Electrical & Computer ENGINEERING

18-642:
Security Vulnerabilities

11/20/2017

Carnegie Mellon University

Security Vulnerabilities

Edge Case Research

- **Anti-Patterns for vulnerabilities**
  - Ignoring vulnerabilities until attacked
  - Assuming vulnerabilities won't be exploited:
    - Unsecure embedded networks
    - Reverse engineering of devices
    - Hidden functionality
  - Assuming passwords will be secure

- **Vulnerability: a point in the system susceptible to attack**
  - Includes HW, SW, network, people, infrastructure, organization
  - Exploit: a method of converting a vulnerability to a security breach
  - Attack: someone uses an exploit to breach system security

Even Simple Devices Are Targets

Edge Case Research

DON'T BREW THAT CUPPA! Your kettle could be a SPAMBOT

https://goo.gl/zxGH4S

Russian report says Chinese appliances hide Wifi slurping spam-spreaders

29 Oct 2013 at 07:03, Simon Sharwood

Russian authorities have claimed that household appliances imported from China contain tiny computers that seek out open WiFi networks and then get to work sending spam and distributing malware.

St Petersburg news outlet *Rosbalt* reported last week that local authorities had examined kettles and irons and found “20 to 30 pieces of Chinese home appliance 'spy' microchips” that “sends some data to the foreign server”.

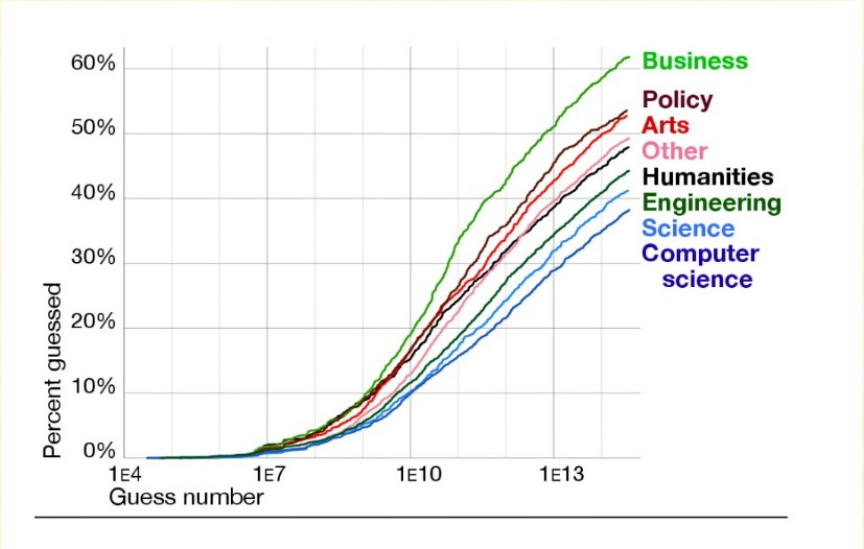
A bit of digging suggests it is legitimate. One source the story mentions, Gleb Pavlov of customs broker Panimport can be found at the link we've popped in on the company's name. We've also been able to find this linkto an appliances company called “Sable Ltd”, the very name translation engines say is the employer of one Innokenty Fedorov whose company found the bugged appliances.

https://goo.gl/fZQP4D

Weak or Master Passwords

Edge Case Research

- **Weak passwords are bad**
  - 1234, 777 (US), 888888 (China)
  - password, iloveyou, qwerty
- **Factory master passwords are worse!**
  - Once one user knows, everyone will know
- **Don't use the same key in all systems**
  - Keeloq car remote broken due to using same manufacturer key in all units
- **Use long enough crypto keys**
  - https://www.keylength.com/en/5/
  - Every year safe key size gets a little longer
  - E.g.: 256 bit symmetric key
    3072 bit public key



PASSWORD STRENGTH BY USER TYPE (UP IS BAD!)
https://goo.gl/ozKDt1

Avoid Default Passwords

Edge Case Research

Home › Cybercrime

Brian Krebs' Blog Hit by 665 Gbps DDoS Attack

https://goo.gl/2aXD4s

By Eduard Kovacs on September 21, 2016

Share 157 G+ Tweet Recommend 165 RSS

Investigative cybercrime journalist Brian Krebs reported on Tuesday that his website, KrebsOnSecurity.com, was hit by a massive distributed denial-of-service (DDoS) attack that could be the largest in history.

According to Krebs, his site was targeted with various types of DDoS attacks, including SYN and HTTP floods. The attack peaked at 665 Gbps and 143 Mpps (million packets per second), but it was successfully mitigated by Akamai, the company that provides DDoS protection services for KrebsOnSecurity.

These 60 dumb passwords can hijack over 500,000 IoT devices into the Mirai botnet

Always change your device's default password.

https://goo.gl/n82V4u

Graham Cluley | October 10, 2016 2:43 pm | Filed under: **Botnet**, **Denial of Service**, **Malware** 4

Username	Password	Username	Password
666666	666666	root	7ujMko0admin
888888	888888	root	7ujMko0vizxv
admin	(none)	root	888888
admin	1111	root	admin
admin	1111111	root	anko
admin	1234	root	default
admin	12345	root	dreambox
admin	123456	root	hi3518
admin	54321	root	ikwb
admin	7ujMko0admin	root	juantech
admin	admin	root	jvbzd
admin	admin1234	root	klv123
admin	meinsm	root	klv1234
admin	pass	root	pass
admin	password	root	password
admin	smcadmin	root	realtek
admin1	password	root	root
administrator	1234	root	system
Administrator	admin	root	user
guest	12345	root	vizxv
guest	guest	root	xc3511
mother	f***er	root	xmhdipc
root	(none)	root	zlxx.
root	0	root	Zte521
root	1111	service	service
root	1234	supervisor	supervisor
root	12345	support	support
root	123456	tech	tech
root	54321	ubnt	ubnt
root	666666	user	user

Mistakes Using Cryptography

Edge Case Research

- **Attackers go after implementation mistakes**
  - Usually you don't have to break the cryptography
- **Typical mistakes**
  - Sending initial passwords or secrets without encrypting
  - Using known flawed protocols (e.g., flawed secret key exchange, flawed software)
  - Implementing your own crypto from books
  - Permitting weak passwords
  - Not applying security patches

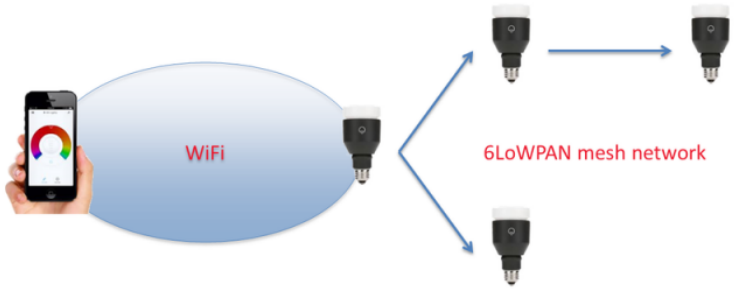
Crypto weakness in smart LED lightbulbs exposes Wi-Fi passwords

https://goo.gl/v4xgKu

More evidence the Internet of things treats security as an afterthought.

by **Dan Goodin** - Jul 7, 2014 3:20pm EDT

Share Tweet 90



Context

In the latest cautionary tale involving the so-called Internet of things, white-hat hackers have devised an attack against network-connected lightbulbs that exposes Wi-Fi passwords to anyone in proximity to one of the LED devices.

The attack works against LIFX smart lightbulbs, which can be turned on and off and adjusted using iOS- and Android-based devices. Ars Senior Reviews Editor Lee Hutchinson gave a good overview here of the Philips Hue lights, which are programmable, controllable LED-powered bulbs that compete with LIFX. The bulbs are part of a growing trend in which manufacturers add computing and networking capabilities to appliances so people can manipulate them remotely using smartphones, computers, and other network-connected devices. A 2012 Kickstarter campaign raised more than $1.3 million for LIFX, more than 13 times the original goal of $100,000.

According to a blog post published over the weekend, LIFX has updated the firmware used to control the bulbs after researchers discovered a weakness that allowed hackers within about 30 meters to obtain the passwords used to secure the connected Wi-Fi network. The credentials are passed from one networked bulb to another over a mesh network powered by 6LoWPAN, a wireless specification

Embedded Network Attacks

- **"Proprietary protocol" does not provide much protection**
  - Automotive CAN with proprietary messaging

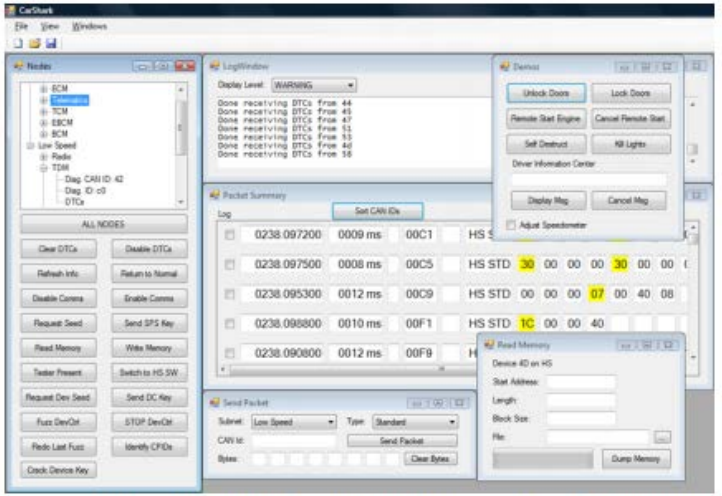


Figure 4. Screenshot of the CARSHARK interface. CARSHARK is being used to sniff the CAN bus. Values that have been recently updated are in yellow. The left panel lists all recognized nodes on high and low speed subnets of the CAN bus and has some action buttons. The demo panel on the right provides some proof-of-concept demos.

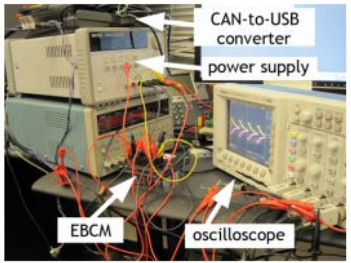


Figure 1. Example bench setup within our lab. The Electronic Brake Control Module (ECBM) is hooked up to a power supply, a CAN-to-USB converter, and an oscilloscope.

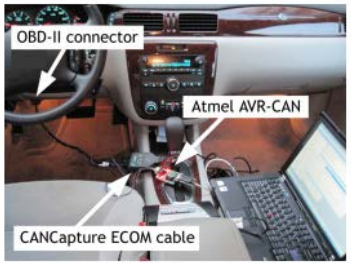


Figure 2. Example experimental setup. The laptop is running our custom CARSHARK CAN network analyzer and attack tool. The laptop is connected to the car's OBD-II port.

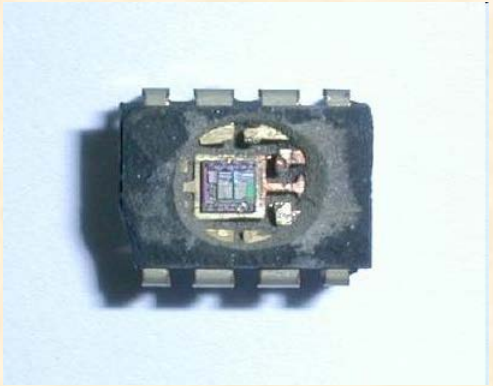
Figure 3. To test ECU behavior in a controlled environment, we immobilized the car on jack stands while mounting attacks.

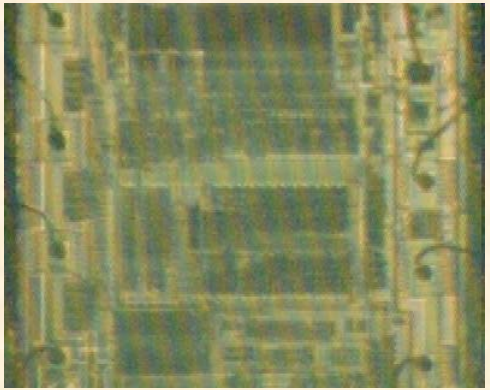
http://www.autosec.org/pubs/cars-oakland2010.pdf

Physical Access to System

Edge Case Research

- **How easy is it for someone to steal your design?**
  - Hardware design
  - Software design
- **Chip peels are no big deal**
  - Can recover hardware schematics from silicon
  - Can recover software from memory
  - “Tamper resistant” is a good way to slow down attacks – but does not stop them





http://www.scienceprog.com/safety-protection-guides-and-fact-about-microcontroller-you-should-know/

Hidden Functionality

- **Assume that any "secret" functionality will be revealed**
  - Factory test modes
  - Factory service modes
  - "Easter eggs"
- **This includes:**
  - Service technician master password
  - Ability to reset system
  - Default administrative accounts
- **Potential better approach:**
  - "Factory test" jumper on internal board
  - Factory test mode warning on screen

https://goo.gl/Ty9aYJ

Counterfeit Systems

Edge Case Research

- **How do you know components are legitimate?**
  - Often chips/boards fail to meet specifications, but are superficially the same function
    - Rejects that failed non-functional testing
    - Salvaged used components
    - "Clone" hardware without safety mechanisms
  - What if fake shows up in a critical application?
  - US Customs seizes ~1-2 million fake ICs per year

http://www.eetimes.com/electronics-news/4229964/Chip-counterfeiting-case-exposes-defense-supply-chain-flaw?pageNumber=3

- **What if someone wants to clone your whole product?**
  - "Tamper-proofing" may help, but not if attack is lucrative
  - Clones might be built in part by scavaging authentic components
  - Will need to have some way to authenticate and track serial numbers

Cloud Connected Devices

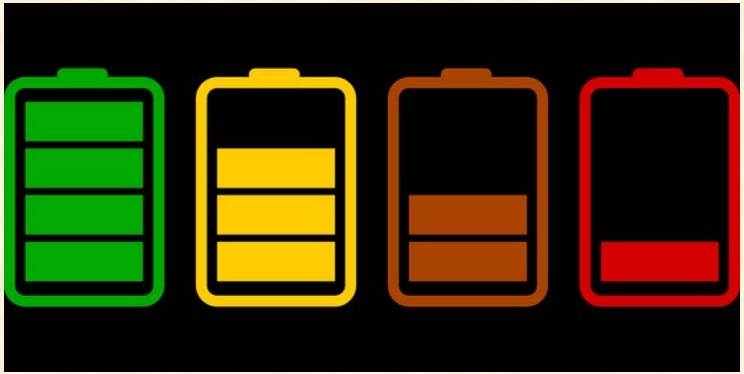
Edge Case Research

- **Embedded meets Internet Security**
  - Need good practices for IT security
  - Need good practices for embedded
  - IT penetration can cause safety issues via embedded device(!)

http://vint.sogeti.com/internet-things-world-fridge-spambot/

- **Questions to ask in design**
  - How does Cloud know it is a legitimate device?
    - Deploy each device with a unique public key signed by factory
  - How does user securely connect smart phone to device?
    - Print unique WPA (etc.) key on sticker inside unit
  - What if user forgets password?
    - Provide “factory reset” ability; NOT a shared master factory password
  - How will you do secure update? Factory Key revocation?

More Embedded-Specific Security Issues



- **Resources are scarce**
  - Consider a Smart Card chip (TPM) for keys & crypto
- **Embedded networks are generally insecure**
  - Short network messages, no built-in security
  - Power, memory, CPU constrain security resources
- **Power drain attacks**
  - Attacks designed to deplete batteries
- **Real time operation attacks**
  - Only a slight overload might cause real time schedule problems
- **Tamper resistance & evidence for critical properties**
  - How can you prove someone didn't alter your safety critical system? (Even the owner?)
- **Ensuring updates are authentic & are installed**
  - How can you ensure only certified configurations will run?
  - How do you ensure installation of required updates with intermittent external connectivity?

Security Vulnerabilities Best Practices

Edge Case Research

- **Be realistic with vulnerabilities**
  - Users won't change default passwords
  - Weak passwords will be used
  - Counterfeit systems will be built
  - All network systems will be attacked

- **Pitfalls:**
  - Assuming users will practice excellent security hygiene
  - Using a master password
  - Assuming attackers can't extract secrets from at least one device
    - Using a given symmetric key in more than one device instance