Dr. Etienne B. Roesch (Coordinator)
Associate Professor of Cognitive Science
University of Reading

EU FP7 CHIST-ERA 2017

The people of who do the work

The people who pay for it (thanks!)

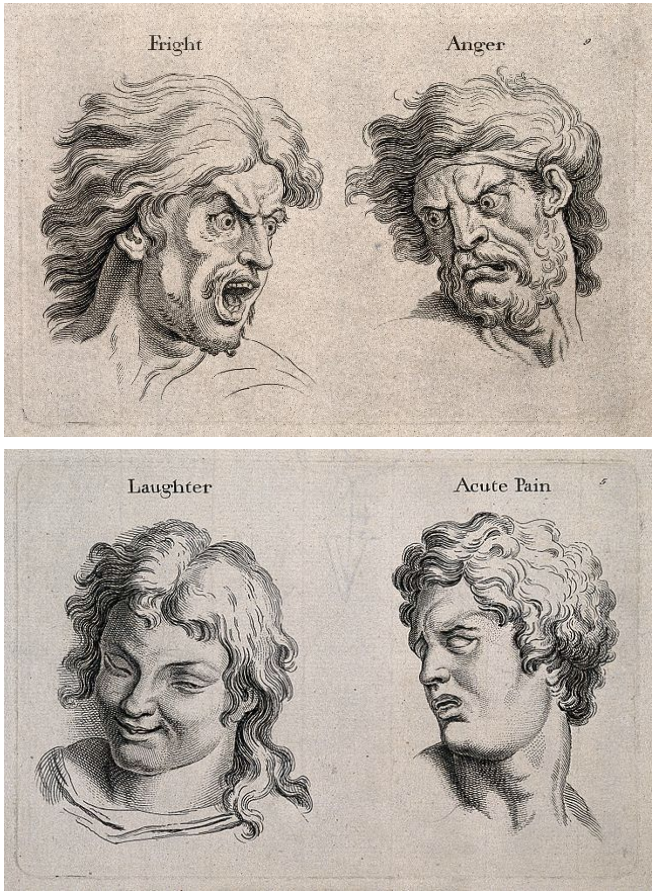
In Cocoon, we want to **understand** and **build** from the User's experience, as a central part in the definition of intrusion detection systems.

Home is a sacred, safe, warm haven.

A user's experience is **emotional** at its core. Anything that goes wrong, will go.. terribly wrong.

Emotions go beyond happy/sad.
They are cognitive **processes** that allow us to interpret the world and colour our lives.

- Appraisal of the situation
- Motivation, personality, goals
- Reasoning
- Expressed in a wide range ways



Top: A frightened, an angry face. **Bottom:** Faces of laughter and pain. Engraving, c. 1760, after C. Le Brun. Wellcome Images.

When a user's home is attacked...

Would users **notice** at all?

Would they **identify** the irregularities in the behavior of their IoT network?

To what would they **attribute** these irregularities?

Would it **hamper their goals**? Would home not be as a safe haven any more?

What emotions would they **experience**?

How would they **cope** with the situation?

How do **personal variables moderate** these reactions?

...

… can we use the User as an integral part to an Intrusion Detection System?

Different people will react differently

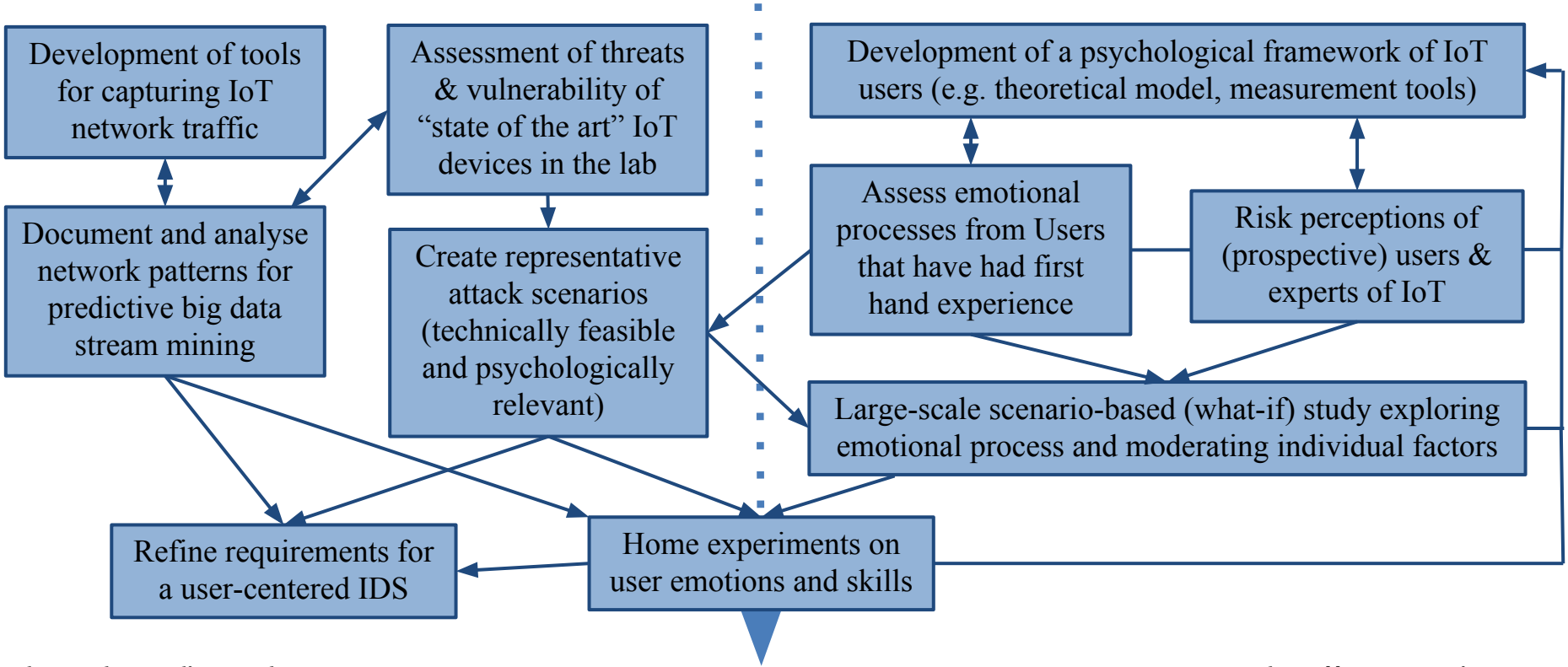
Different people will need different kinds of information

Different people will have different levels of tolerance

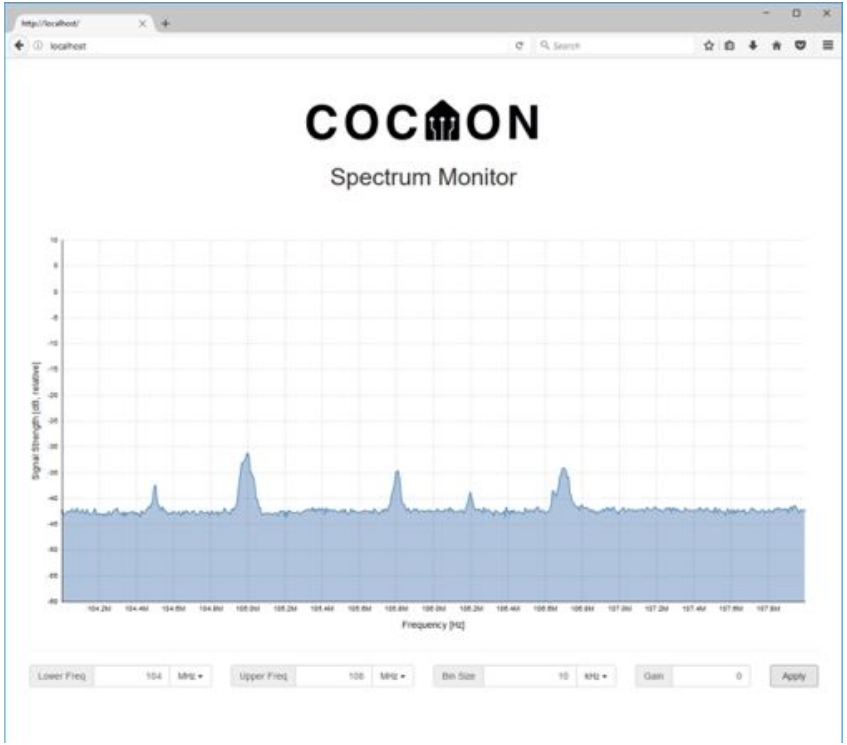
Objective 1 Examine the User's emotional experience

Objective 2 Put mainstream IoT to the test & develop a new kind of IDS

Cocoon's roadmap



The “Cocoon node” to capture IoT network traffic



“Lab” experiments: Assessment of threats

Assess vulnerability of current “state of the art” IoT devices

Gather and label network patterns

Cocoon staff already revealed two **zero-day exploits** in off-the-shelf IoT devices

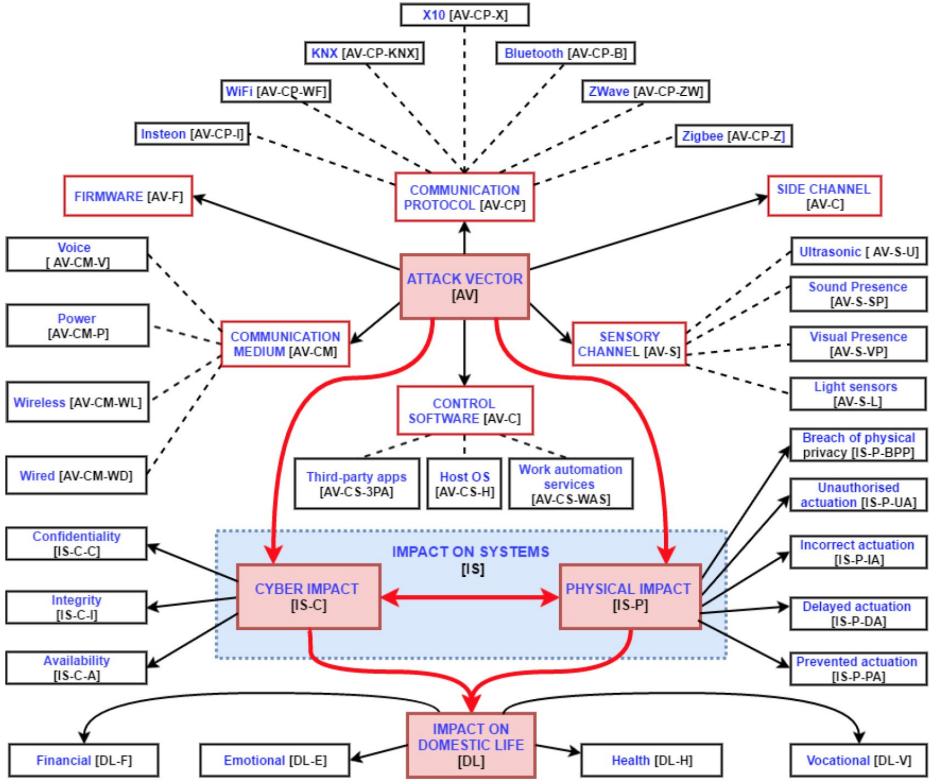
From the lab to realistic scenarios

Taxonomy of cyber threats

Benchmarking

Impact

- cyber (confidentiality, integrity, availability)
- physical (access, actuation)
- domestic life (emotional, financial, health)



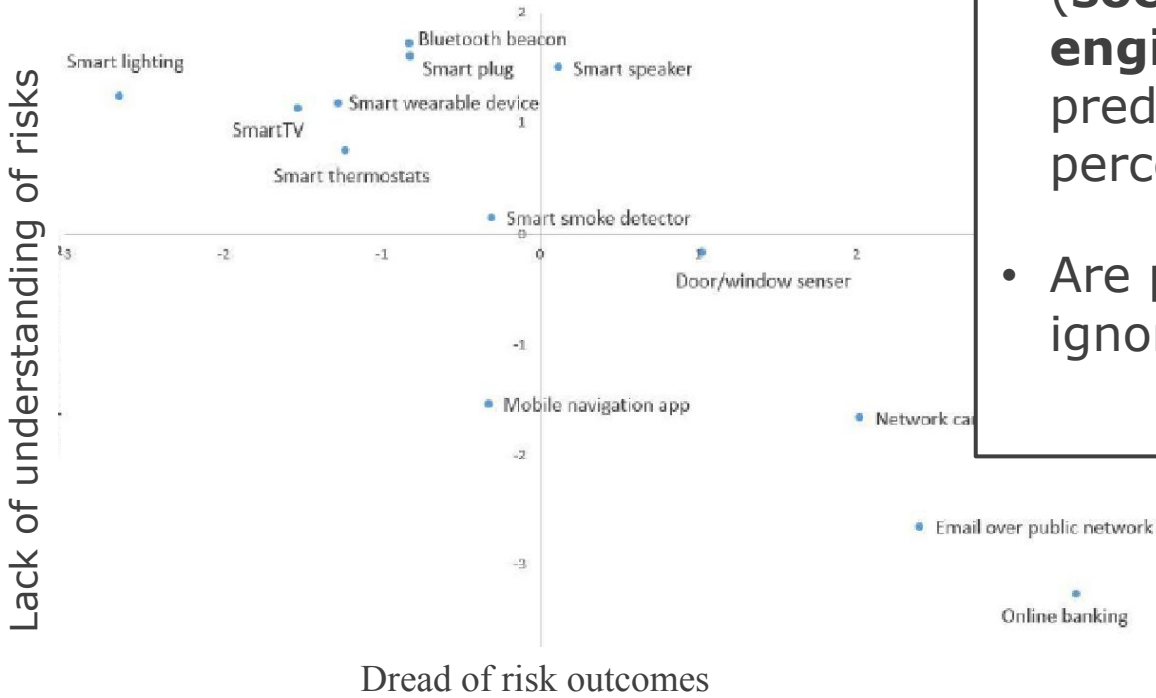
(Prospective) users don’t fully comprehend the risks

Table 6.2 Mean judgments of risk and benefit about 13 technologies

Technology	Perceived benefit	Perceived risk	Risk adjustment factor[a]	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		

- 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?



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

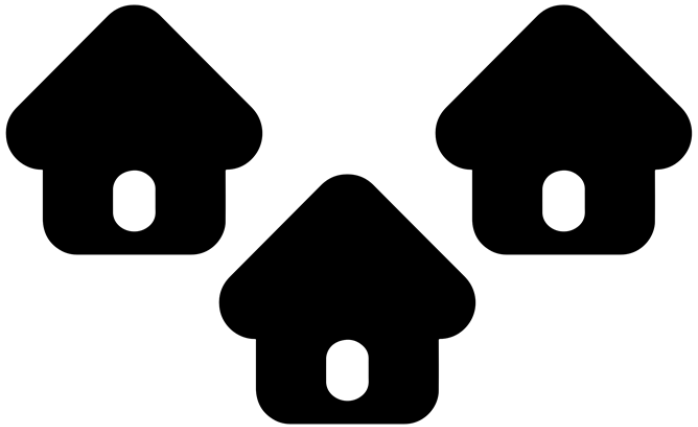
What’s next for Cocoon? The “Home” experiment

Volunteering households fitted with Cocoon IoT network of devices

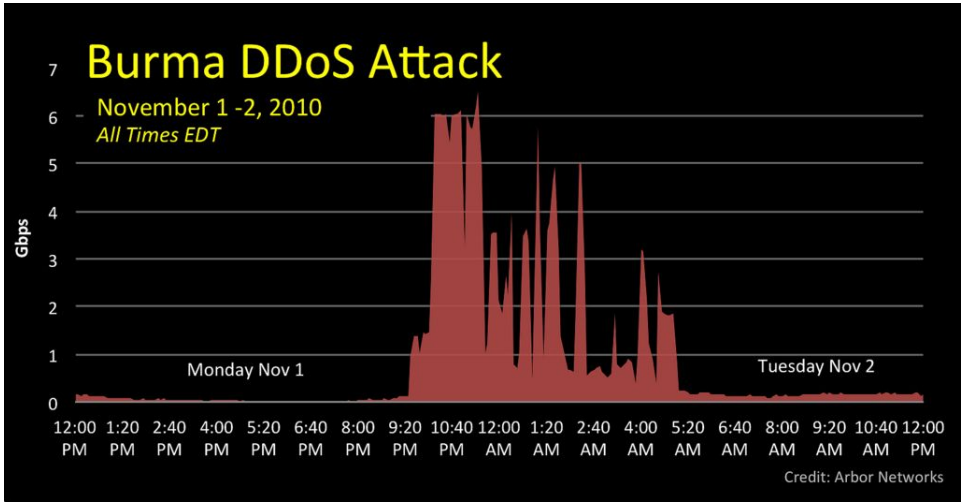
Simulated attacks (IFTTT, Stringify)

Diary & real-time probing

– How do users respond to irregularities?
– How do personal characteristics moderate such responses?
– **Users as sensors** of the health status of their IoT network?



What’s next for Cocoon? A network-wide IDS



Heterogeneous streams

Stream is infinite and cannot be stored easily

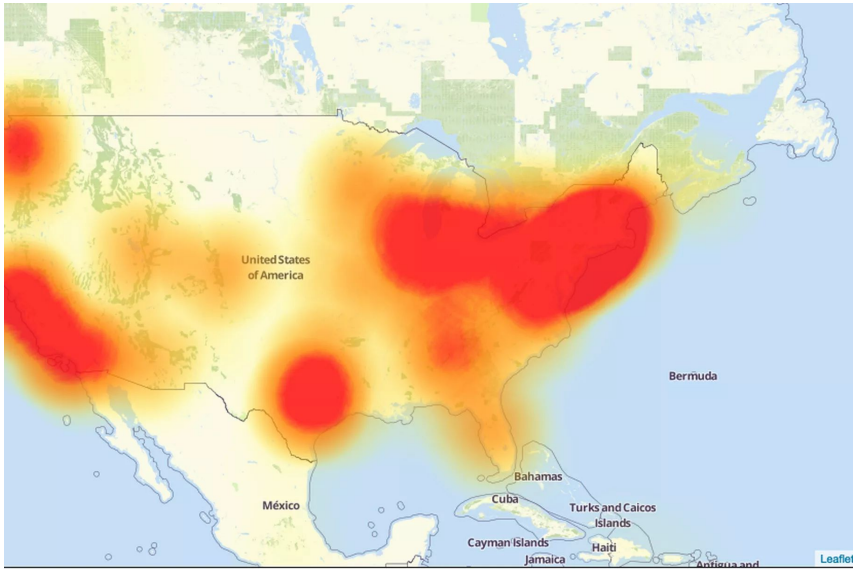
Stream is not easy to label and changing

Predictive data stream mining: Concept drifts, classification with sparse class labels

Dyn DDOS cyberattack, 16:45 UTC, 21 October 2016.

“Dyn disclosed that, according to business risk intelligence firm FlashPoint and Akamai Technologies, the attack was a botnet coordinated through a large number of Internet of Things-enabled (IoT) devices, including cameras, residential gateways, and baby monitors, that had been infected with Mirai malware.”

https://en.wikipedia.org/wiki/2016_Dyn_cyberattack



Cyber-threat real-time map (9/10/2017): https://cybermap.kaspersky.com/

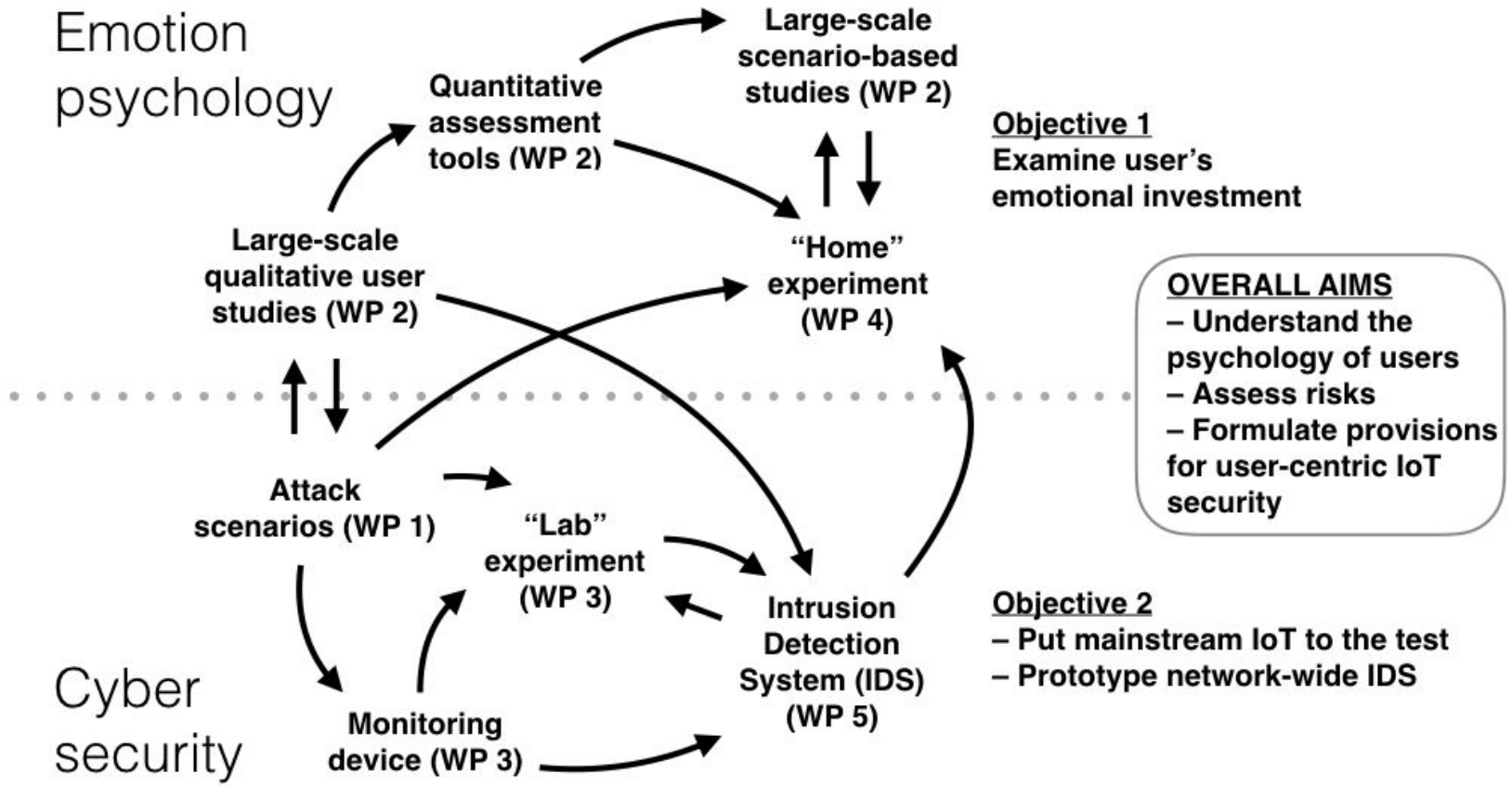
The future is not that gloomy: A successful and safe IoT strategy can only be based on how users interact with your system.

Thank you for your attention… and get involved!

1. **Come and say hi, and give me your email address.** We will..
    - .. keep you posted on what we do
    - .. provide opportunities to be involved in the research
    - .. talk about your particular situation
    - .. maybe engage on new research ideas?

2. Survey #1: Users with firsthand experience of hacking: http://bitly.com/cocoon-experience

3. Survey #2: Cyber-security experts about perceived risks: http://bitly.com/cocoon-risks


Emotion psychology
Quantitative assessment tools (WP 2)
Large-scale scenario-based studies (WP 2)
Objective 1
Examine user's emotional investment
Large-scale qualitative user studies (WP 2)
"Home" experiment (WP 4)
OVERALL AIMS
– Understand the psychology of users
– Assess risks
– Formulate provisions for user-centric IoT security
Attack scenarios (WP 1)
"Lab" experiment (WP 3)
Intrusion Detection System (IDS) (WP 5)
Objective 2
– Put mainstream IoT to the test
– Prototype network-wide IDS
Cyber security
Monitoring device (WP 3)