The ‘P’ in IoT is for Privacy*

* Adapted from Radu Grigore’s remark: *The ‘S’ in IoT is for Security*

Budi Arief

b.arief@kent.ac.uk

Sensing and Privacy Workshop – Queen Mary University of London – 20 June 2017

Image Source: https://upload.wikimedia.org/wikipedia/commons/a/ab/Internet_of_Things.jpg

Image Source: https://www.abine.com/blog/2011/what-is-privacy-about/

- Behavioural and multi-dimensional concept
  - No “one solution fits all”
  - Individuals dynamically manage their privacy according to different situations in their life

IoT and Privacy

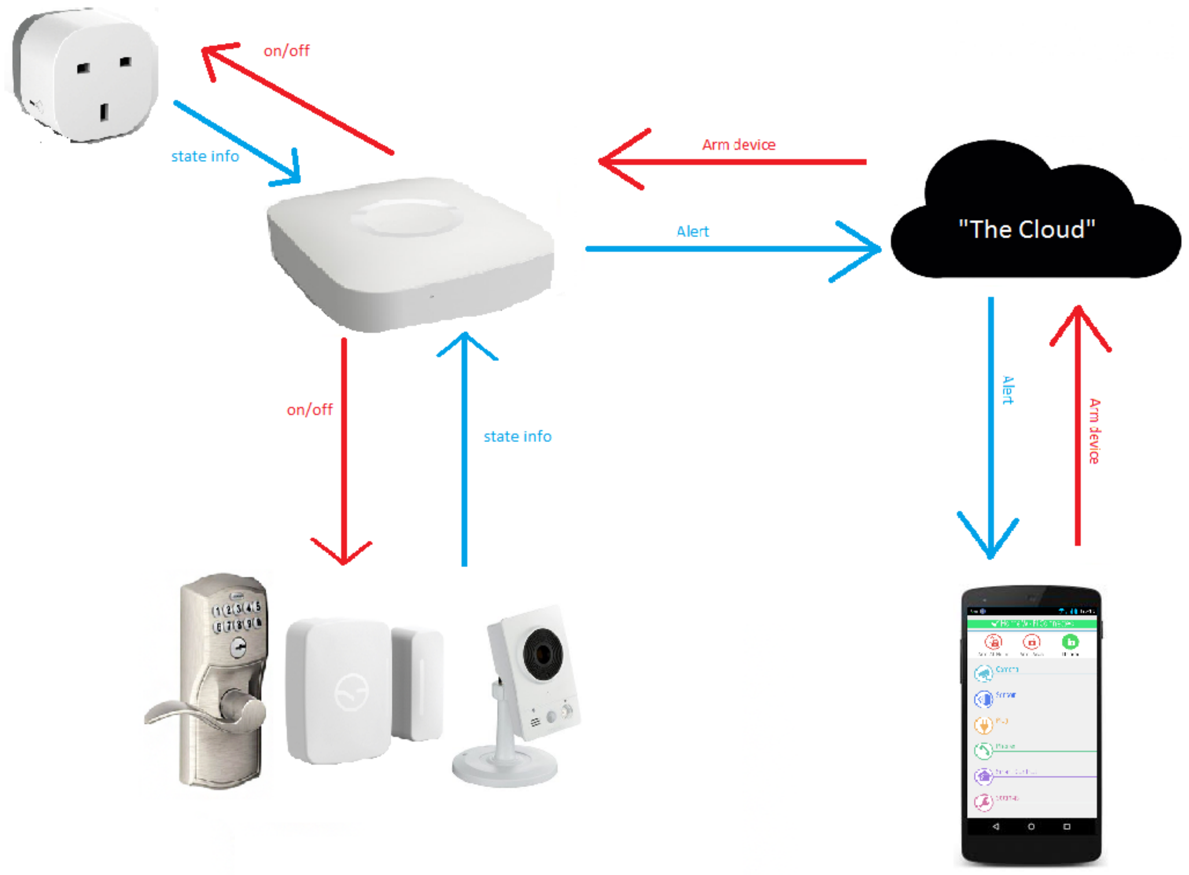
- IoT’s success relies on the abundance of data
  - Sensor data, user data, various other metadata
- The concept of IoT seems to be at odds with privacy
  - End users might not be willing to engage if there is a lack of useful information
  - But they will not be too happy either if their data are not protected or easily accessible to third parties

IoT and Privacy (contd.)

- There is an increase of user awareness of their data
  - Horror stories in popular media
    - E.g. smart TV listening to your private conversation
  - Generating values from personal data
- Passing the control back to the end users is still a big challenge

Example

- Smart Home Kits



(Taggart, 2017)

Example (contd.)

- Nice features
  - A mature platform supporting hundreds of devices
  - Allows third party developers to build smart-home apps through a programming framework
    - Apps providing rich user experience and control
- Potential issues
  - Over privileged access to IoT devices
    - Why do devices collect certain data? What else are they collecting without my knowledge?
  - Unobfuscated app source code

Privacy Threats in IoT

(Ziegeldorf et al., 2014)

- Identification
- Localization and tracking
- Profiling
- Interaction and presentation
- Lifecycle transitions
- Inventory attacks
- Linkage

Potential Solutions

(Aleisa and Renaud., 2017)

- Cryptographic techniques and information manipulation
- Data minimization
- Privacy/context awareness
- Access control

Potential Solutions

(Aleisa and Renaud., 2017)

- Cryptographic techniques and information manipulation
- Data minimization
- Privacy/context awareness
- Access control

Can potentially be done without human involvement

Potential Solutions

(Aleisa and Renaud., 2017)

- Cryptographic techniques and information manipulation
- Data minimization

Can potentially be done without human involvement

- Privacy/context awareness
- Access control

Will likely involve human

Potential Solutions

(Aleisa and Renaud., 2017)

- Cryptographic techniques and information manipulation
- Data minimization

Can potentially be done without human involvement

- Privacy/context awareness
- Access control

Will likely involve human

But solutions still seem to be designed with an **assumption** that users will willingly spend effort to preserve their privacy

Summary

- Privacy vs. convenience trade-off in IoT
- Challenges with IoT
  - No clear boundaries
  - Limited resources
- Issues on IoT security seems to be more pressing than those concerning its privacy
  - Mirai botnet
  - Default passwords
  - Unpatched devices

Summary (contd.)

- How can we put ‘P’ in IoT?
    - Knowing what data are recorded before buying a device
    - Knowing how user data are protected by the device
        - On the device and during transmission
        - After decommissioning
    - Allowing end users to configure their privacy preferences easily
        - Developers of (IoT) privacy solutions need to know their users better

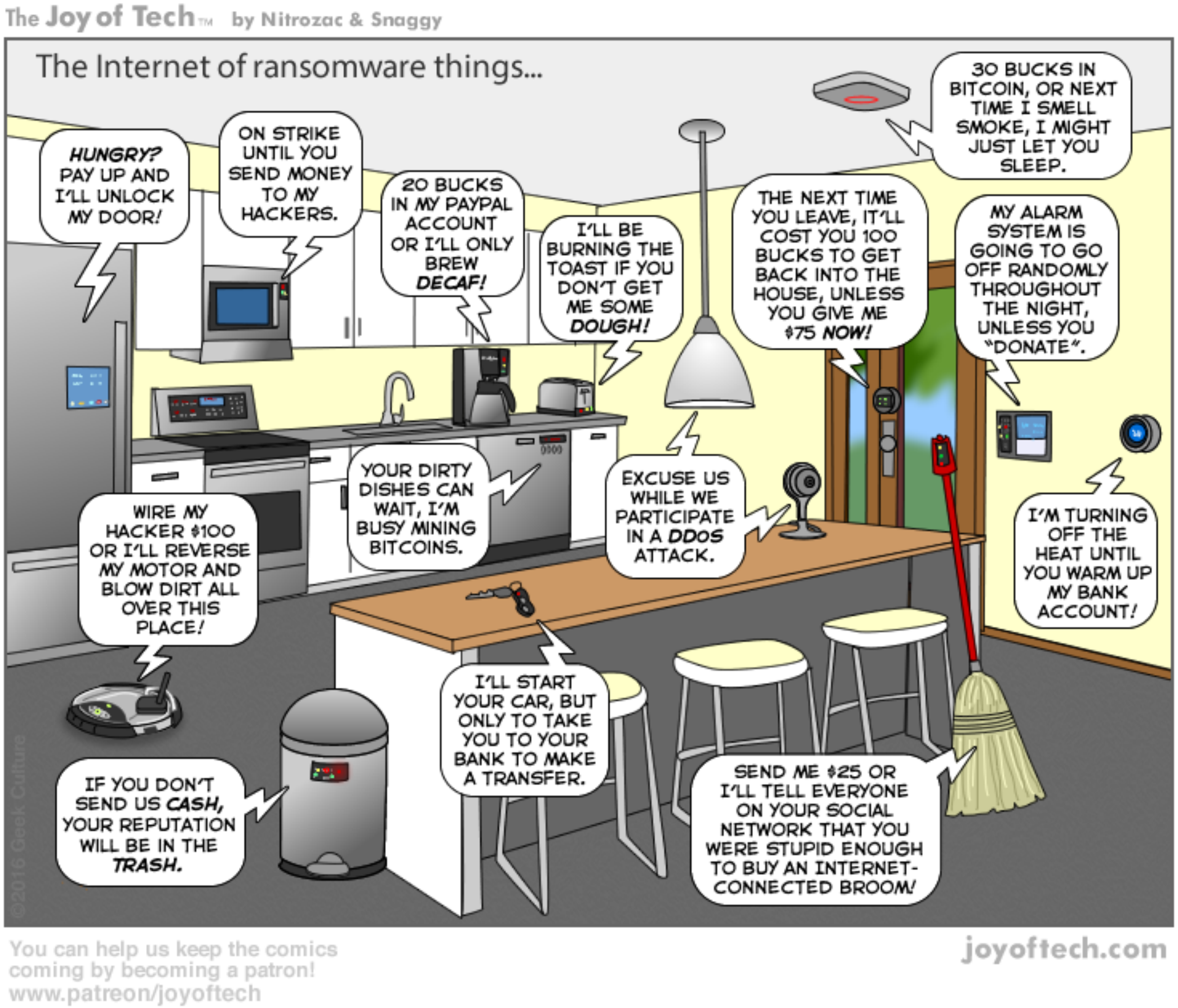

The Joy of Tech™ by Nitrozac & Snaggy
The Internet of ransomware things...
HUNGRY? PAY UP AND I'LL UNLOCK MY DOOR!
ON STRIKE UNTIL YOU SEND MONEY TO MY HACKERS.
20 BUCKS IN MY PAYPAL ACCOUNT OR I'LL ONLY BREW DECAF!
I'LL BE BURNING THE TOAST IF YOU DON'T GET ME SOME DOUGH!
THE NEXT TIME YOU LEAVE, IT'LL COST YOU 100 BUCKS TO GET BACK INTO THE HOUSE, UNLESS YOU GIVE ME $75 NOW!
30 BUCKS IN BITCOIN, OR NEXT TIME I SMELL SMOKE, I MIGHT JUST LET YOU SLEEP.
MY ALARM SYSTEM IS GOING TO GO OFF RANDOMLY THROUGHOUT THE NIGHT, UNLESS YOU "DONATE".
WIRE MY HACKER $100 OR I'LL REVERSE MY MOTOR AND BLOW DIRT ALL OVER THIS PLACE!
YOUR DIRTY DISHES CAN WAIT, I'M BUSY MINING BITCOINS.
EXCUSE US WHILE WE PARTICIPATE IN A DDoS ATTACK.
I'M TURNING OFF THE HEAT UNTIL YOU WARM UP MY BANK ACCOUNT!
I'LL START YOUR CAR, BUT ONLY TO TAKE YOU TO YOUR BANK TO MAKE A TRANSFER.
IF YOU DON'T SEND US CASH, YOUR REPUTATION WILL BE IN THE TRASH.
SEND ME $25 OR I'LL TELL EVERYONE ON YOUR SOCIAL NETWORK THAT YOU WERE STUPID ENOUGH TO BUY AN INTERNET-CONNECTED BROOM!
©2016 Geek Culture
You can help us keep the comics coming by becoming a patron! www.patreon/joyoftech
joyoftech.com

Image Source: http://www.geekculture.com/joyoftech/joyarchives/2340.html

References

- N. Aleisa and K. Renaud, “Privacy of the Internet of Things: A Systematic Literature Review”, Proceedings of *50th Hawaii International Conference on System Sciences*, pp. 5947-5956, 2017.
- E. Fernandes, A. Rahmati, J. Jung, A. Prakash, “Security Implications of Permission Models in Smart-Home Application Frameworks”, *IEEE Security and Privacy*, 15(2):24-30, 2017.
- A. Taggart, “Vulnerabilities in Internet of Things”, *BSc dissertation, School of Computing, University of Kent,* 2017.
- J.H. Ziegeldorf, O. G. Morchon, and K. Wehrle. “Privacy in the Internet of Things: Threats and Challenges”, *Security and Communication Networks*, 7(12):2728-2742, 2014.