

# NETT I HJERTET

Da sikkerhetseksperter Marie Moe (37) fikk hjerteproblemer, oppdaget hun at det er mulig å hacke livskritiske, medisinske apparater som pacemakere, morfinpumper og insulinutstyr.

TEKST OSMAN KIBAR FOTO MAXIM SERGIENKO  
Hamburg

– **DET ER EN** grunn til at USAs visepresident Dick Cheney fikk fjernet den trådløse enheten i den implanterte hjertestarteren sin, sier Sinforsker og sikkerhetseksperter Marie Moe.

Cheneys kardiolog fryktet et attentatforsøk gjennom hacking av enheten. Da Moe selv fikk operert inn en pacemaker, oppdaget hun at den hadde egenskaper ingen hadde fortalt henne om.

Marie Moe er godt vant med uforutsigbare hendelser, som plutselige nettangrep mot norske banker eller spionasje mot norske olje- og gasselskaper. Hun visste hva hun skulle gjøre hvis det ble meldt om sårbarhet i norske kraftsentralers kontrollsystemer. Moe var en landets fremste eksperter på hendelseshåndtering, informasjonssikkerhet og nettverksikkerhet. Hun ledet de hemmelige tjenestenes operasjonssenter Norcert, som følger datatrafikken inn og ut av Norge i sanntid.

Trusselen som rammet henne en helt vanlig novembermorgen for fire år siden, var hun ikke like godt forberedt på.

**ESKEN.** Moe var alene i leiligheten, klar til å gå på jobb på operasjonssentralen på Akershus festning. Hun skulle bare ta seg et glass appelsinjuice først. Plutselig kollapset hun. Da hun våknet opp igjen, lå hun på gulvet omgitt av glasskår. Moe ante ikke hvor lenge hun hadde ligget bevisstløs på gulvet og dro til legevakten for å utelukke hjernerystelse. Det viste seg

høyt, sårbarheter i kildekoden, mulige programmeringsfeil som kunne føre til at apparatet ikke fungerte som det skulle.

– Men jeg hadde ikke noe valg. Jeg måtte ha den, sier Moe.

Nå fikk hun installert software i kroppen som hun ikke kunne verifisere, tilsynelatende uten anledning til å «patche» eventuelle sikkerhetshull.

En enkel operasjon, så var problemet løst, og hun følte hun seg bra. Men komplikasjoner skulle oppstå.

**GOOGLE OG EBAY.** Helsepersonellet var ikke vant til å forholde seg til krypteringsprotokoller, trådløse aksesspunkter og implementering – dagligdagse temaer for Marie Moe, som hadde doktorgrad i informasjonssikkerhet fra NTNU og mastergrad i matematikk med spesialisering innen kryptografi. De forsto ikke hva hun snakket om.

– De hadde ikke fått slike spørsmål før. De hadde aldri tenkt på det, forteller hun.

Da Moe googlet saken, oppdaget hun at det ikke fantes så mye sikkerhetsforskning på medisinsk utstyr generelt – og pacemakere spesielt. Hun logget seg inn på Ebay, cashet ut et titall tusenlapper og bestilte brukt pacemakerutstyr. Så fant hun frem til den tekniske manualen for sin egen pacemaker.

– Jeg er jo forsker. Jeg ville gjerne finne ut mer.

med innstillingene på Moes pacemaker. Man klarte ikke å finne årsaken.

– Hvis kroppen din trenger oksygen og plutselig ikke får det, er det en veldig ubehagelig følelse, sier hun.

Det viste seg at pacemakeren var innstilt på altfor lav maksimpuls. Da Moe nådde maksimumspuls på 160 slag i minuttet, halverte den automatisk antallet hjerteslag.

– Det tok nærmere tre måneder å finne svaret, sier Moe.

Mistankene hennes om tekniske svakheter viste seg å stemme.

**EIREANN.** Hun tok kontakt med den britiske hackeren og risikoforskeren Eireann Leverett, som hun kjente fra da han tipset norske myndigheter om mulige, kritiske svakheter i industrielle kontrollsystemer som lå åpent på nett. I motsetning til personlige datamaskiner som jevnt var blitt forbedret, var industrielle kontrollsystemer et sikkerhetsmessig jomfruterritorium med svake passord og minimal sikkerhetstenkning. Bevisstheten rundt sårbarhetene deres hadde økt noe da sentrifuger i Irans atomprogram ble angrepet, men fortsatt var mange kritiske anlegg usikrede på nett.

– Eireann var veldig interessert i kode som styrer nasjonal infrastruktur. Men her var det jo snakk om kode som styrer personlig infrastruktur, sier Moe.

Sammen med Leverett, som i tillegg til å





# The battle for privacy?

Forbes / Tech

AUG 18, 2015 @ 08:15 PM 72,558 views

## How A Creep Hacked A Baby Monitor To Say Lewd Things To A 2-Year-Old



Kashmir Hill  
FORBES STAFF

Warning: The New York Times' privacy policy is not valid.

FOLLOW ON FORBES (2015)



FULL BIO >

Comments expressed by Forbes.com are not valid.



This looks like a Foscam baby monitor (via ABC News)



Before I hacked a stranger's smart home, I asked for permission. An anonymous creep who hacked a Texas family's baby monitor was not as polite. ABC News reports that a Houston couple heard an unfamiliar voice talking to their sleeping 2-year-old daughter on Saturday night and realized that a stranger had taken control of their camera-enabled monitor. And he wasn't a very nice stranger:

“Mare Gilbert was doing the dishes after his birthday dinner and he heard strange noises coming from his daughter Allyson's room while she was sleeping.

“Right away I knew something was wrong,” he told ABC News.

As he and his wife got closer to the room, they heard the voice calling his daughter an “effing moron,” and telling her, “wake up you little slut.”

So not the best birthday. Luckily (?) his daughter is deaf and her cochlear implants were turned off. So the hacker turned his vitriol on her parents:

“The hacker then began shouting expletives at her parents and calling Gilbert a stupid moron and his wife a b\*\*\*\*.

“At that point I ran over and disconnected it and tried to figure out what happened,” said Gilbert. “[I] Couldn't see the guy. All you could do was hear his voice and [that] he was controlling the camera.”

In comments on an article about the hack, Mare Gilbert said he did take basic security precautions, including passwords for his router and the baby-stalking IP cam, as well as having a firewall enabled. Looking at the footage taken by ABC News, it appears that Gilbert was using a Foscam wireless camera. That may have been the problem, as a vulnerability in that product was disclosed by security researchers just months ago in a

betanews

Hot Topics: Windows 10 Microsoft Apple Cloud Tablets Android Security Reviews

## Vault 7: WikiLeaks reveals CIA's secret hacking tools and spy operations



By Mark Wilson

Published 21 hours ago

Follow @MarkWilsonWords

71 Comments

Like 500

Share 55

G+ 15

Tweet



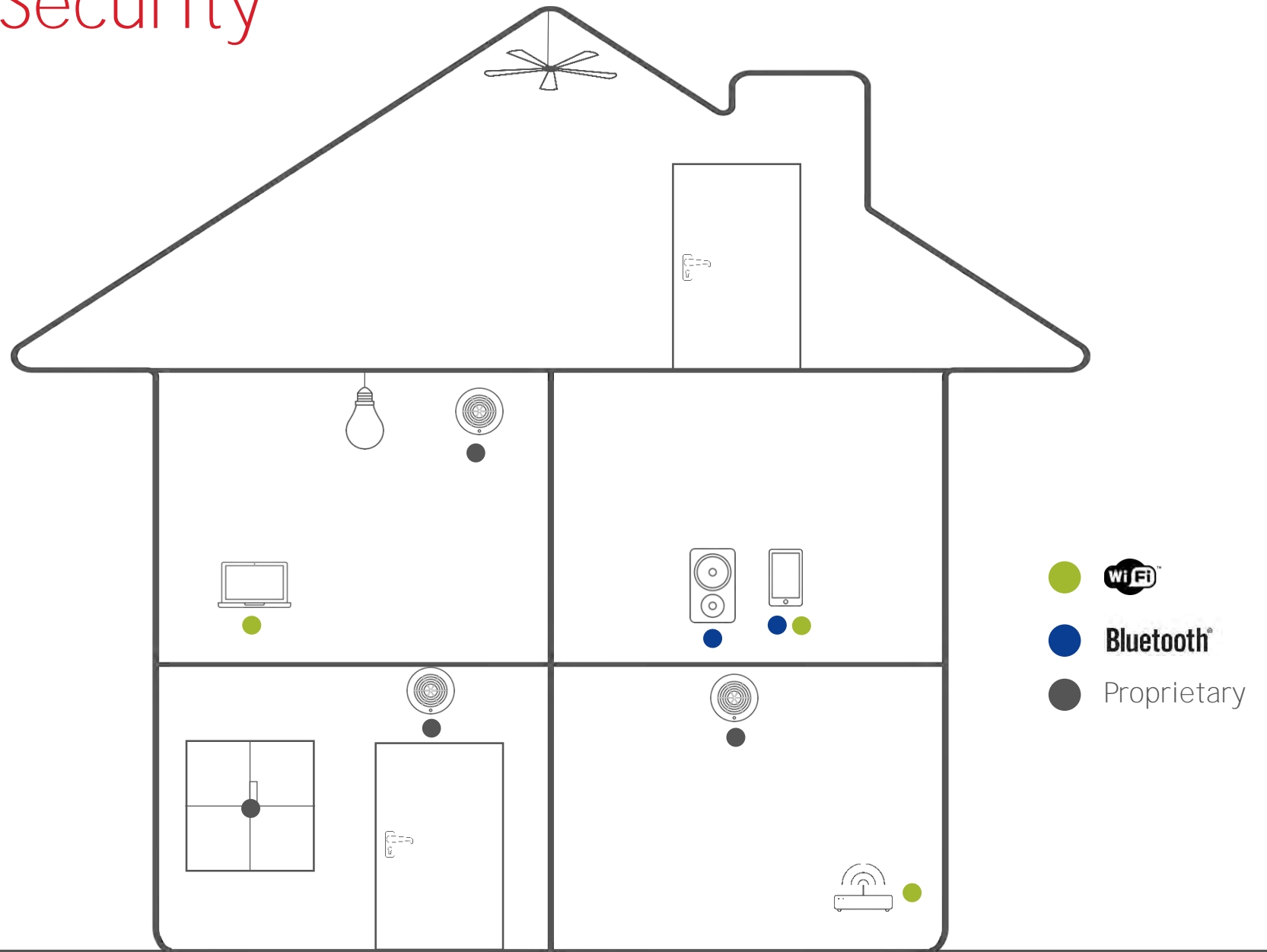


# Ransomware of the future?





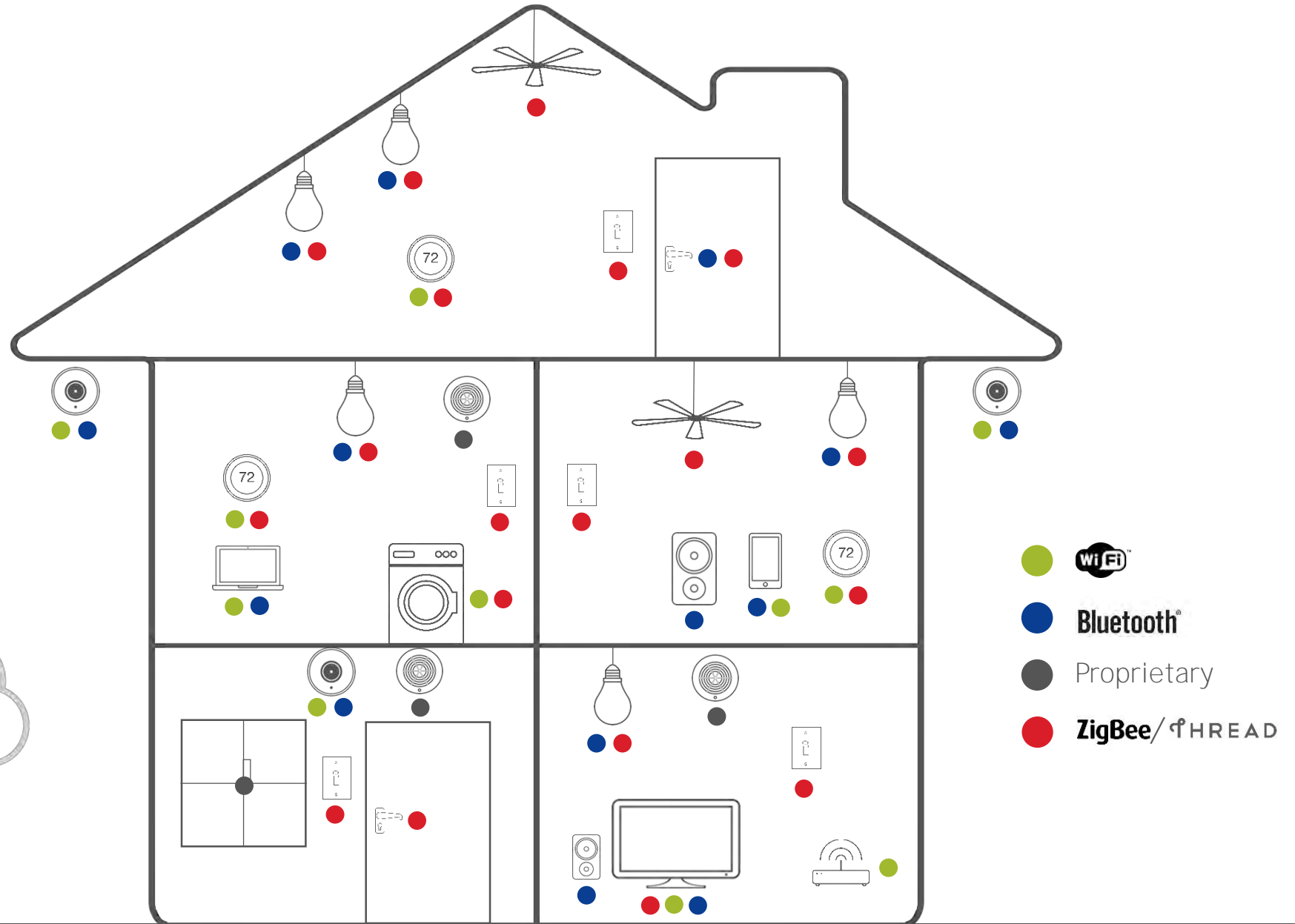
# Classical Cyber Security





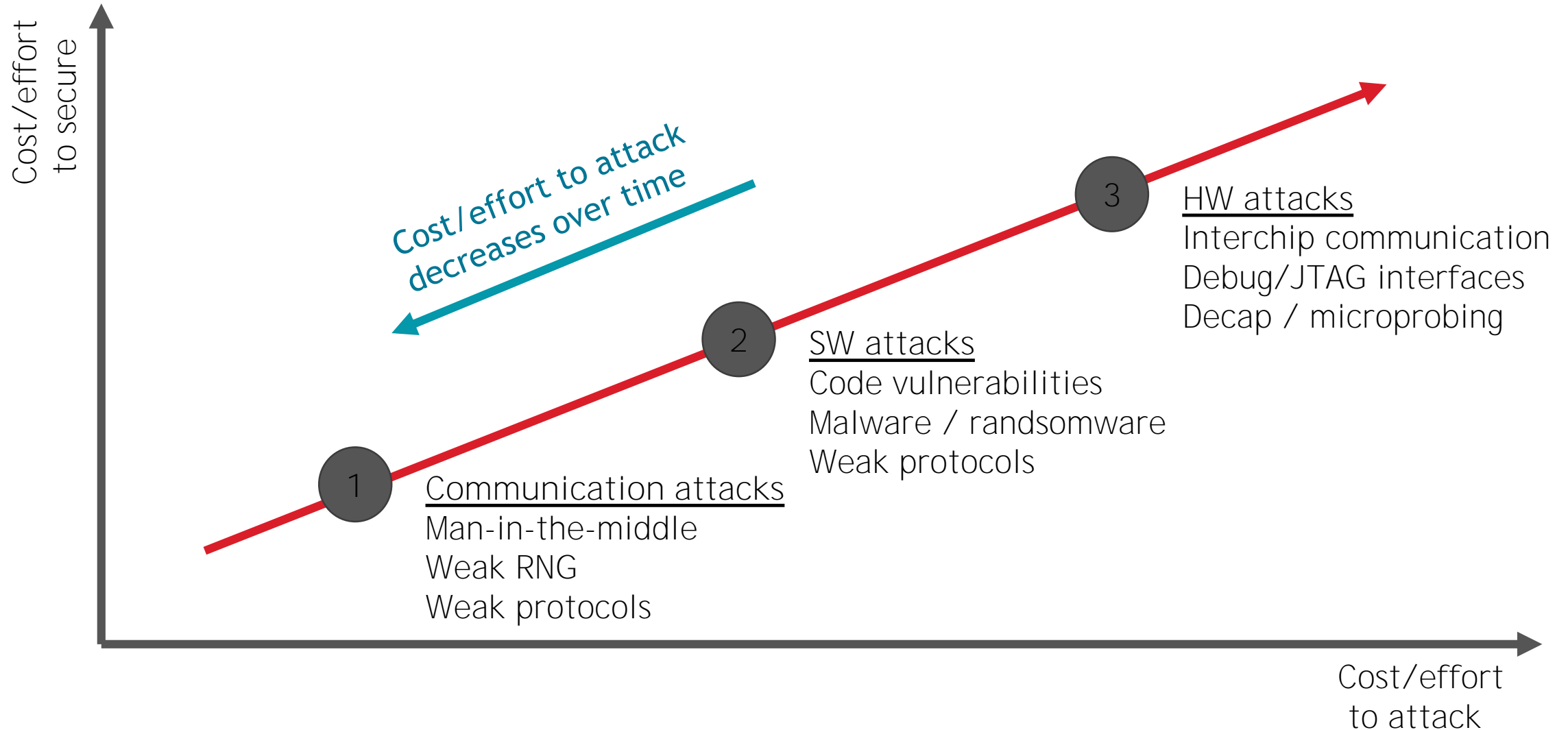
# IoT Security

- Increased attack surface
- Accessibility to hardware
- Limited processing power in end nodes





# Cost of security





# Who is the adversary?



**IOActive**  
**RAPID7**



Class	Hobbyist / script-kiddie	Advanced hackers	Security researchers	Nation state attacks
Motivation	Fun, curiosity, fame	Fame, financial	Curiosity, improve security, novel ideas and attacks	Espionage, sabotage
Resources	Limited, commodity hacking equipment	Commodity, makes tools when necessary	Significant	Unlimited

Exponentially increasing cost of security





# Security/privacy is a balancing act

- Security/privacy
- Easy of use
- Functionality





# UK: GCHQ is enforcing proper security

## the INQUIRER

### GCHQ intervenes to prevent catastrophically insecure UK smart meter plan

One key to decrypt them all

By **Graeme Burton**

Mon Mar 21 2016, 12:48



**INTELLIGENCE AGENCY GCHQ** has intervened in the rollout of smart meters to demand better encryption to protect UK electricity and gas supplies.

GCHQ barged in after spooks cast their eyes over the plans and realised that power companies were proposing to use a single decryption key for communications from the 53 million

smart meters that will eventually be installed in the UK.

The agency was concerned that the glaring security weakness could enable hackers, once they'd cracked the key, to gain access to the network and potentially wreak havoc by shutting down meters *en masse*, causing power surges across the network.

The security flaws would have been particularly catastrophic as the UK's 'Rolls Royce' (i.e. unnecessarily expensive) smart metering system doesn't just automate meter reading. It enables power companies to engage in power management and

- Old news, disregard date
- Smart energy critical for national security
- GCHQ = CIA
- GCHQ helped architect security scheme for UK Smart Energy



# US: FTC continue suing insecure IoT vendors





# EMEA: EU / Germany taking a lead?



JUSTICE  
Building a European Area of Justice

European Commission > Justice > Data protection

HOME ALL TOPICS

Search

DATA PROTECTION

Reform of the data protection legal framework

Data transfers outside the EU

Article 29 Working Party

Entities collecting data

Protecting your personal data

Data protection bodies

Legislation

Funding opportunities

Public consultations

Events

## Protection of personal data

In January 2012, the European Commission proposed a comprehensive **reform of data protection rules in the EU**. The completion of this reform is a policy priority for 2015. The objective of this new set of rules is to give citizens back control over of their personal data, and to simplify the regulatory environment for business. The data protection reform is a key enabler of the Digital Single Market which the Commission has prioritised. The reform will allow European citizens and businesses to fully benefit from the digital economy.

Whenever you open a bank account, join a social networking website or book a flight online, you hand over vital personal information such as your name, address, and credit card number.

What happens to this data? Could it fall into the wrong hands? What rights do you have regarding your personal information?

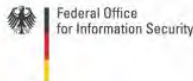
### Everyone has the right to the protection of personal data.

Under EU law, personal data can only be gathered legally under strict conditions, for a legitimate purpose. Furthermore, persons or organisations which collect and manage your personal information must protect it from misuse and must respect certain rights of the data owners which are guaranteed by EU law.

Every day within the EU, businesses, public authorities and individuals transfer vast amounts of personal data across borders. Conflicting data protection rules in different countries would disrupt international exchanges. Individuals might also be unwilling to transfer personal data abroad if they were uncertain about the level of protection in other countries.

Therefore, common EU rules have been established to ensure that your personal data enjoys a high standard of protection everywhere in the EU. You have the right to complain and obtain redress if your data is misused anywhere within the EU.

The EU's **Data Protection Directive** also foresees specific rules for the transfer of personal data outside the EU to ensure the best possible protection of your data when it is exported abroad.



## Certification Report

### BSI-CC-PP-0073-2014

for

### Protection Profile for the Gateway of a Smart Metering System (Smart Meter Gateway PP)

### Schutzprofil für die Kommunikationseinheit eines intelligenten Messsystems für Stoff- und Energiemengen


Version 1.3

from

### Federal Office for Information Security



# Congress hearing November 16<sup>th</sup> on IoT Security



**THE ENERGY AND COMMERCE COMMITTEE**

Home » Hearings and Votes

## Understanding the Role of Connected Devices in Recent Cyber Attacks

Wednesday, November 16, 2016 - 10:00am  
Location: 2175 Rayburn House Office Building  
Understanding the Role of Connected Devices in Recent Cyber Attacks

Understanding the Role of Connected Devices in Recent Cyber Attacks  
November 16, 2016 09:29 AM

**Committee on Energy & Commerce**

The image shows a banner for a congressional hearing. At the top is the Seal of the United States. Below it, the text 'THE ENERGY AND COMMERCE COMMITTEE' is displayed in large, bold, white letters. Underneath, there is a navigation link 'Home » Hearings and Votes'. The main title of the hearing is 'Understanding the Role of Connected Devices in Recent Cyber Attacks', followed by the date and time 'Wednesday, November 16, 2016 - 10:00am' and the location 'Location: 2175 Rayburn House Office Building'. A video player is embedded below the text, showing a still from the hearing with the text 'Committee on Energy & Commerce' overlaid in large, bold, yellow letters. The video player also shows the title 'Understanding the Role of Connected Devices in Recent Cyber Attacks' and the timestamp 'November 16, 2016 09:29 AM'. To the right of the video player are social media sharing icons for Twitter, Facebook, YouTube, Instagram, and RSS.

- Caused by the Mirai botnet attacks
- Key witnesses:
  - Bruce Schneier, Lecturer, Harvard University
  - Kevin Fu, CEO, Virta Labs
  - Dale Drew, SVP and CSO Level 3 Communications
- Key feedback:
  - IoT (in) Security is a externality -> needs regulation
  - Schneier called for a department of IoT Security



# Final thoughts

- IoT represents unprecedented challenges for security and privacy
- Already been a number of hacks
- Necessary to revisit the balance between security, privacy and functionality
- A number of governments, organizations and companies are ramping activities to secure the IoT





# Thank You!

www.silabs.com