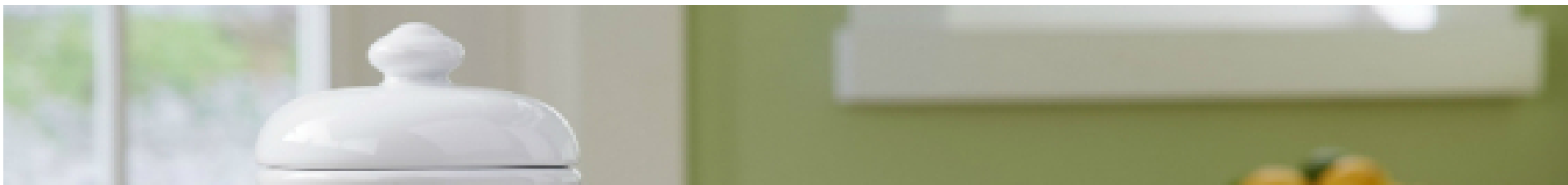IoT Privacy IoT Security

THE SIMPLE REASON IOT DEVICES ARE SO HACKABLE

The insecurity of IoT devices is a common theme on this blog. Cool and novel yes, but smart "Things" often fall short on security and privacy. We've talked about the pitfalls of smart baby monitors, water kettles, cars, and Hello Barbie. Why do these connected things slip up so badly when it comes to security? [ ]

MELISSA MICHAEL   MARCH 4, 2016

The insecurity of IoT devices is a common theme on this blog.

Cool and novel yes, but smart "Things" often fall short on security and privacy. We've talked about the pitfalls of smart baby monitors, water kettles, cars, and Hello Barbie.

Why do these connected things slip up so badly when it comes to security?

Let's look at it from another point of view – the view of the maker of an IoT device.

Imagine you own a company that has been making cookie jars for 30 years.

You make cute, classy and creative cookie jars to fit every type of kitchen decor. You know everything about them – the best materials, most popular designs, ideal sizes, the best-sealing lids for the freshest cookies, everything. You are an authority in making great cookie jars.

Now you decide to get on the IoT train and introduce a smart cookie jar. It will be the first of its kind!

This cookie jar will put an end to the age-old problem of kids sneaking treats before dinner and ruining their appetites. It will connect to an app in the user's phone. The app will alert the user when someone is opening the cookie jar. From the app, the user will also be able to remotely lock and unlock the cookie jar.

So even if Mom is away, she can still keep Billy out of the Chocolate Chunkies.

You've been making cookie jars for three decades – you're an expert. But when it comes to making a smart cookie jar, that's another thing. Because you are not an expert in software tech. In fact, you pretty much know nothing about it.

You're excited about your new product. You're thinking of new features you could build in, like password protection right on the jar, or a sensor that can tell how many cookies have been removed. You're in a hurry to get the product to market. After all, you've heard that some new Silicon Valley startup is working on a similar product, and you don't want to be upstaged.

In all your excitement, security is forgotten. Or rather not forgotten, since you never had it in your mind to begin with. Because you, after all, are a cookie jar maker.

You're working with a few other companies on the technology. Your goal is to get the jar made as quickly and as inexpensively as possible. None of the other vendors stress about security. After all, it's not going to be their brand name on the final product. It will be yours.

You don't realize that the software being used in your product is five years old. You've never thought about what might happen if a vulnerability needs to be patched. Is it even possible to patch, and if so, how will you alert your customers who purchase the jar?

But these thoughts don't enter your mind. Your main concern is that it will work, and that it will look cool, and have that "wow" factor.

So you keep working. Eventually your cookie jar gets made and hits the market. It works. It looks cool. And it has that "wow" factor.

But, oops. It leaks the password to the home Wi-Fi network.

It's really no surprise.

You are, after all, a cookie jar maker.*

Security is challenging enough to get right for the software industry itself – how much more so for those companies who are completely new to software and security.

As security researcher Runa Sandvik put it, "When you put technology on items that haven't had it before, you run into security challenges you haven't thought about before."

*No disrespect to cookie jar makers – I myself am a big fan of cookies of all kinds, and cookie jars are a great way to keep them accessible. I would trust my cookies any day to them, but I'd be more careful about my data.

Banner image courtesy Personal Creations, flickr.com. Modified.

Share this post:

Like   g +1   Share   Tweet   i
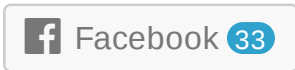
Most Popular Articles

F-Secure SENSE – Smart Security, Smart You

The Simple Reason IoT Devices Are So Hackable

3 Ways to Keep Hackers out of your Smart Home
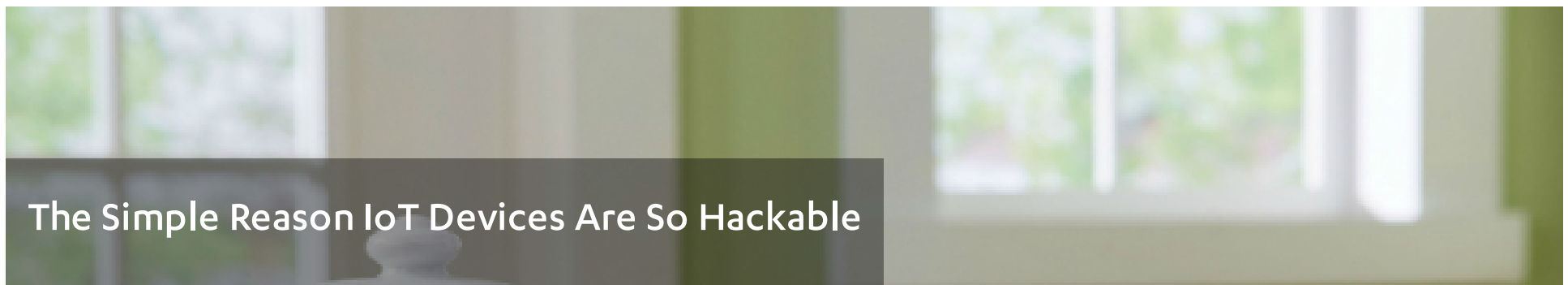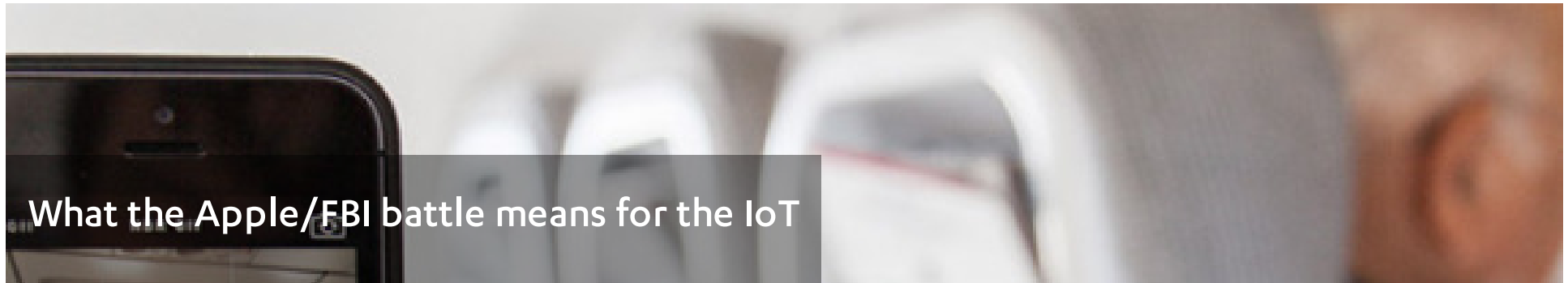
What's keeping the Military off the IoT?
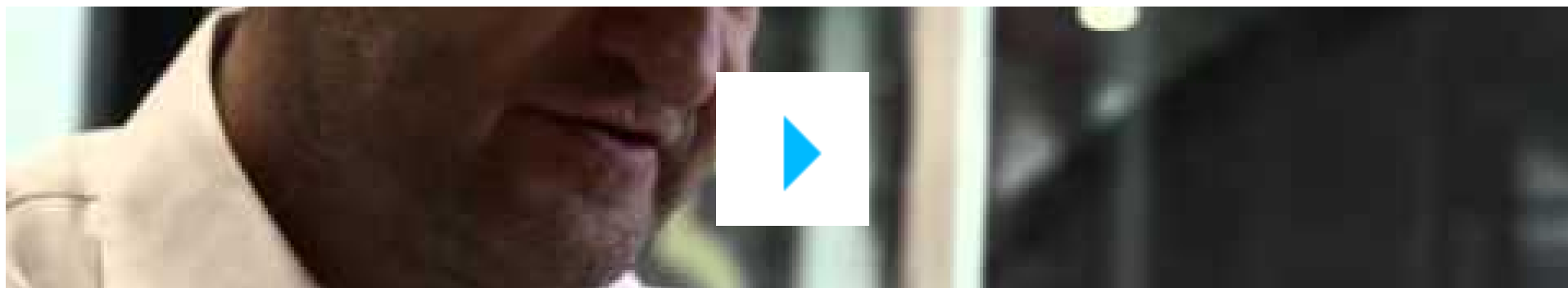
Topics

About ▶

Twitter

My Tweets

More from this category

What the Apple/FBI battle means for the IoT
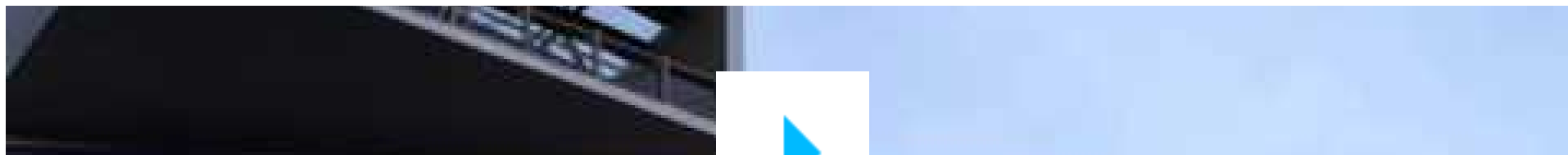
The Simple Reason IoT Devices Are So Hackable

Meet F-Secure SENSE at #MWC16

Why hackers love routers

Latest Media

Designing the User Experience of Sense

Protection technology behind Sense

Topics

About

Lab News

Soon

Work In Progress

"IOS Crash Report" Update: Safari Adds Block Feature

Duke APT group's latest tools: cloud services and Linux support

Safe&Savvy News

#AskFreedomeVPN – Your one-stop Youtube Channel for Privacy Questions

5 Things You Need to Know About the Threat of Election Hacking

An Open Letter to Businesses that Block VPNs on their Free Wi-Fi

Copyright 2016 by F-Secure