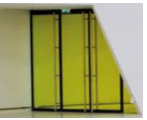
COCOON

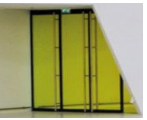
Emotion psychology meets cyber security in IoT smart homes

Antal Haans
Human-Technology Interaction group
Eindhoven University of Technology



The COCOON project

- Interdisciplinary project bridging cyber-security and emotion psychology
- Goals:
  - **Assess (perceptions of) risks** of Smart Home IoT
  - Offer a better **understanding of users' "emotional" responses to cyber-physical risks & attacks**
  - Explore pathways towards the development of novel intrusion detection systems by **recasting the user as an integral part of the system**



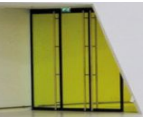
What do emotions entail?

- In the Cocoon project, emotions are regarded to be more than such experiences as anger, fear, disgust, pleasure, and the like

- Emotions instead are seen as a process including:
  - The appraisal of the situation at hand (Is it relevant, novel, pleasant / unpleasant?)
  - Motivational implications (Does it hamper or support my goals?)
  - Reasoning (Can I cope with the situation?)
  - As well as their joint effect of the individual bodily reactions and conscious experience

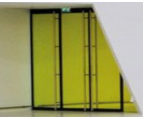
From understanding emotions to user-centered IDS

- When attacked:
  - How **could users notice** the attack (e.g., some irregularity in an IoT's functioning)?
  - **Would they detect** the irregularities in the behavior of their IoT?
  - To what would they **attribute** these irregularities (e.g., their own mistake, a system / network error, or an intentional attack)?
  - Would it **hamper their goals** (e.g., home as a safe haven)?
  - Would they become **scared** or **angry**? How would they **cope** with the situation?
  - How do **personal variables** (personality, attachment to the home) **moderate** these reactions?

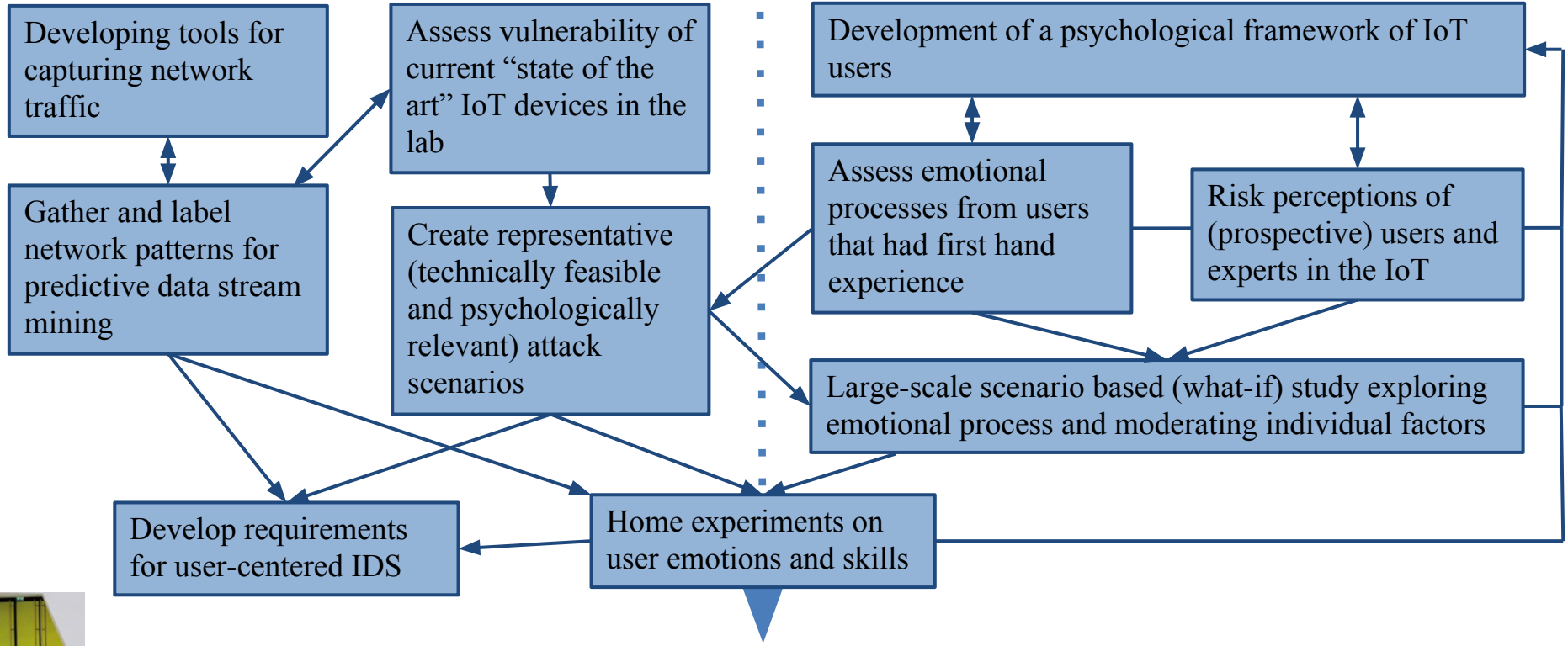


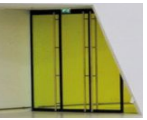
From understanding emotions to user-centered IDS

- Such insights are important for designing user-centered IDS as:
  - Different people will be differently equipped to be a part of the IDS
  - Different people may require different types of information from an IDS
  - Different people may have different levels of tolerances (e.g., with respect to the number of false positives)

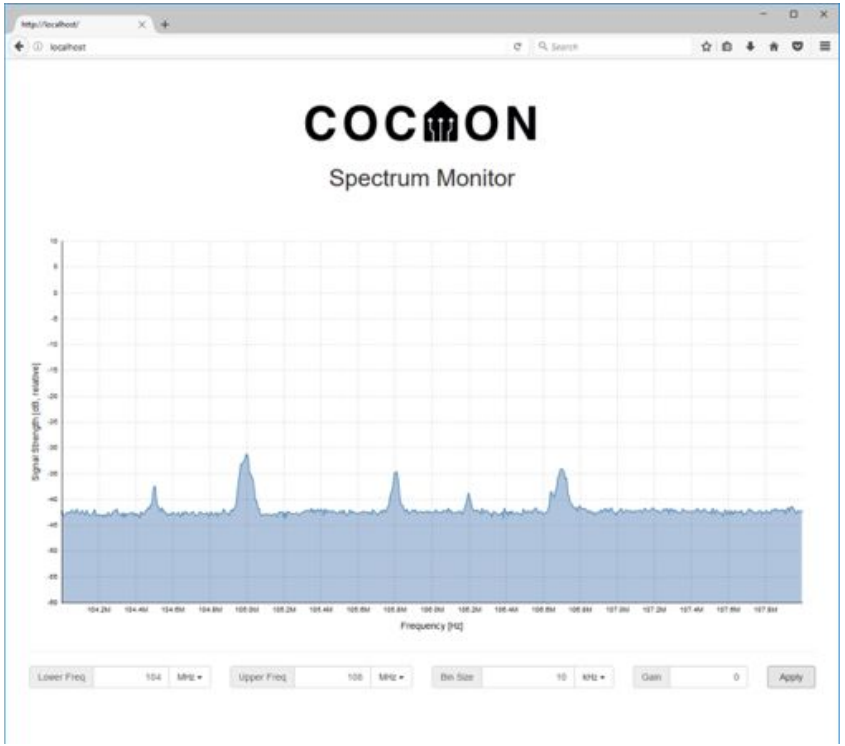


Project overview



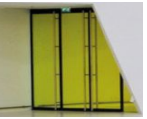


Tools for capturing network traffic



Lab experiments: Testing risks

- Assess vulnerability of current “state of the art” IoT device
- Cocoon staff already revealed two zero-day exploits in off-the-shelf IoT devices
- Gather and label network patterns for predictive network streaming



Lab experiments: Attack scenarios

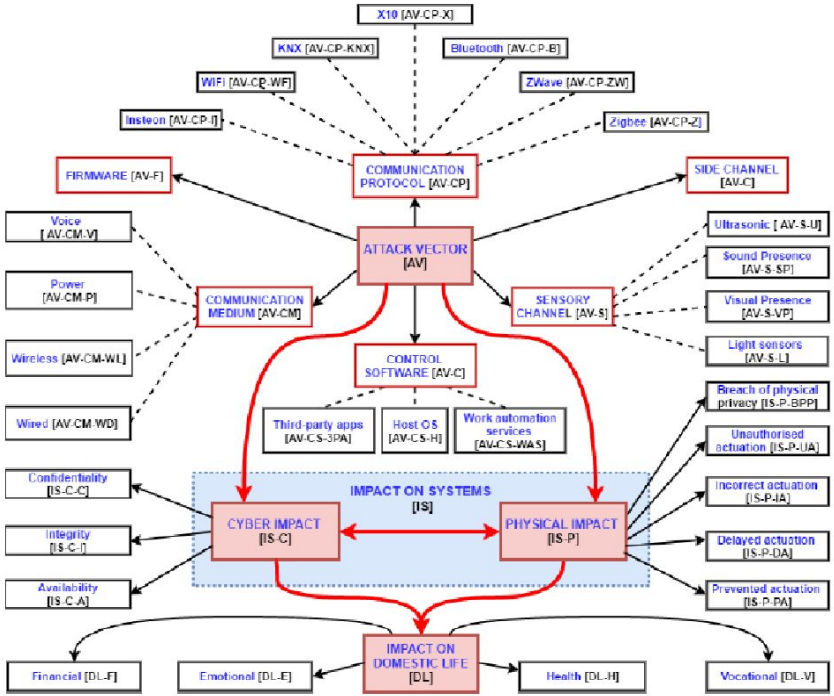
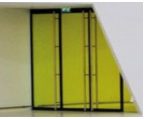


Figure 2: Smart Home cyber threat taxonomy topology (red line represents the linear relationship between attack vectors, their potential impact on systems in the smart home and resultant impact this may have on smart home users)

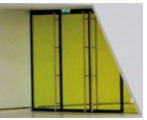


(Prospective) users' risk perceptions

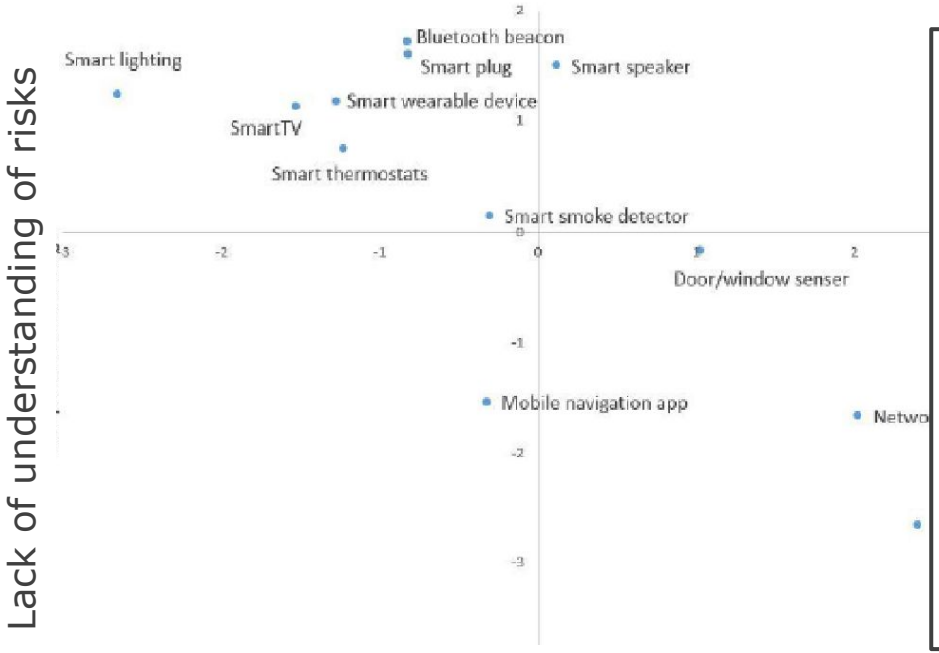
Table 6.2 Mean judgments of risk and benefit about 13 technologies

Technology	Perceived benefit	Perceived risk	Risk adjustment	Acceptable level
Online banking*	66	79		
Email over public network*	46	74		
Network camera	42	60		
Door/window sensor	32	44		
Smart speaker	24	43		
Smart smoke detector	53	36		
Smartphone navigation app*	60	35		
Smart plug	24	35	1.41	25

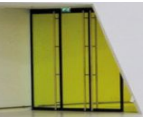
- Participant perceived risks (and benefits) of smart home IoTs to be lower then online banking or e-mailing over public network
- Are (prospective users) underestimating risks?



What determines risks? (disclaimer: preliminary findings)



- Lack of perceived understanding of IoT risks (**societal** and **amongst engineers**) was most predictive of risk perceptions!
- Are prospective users ignorant of the risks?

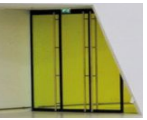


Need help with completing questionnaires!

- We seek **users** who have firsthand experience with IoT attacks (or related computer / smart phone hackings): https://ghentpmwop.eu.qualtrics.com/jfe/form/SV_b325lpiEKIQU93D

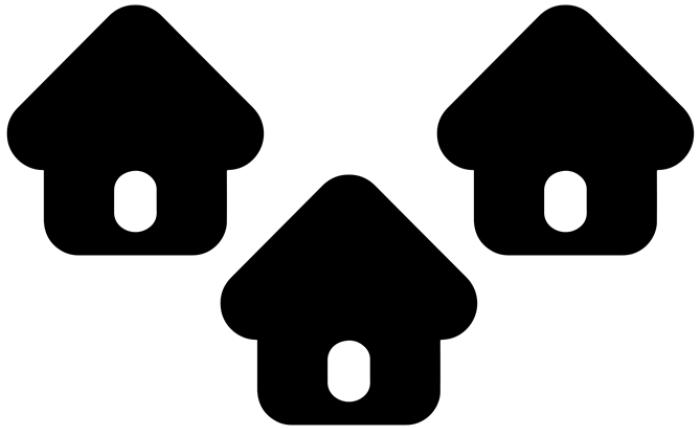
- We seek **cyber security experts** to complete survey on risk perceptions (to compare users and experts): http://www.antalhaans.nl/limesurvey/index.php/268481

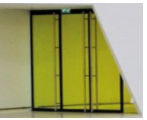
- More info: a.haans@tue.nl / www.cocoon-project.eu



Home experiments

- Later we will install a network of IoT devices in 20 households and will use a both qualitative and quantitative methods to:
  - Explore how residents **respond "emotionally" to irregularities** in the behavior of the network of IoT devices
  - Explore **how personal characteristics moderate** such responses
  - Explore the **feasibility of residents becoming "human sensors"** as part of a intrusion detection system





Wrapping up

- The Cocoon project bridges cyber-security and emotion psychology
- It aims to:
  - put mainstream IoT to the test
  - better understand users' emotional responses to cyber-physical risks & attacks, with the aim
  - to support the development of novel intrusion detection systems by recasting the user as an integral part of the system
- I have shown the ongoing and the future work that we feel is necessary to meet these aims
- **Question for discussion:** Where do you see opportunities for cyber-security and psychology to cooperate?