SECURITY:
THE BLIND SPOT OF ENGINEERING

Vassil Roussev

GREATER NEW ORLEANS
CENTER FOR INFORMATION ASSURANCE

WIRED

LILY HAY NEWMAN SECURITY 07.19.17 09:00 AM

WATCH HACKERS TAKE OVER A SEGWAY WITH SOMEONE ON IT

- Segway MiniPro Bluetooth app
  - » *user PIN number not always used for authentication*
  - ➔ *attacker can send arbitrary commands without the user-chosen PIN*
  - » *unauthenticated firmware update*
  - ➔ *man-in-the-middle can force update with malicious firmware*

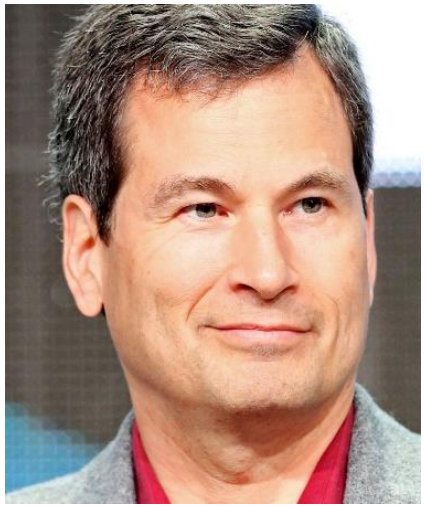
WIRED

ANDY GREENBERG GEAR 08.06.14 06:30 AM

HOW HACKABLE IS YOUR CAR? CONSULT THIS HANDY CHART

Car	Attack Surface	Network Architecture	Cyber Physical
2014 Audi A8	++	--	+
2014 Honda Accord LX	-	+	+
2014 Infiniti Q50	++	+	+
2010 Infiniti G37	-	++	+
2014 Jeep Cherokee	++	++	++
2014 Dodge Ram 3500	++	++	--
2014 Chrysler 300	++	-	++
2014 Dodge Viper	++	-	--
2015 Cadillac Escalade	++	+	+
2006 Ford Fusion	--	--	--
2014 Ford Fusion	++	-	++
2014 BMW 3 series	++	--	+
2014 BMW X3	++	--	++
2014 BMW i12	++	--	+
2014 Range Rover Evoque	++	-	++
2010 Range Rover Sport	-	--	-
2006 Range Rover Sport	-	--	-
2014 Toyota Prius	+	+	++
2010 Toyota Prius	+	+	++
2006 Toyota Prius	-	--	--

SCIENTIFIC AMERICAN®

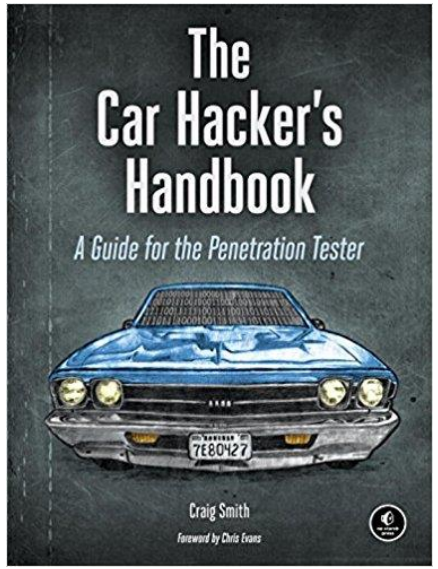


Why Car Hacking Is Nearly Impossible

Despite recent claims, your car is not about to get crashed by hackers

By David Pogue on October 28, 2016

MOVING ALONG THEN, NOTHING TO SEE HERE …



Johnson & Johnson warns of insulin pump hack risk

Elizabeth Weise, **USATODAY** Published 12:57 p.m. ET Oct. 4, 2016 | **Updated 7:35 a.m. ET Oct. 5, 2016**

"Someone would have to have malicious intent, they would have to want to harm another human being. And they've have to have technical expertise, they've have to have radio antennas and they'd have to be within 25 feet, unobstructed," said Marene Allison, the company's chief information security officer.

"Someone would have to go to extreme measures to hack in and command the insulin pump without the person's knowledge. At this point it seems like an unnecessary worry," she said.

Extreme measures?

- (CVE-2016-5084) Communications transmitted in cleartext
- (CVE-2016-5085) Weak pairing between remote and pump
  - *Attackers can trivially sniff the remote/pump key and then spoof being the remote or the pump. This can be done without knowledge of how the key is generated. This vulnerability can be used to remotely dispense insulin and potentially cause the patient to have a hypoglycemic reaction.*
- (CVE-2016-5086) Lack of replay attack prevention or transmission assurance
  - *Communication between the pump and remote have no sequence numbers, timestamps, or other forms of defense against replay attacks. Because of this, attackers can capture remote transmissions and replay them later to perform an insulin bolus without special knowledge, which can potentially cause them to have hypoglycemic reaction.*

When strangers can control our lights …

FAU Friedrich-Alexander Universität Erlangen-Nürnberg

August 30, 2017

- FAU researchers discover security flaws in smart home products
  - » *Security weaknesses in ZigBee, an important wireless standard employed for the control of smart home products.*
  - » *More than 100 million products that use ZigBee technology are estimated to have been distributed around the world.*
  - » *The most recent version, ZigBee 3.0, was released in December 2016*

ZigBee®
Control your world

At least my phone is safe, right?

DAN GOODIN - 9/12/2017, 8:00 AM

"Just by having Bluetooth on, we can get malicious code on your device," Nadir Izrael, CTO and cofounder of security firm Armis, told Ars. "BlueBorne abuses the fact that when Bluetooth is on, all of these devices are always listening for connections."

- 5.3 Billion devices affected
- 8 zero-day vulnerabilities

1. Linux kernel RCE vulnerability - CVE-2017-1000251
2. Linux Bluetooth stack (BlueZ) information Leak vulnerability - CVE-2017-1000250
3. Android information Leak vulnerability - CVE-2017-0785
4. Android RCE vulnerability #1 - CVE-2017-0781
5. Android RCE vulnerability #2 - CVE-2017-0782
6. The Bluetooth Pineapple in Android - Logical Flaw CVE-2017-0783
7. The Bluetooth Pineapple in Windows - Logical Flaw CVE-2017-8628
8. Apple Low Energy Audio Protocol RCE vulnerability - CVE-2017-14315

DEFCON

- “90 min after doors open: Complete remote control on the operating system level of the Winvote voting terminal (including election data).”
- “On the e-pollbook front: internal data structure already discovered and reverse engineered within an hour.” #VotingVillage

My point: Don't be a Pogue!!

- Safety and security are **very different** requirements
  - *… despite their failures often leading to similar results*
- Security must be a first class **design** concern
  - *Security "fixes" are nothing of the sort; bad design cannot be patched in*
- Do **not** do homegrown crypto, *a la* WEP
  - ***Do** talk to your friendly security expert*
- Do **not** assume away vulnerabilities
  - *Attacks only get better*
- Performance requirements are **not** an excuse for poor security

Legal concerns (prediction)

- Most security engineering failures are **entirely** avoidable
  - *This raises professional standard of care liability*
- It is only a matter of time before a case of device malicious device misuse leads to a death/severe injury to a sympathetic client
  - *Company gets sued for negligence*
  - *Angry jury awards **big** money*
  - *Company starts paying attention (or goes out of business)*
  - *Other companies start paying attention*
- Q: Do we have the engineers who can fix this?

Engineering education

- How many hours does an engineering student spend on security as a concern?
- Have they had anyone “redteam” their design/ implementation?
- Do we have the necessary faculty to incorporate security into the curriculum?
  - *This is a newish concern—**they** haven’t had to deal with it in college*
- It seems inevitable that secure engineering practices would **need** to be incorporated systematically

Why not start **NOW**?