Infecting Internet of Things

Axelle Apvrille - Fortinet
aapvrille@fortinet.com

DefCamp, November 2016

© Copyright Fortinet Inc. All rights reserved.

Outline

Who am I?

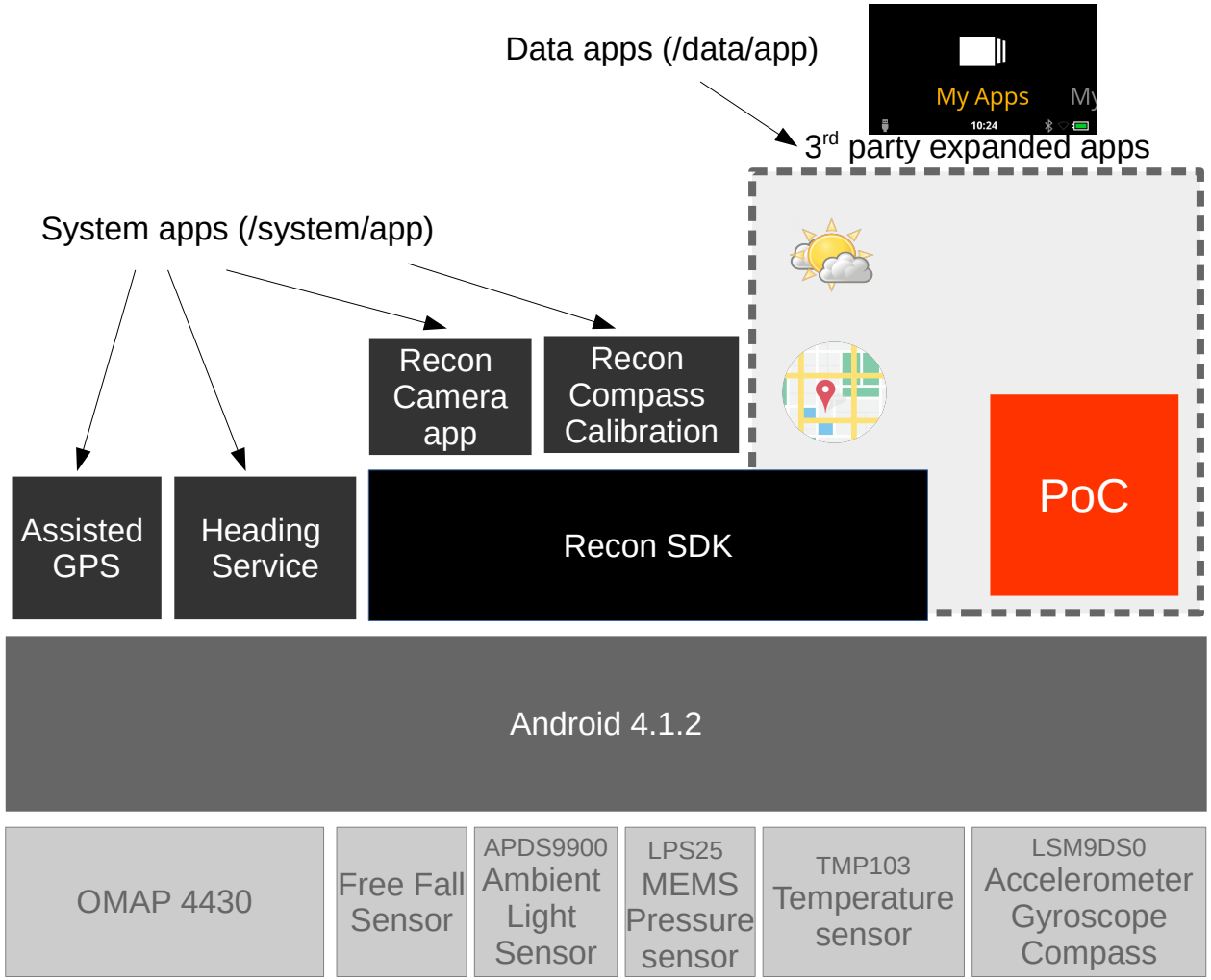
whoami

```
my $self = {
    realname => 'Axelle Apvrille',
    nickname => 'Crypto Girl',
    company => 'Fortinet, Fortiguard Labs, Research EMEA',
    time => '8 years',
    job => 'Senior Anti-Virus Researcher',
    topics => 'Malware for smart objects (phones, IoT...)',
    twitter => '@cryptax',
    languages => 'French, English, Hexadecimal :)'
};
```

Outline

Demo: Ransomware on Smart Glasses

How the PoC works: architecture

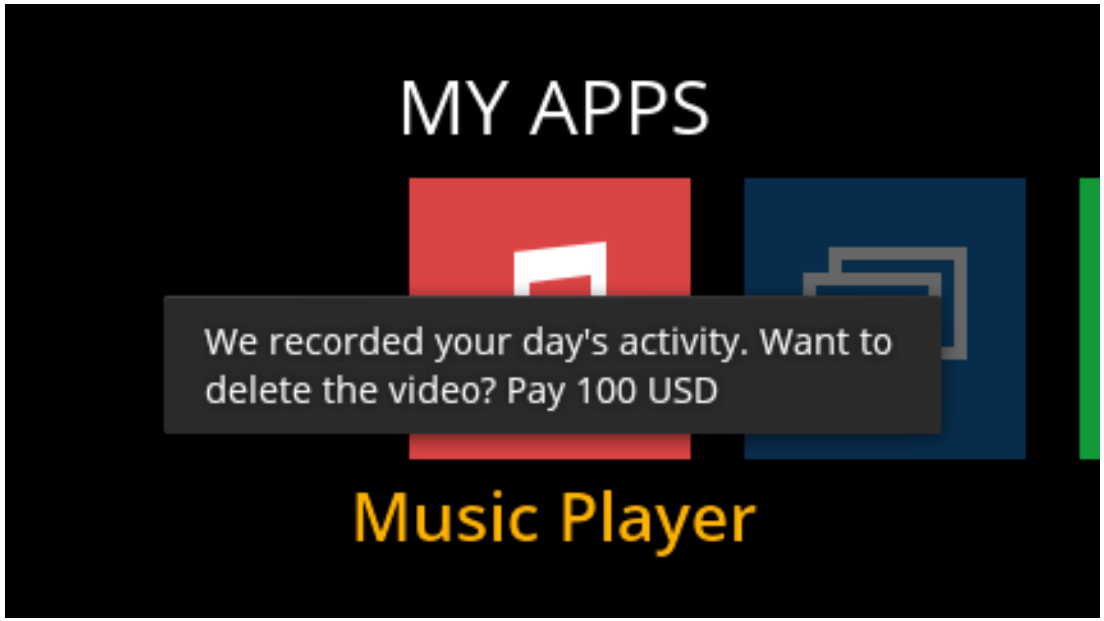


How the PoC works: source code

```
public void onCreate(Bundle savedInstanceState) {
  super.onCreate(savedInstanceState);
  CharSequence msg = (CharSequence)
     this.getIntent().getStringExtra("message");
  if (msg == null) {
    msg = "No text provided!";
  }
  int duration = Toast.LENGTH_LONG;
  for (int i=0; i<40; i++) { // Quick hack for a longer toast ;)
    Toast.makeText((Context)this,
          (CharSequence)msg, duration).show();
  }
  this.finish();
}
```

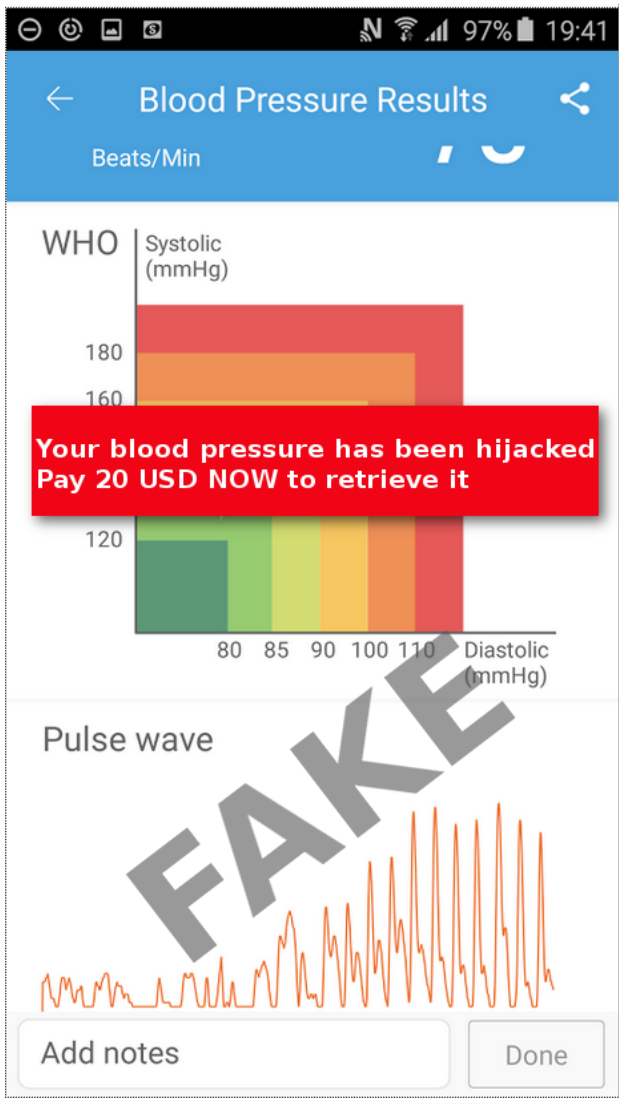
That simple? **Yes**. That makes even more scary :=)

What will you do? 1/3



Did they **really** record your activity? Perhaps...
Smart glasses cost 500 USD $\approx$ 2030 RON

What will you do? 2/3



You can't use your blood pressure monitor any longer.

But, given your medical condition, you **need** it

This is a fake screenshot - no known ransomware on that app (yet)

What will you do? 2bis /3

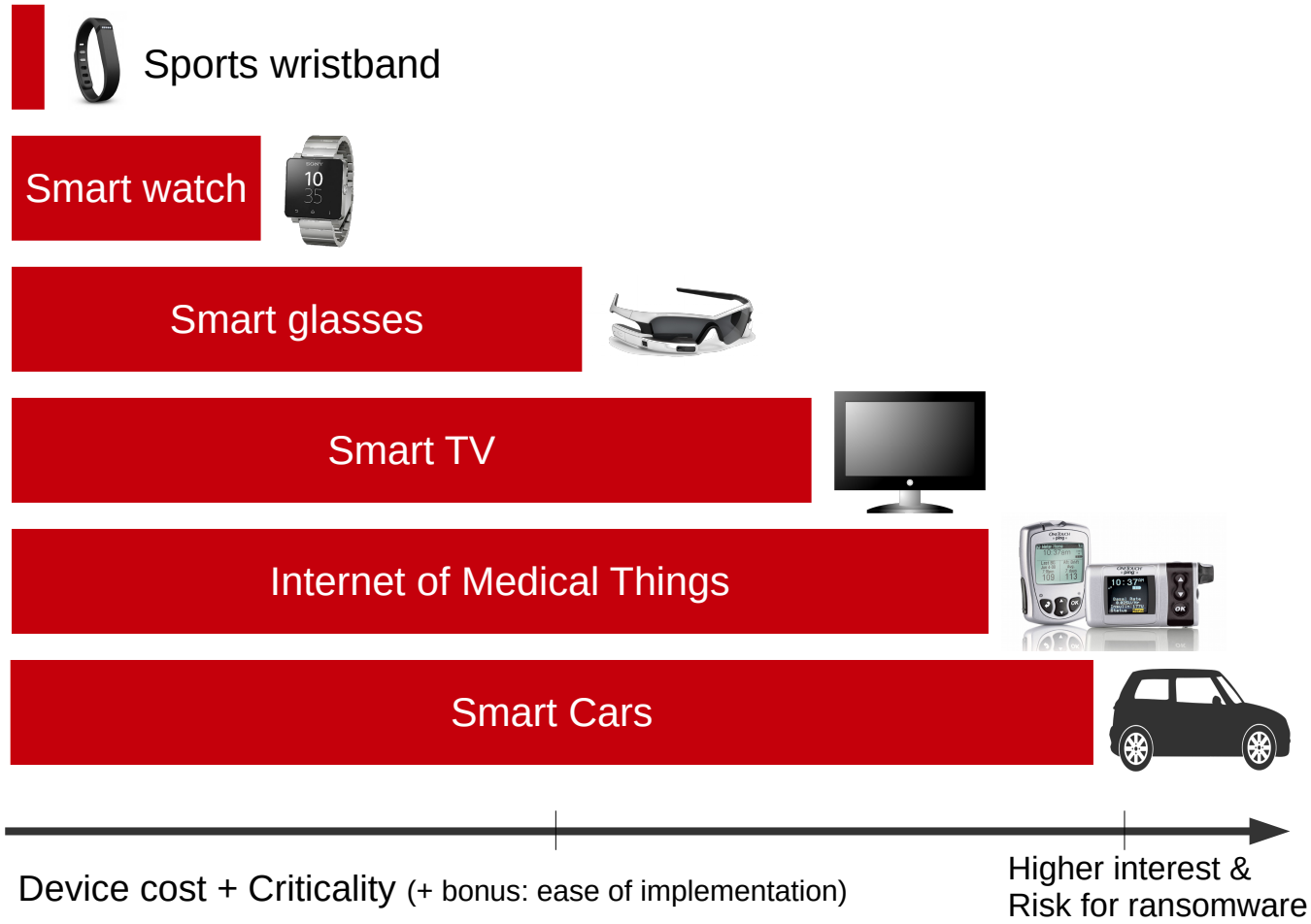
Your insulin pump has been hacked!

NB. This is a *fake* screenshot - however vulnerabilities exist

- October 2016 - R7-2016-07: Multiple Vulnerabilities in Animas OneTouch Ping Insulin Pump
- More on medical devices: see Marie Moe's talks on pacemakers

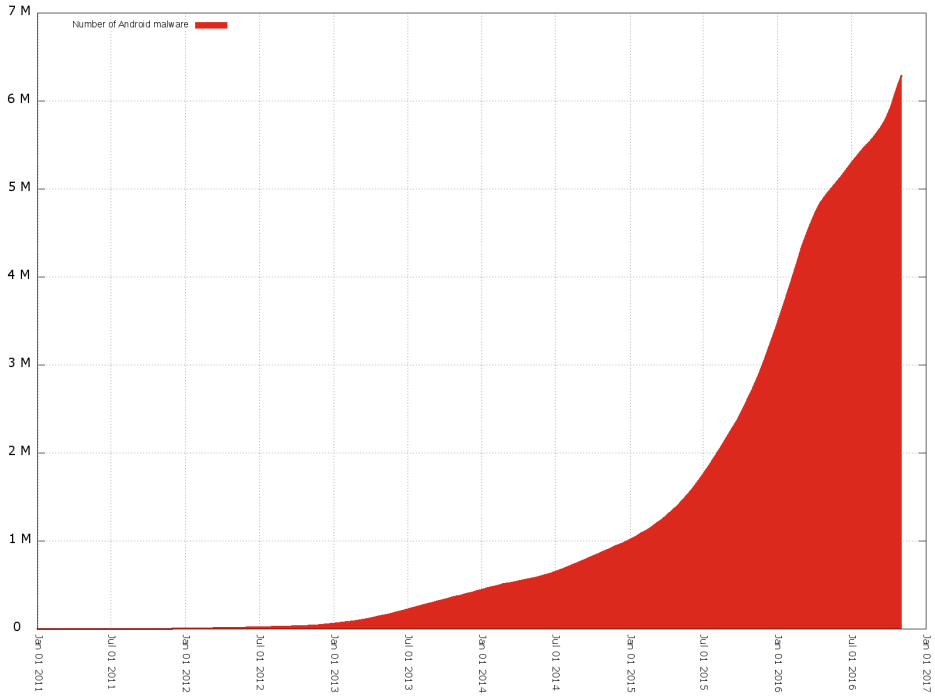
What will you do? 3/3

Ransomware on IoT "business case"



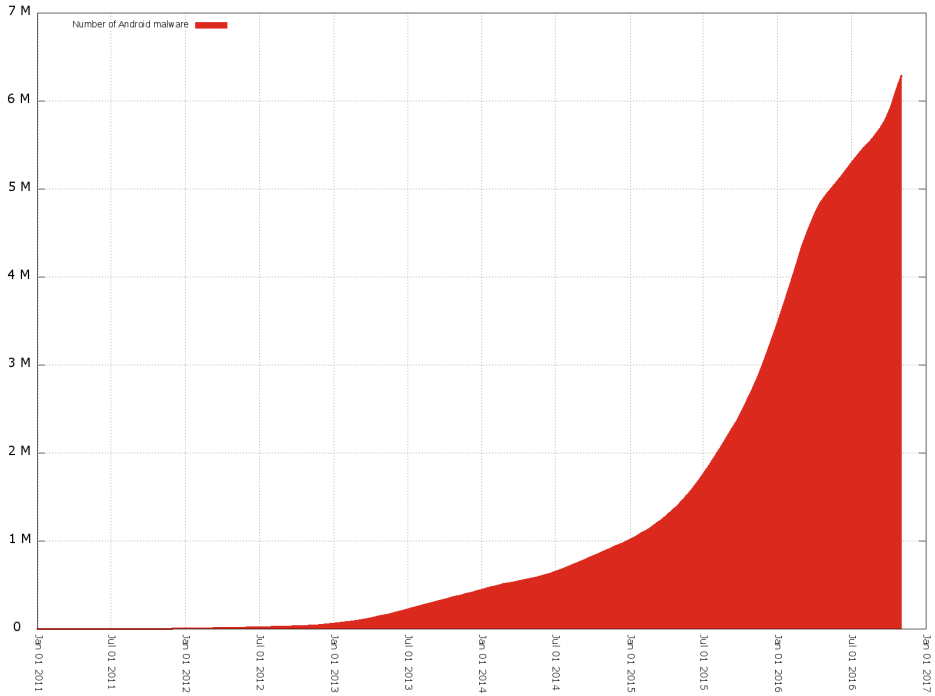
Outline

Advanced Trojan Malware on Smart Glasses



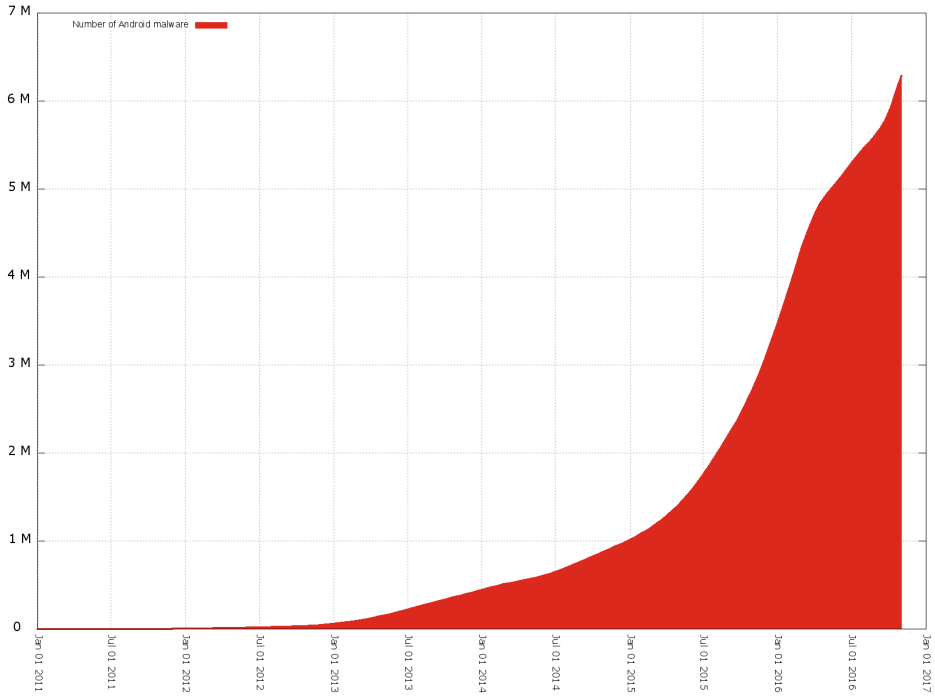
- $\approx$ 5,000 new Android malware per day

Advanced Trojan Malware on Smart Glasses



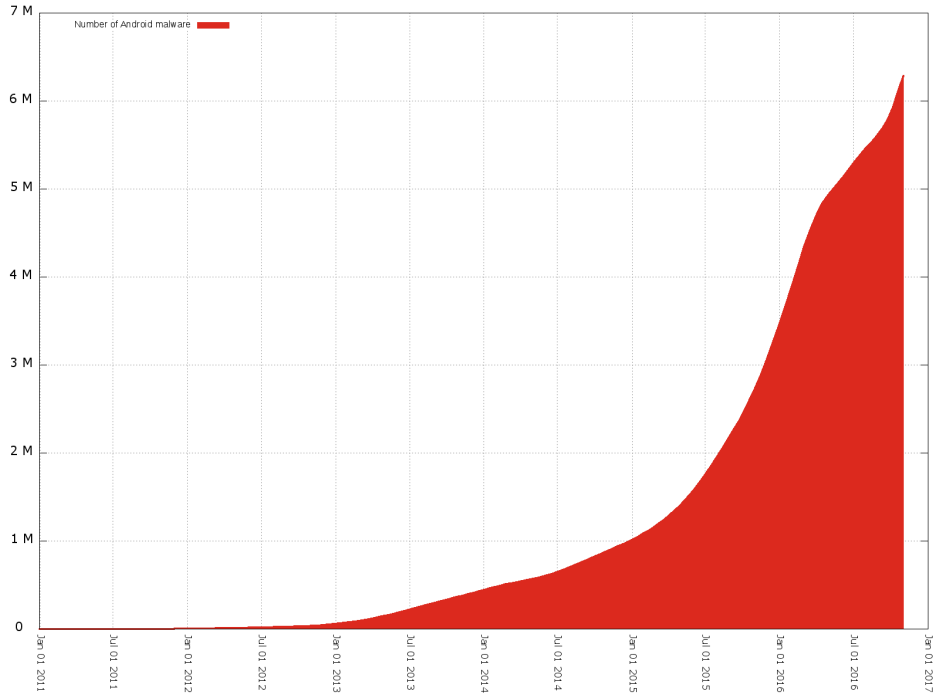
- $\approx$ 5,000 new Android malware per day
- Are the smart glasses vulnerable to those?

Advanced Trojan Malware on Smart Glasses



- $\approx$ 5,000 new Android malware per day
- Are the smart glasses vulnerable to those?
- In theory, yes.

Advanced Trojan Malware on Smart Glasses

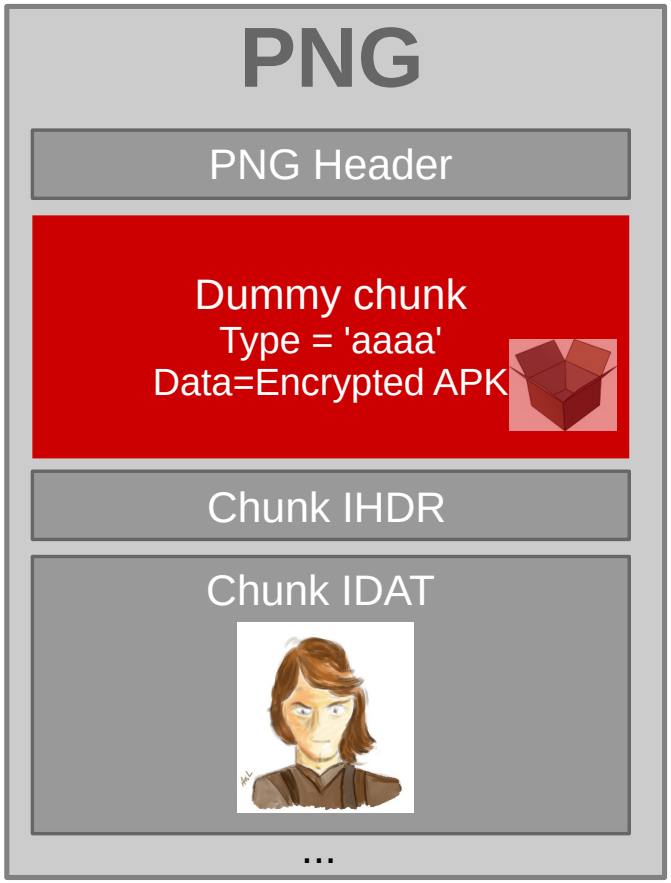


- $\approx$ 5,000 new Android malware per day
- Are the smart glasses vulnerable to those?
- In theory, yes.
- In practice, it's worth checking: no GSM/3G, wifi possible but not easy, virtual keyboard, difficult to upgrade the OS...

Android AngeCryption PoC on Smart Glasses

See A. Apvrille, A. Albertini, *Hide Android Applications in Images*, BlackHat Europe 2014

AngeCryption "trick"



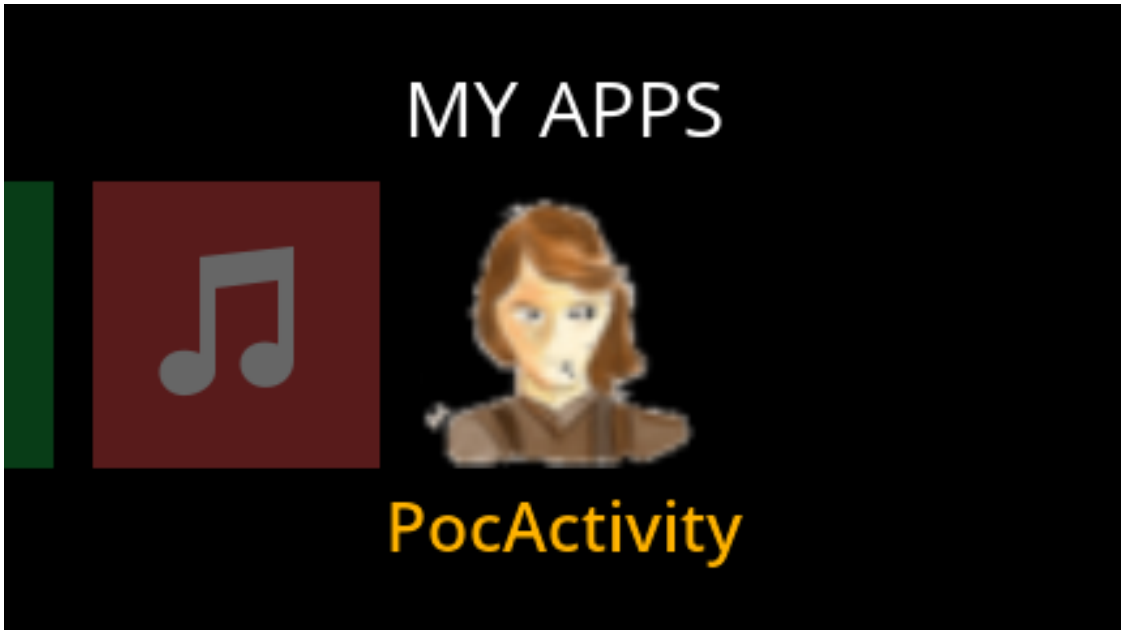
Works on **Android 4.4.2**.
Smart glasses are **Android 4.1.2**.
Should work.

1. Put the image in an *apparently benign* Android application
2. Trigger decryption...
3. ... Install malicious application

Step 1: Install benign application

```
$ adb install PocActivity.apk
```

Screenshots taken from the smart glasses:

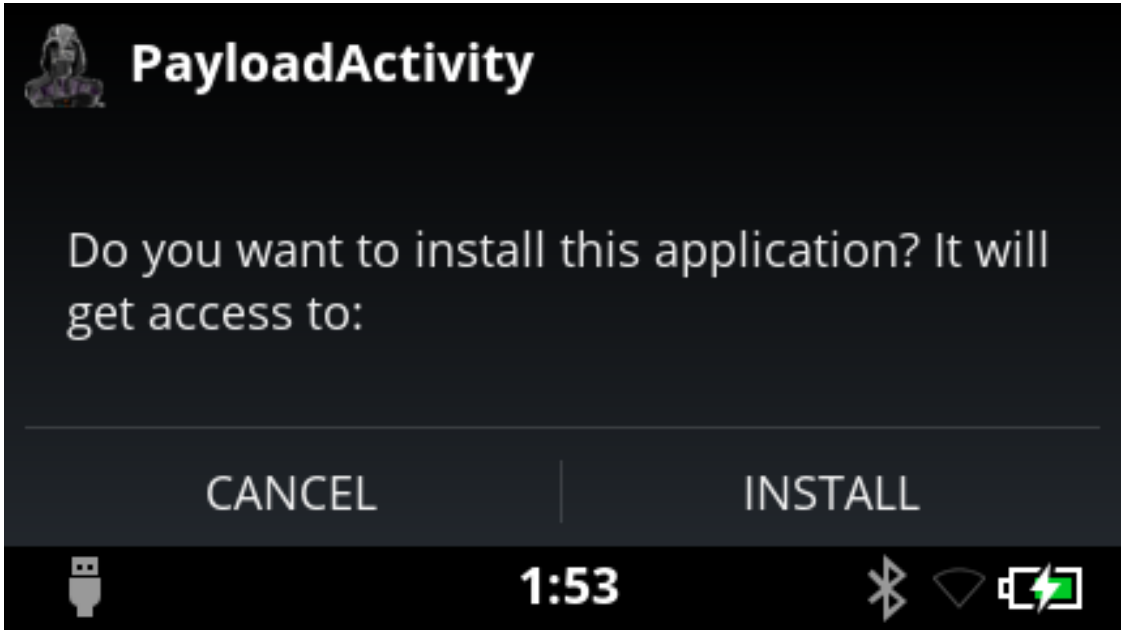


Step 2: Trigger decryption

Click!

Step 2: Trigger decryption

Click!



This is *PoC for encrypting APK as image*
not a PoC for *hiding install*
but this is possible via *DexClassLoader*

Step 3: Malware installed on the smart glasses

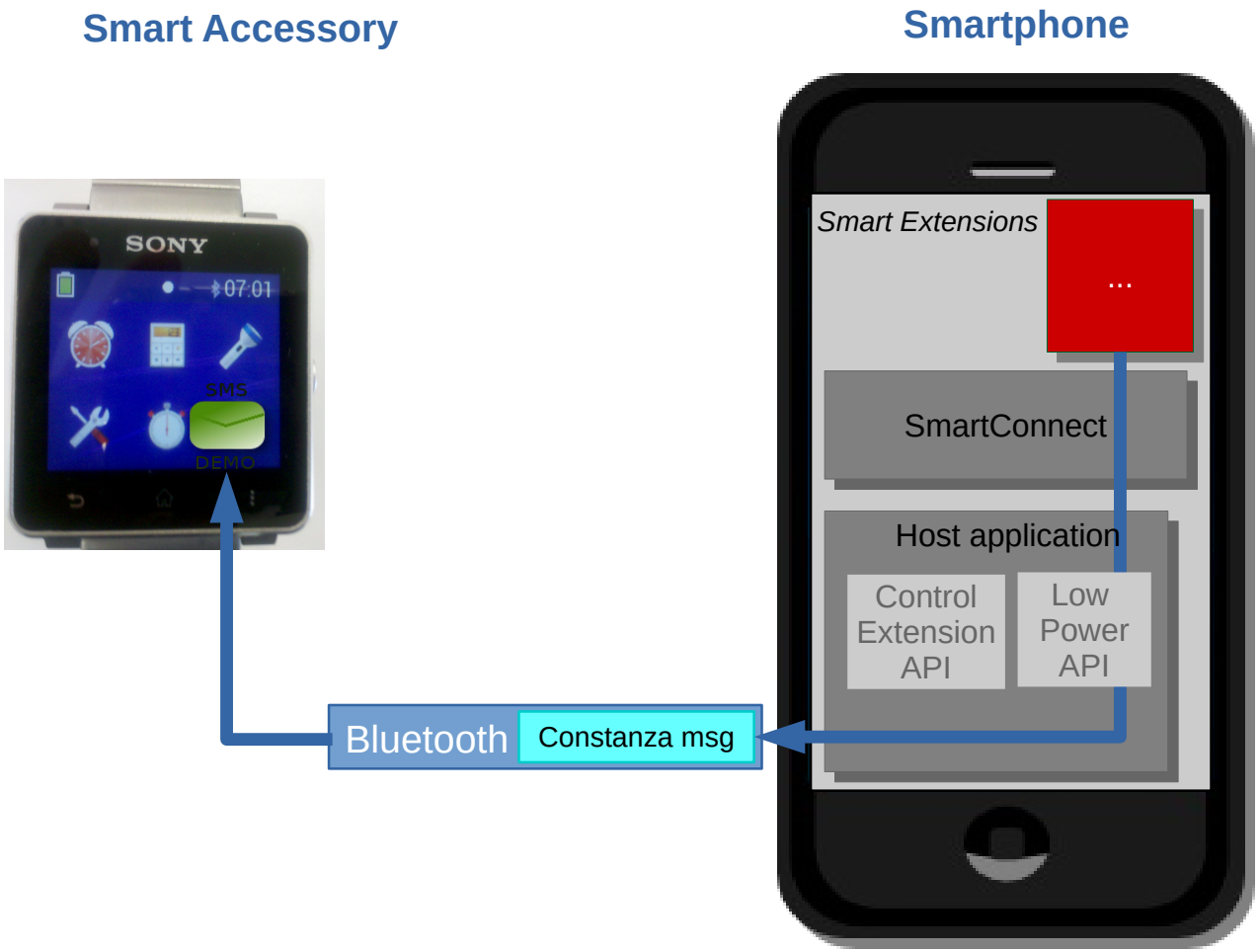
So, **yes, it worked** - without modification

Outline

Demo: SMS Dialer on a Smart Watch

- Sony SmartWatch SW2
- ARM Cortex M4 with Micrium μC/OS-II
- Light sensor and accelerator
- NFC, Bluetooth 3.0
- Launched in Sept 2013
- $\approx$ 600 RON

How it works: architecture



How it works: code

Trigger a command from the Smart Watch

```
class SmartWatchSms extends ControlExtension {
```

Act when clicked

```
ControlView btn = mLayout.findViewById(...);
btn.setOnClickListener(new OnClickListener() {
  public void onClick() {
    sendSms();
  }
});
```

Work when not lit

```
public boolean supportsLowPowerMode() {
  return true;
}
```

Outline

Mom Attack :)

Credits: Dilbert Comic Strips

"Business" case for attacker depends on:

Onboard sensors, Wearable or not, Target population

Outline

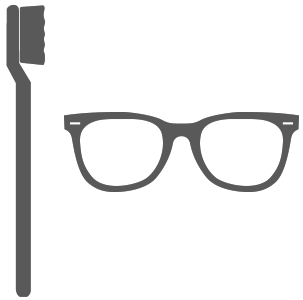
Some of the (in)famous IoT malware

Carna	2012	Research botnet
Linux/Darlloz	2013	Worm exploiting PHP vuln. Infects ADSL routers, satellite and television receivers. Mine cryptocurrencies.
The Moon	2014	Worm exploiting CGI exploit. Infects Linksys routers
ELF/Gafgyt	2014	DDoS. Targets CCTV
Linux/Wifatch	2015	Trojan/Vigilante. Targets DVR, CCTV
Linux/Moose	2015	Perform illegimate likes/follows
Linux/PnScan	2015	DDoS. Targets routers (India mainly)
Linux/Remaiten	2016	DDoS. IRC based
Linux/Mirai	2016	DDoS. Targets DVR, CCTV...
Linux/IRCTelnet	2016	DDoS. IRC based. IPv6 ready

Outline

Worm propagation via wearable

Attacker

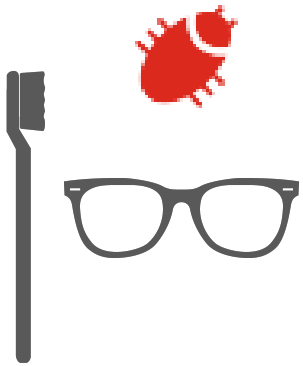


Victim's laptop

Worm propagation via wearable

Attacker

INJECT MALICIOUS CODE

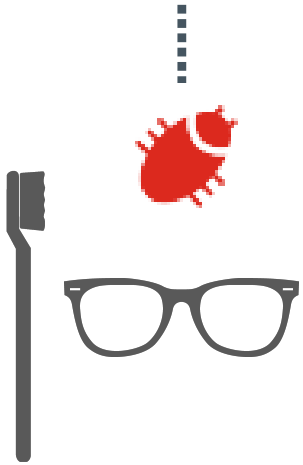


IoT is infected

Victim's laptop

Worm propagation via wearable

Attacker

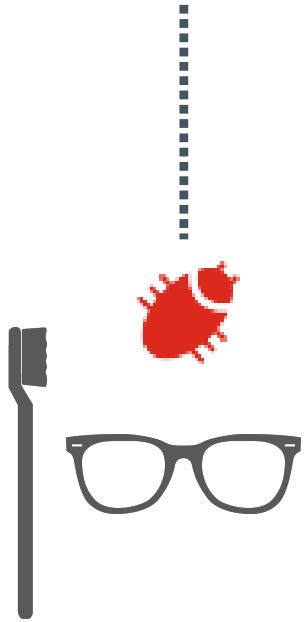


Victim's laptop

Worm propagation via wearable

Attacker

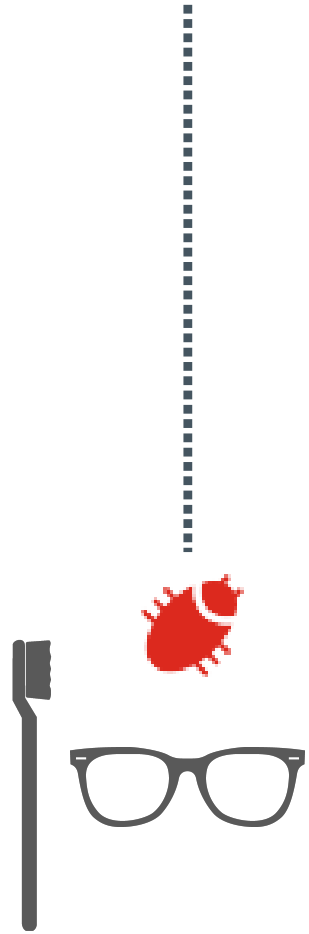
Victim's laptop



Worm propagation via wearable

Attacker

Victim's laptop

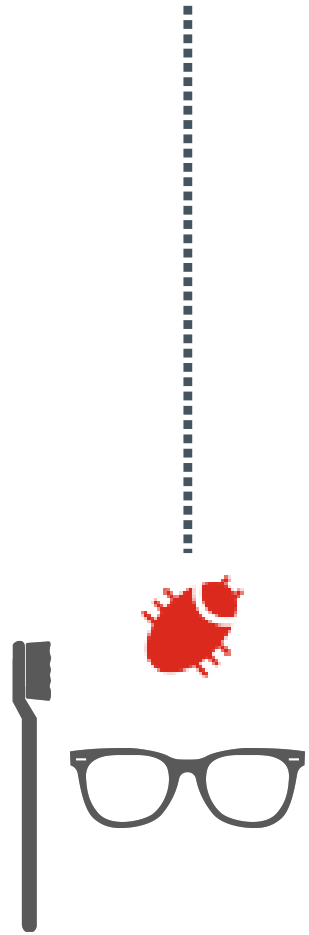


Worm propagation via wearable

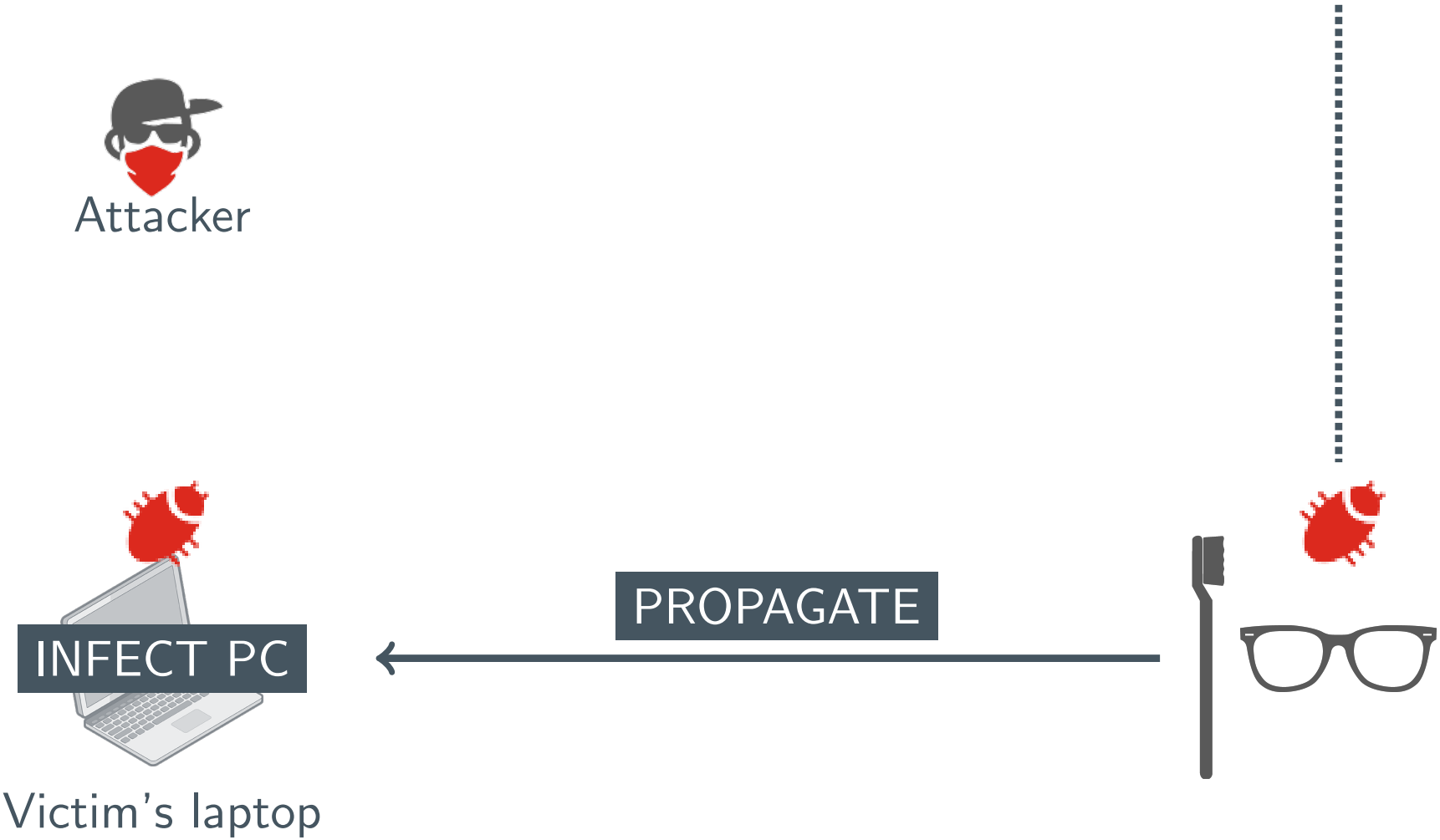
Attacker

Victim's laptop

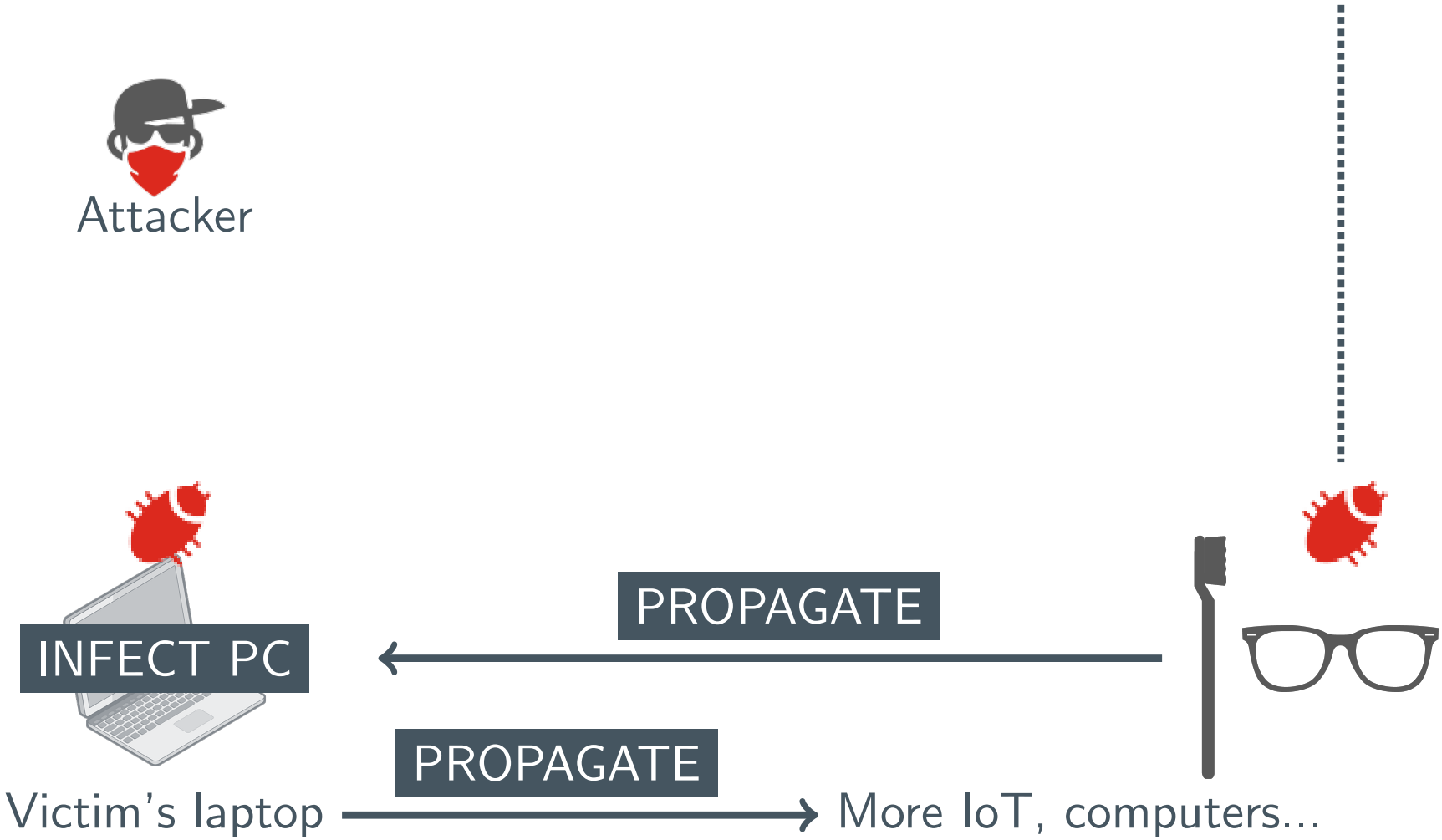
PROPAGATE



Worm propagation via wearable

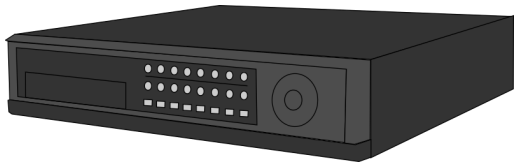


Worm propagation via wearable



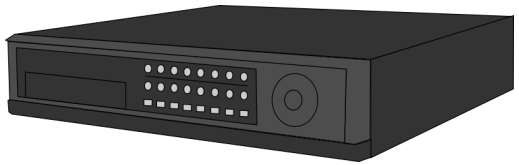
Malware of (Every)Things

So far, we have had malware on complex IoT


Malware of (Every)Things

So far, we have had malware on complex IoT


Prediction: we will have them everywhere




They have a firmware. They can have a malware ;)

Outline

References

- *Reversing Internet of Things from Mobile Applications*, presented at AREA 41, 2016
- *Is Ransomware Coming to IoT?* by Candid Wüest (Symantec), presented at Insomni'hack, 2016
- Mirai: source code, analysis, protocol
- *Thermostat Ransomware: a lesson in IoT security* by Ken Munro, August 2016
- IoT Goes Nuclear: Creating a ZigBee Chain Reaction by Eyal Ronen et al - worm propagation with ZigBee on Philips Hue lightbulbs - 2016
- SDK: Sony Smart Watch, Recon Instruments
- Videos: Remotely controlling a toothbrush, Fitness tracker hacking

Thanks for your attention!

PowerPoint slides? No way! This is LaTeX/ Beamer