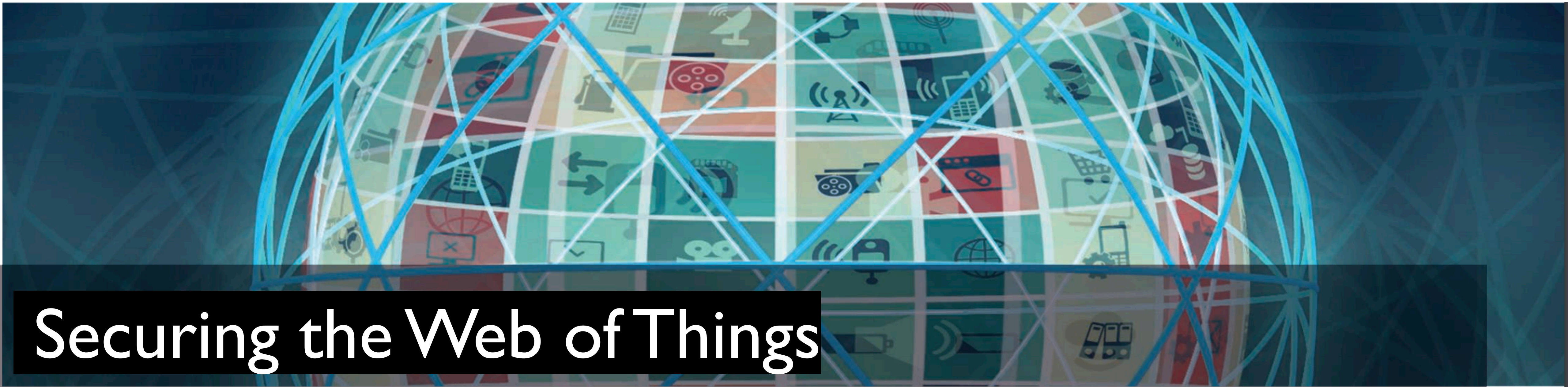


Securing the Web of Things

Andrei Sabelfeld
@asabelfeld

CHALMERS

Web of Things

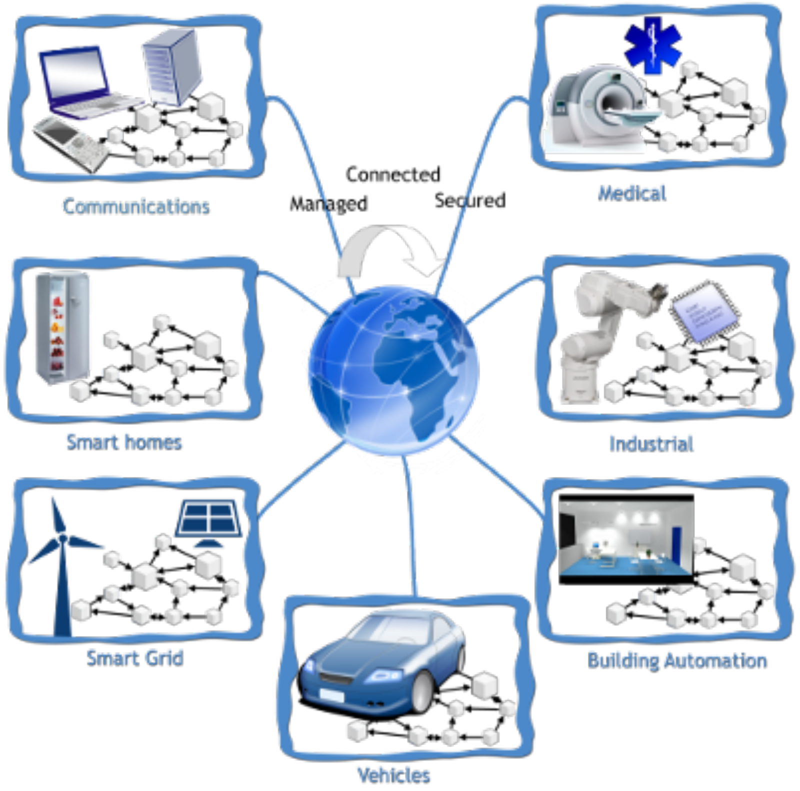
Internet of Things (IoT)

- Incompatible standards, platforms, technologies

"World Wide Web Consortium (W3C) is in a unique position to create the royalty-free and platform-independent standards needed to overcome the fragmentation of the IoT"

-W3C CEO Dr. Jeff Jaffe, 2017

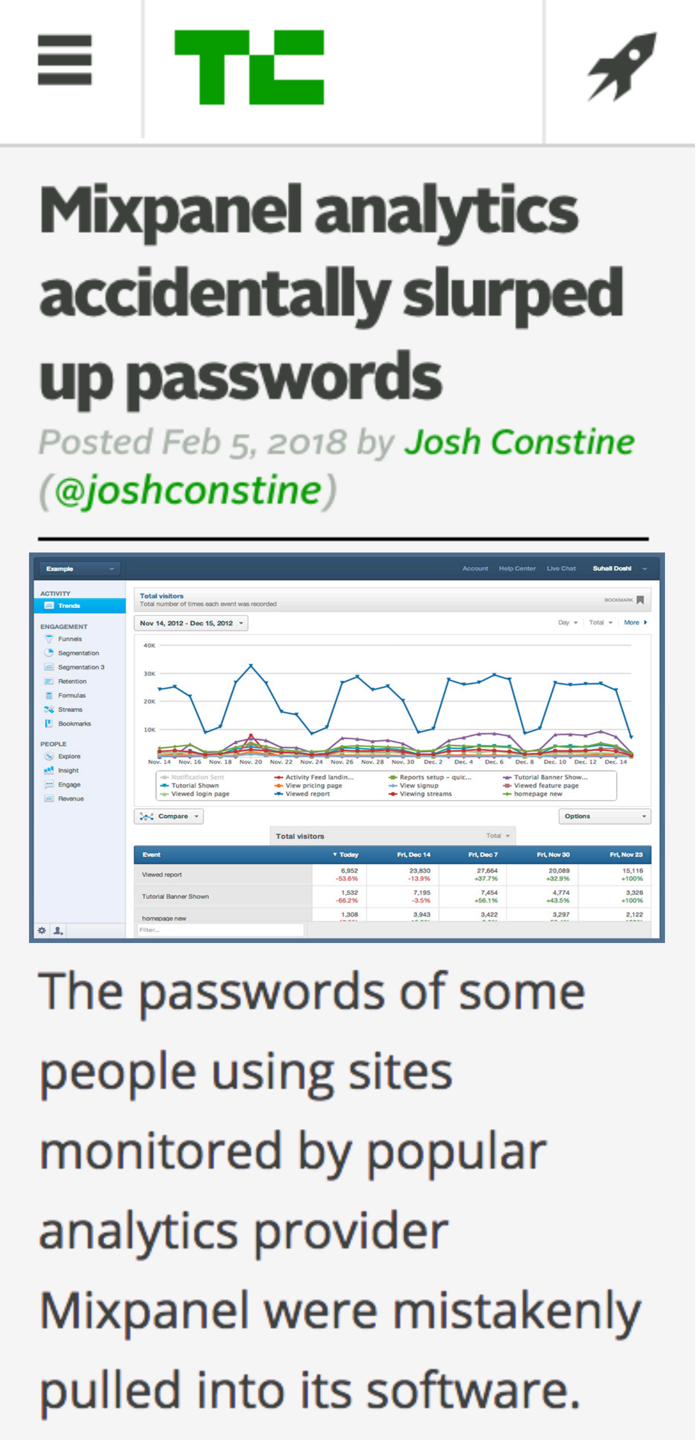
Security implications?



Software as enabling technology

- Software at the heart
  - Third-party code everywhere
  - Libraries, gadgets, ads, analytics, tracking, fingerprinting,..
- Malicious/buggy code
  - Ex-filtrating private information
  - Malwartising
  - Defacing web sites
  - Phishing attacks
  - Cryptojacking

Securing software is a must for IoT



Mixpanel analytics accidentally slurped up passwords

Posted Feb 5, 2018 by Josh Constine (@joshconstine)

The passwords of some people using sites monitored by popular analytics provider Mixpanel were mistakenly pulled into its software.

IoT apps

"Connecting otherwise unconnected services"

IoT apps

- “Managing users’ digital lives”
  - Smart homes, smartphones, cars, fitness armbands
  - Online services (Google, Dropbox,…)
  - Social networks (Facebook, Twitter,…)
- End-user programming
  - Anyone can create and publish apps
  - Most apps by third parties
- Web interface + smartphone clients

IFTTT

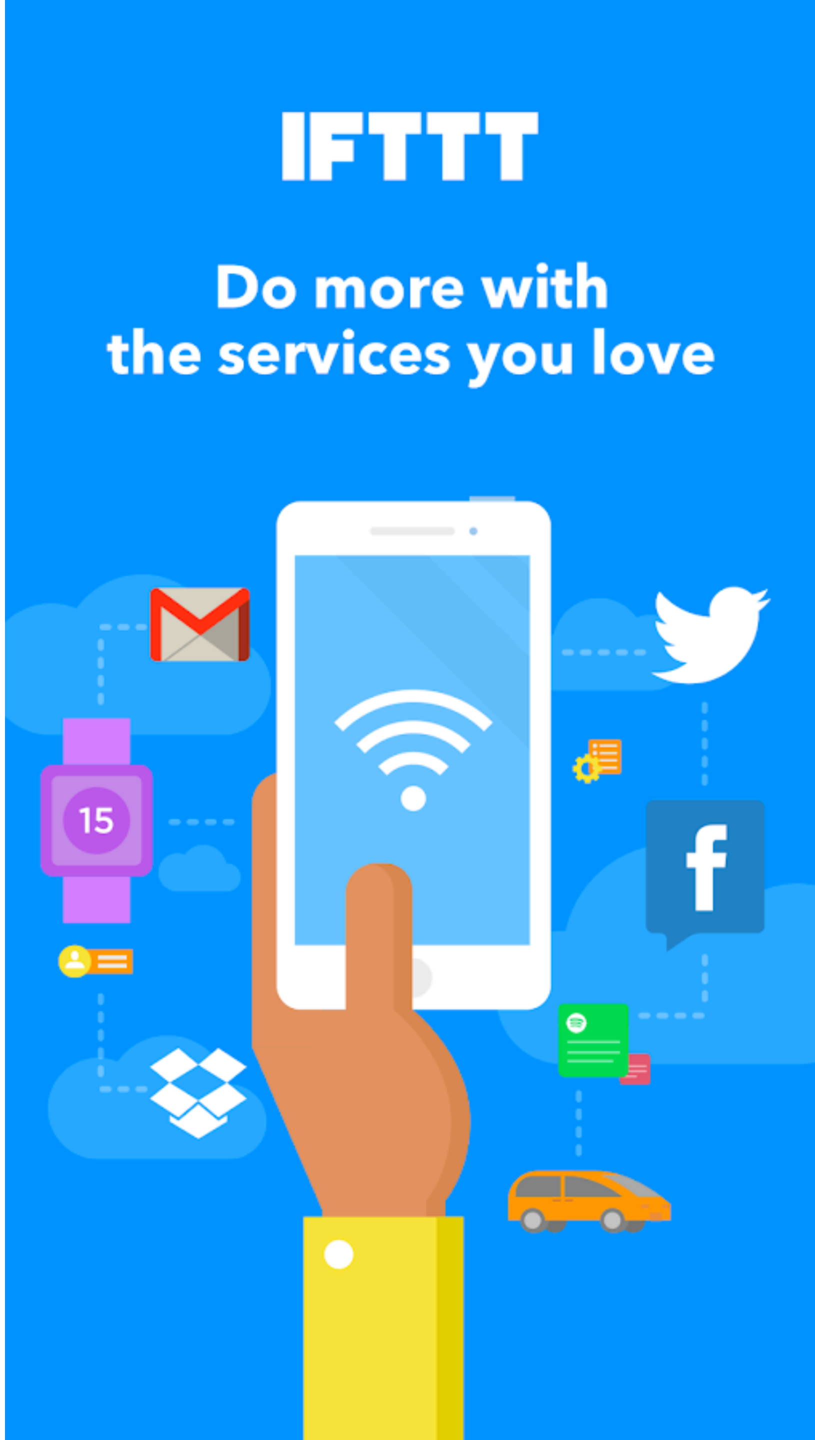
Do more with the services you love

zapier

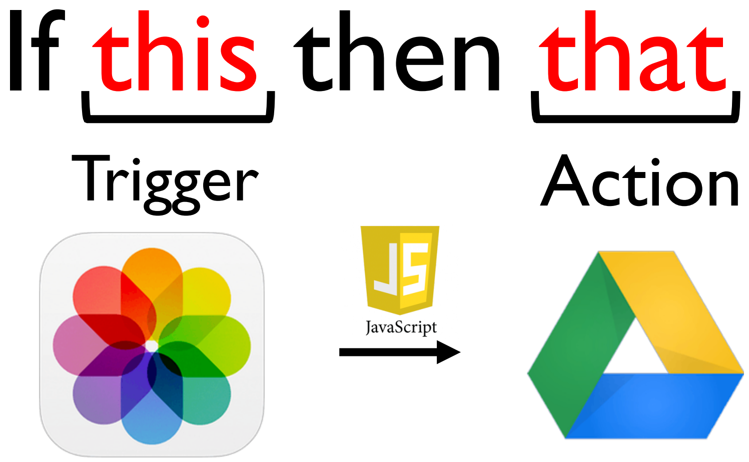
Microsoft Flow

IFTTT “If This Then That”

- Trigger-action programming
- Largest IoT app platform
- Over 500 integrated services
- Millions of users and billions of running apps



IFTTT app

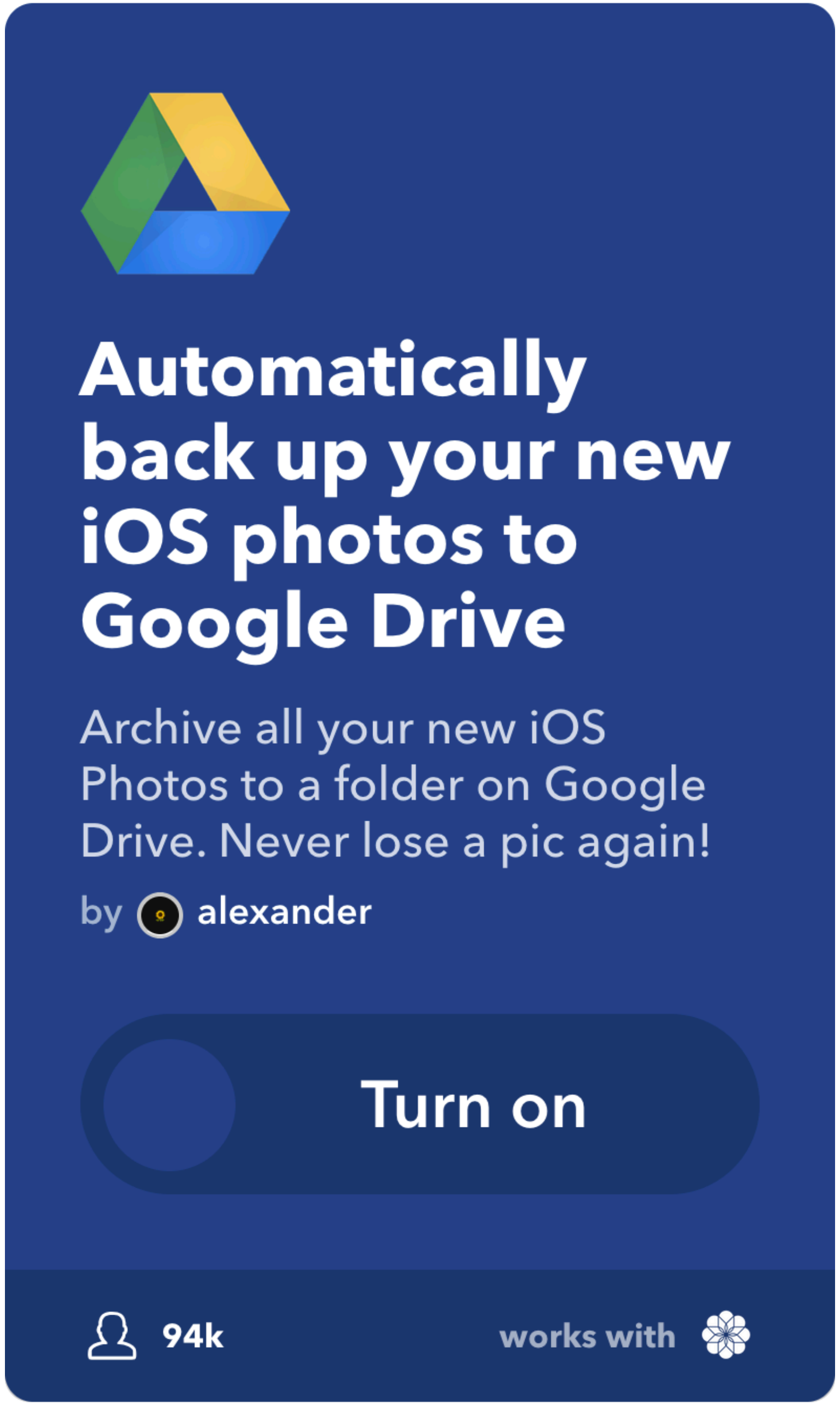


If this then that

Trigger

Action

What can go wrong? ☺



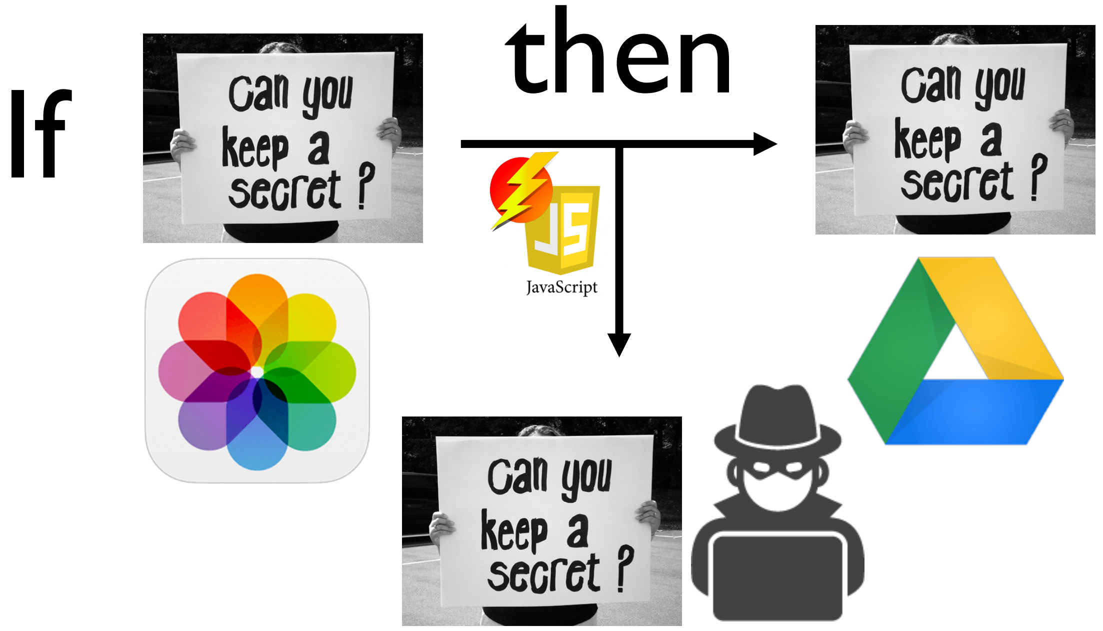
Automatically back up your new iOS photos to Google Drive

Archive all your new iOS Photos to a folder on Google Drive. Never lose a pic again!

by alexander

Demo

Attack by malicious app maker

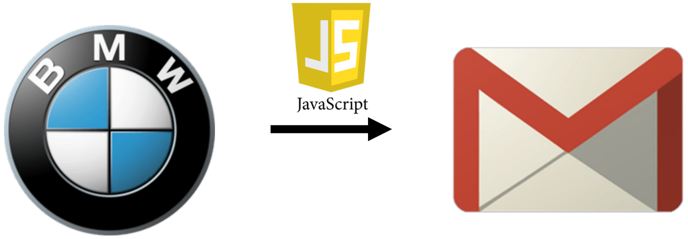


If

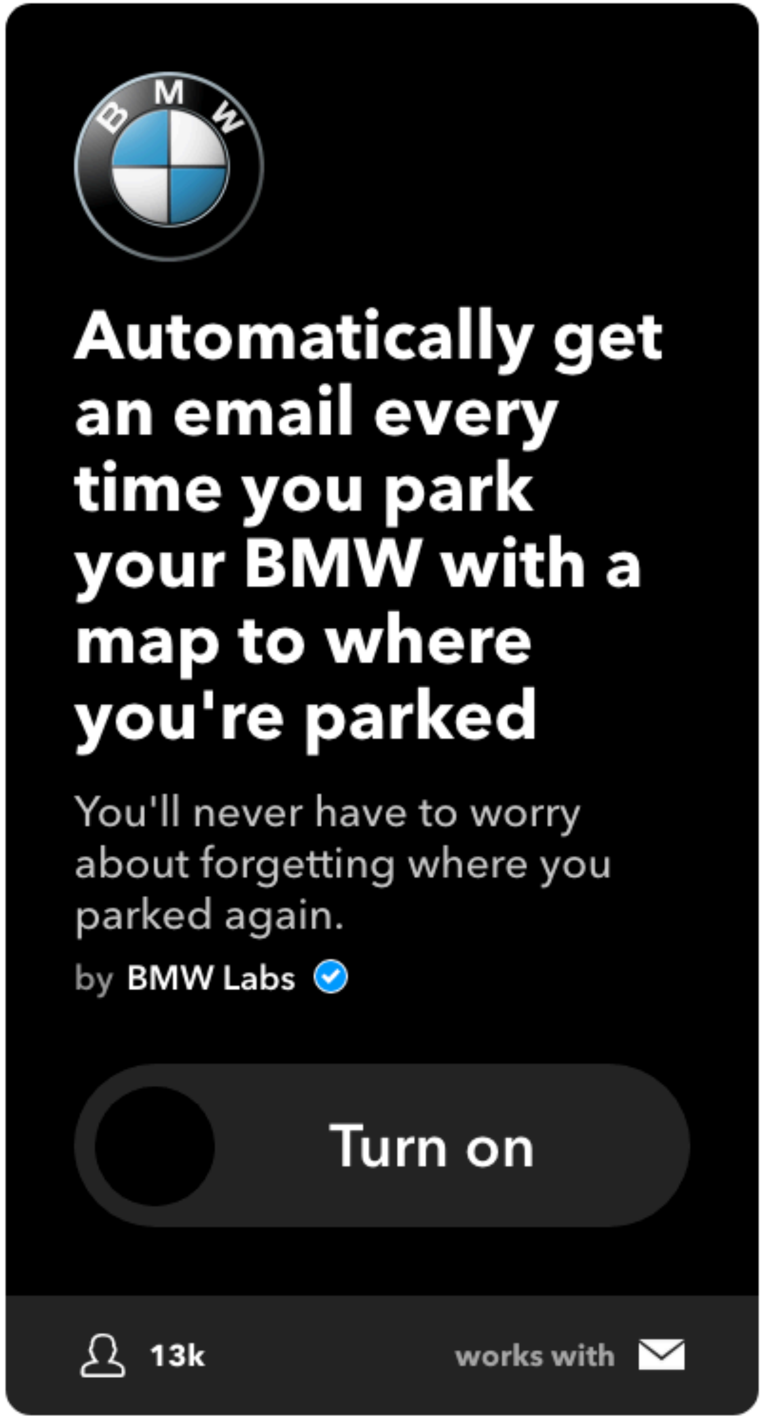
then

IFTTT app

$$\text{If } \underbrace{\text{this}}_{\text{Trigger}} \text{ then } \underbrace{\text{that}}_{\text{Action}}$$



What can go wrong? ☺

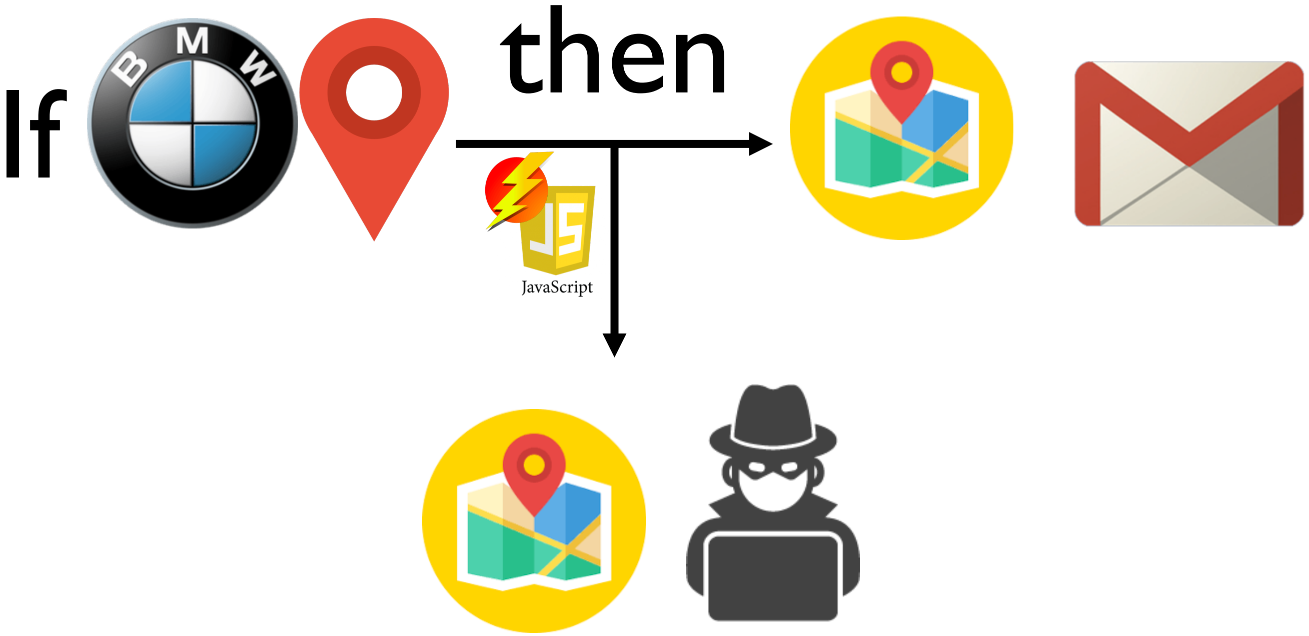


Automatically get an email every time you park your BMW with a map to where you're parked

You'll never have to worry about forgetting where you parked again.

by **BMW Labs** ✓

Attack by malicious app maker



If

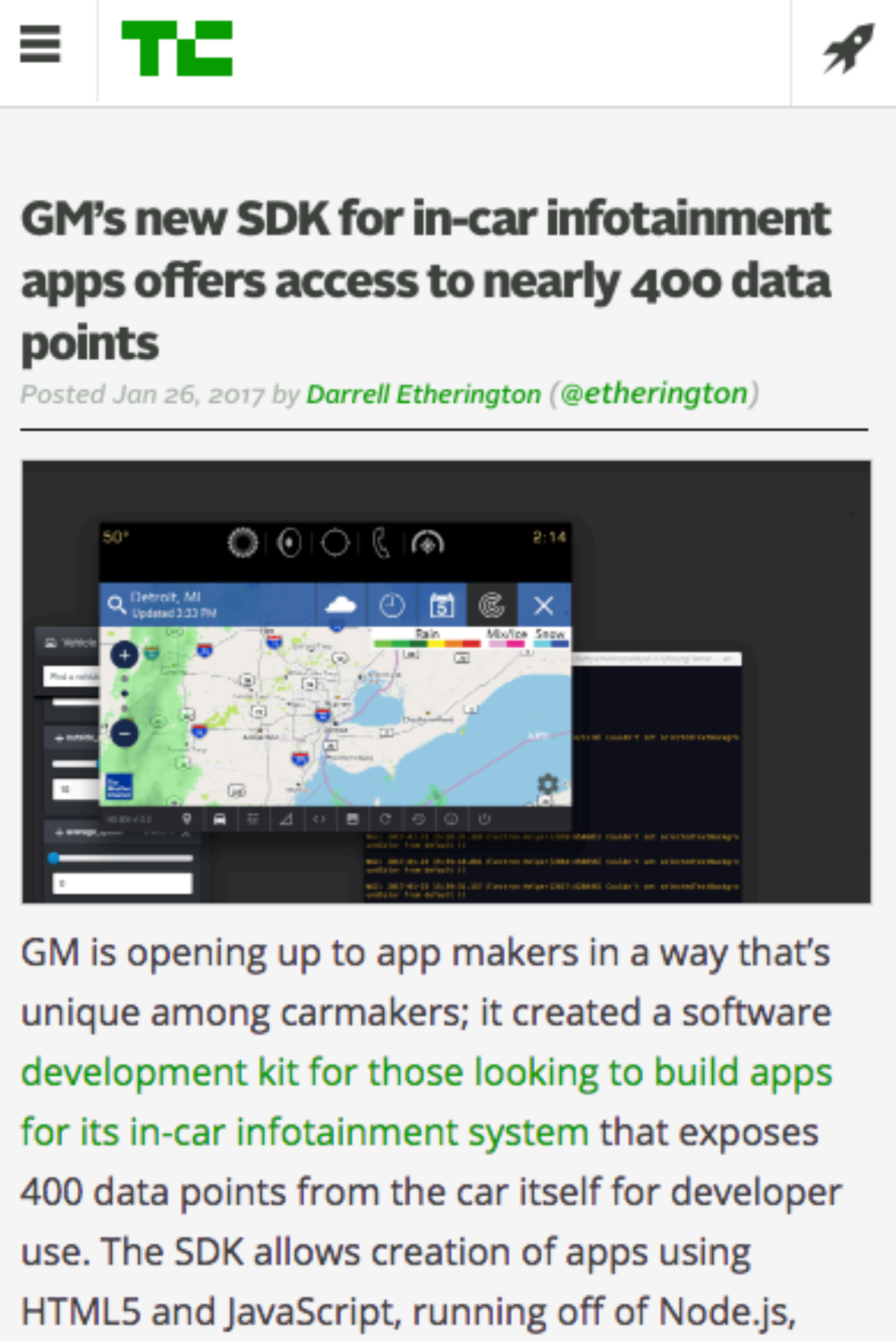
then

In-car infotainment apps

- Stores for 3rd-party in-car apps
  - GM: JavaScript/HTML5
  - Volvo Cars, Renault, Nissan, and Mitsubishi: Android Automotive
- Sensitive sources
  - Location, odometer, current speed, backup camera, microphone

  ⇒ location tracking, audio spying
- Sensitive destinations
  - seat settings, climate control, stereo volume

  ⇒ "soundblast", driver disruption



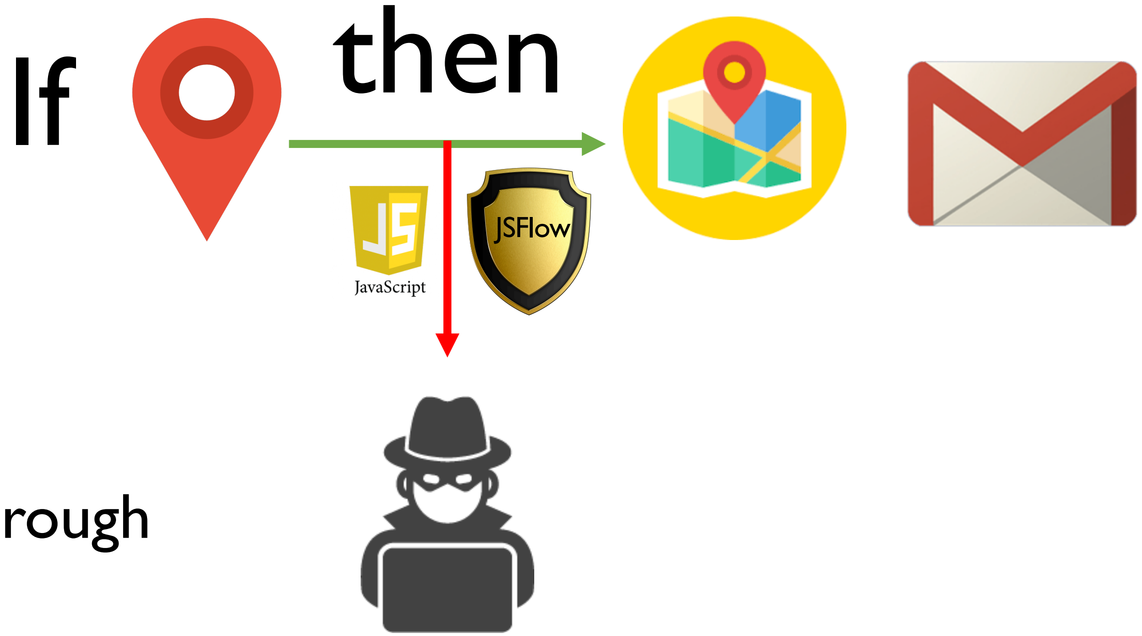
GM's new SDK for in-car infotainment apps offers access to nearly 400 data points

Posted Jan 26, 2017 by Darrell Etherington (@etherington)

GM is opening up to app makers in a way that's unique among carmakers; it created a software development kit for those looking to build apps for its in-car infotainment system that exposes 400 data points from the car itself for developer use. The SDK allows creation of apps using HTML5 and JavaScript, running off of Node.js,

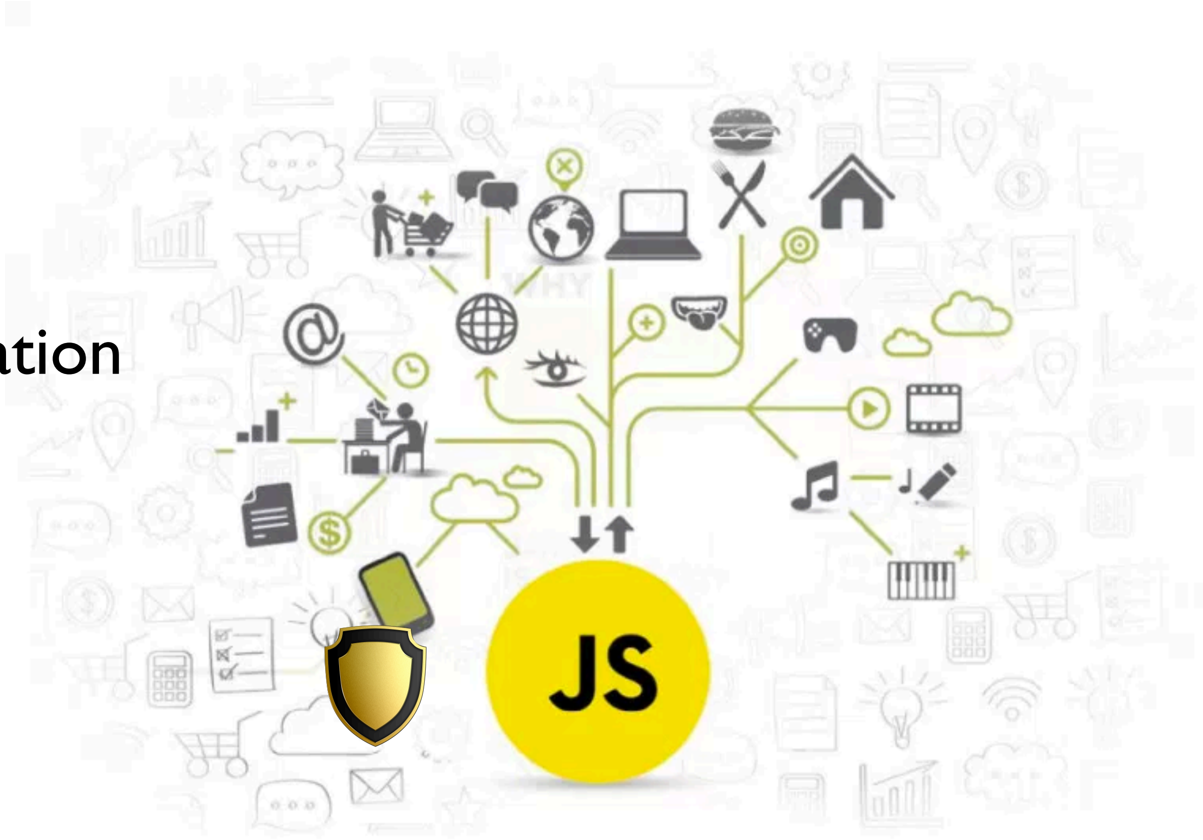
Countermeasures

- Application-level security
  - Secure code in control of IoT!
- API control
  - Location API
  - Voice command API
- Information flow control
  - Track the flow of information through JavaScript code
  - Block flow from sensitive sources to attacker



Securing IoT apps

- Securing IoT a presssing challenge
  - Incompatible standards, platforms and technologies
- Web of Things to reduce IoT fragmentation
- Need to secure code in control of IoT applications
  - JavaScript at heart
  - IFTTT security
    - Informaiton flow control
  - In-car app security
    - Permissions and API security



IEEE
SECURITY & PRIVACY

Read more in IEEE Security & Privacy Magazine 2019

Joint work
in part with Iulia Bastys and Musard Balliu
and in part with Benjamin Eriksson

Securing IoT Apps

Musard Balliu | KTH Royal Institute of Technology
Iulia Bastys and Andrei Sabelfeld | Chalmers University of Technology

Users increasingly rely on Internet of Things (IoT) apps to manage their digital lives through the overwhelming diversity of IoT services and devices. Are the IoT app platforms doing enough to protect the privacy and security of their users? By securing IoT apps, how can we help users reclaim control over their data?

The world of the Internet of Things (IoT) is fascinating, but who is in charge? Meet Iona, whose story of ups and downs in the IoT world will help us illustrate how the technical aspects of securing IoT apps can have real-life impact on nontechnical users.

Users Lack Control Over Their Digital Lives

Scenarios like this illustrate that users often lack sufficient control over their digital lives. The heterogenous nature of the IoT implies that although the services and devices might be connected by a network, robust application support is needed so that the interacting services and devices can be controlled by the users. Rather than reinventing new protocols and standards for the IoT, the Web of Things[1] reuses well-known web standards to enable a smooth application layer for IoT applications. Billions of devices, from printers to smart TVs, already routinely run web

Take 1: Help!

On her way home, Iona parks her car at a shopping mall, takes a picture of the season's first snow in a nearby park, and heads to the mall for some shopping. However, when her shopping is done, she has a hard time remembering where she parked her car. She realizes she accidentally deleted the first-snow picture as she was fiddling with her phone. To make things worse, she also realizes that she forgot to turn on the thermostat at home, which is unfortunate given the chilly weather. All of this is especially frustrating because her phone is an Internet-connected smartphone; her car is a connected car, with rich Internet and infotainment features; and her thermostat is connected to the Internet through the vendor's portal. Connectivity alone is clearly not enough to manage Iona's digital life through the overwhelming diversity of IoT services and devices.

Digital Object Identifier 10.1109/MSEC.2019.2914190
Date of publication: 5 June 2019