Welcome to the IoT This Week Newsletter!

IoT This Week

The Latest from the Internet of Things!

IoT This Week Podcast | Episode 23

Click here to view media.

April 4, 2017

Catching you up on the latest from IoT, InfoSec and Tech. Episode 23 includes: Samsung writes code like it's the 90s, baby boomers like Alexa, ATM use in the US is risky, Verizon is just dumb, Wired makes a ramp and more...

IoT

• Samsung's Tizen OS is essentially riddled with security vulnerabilities. 40 previously unknown vulnerabilities were discovered by Israeli researcher Amihai Neiderman. One of the researcher's quotes, "It may be the worst code I've ever seen". According to the researcher the Tizen system can be updated with any malicious code. It is also stated that many of the of the vulnerabilities were caused by mistakes programmers were making 20 years ago. This all seems eerily familiar from past research I've performed on IoT firmware. He cites one example in the use of strcpy() which can cause buffer overrun conditions. This function is no longer used today by programmers, however Samsung uses it all over the place in Tizen apparently. Tizen runs on Samsung smart TVs, smart watches and mobile phones.

• California is looking to force the issue on IoT Security with **California SB 327 Information privacy: connected devices**. Basically it tries to compel manufacturers ensure the device has reasonable security features and to obtain consumer consent when collecting information. While this might be a good start, there are the usuals concerns like who is defining what reasonable security features are going to be and what types of information collection require consumer consent. There is one part I like that requires the seller of the product to provide a short notice of the types of information being collected. And it would also require the manufacturer to directly notify consumers in regards to security patches and updates.

• I thought this was a neat story in that baby boomers are embracing the internet of things like the Amazon Echo. Most of that embrace is due to the auditory interaction of devices like the Echo instead of having to visually interact with small screens on devices like smartphones or thermostats. "Alexa, I've fallen and can't get up."

• This is another one of those IoT stories that isn't much of a revelation but is still interesting. Ponemon Institute released its **2017 Study on Mobile and Internet of Things Application Security** report which says that companies are mostly unprepared for IoT risks. Probably not much a surprise to most. Some of the findings:
• 55% of respondents say there is a lack of quality assurance and testing procedures
• Securing IoT apps is performed primarily via penetration testing
• The race to release products is the major cause of vulnerable devices
• Half of respondents think their companies have had a breach due to IoT

devices, but only 4% know for sure

- Companies would consider increasing security budgets if a severe hacking incident occurs (54%) or new regulations were put in place (46%)
- Less than a third of respondents say they train developers on secure coding techniques
- Half of respondents say that IoT testing does NOT occur

- A dishwasher has a directory traversal vulnerability. According to the article this involves a commercial dishwasher and not a consumer device. Which might actually be worse since it's commercial instead of consumer.

InfoSec

- Apple security updates page. If you are interested in seeing what has changed from a security standpoint in each release.

- US ATM fraud is up a lot despite chip-and-pin cards. According to the story, the number of payment card compromises rose 70% last year. Compromises of ATMs and merchant devices in the US rose 30%. The story notes that vendors are detecting compromised devices more quickly. I think the obvious issue right now is that payment cards and merchant devices are a completely broken ecosystem at the moment. Any kind of physical interaction with payment devices is risky and because of the high incidents of fraud, actually using a card is becoming increasingly onerous for the consumer. I've lost count of how many times I have had to call the card company to say that a sale was actually me and not fraud. For me, card declines because of suspected fraud have been 100% false positive. Apple Pay and other similar payment solutions are a great alternative but since everyone wants to get in on the mobile payment game, there's currently no standard provider which will inevitably mean we are stuck with plastic that much longer.

- Verizon will supposedly be installing an app on its Android phones that collects data on users. The application is called AppFlash which is a universal search bar. Incidentally the app can not be removed without rooting your phone. Glad

I'm not a Verizon customer wanting an Android phone.

- And the whole encryption backdoor discussion is again being brought up by the FBI. This time they are hoping for an "international framework" for enabling backdoors to encryption. Not sure how many times this has to be explained on why this is a completely horrible idea.

- A long the same lines regarding encryption backdoors, the European Commission was going to be pushing for access to data stored in cloud by encrypted apps in June. The interesting part of this is that the original statements have already been backed away from stating there is no plan now to introduce legislation covering encryption. "So let's see what the people think...yikes, nevermind."

- FBI warns that medical offices have exposed FTP servers. Given all the regulation in the medical field, not sure how that even gets by. Apparently FTP is still built into medical devices.

- Symantec has security issues with its third-party API for resellers that can allow someone to steal private keys and certificates and they have known about it since 2015. Not a good time lately for Symantec.

Tech

- Wired went to the trouble to determine if Atlanta could just build a ramp to jump the collapsed part of I-85. Apparently it could work to clear the 94 foot gap in the highway. A vehicle would need to be going 60 mph to jump the gap with identical launching and landing ramps about 2 meters high. The obvious question here is, how many people would actually try it?

- Amazon launches Amazon Cash which allows consumers to add cash to their amazon.com balance by showing a barcode at a participating retailer. So now, even those of you hoarding cash in your mattress can buy from Amazon. Nice!

- Verizon is rebranding Yahoo and AOL as Oath. So Verizon likes to spy on their customers, Yahoo had massive breaches they didn't tell anyone about and AOL... not sure why they are even still around, Oath makes total sense.

- Tesla is now worth more than Ford, at least on paper. Tesla had good news today which led to a stock price increase while Ford had the opposite happen. Today at least, Tesla has a market cap of 47.46 billion and Ford has a market cap of 44.89 billion.

Random

- Formula 1 racing in China this coming weekend
- Nintendo Switches are warping in their docks
- The FCC is killing Charter merger conditions... big surprise there
- Apple to start making its own GPU
- Netflix for Windows 10 gets offline viewing
- AT&T and Comcast say they will respect your privacy

Read more.

Contact: @craigz28 on twitter or podcast@iotthisweek.com