Security problems in IoT

Computest

About me

Thomas Stols

- Security specialist at Computest
- Member of Retail / Industry / IoT team
- Developer, system administrator, hacker
- Kerckhoffs security master

Security research

Advisories

2018-08-14 - XenServer
Path traversal leading to authentication bypass

2018-07-19 - Volkswagen MIB infotainment system
Unauthenticated remote code execution as root

2017-07-12 - NAPALM -
Command execution on NAPALM controller from host

2017-04-25 - MySQL Connector/J
Unexpected automatic deserialisation of Java objects

2017-01-09 - Ansible
Command execution on Ansible controller from host

2016-11-10 - Observium
Unauthenticated remote code execution

2016-08-18 – cSRP/srpforjava
Obtaining of hashed passwords

2016-06-30 - StartEncrypt
Obtaining valid SSL certificates for unauthorized domains

THE MORE COMPLEX IT GETS,
THE MORE EXCITED WE ARE.

Compu**test**
always on.

> “The networks of the future will be necessarily more complex, and therefore less secure. The technology industry is driven by the demand for features, for options, for speed. There are no standards for quality or security, and there is no liability for insecure software. Hence, there is no economic incentive to build in high quality. In fact, it's just the opposite. There is an economic incentive to create the lowest quality the market will bear. Unless customers demand higher quality and better security, this will never change.”

–Bruce Schneier

i am faster than wap
MODE
i-am-i-mode.co.uk

Windows, Apple, Application, Abandonware and Game Beta Downloads/Repository - BetaArchive - Microsoft Internet Explorer
File
Edit
View
Favorites
Tools
Help
Back
Search
Favorites
History
Address
http://www.betaarchive.com/
Go
Links
BetaArchive V2
The community for beta collectors
Established in August 2006
Website Navigation
FTP
FORUM
RSS FEED
RULES
PLEASE DONATE
Beta Archive
{The community for beta collectors}

Total Current Archive Size: 2002.77GB in 1023

60MB of 12279MB used

BetaArchive

Repositories!

About BetaArch

Forum Topics

BetaArchive - A Free Beta Reposito

With over 1000GB in our Beta Repository
largest repository of it's kind on the web!

We invite you to join our website and for
Beta Downloads and Apple Beta Download
We also have a huge Abandonware Repo
old classics, and a Beta Games Repository
your favourite games were made.

Total Current Archive Size: 2002.77GB in 10233 files

osts | View Unanswered Po
Active Topics

	Replies	Last Reply
erver 2003...	3	Someguy2 14 Jun @ 02:29
or &quo...	2	jamesadalpiaz 14 Jun @ 02:55
by TreyITGuy on 14 Jun @ 07:34	1	Andy 14 Jun @ 11:01

About Internet Explorer

Version: 5.00.2920.0000
Cipher Strength: 56-bit (Update Information)
Product ID:51873-000-0000007-09898

Based on NCSA Mosaic. NCSA Mosaic(TM); was developed at the National Center for Supercomputing Applications at the University of Illinois at Urbana-Champaign.

Copyright ©1995-1999 Microsoft Corp.

“I see two alternatives. The first is to recognize that the digital world will be one of ever-expanding features and options, of ever-faster product releases, of ever-increasing complexity and of ever-decreasing security. This is the world we have today, and we can decide to embrace it knowingly.

The other choice is to slow down, simplify and try to add security. Customers won't demand this--the issues are too complex for them to understand--so a consumer advocacy group is required. This solution might not be economically viable for the Internet, but it is the only way to get security.”

–Bruce Schneier

220 times more connected devices than in 1999

90 million vs 20 billion

So, are we in worse shape than 20 years ago?

Sprint
12:00 PM
M
T
W
T
F
S
S
Today, August 24
29
of ~73 oz
Connected
39%
of Goal
2
Bottles to Go
4
7 Day Streak

THE FUTURE OF HAIR CARE
The world's first
smart hairbrush
Embedded technolog
a holistic hair assess
Coaching on y
phone

流す大
流す小
止
おしり
ビデ
TOTO

“YOUR SCIENTISTS WERE SO PREOCCUPIED WITH WHETHER THEY COULD THEY DIDN’T STOP TO THINK IF THEY SHOULD.”

154.2
fitbit

3:18 AM
1
2
3
20
15
10
5
2.2
5.1
mmol/L
Act Ins.
0.10 u
Bolus
Basal

IS-1
ST. JUDE MEDICAL
Sylmar, CA USA
VICTORY™ SR
5610 SSIR
S/N 1723182

So, what are some of the main problems?

Costs

Model No.: EVW3226

S/N:UAAP41234567

[redacted]

Manufacturer Name: Ubee
Ubee Part No.: EVW3226EU

CM MAC:647C34123452

[redacted]

Input: +12V⎓ 2A

MTA MAC:647C34123453

[redacted]

Made in China

Default Wi-Fi : 2.4GHz
WPA2-PSK

2.4 GHz	SSID : 🔒 :	UPC2659797 IVGDQAMI
5 GHz	SSID : 🔒 :	UPC2870546 PXKRLPCC

Insecure communication

1
2
3
4
5
6
7
8
9
0
ESC
MENU
ON/OFF
OK
RES
SD

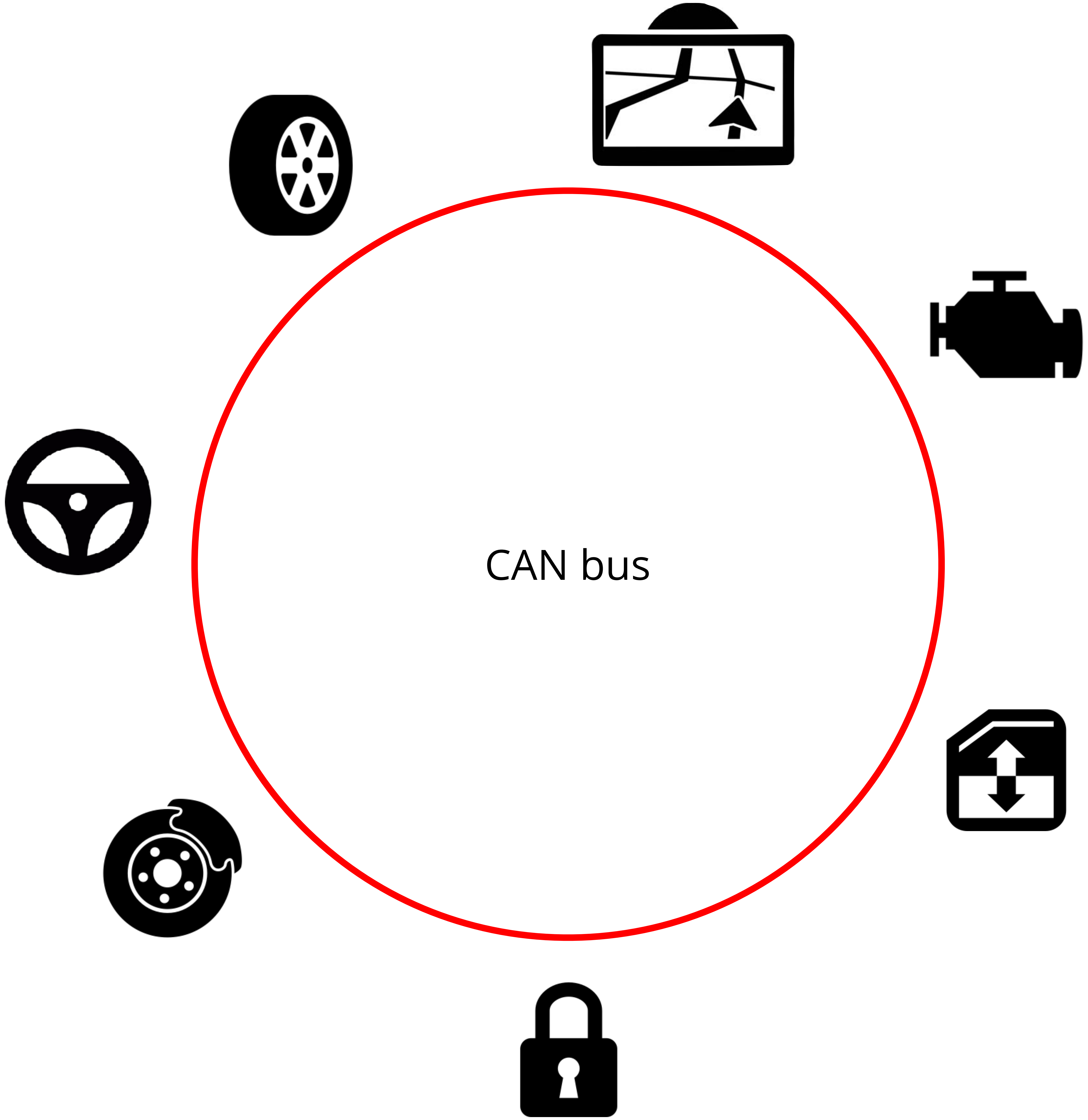
```
POST /api/device_management?serial=11-22-33-44-55
Host: xxx.xxx.xxx.xxx
Content-Type: application/x-www-form-urlencoded

action=add_user&name=Thomas&pin=1234
```

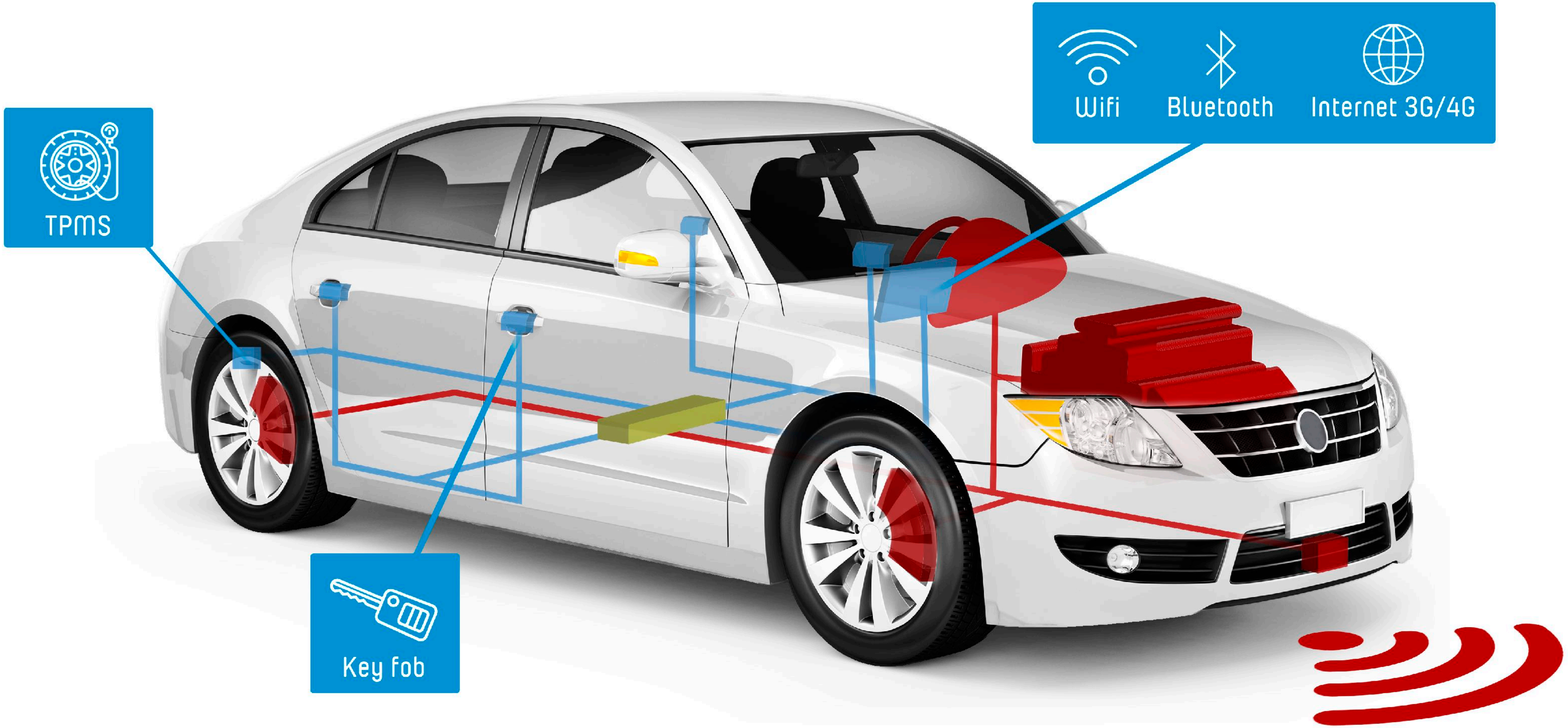
No (convenient) update mechanism

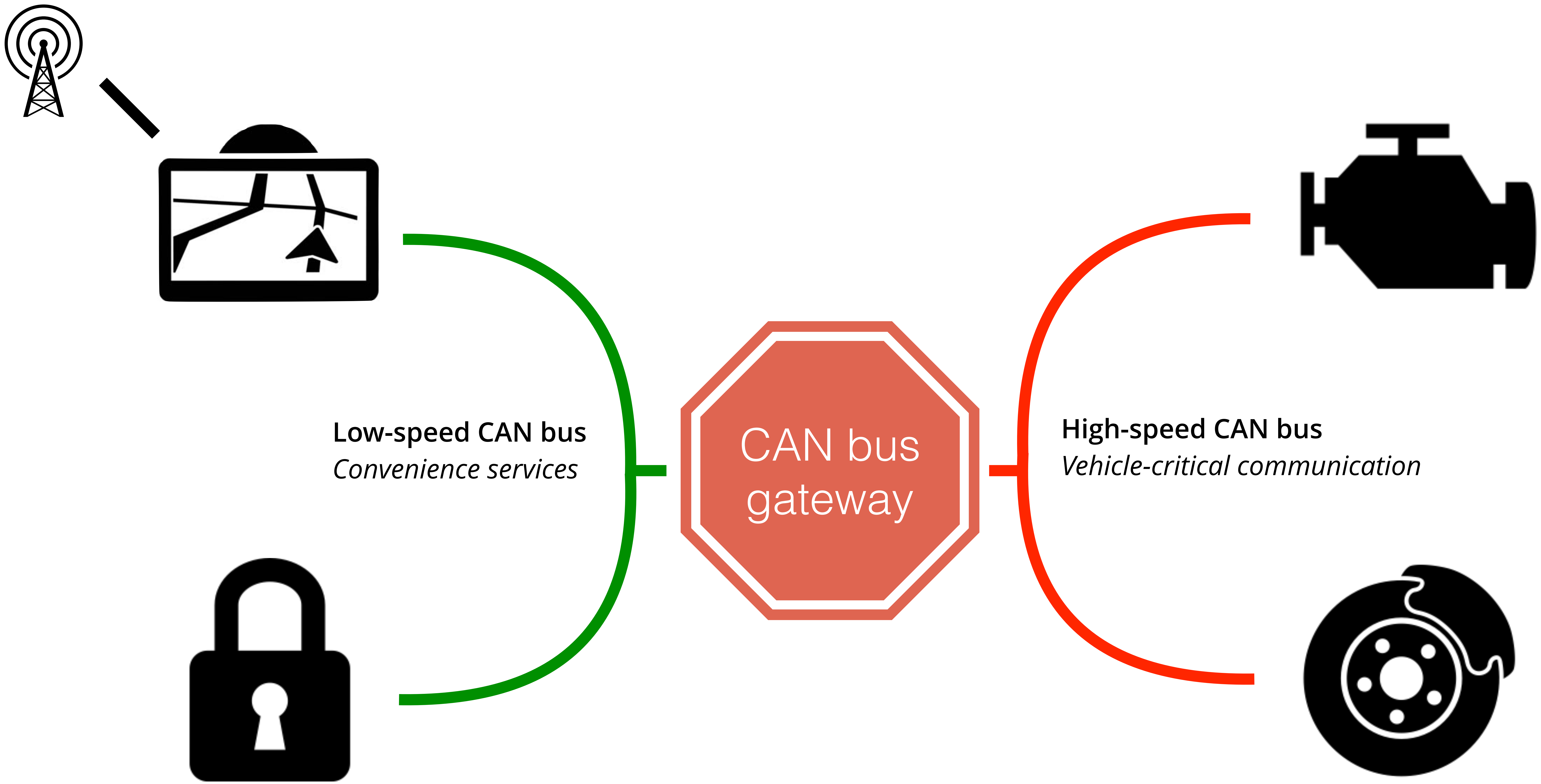
Life span

Complexity



CAN bus


Wifi
Bluetooth
Internet 3G/4G
TPMS
Key fob

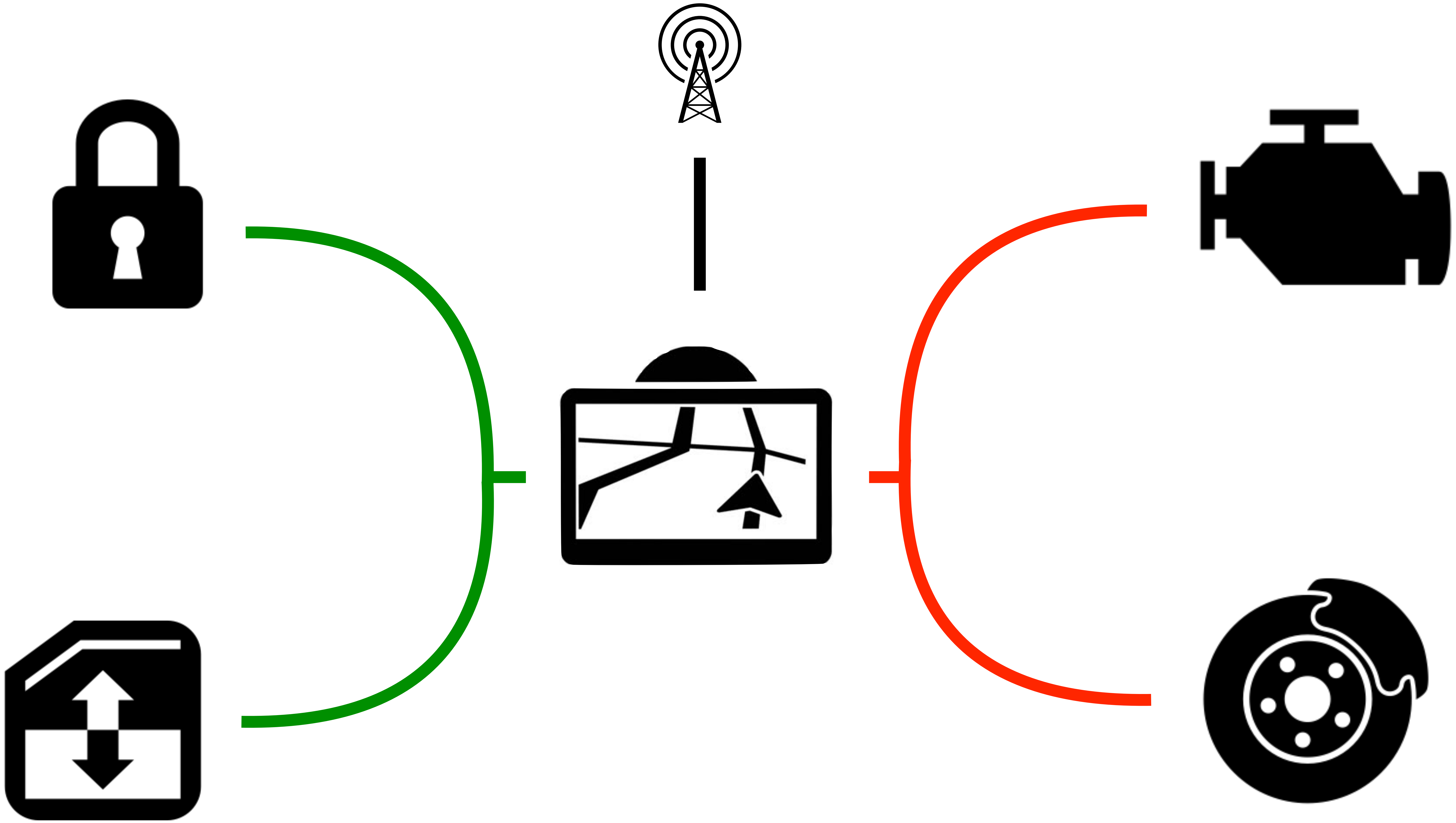


Low-speed CAN bus
Convenience services

CAN bus gateway

High-speed CAN bus
Vehicle-critical communication

Jeep



Consumer is responsible for security

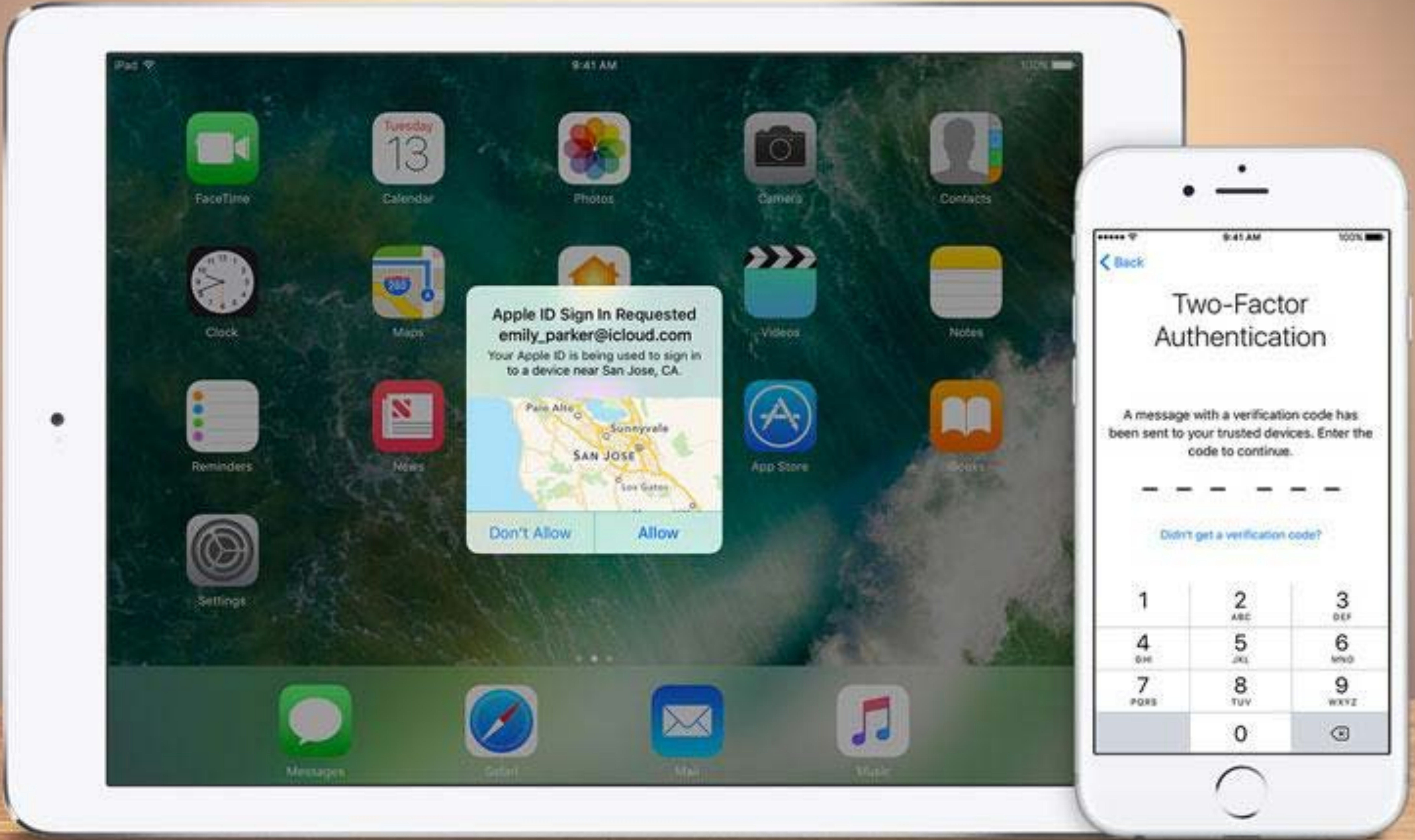
MIRAI

> “There’s been an almost tenfold increase in the volume of these (ELF) samples submitted to Virus Total over the past two years.”
>
> –Software and System Security group EURECOM

Information asymmetry

Knowledge gap

IF HISTORY REPEATS ITSELF, I'M GETTING A DINOSAUR



Apple ID Sign In Requested
emily_parker@icloud.com

Your Apple ID is being used to sign in to a device near San Jose, CA.

Don't Allow | Allow

Back

Two-Factor Authentication

A message with a verification code has been sent to your trusted devices. Enter the code to continue.

Didn't get a verification code?

ngs
Search settings

About Chrome

Google Chrome

Updating Google Chrome

Version 62.0.3202.94 (Official Build) (64-bit)

Automatically update Chrome for all users Learn more

Get help with Chrome

Report an issue

Google Chrome

Copyright 2017 Google Inc. All rights reserved.

Google Chrome is made possible by the Chromium open source project and other open source software.

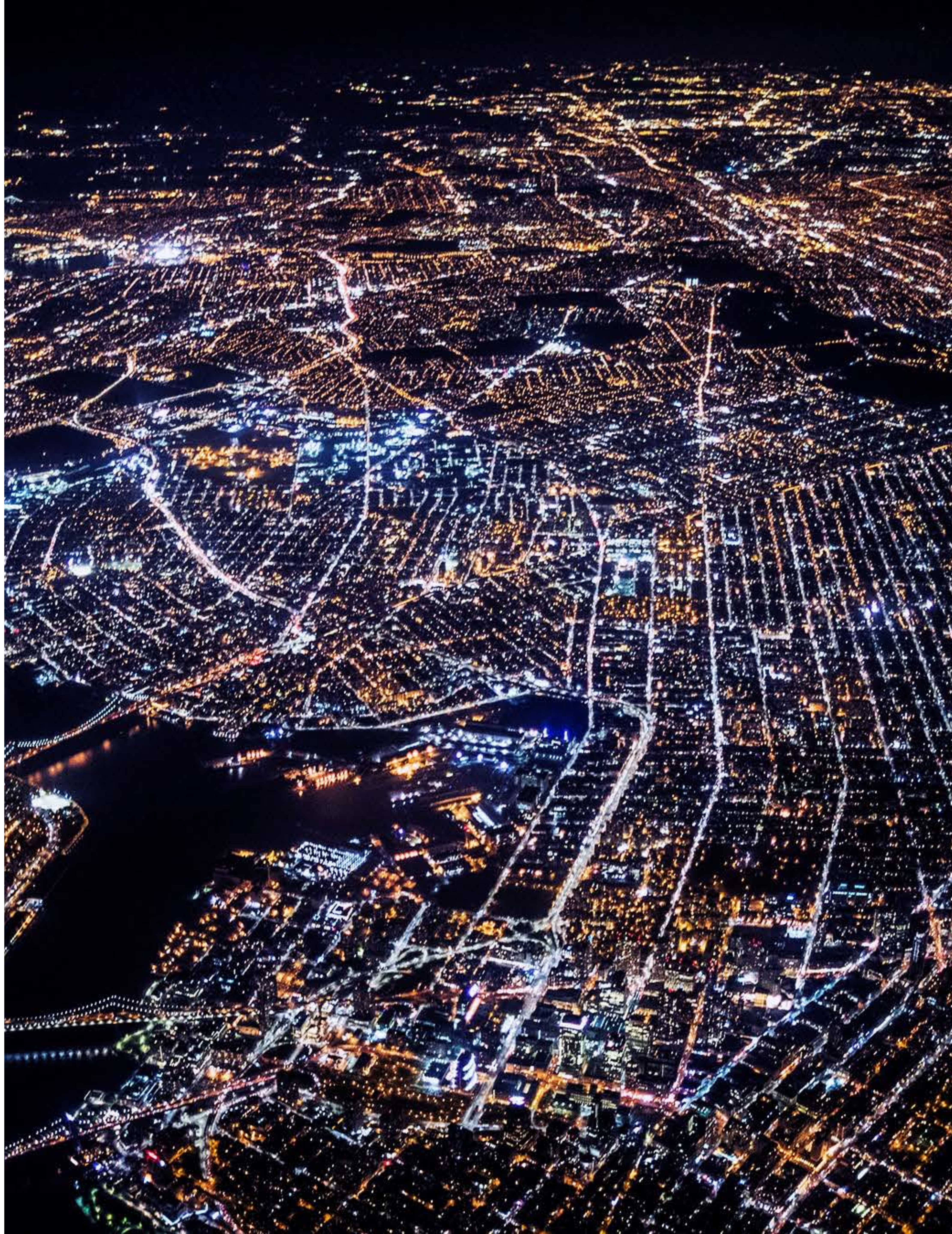
Google Chrome Terms of Service

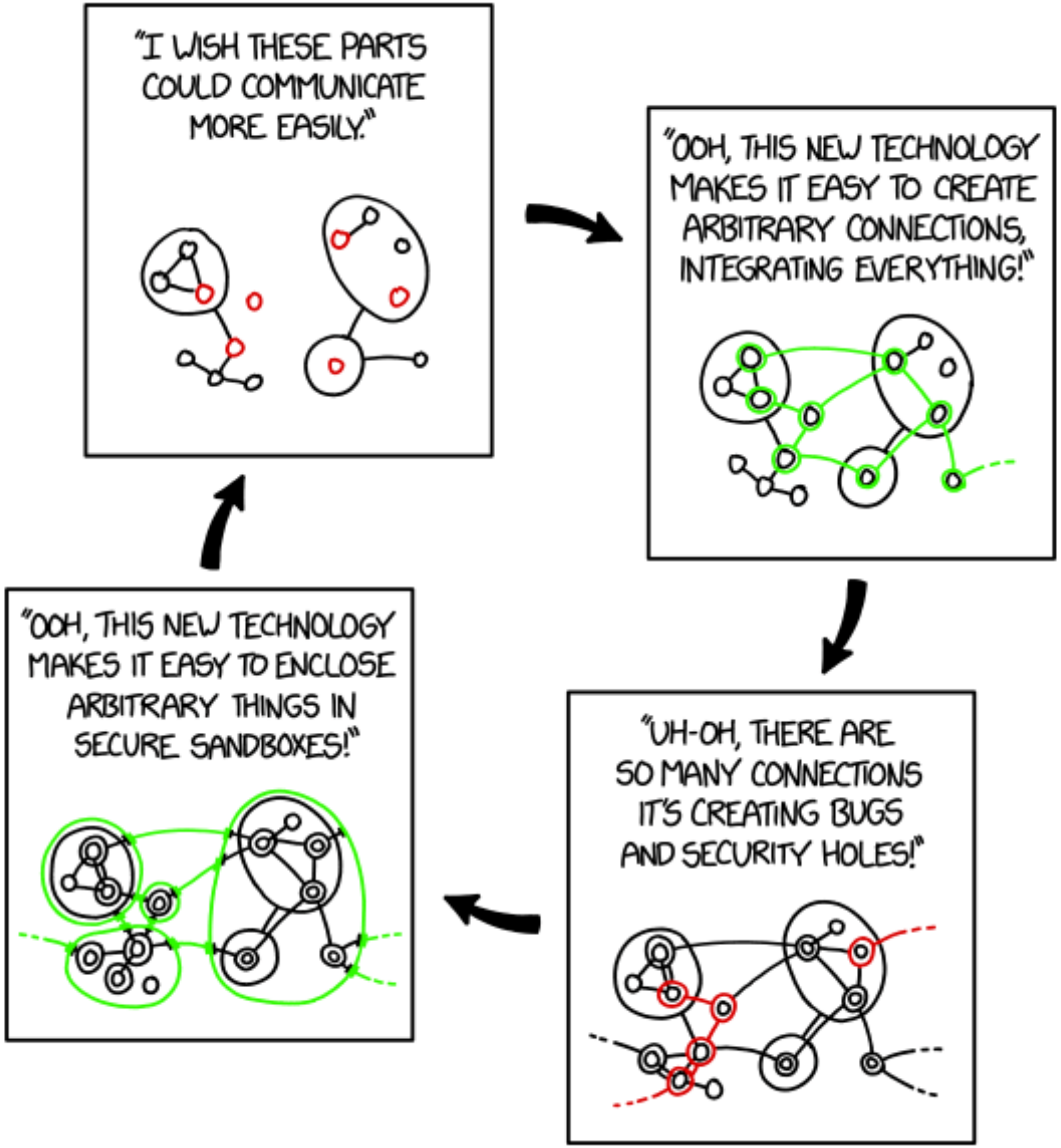
53
Young Blood
Radio
Streaming
TuneIn
Phone
Young Blood
FAVORITES
RECENT
72°
72°

So, is this an unsolvable problem?

Are we doomed?

- There are good initiatives to make IoT more resilient
  - AWS IoT Core, Azure IoT Kit, Google IoT Cloud Core etc
- Several manufacturers now have dedicated security teams
- Governments/EU are looking at regulations
  - Downside, this is only a solution for the long-term




"I WISH THESE PARTS COULD COMMUNICATE MORE EASILY."
"OOH, THIS NEW TECHNOLOGY MAKES IT EASY TO CREATE ARBITRARY CONNECTIONS, INTEGRATING EVERYTHING!"
"UH-OH, THERE ARE SO MANY CONNECTIONS IT'S CREATING BUGS AND SECURITY HOLES!"
"OOH, THIS NEW TECHNOLOGY MAKES IT EASY TO ENCLOSE ARBITRARY THINGS IN SECURE SANDBOXES!"

Thank you for listening

tstols@computest.nl