Security Digest
Information Security Branch

BRITISH COLUMBIA

OCIO
Office of the Chief Information Officer

August 14th, 2018

August is "Wi-Fi" Month

This week's stories:

- Fax protocol vulnerability lets malware be sent over phone line
- Privacy group wants better regulation for GPS starter interrupt devices
- When a simple tire change becomes a debate over personal privacy
- Google is tracking your movements — even if you tell it not to
- Hacking pacemakers, insulin pumps and patients' vital signs in real time
- Police Bodycams Can Be Hacked to Doctor Footage
- Banks and Retailers Are Tracking How You Type, Swipe and Tap
- Free Facial Recognition Tool Can Track People Across Social Media Sites
- FBI Warns Of Pending Large Scale ATM Cashout Strike
- WannaCry Outbreak Hits Chipmaker, Could Cost $170 Million

Fax protocol vulnerability lets malware be sent over phone line

https://www.itworldcanada.com/article/fax-protocol-vulnerability-lets-malware-be-sent-over-phone-line-report/407967

Using fax for business communications in North America is increasingly disappearing, but it's still important in some sectors — particularly healthcare and legal. Which is why a warning by Check Point Software of a fax machine protocol vulnerability that could lead to network infiltration needs to be heeded.

Click link above to read more

Privacy group wants better regulation for GPS starter interrupt devices

http://www.cbc.ca/news/canada/nova-scotia/gps-starter-interrupters-privacy-technology-laws-1.4780860

They are small devices, but they can wield a lot of power.

GPS starter interrupt devices seem to have flown under the radar in Canada and the president of one privacy group says they need to be regulated.

No one knows how many of the devices are in vehicles in Canada, but some auto finance companies are requiring people with bad credit to pay for them, and have them installed, as a condition of receiving a car loan.

The device can track a vehicle and sound an alarm when the car is started if a payment is late. It can even remotely disable the vehicle if the owner is in serious arrears.

One company that sells them, Imetrik, says on its website the devices go a long way toward "maximizing cash flow and encouraging on-time payments."

But privacy advocates say there's another side to the story.

Click link above to read more

When a simple tire change becomes a debate over personal privacy 

https://www.cbc.ca/news/canada/nova-scotia/when-a-simple-tire-change-becomes-a-debate-over-personal-privacy

A Timberlea, N.S., man is questioning Canadian Tire's collection of personal information after he says he was told he must provide his vehicle permit and insurance before the business would change a tire.

Dan MacDonald went to the Bayers Lake Canadian Tire in Halifax last week to get his tire changed.

He left without the work being done after he said he was asked for his vehicle permit and proof of insurance. He refused and said he was told by the woman behind the counter, "If you want to get your tire changed, that's what you're going to have to do."

Click link above to read more

Google is tracking your movements — even if you tell it not to

https://business.financialpost.com/technology/personal-tech/ap-exclusive-google-tracks-your-movements-like-it-or-not-2?video_autoplay=true

Google wants to know where you go so badly that it records your movements even when you explicitly tell it not to.

An Associated Press investigation found that many Google services on Android devices and iPhones store your location data even if you've used privacy settings that say they will prevent it from doing so.

Click link above to read more

Hacking pacemakers, insulin pumps and patients' vital signs in real time

https://www.csoonline.com/article/3296633/security/hacking-pacemakers-insulin-pumps-and-patients-vital-signs-in-real-time.html

Medical device insecurity was covered at the recent Black Hat and Def Con security conferences in Las Vegas. One set of researchers showed off hacks to pacemakers and insulin pumps that could potentially prove lethal, while another researcher explained how hospital patients' vital signs could be falsified in real time.

A decade has passed since we learned about pacemaker hacks, but still implantable medical devices that can save patients' lives can be hacked to potentially kill them. Even now, as was highlighted at Black Hat USA, attackers can cause pacemakers to deliver a deadly shock to the heart or deny a life-saving shock, as well as prevent insulin pumps from delivering needed insulin.

Click link above to read more

Police Bodycams Can Be Hacked to Doctor Footage

https://www.wired.com/story/police-body-camera-vulnerabilities/?mbid=social_twitter_onsiteshare

As they proliferate, police body cameras have courted controversy because of the contentious nature of the footage they capture and questions about how accessible those recordings should be.

But when it comes to the devices themselves, the most crucial function they need to perform—beyond recording footage in the first place—is protecting the integrity of that footage so it can be trusted as a record of events. At the DefCon security conference in Las Vegas on Saturday, though, one researcher will present findings that many body cameras on the market today are vulnerable to remote digital attacks, including some that could result in the manipulation of footage.

Click link above to read more

Banks and Retailers Are Tracking How You Type, Swipe and Tap

https://www.nytimes.com/2018/08/13/business/behavioral-biometrics-banks-security.html

When you're browsing a website and the mouse cursor disappears, it might be a computer glitch — or it might be a deliberate test to find out who you are.

The way you press, scroll and type on a phone screen or keyboard can be as unique as your fingerprints or facial features. To fight fraud, a growing number of banks and merchants are tracking visitors' physical movements as they use websites and apps.

Some use the technology only to weed out automated attacks and suspicious transactions, but others are going significantly further, amassing tens of millions of profiles that can identify customers by how they touch, hold and tap their devices.

Click link above to read more

Free Facial Recognition Tool Can Track People Across Social Media Sites

https://thehackernews.com/2018/08/social-mapper-osint.html

Security researchers at Trustwave have released a new open-source tool that uses facial recognition technology to locate targets across numerous social media networks on a large scale.

Dubbed Social Mapper, the facial recognition tool automatically searches for targets across eight social media platforms, including—Facebook, Instagram, Twitter, LinkedIn, Google+, the Russian social networking site VKontakte, and China's Weibo and Douban—based on their names and pictures.

The tool's creators claim they developed Social Mapper intelligence-gathering tool predominantly to help pen testers and red teamers with social engineering attacks.

Although the searches of names and pictures can already be performed manually, Social Mapper makes it possible to automate such scans far faster and "on a mass scale with hundreds or thousands of individuals" at once.

Click link above to read more

FBI Warns Of Pending Large Scale ATM Cashout Strike

https://www.databreachtoday.com/fbi-warns-pending-large-scale-atm-cashout-strike-a-11329

The FBI warns that cybercriminals are planning a large-scale operation aimed at emptying ATMs of their holdings, a type of attack that has caused swift and costly losses for financial institutions.

The confidential alert was shared privately with banks on Friday, reports security blogger Brian Krebs, who obtained it.

The alert says that the scheme is likely associated with a data breach at an "unknown card issuer." The FBI says it obtained the tip through unspecified reporting.

The FBI's alert will give banks a heads-up, but there's been plenty of fair warning already as multiple incidents of ATM fraud have affected financial institutions. ATM cashout schemes are referred to as "unlimited" operations due to their high takings.

Click link above to read more

WannaCry Outbreak Hits Chipmaker, Could Cost $170 Million

https://www.databreachtoday.com/wannacry-outbreak-hits-chipmaker-could-cost-170-million-a-11285

Taiwan Semiconductor Manufacturing Co., the world's largest chip manufacturer, says a WannaCry infection hit unpatched Windows 7 systems in its fabrication facilities, leaving multiple factories crippled. The chipmaker traced the infection to a new software tool that it failed to scan for malware before installation, and says the outbreak could cost it $170 million.

Click link above to read more

Click Unsubscribe to stop receiving the Digest.

****

For previous issues of Security News Digest, visit the current month archive page at:
http://www2.gov.bc.ca/gov/content/governments/services-for-government/information-management-technology/information-security/security-news-digest

To learn more about information security issues and best practices, visit us at:
Information Security Awareness Team - Information Security Branch
Office of the Chief Information Officer,
Ministry of Citizens' Services
4000 Seymour Place, Victoria, BC V8X 4S8
https:www.gov.bc.ca/informationsecurity
OCIOSecurity@gov.bc.ca