Security Now! #508 - 05-19-15

Exploiting Keyless Entry

This week on Security Now!

- Starbucks discovers the downside of convenience over security.
- Yet another remote router takeover.
- The largely overblown "Venom" vulnerability.
- Why it's never a good idea to hack into planes you're flying in.
- The growing ad-wars.
- GRC's troubles with Google.
- Some fun miscellany...
- And a look at how crooks are ransacking and stealing cars.

Security News!

Starbucks customers having accounts emptied

- http://13wham.com/news/features/top-stories/stories/hackers-use-steal-money-via-starbucks-app-22800.shtml
- Leveraging the "autonomous auto refill"
- Crooks get a Starbucks gift card
- Hack into a user's account, presumably brute-forcing a weak password.
  - (One victim admitted to using the same password for her eMail as for her Starbucks account.)
- Enable auto-reload if it's not already enabled.
- Repeatedly transfer funds to the gift card they control.
- Auto-reload is triggered... and funds are transferred again.
- Until some stronger protections are put in place:
  - Use a unique strong password.
  - Erase any payment methods from the account.
  - Disabling auto-reload is insufficient since it can be turned back on.

Ubiquiti -- DDoS botnet, 40,000+ strong

- https://www.incapsula.com/blog/ddos-botnet-soho-router.html
- Incapsula detected 40,269 different IP addresses from 1,600 ISPs in 109 countries associated with the botnet.
  - 64% Thailand
  - 21% Brazil
  - 4% U.S.
  - 3% India

- 60 C&C servers located in China and the U.S.
- Exposed HTTP and SSH management interfaces with default logon credentials.
- Often multiple instances of malware infected.
- Running scripts scanning the Net for additional victims.
- LOTS of opportunity for abuse:
  - Not just DDoS... but also for messing with their user's traffic.
- Control attributed to Anonymous and more recently Lizard Squad.
- HTTP query flood attacks.

"Venom"   (naming: Heartbleed / Shellshock)

- http://venom.crowdstrike.com/
- A flaw in the Virtual Floppy Disk Controller (FDC) code uses by several virtualization platforms derived from the QEMU (quick emulator)... which is about 11 years old.
- Which?
  - Vulnerable: KVM, Xen, VirtualBox & the QEmu client
    - Amazon is okay since they use a modified version of Xen.
  - NOT vulnerable: VMware, Microsoft's Hyper-V and Bochs.
    - Use their own, non-QEMU-derived, code.
- Buffer overflow in the VM hypervisor.
- Potentially allows a malicious process to break and escape from VM containment.
- Attackers need Admin/Root privileges... but shared hosting VM systems typically do that.

Feds Say That Banned Researcher Commandeered a Plane

- http://www.wired.com/2015/05/feds-say-banned-researcher-commandeered-plane/
- http://arstechnica.com/security/2015/05/alleged-plane-hacker-said-he-pierced-boeing-jets-firewall-in-2012/
- https://en-maktoob.news.yahoo.com/fbi-says-plane-hacker-threat-public-safety-122855311.html
- Chris Roberts of One World Labs
- Four days before the RSA conference, while on an unrelated flight, Chris tweeted:
  - "Find myself on a 737/800, lets see Box-IFE-ICE-SATCOM, ? Shall we start playing with EICAS messages? 'PASS OXYGEN ON' Anyone ? :)"
  - (EICAS: Engine-Indicating and Crew-Alerting System)
  - That is believed to be a joke. (Though few were laughing.)
- He was then detained by the FBI and questioned for four hours.
- Subsequently he was denied travel on United when attempting to fly to the RSA conference to give a presentation.
- But in an affidavit as part of a recently obtained search warrant application, Chris told the FBI that he: <quote> connected to other systems on the airplane network after he exploited/gained access to, or "hacked" the [in-flight entertainment] system. He stated that he then overwrote code on the airplane’s Thrust Management Computer while aboard a flight. He stated that he successfully commanded the system he had accessed to issue the climb command. He stated that he thereby caused one of the airplane engines to climb resulting in a lateral or sideways movement of the plane during one of these flights. He also stated that he used Vortex software after compromising/exploiting or "hacking" the airplane’s networks. He used the software to monitor traffic from the cockpit system.

Mobile networks plan to block online ads in Europe to target Google, says report

- http://venturebeat.com/2015/05/15/mobile-networks-plan-to-block-online-ads-in-europe-to-target-google-says-report/
- A story reported by the Financial Times (FT - Behind a paywall) states that: "several" carriers have installed ad-blocking software — developed by an Israeli company called **Shine** — in their data centers, and plans are afoot to switch the technology on by the end of the year. The software would stop most web-based ads from loading, though "in-feed" ads like those on Twitter or Facebook would not be affected.

  Citing a source at one European carrier, the report suggests that the network will introduce an opt-in ad-free service initially, but is also considering extending it to its entire network automatically. It's not clear whether this would be a paid or free offering, but ultimately it's designed to target the major online ad companies such as Google.
- Shine: http://www.getshine.com/
  - WE CHAMPION THE CONSUMER'S RIGHT TO CONTROL MOBILE ADS
  - <quote> Advertising technology has gone unchecked, polluting our Web and App experiences with privacy infringing and obtrusive advertising. We work with mobile carriers who are redefining their services to meet the true needs of consumers by offering the power of ad control to millions of subscribers around the world.

A security researcher finds a bug in ESET's Authentication Vulnerability (one click free purchase)

- http://egyptiangeeks.com/information-security/eset-broken-authentication-vulnerability/
- Mohamed Abdelbaset Elnoby found a way to bypass the web-based NOD 32 license purchase system to auto-issue $30 annual licenses.
- He reported the problem... and, in thanks, was offered a $30 annual license.

Google's False Positive on GRC: fp.exe

- Compressed with UPX.
- <quote> Google has detected harmful code on some of your site's pages. We recommend you remove it as soon as possible. Until then, Google's search results might display a warning to protect users when they click a link to your site.
- <quote> Undetermined malware
  - These pages directed users to a site that serves malware or unwanted software. Unfortunately, the malicious code within the page could not be isolated.
  - (Show Details)
- <details> Undetermined malware
  - Pages like the sample URLs returned content that directed the browser to a site that serves malware or unwanted software. The source of malware may be embedded ads or other third-party content on these URLs. Unfortunately, the malicious code within the page could not be isolated.
- The URL for /miscfiles/fp.exe (March 2013)

Miscellany

Verizon bought AOL... and they stopped caching the original TWiT podcasts.

- Fortunately, CACHEFLY has them all, and much more nicely setup, too!

Ex Machina

- TOTALLY AGREE about the unbelievable plot mistake at the end!!
- Also -- the young programmer's acting was terrific, but his boss didn't sell it.
  No way did I believe that HE was capable of designing and building those droids.

Logic gates without scripting...

- http://silon.slaks.net/

Great discussion between experts on both sides:

- http://bit.ly/UKbackdoor
- 12 minute discussion from earlier this year following David Cameron's stated intentions.

SQRL

Yesterday's release update milestone.

- 'ask'
- Client UI details
- Text

SpinRite

Nir Yaniv in Israel
Subject: Overdue Spinrite Success Story and Password Haystacks Request

Hi Steve,
I've been listening to "Security now!" for a few years, but I knew of some of your work before that, mostly thanks to "Shields Up!". Up front - Thanks for everything you and Leo do, I learn so much every episode and I use and recommend your products and services to everyone I know or even randomly encounter.

Spinrite Success Story - I purchased Spinrite mostly out of appreciation for the podcast. I have never used it to fix or even maintain one of my personal computers, but I have used it a few times in my previous work as Systems Administrator. I successfully used Spinrite to recover a few ESXi servers which refused to boot or failed to load their VMs, but the real success was this:

We had a network traffic generator and analyzer for various tests. This was one of the more expensive systems in the lab network I managed. One day it crashed (I think it was a power failure) and refused to boot. I don't recall the specific error, but the Windows operating system underneath simply wouldn't boot. We had a support contract for the device, but the only solution offered was sending a replacement drive from abroad which would have taken a couple of days.

So, I took out my copy of Spinrite, booted the machine from it, and let it run overnight. In the morning I rebooted the system. Lo and behold - it booted and resumed normal work... Obviously, I had my boss set aside budget for 4 copies of Spinrite after this. We ordered the replacemnet drive and it stayed in a closet, as a backup for the next crash (which hadn't occurred by the time I finished that employment.)

Exploiting “Passive Keyless Entry & Start” (PKES)

In the News:

- In Toronto, since January police have seen a spike in thefts from Toyota and Lexus SUVs parked in owners' driveways with no signs of damage.
- In Los Angeles, a reporter noticed the same problem in his own neighborhood. He watched two teens on bicycles open his locked Prius as it sat on the street in front of his house.
- In Tonawanda, N.Y., people who swore they had locked their car doors returned to their vehicles to find them rummaged through, spare change gone, but otherwise undamaged.
- In Springfield, Mo., a rash of vehicle break-ins had residents wondering how thieves could go through so many cars and leave no damage.
- In Long Beach, Calif., detectives shared a video on YouTube showing break-ins of two SUVs parked in their owner's driveway.

Our own listener, Gary Beals:

- Many of my neighbors are reporting on nextdoor.com that they locked their car doors and came out the next morning to ransacked glove boxes. I of course thought of you and knew you could explain how my neighbors' cars security systems are getting bypassed. So I was pleased to hear that you are way ahead of me and are planning an episode on the topic.

  In your discussion, could you please address mitigation strategies? A recent CBS This Morning News segment suggested storing car fobs in a shielded box (your fridge). Can you also indicate whether the same hack works on garage door openers? Should we store our garage door openers in the fridge when they're not in use, too? :)

"Putting keys in freezer could prevent car break-ins"

- http://www.usatoday.com/story/money/cars/2015/05/07/technology-car-break-ins/70939336/
- http://www.kare11.com/story/money/cars/2015/05/07/technology-car-break-ins/70939336/

$17 dollar device lets bad guys "reach" your keys...

http://www.networkworld.com/article/2909589/microsoft-subnet/thieves-can-use-17-power-amplifier-to-break-into-cars-with-remote-keyless-systems.html

http://www.3db-technologies.com/
“Relay Attacks on Passive Keyless Entry and Start Systems in Modern Cars”
http://www.isoc.org/isoc/conferences/ndss/11/pdf/2_1.pdf

PKES: Passive Keyless Entry & Start

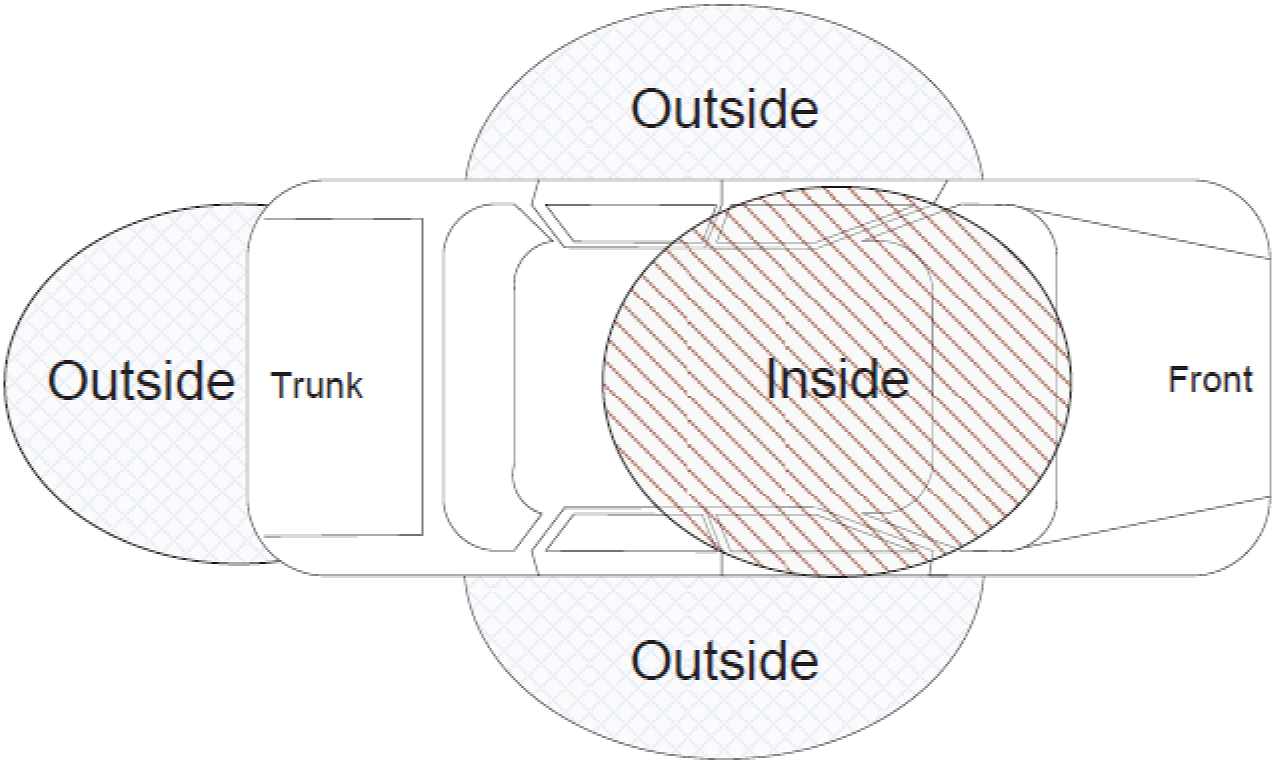
- Three Swiss security researchers, dept of CS at ETH University, Zurich.
- 10 different car models from 8 manufacturers.
- The attacks they developed allowed cars to be opened and started when the car's key was up to 50 meters (164 feet) distant -- non-line of sight.

PKES Technology:

- All of the different systems used the same RF architecture.
- All of the different systems used advanced Challenge/Response Crypto.
- Keys use a battery powered LF receiver and UHF transmitter.
  - LF, short-range, RFID-style receiver: 120-135 KHz
  - UHF, long-range (100m) transmitter: 315 or 433 MHz

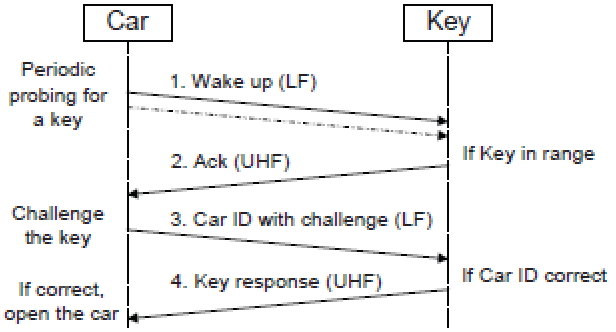
Three "location" modes:

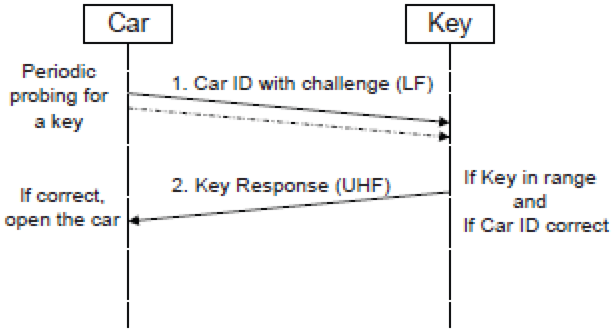
- Remote from the car - typically up to 100m
  - Only lock/unlock car by pushing a button on the key.
- Outside the car - approx 1 to 2 m from the door handle.
  - Lock/unlock the car using the door handle.
- Inside the car
  - Starting the engine is allowed.



Crypto Challenge/Response:

- All autos periodically emit one style of short-range LF "ping" surrounding the immediate car exterior, and a different periodic short-range ping within the car's interior.
- In some designs the ping is a "key wake up", to which the key replies, then the car issues a challenge and the key responds.
- In other designs the ping contains the challenge and the key replies with the response.
- Crypto is a simple shared-key system:
  - AES, and the ping is a never-repeating counter which the key encrypts and returns.
  - Keyed Hash: never-repeating counter, both compute the proper response.



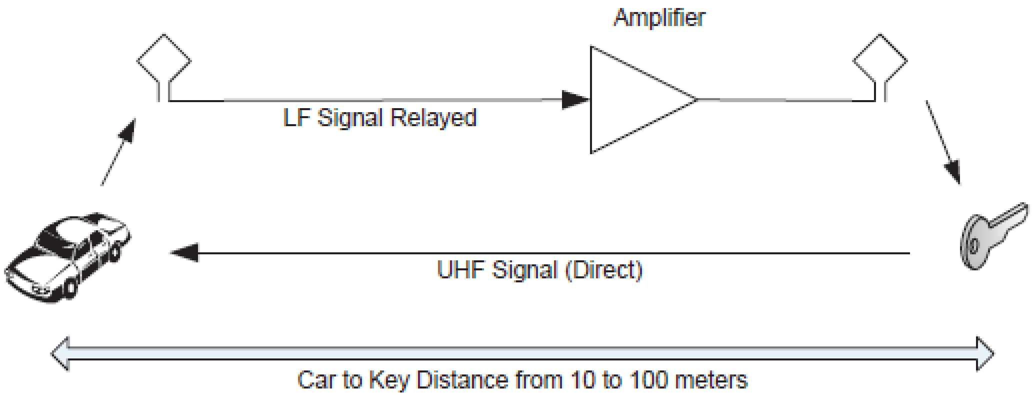

Car
Key
Periodic probing for a key
1. Car ID with challenge (LF)
If correct, open the car
2. Key Response (UHF)
If Key in range and If Car ID correct

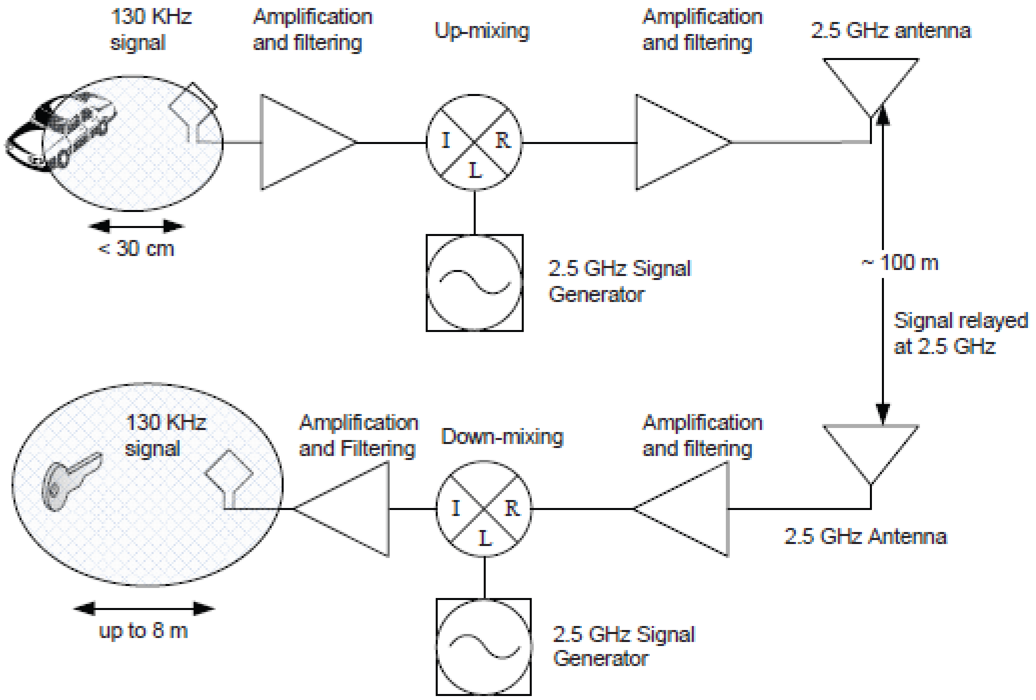
The Crucial Critically-Flawed Assumption:

<quote> We note that the main reason why relay attacks are possible on PKES systems is that, to open and start the car, instead of verifying that the correct key is in its physical proximity, the car verifies if it can communicate with the correct key, assuming that the ability to communicate implies proximity. But this is only true for non-adversarial settings. In adversarial settings communication neighborhood cannot be taken as a proof of physical proximity. Given this, any secure PKES system needs to enable the car and the key to securely verify their actual physical proximity. This is only natural, since the car should open only when the legitimate user (holding the key) is physically close to the car.

The Attack:

- Used a realtime 2.5 GHz radio link to extend the car's LF proximity ping.
- Speed is important, so it was all done in analog using heterodyning.
- Product of Sines == sum and difference.





Once started, presumably for safely reason, NONE of the 10 cars tested stopped.

Attack Mitigations:

- Store the key fob in a "Faraday cage"
- Experiment with removing the battery from the fob.
  - Some auto systems have a "dead battery fallback" provision which relies only upon passive RFID proximity.
- Longer term: RF Distance Bounding
  - Measure the Challenge/Response round trip time.
  - 300,000,000 meters / second (299,792,458)
  - 300 m/uS or 0.3m/ns or 3.336 ns/meter
  - 1 meter round trip: 6.67ns
  - Transponder *must* have a response time variability that's small in relation.