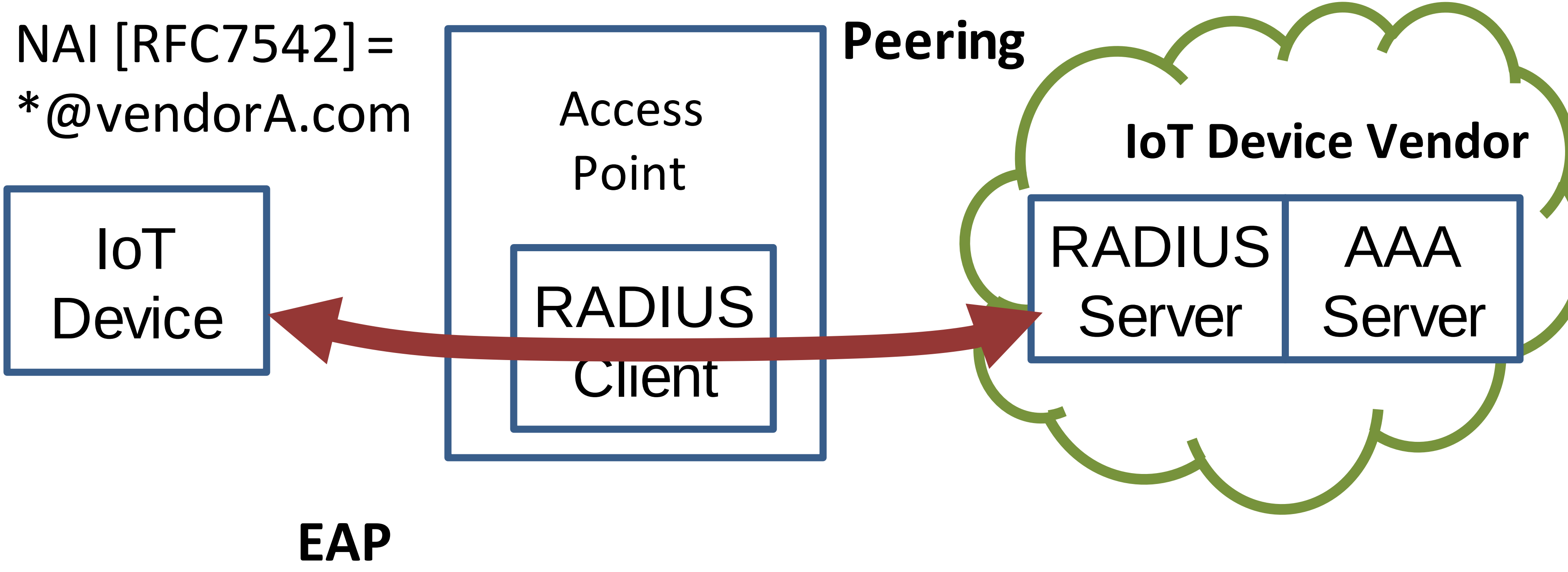


802.1x Enterprise Security



EAP for Bootstrapping

NAI [RFC7542] =
*@vendorA.com



IoT Device

Access Point

RADIUS Client

Peering

IoT Device Vendor

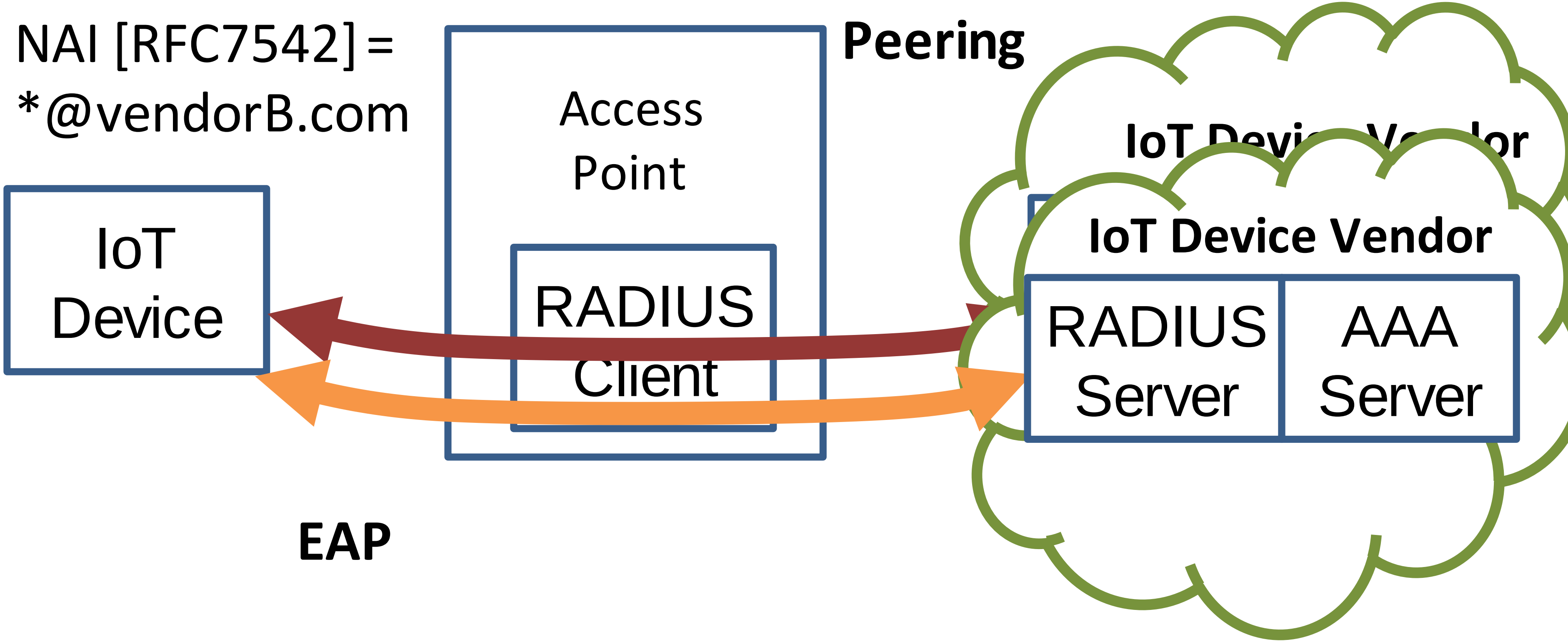
RADIUS Server

AAA Server

EAP

EAP for Bootstrapping

NAI [RFC7542] =
*@vendorB.com



But my manufacture is dead – Börje

- Change AAA RADIUS/DIAMETER peering to new service
- May require transfer of credentials
- Who would run this server?
  - DD-WRT -> OpenWRT
  - Android -> Cynogenmod

Capture Devices - Carsten

- Use EAP methods that provide mutual authentication
- Use Calling-Station-Id and Called-Station-Id to see if the user+device is allowed to connect through given AP

New deployment modes

- Buy new blank device:
  - Feed key (PSK) on device
  - Feed key (PSK) on server
  - Let them discover + mutual authentication (EAP-PSK)
  - Confirm right parties are connected