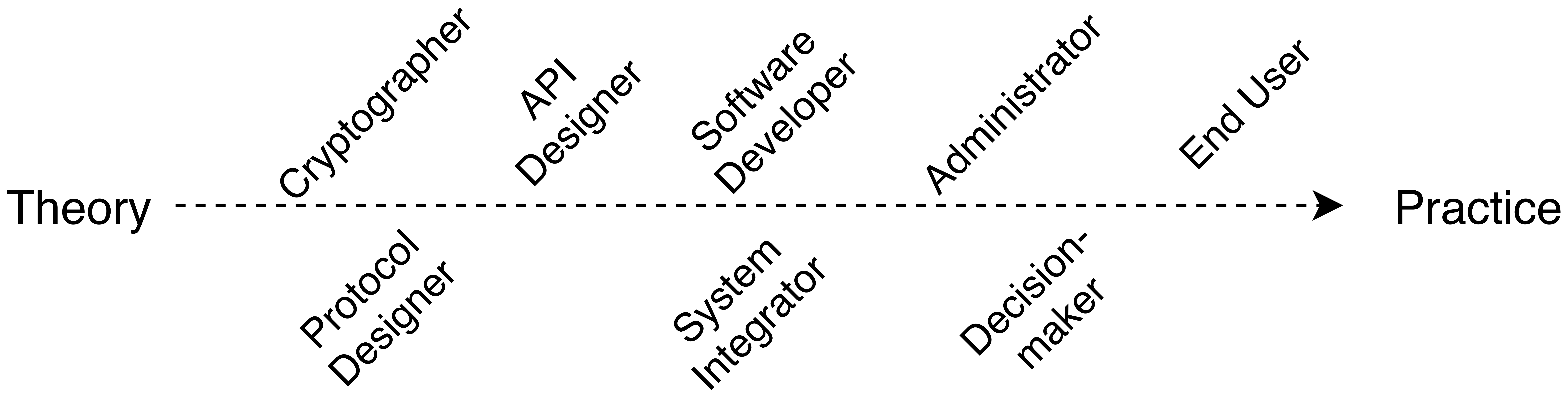
CISPA
HELMHOLTZ CENTER FOR
INFORMATION SECURITY

Mental Models of Cryptographic Protocols - Understanding Users to Improve Security

Katharina Krombholz
RWC 2021

Ultimately, all security vulnerabilities are caused by humans



Theory

Cryptographer

Protocol Designer

API Designer

Software Developer

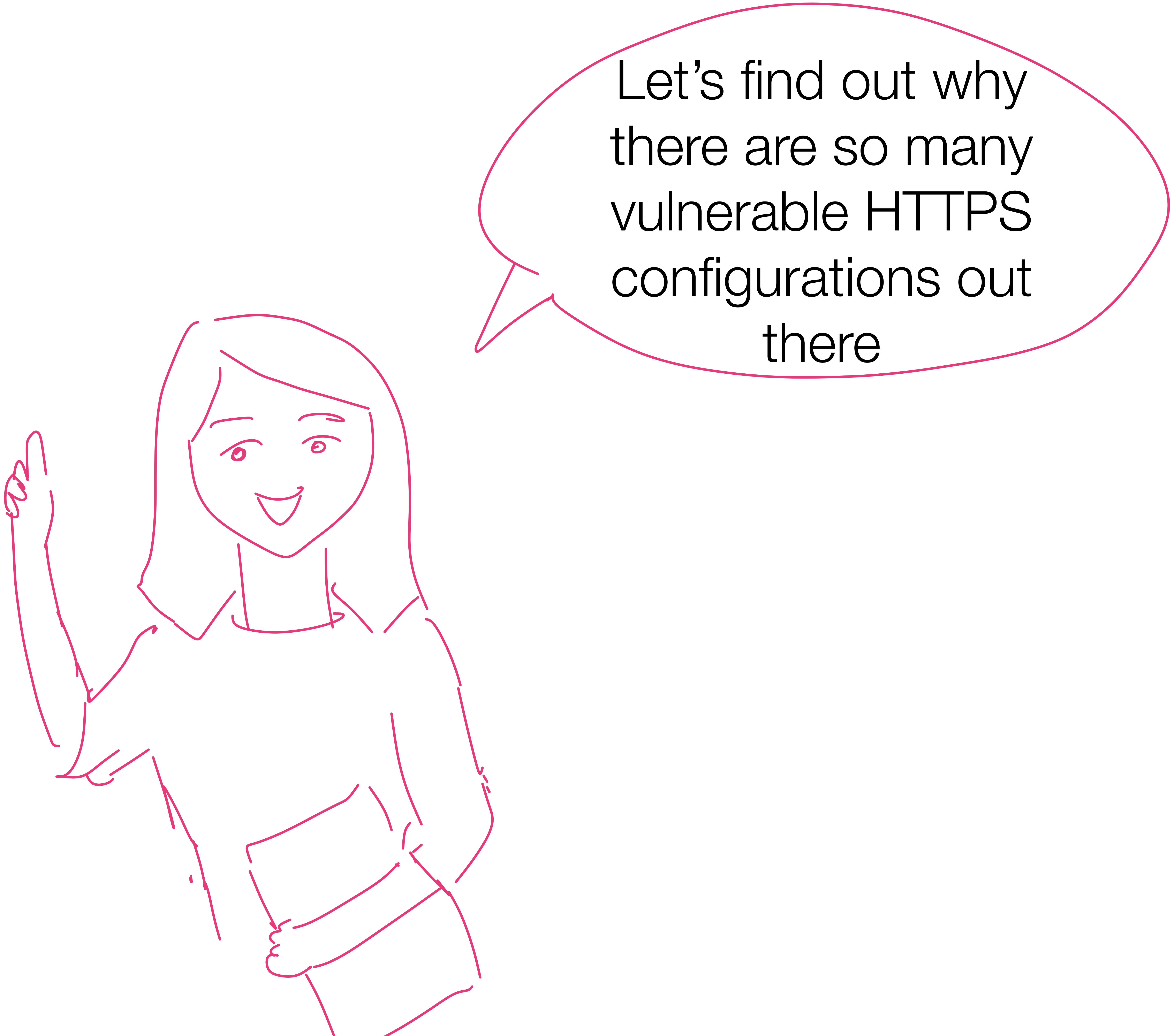
System Integrator

Administrator

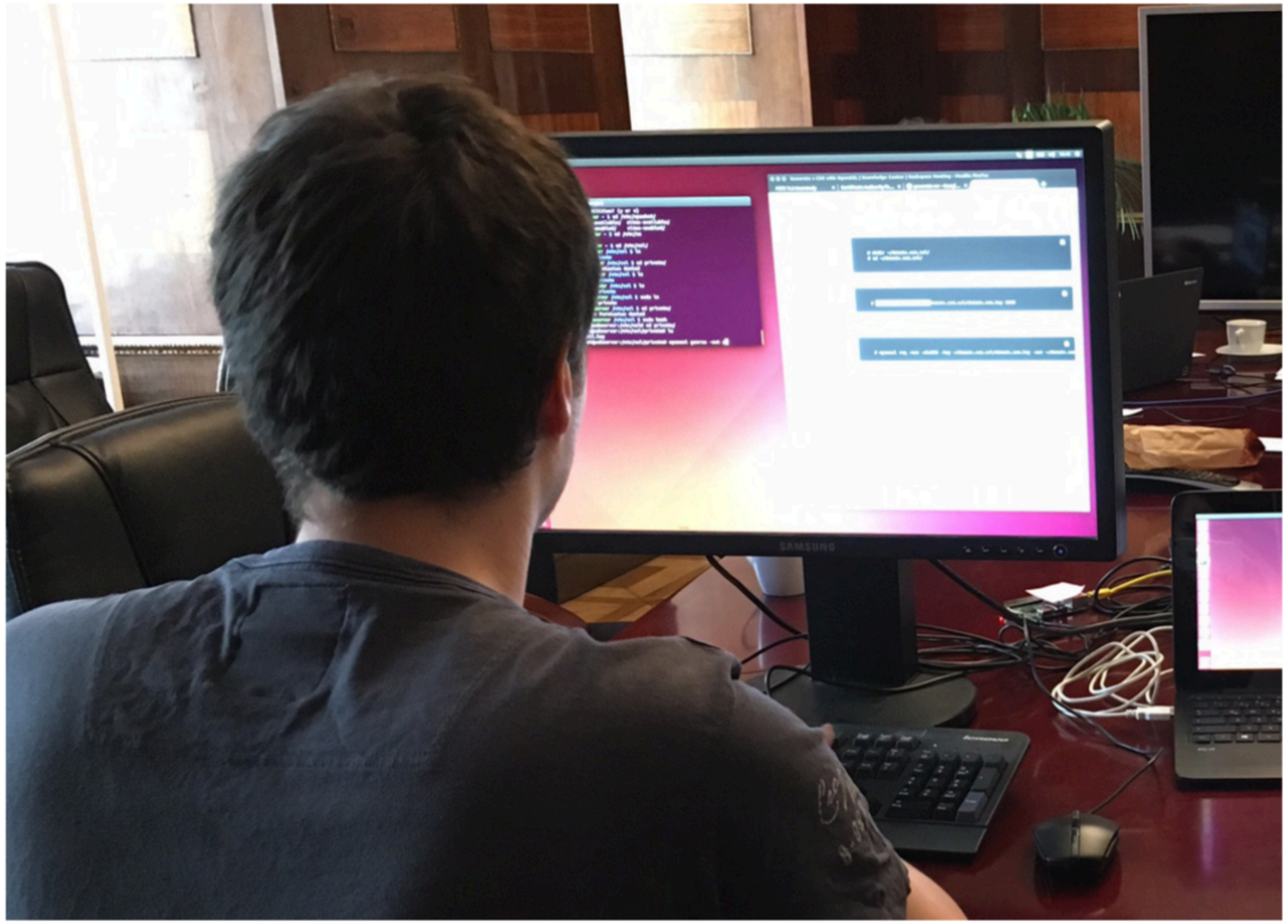
Decision-maker

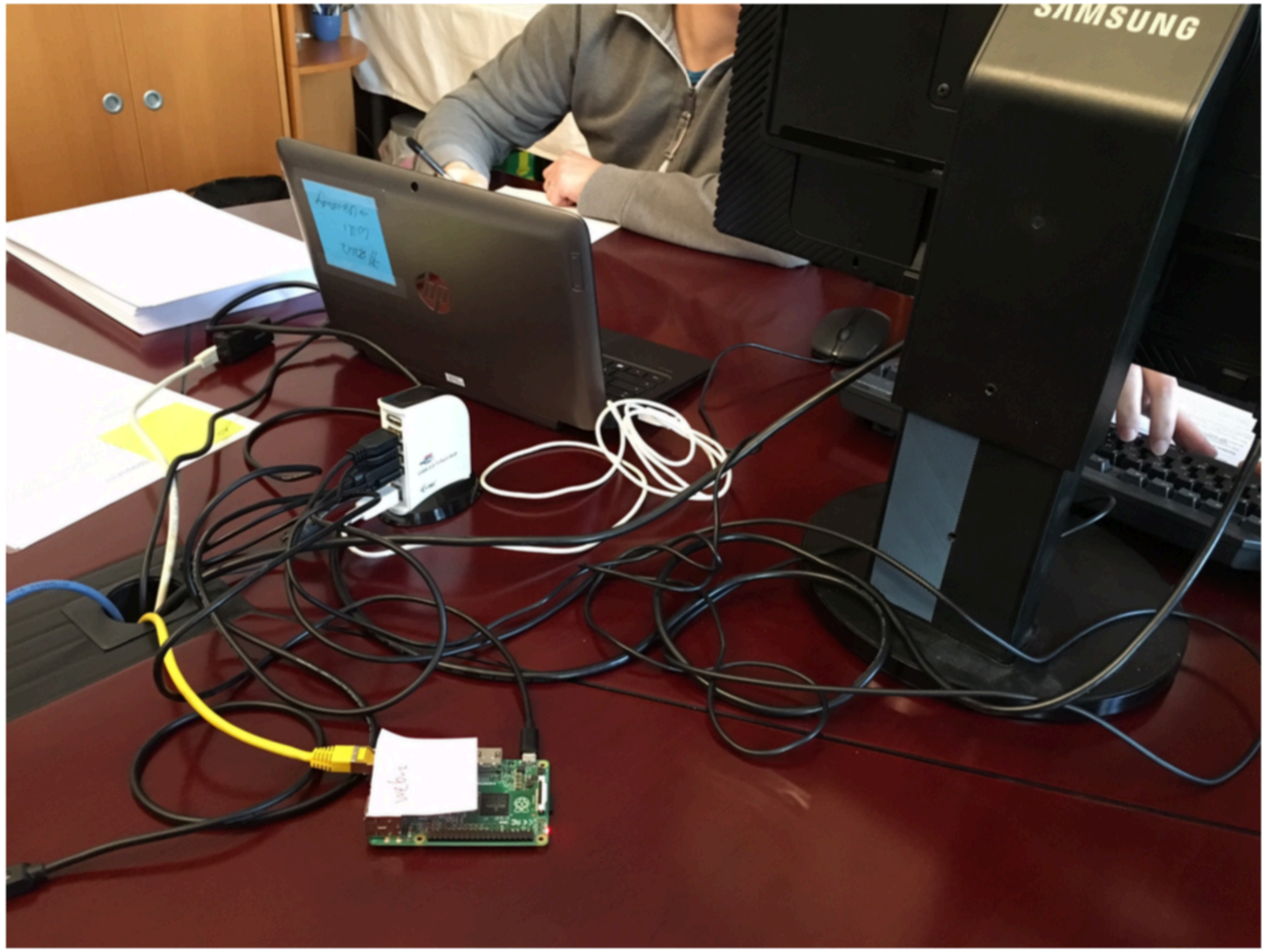
End User

Practice

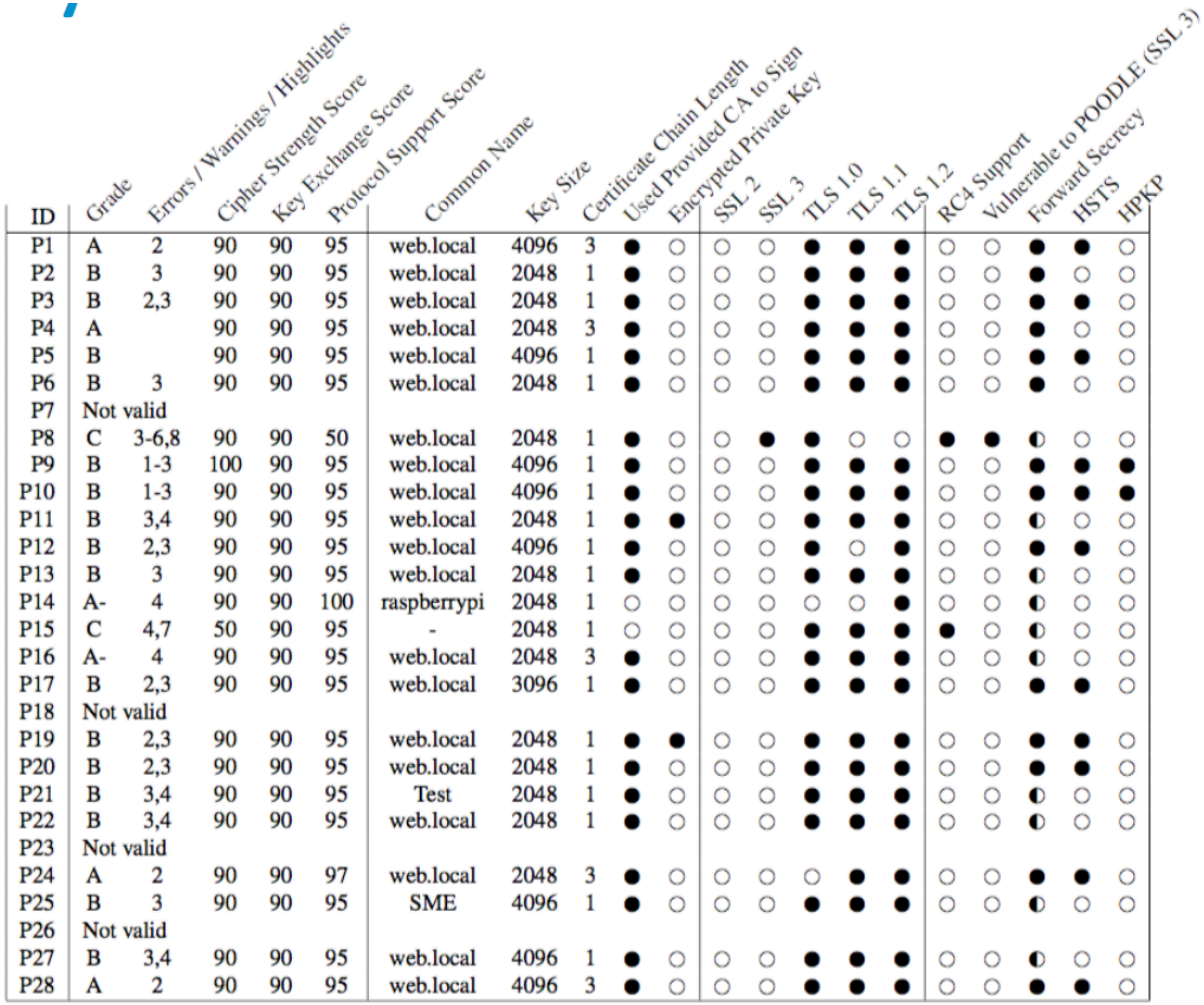

Let’s find out why there are so many vulnerable HTTPS configurations out there

An experiment on the usability of configuring HTTPS





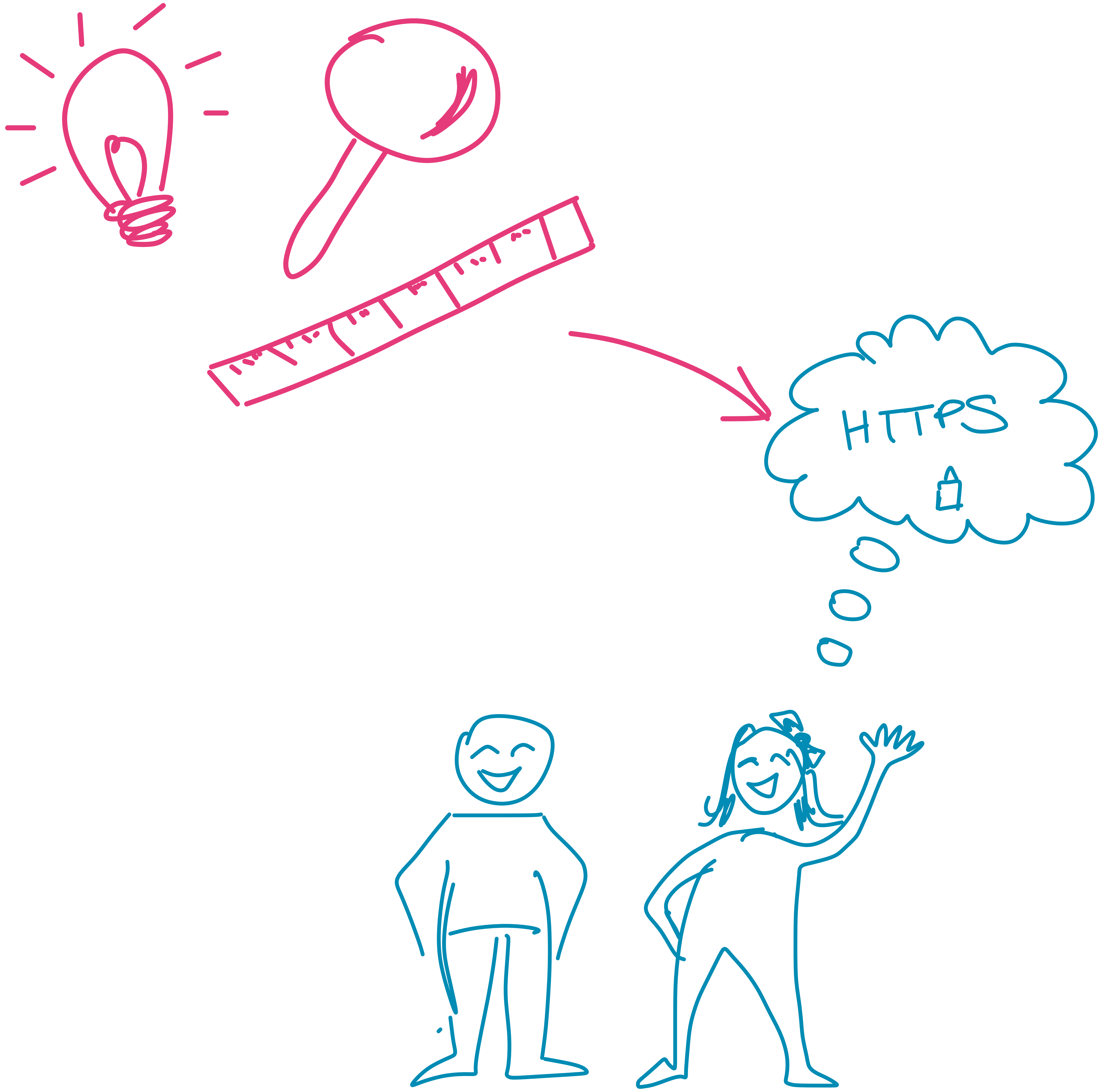
Why experimental data is not sufficient and qualitative data is essential



ID	Grade	Errors / Warnings / Highlights	Cipher Strength Score	Key Exchange Score	Protocol Support Score	Common Name	Key Size	Certificate Chain Length	Used Provided CA to Sign	Encrypted Private Key	SSL 2	SSL 3	TLS 1.0	TLS 1.1	TLS 1.2	RC4 Support	Vulnerable to POODLE (SSL 3)	Forward Secrecy	HSTS	HPKP
P1	A	2	90	90	95	web.local	4096	3	●	○	○	○	●	●	●	○	○	●	●	○
P2	B	3	90	90	95	web.local	2048	1	●	○	○	○	●	●	●	○	○	●	○	○
P3	B	2,3	90	90	95	web.local	2048	1	●	○	○	○	●	●	●	○	○	●	●	○
P4	A		90	90	95	web.local	2048	3	●	○	○	○	●	●	●	○	○	●	○	○
P5	B		90	90	95	web.local	4096	1	●	○	○	○	●	●	●	○	○	●	●	○
P6	B	3	90	90	95	web.local	2048	1	●	○	○	○	●	●	●	○	○	●	○	○
P7	Not valid																			
P8	C	3-6,8	90	90	50	web.local	2048	1	●	○	○	●	●	○	○	●	●	◐	○	○
P9	B	1-3	100	90	95	web.local	4096	1	●	○	○	○	●	●	●	○	○	●	●	●
P10	B	1-3	90	90	95	web.local	4096	1	●	○	○	○	●	●	●	○	○	●	●	●
P11	B	3,4	90	90	95	web.local	2048	1	●	●	○	○	●	●	●	○	○	◐	○	○
P12	B	2,3	90	90	95	web.local	4096	1	●	○	○	○	●	○	●	○	○	●	●	○
P13	B	3	90	90	95	web.local	2048	1	●	○	○	○	●	●	●	○	○	◐	○	○
P14	A-	4	90	90	100	raspberrypi	2048	1	○	○	○	○	○	○	●	○	○	◐	○	○
P15	C	4,7	50	90	95	-	2048	1	○	○	○	○	●	●	●	●	○	◐	○	○
P16	A-	4	90	90	95	web.local	2048	3	●	○	○	○	●	●	●	○	○	◐	○	○
P17	B	2,3	90	90	95	web.local	3096	1	●	○	○	○	●	●	●	○	○	●	●	○
P18	Not valid																			
P19	B	2,3	90	90	95	web.local	2048	1	●	●	○	○	●	●	●	○	○	●	●	○
P20	B	2,3	90	90	95	web.local	2048	1	●	○	○	○	●	●	●	○	○	●	●	○
P21	B	3,4	90	90	95	Test	2048	1	●	○	○	○	●	●	●	○	○	◐	○	○
P22	B	3,4	90	90	95	web.local	2048	1	●	○	○	○	●	●	●	○	○	◐	○	○
P23	Not valid																			
P24	A	2	90	90	97	web.local	2048	3	●	○	○	○	○	●	●	○	○	●	●	○
P25	B	3	90	90	95	SME	4096	1	●	○	○	○	●	●	●	○	○	◐	○	○
P26	Not valid																			
P27	B	3,4	90	90	95	web.local	4096	1	●	○	○	○	●	●	●	○	○	◐	○	○
P28	A	2	90	90	95	web.local	4096	3	●	○	○	○	●	●	●	○	○	●	●	○

- the most interesting findings were in the audio track
- administrators were incapable of making **informed security decisions**
- **misconceptions about protocol components**
- participant statements: “*I’m afraid of using crypto*“ and “*I have no idea what I’m actually doing*”

Understanding mental models of security tools and protocols



High-level findings of recent mental model studies

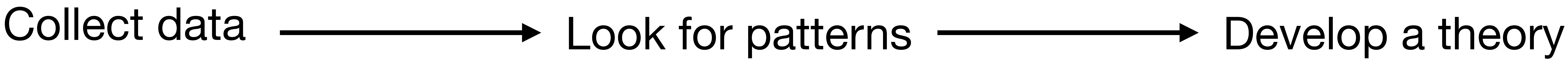
mental models of HTTPS (N=30)

- misconceptions of security benefits and protocol components
- distrust in security indicators
- confusion between encryption and authentication

Bitcoin/Etherium/cryptocurrencies (N=29)

- misconceptions about key management, anonymity and Bitcoin fees

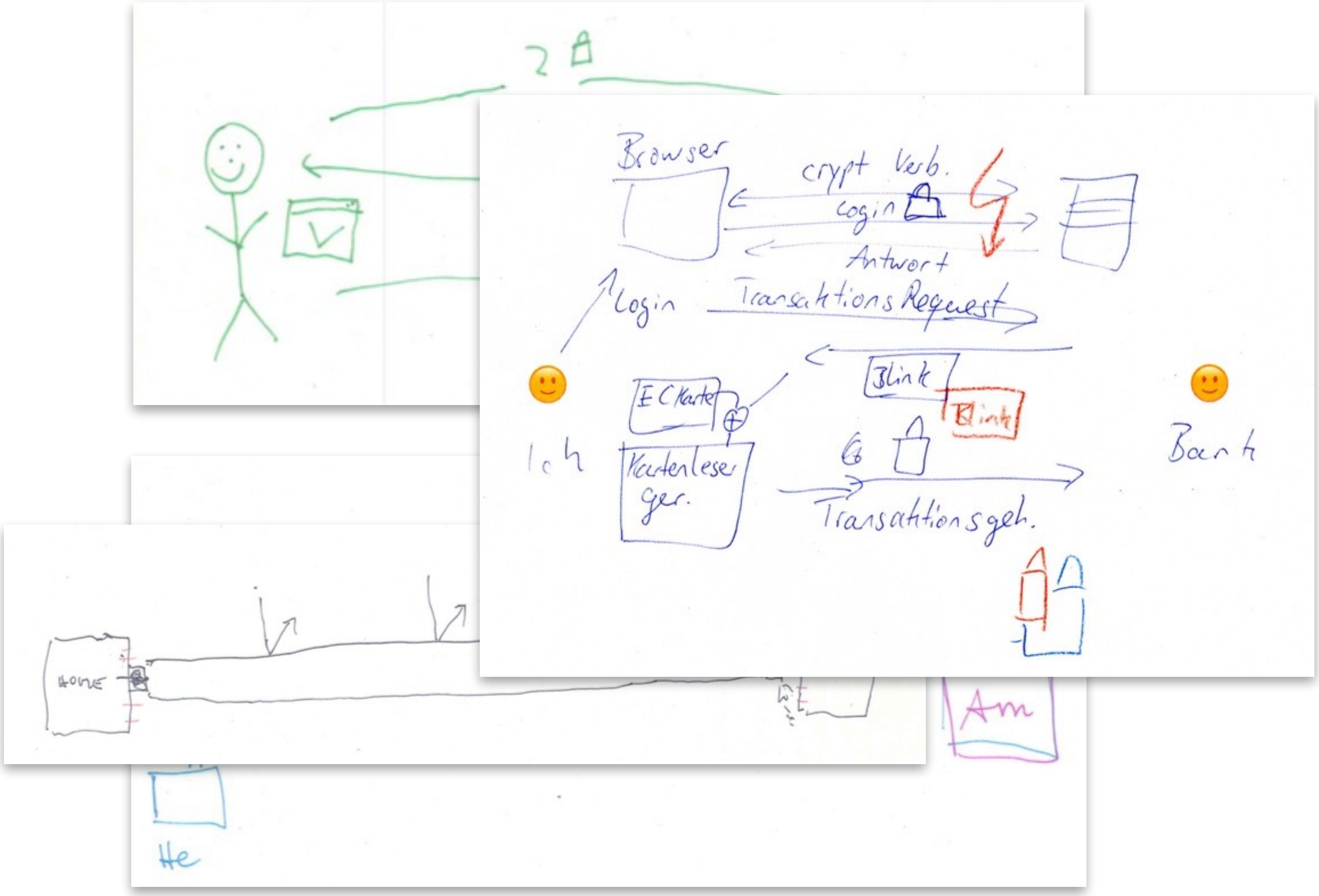
A methodological approach to elicit mental models

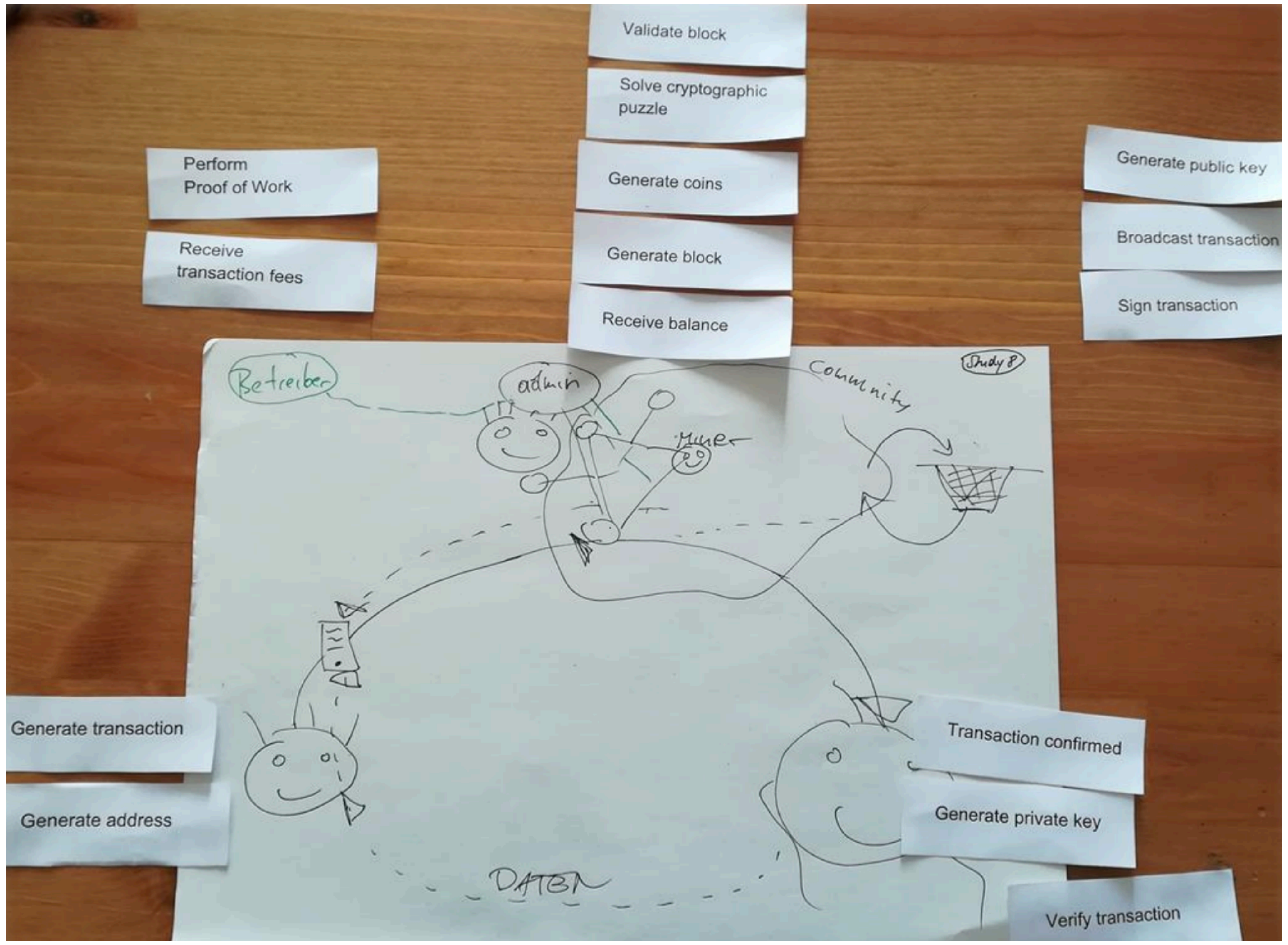


Collect data → Look for patterns → Develop a theory

A methodological approach to elicit mental models

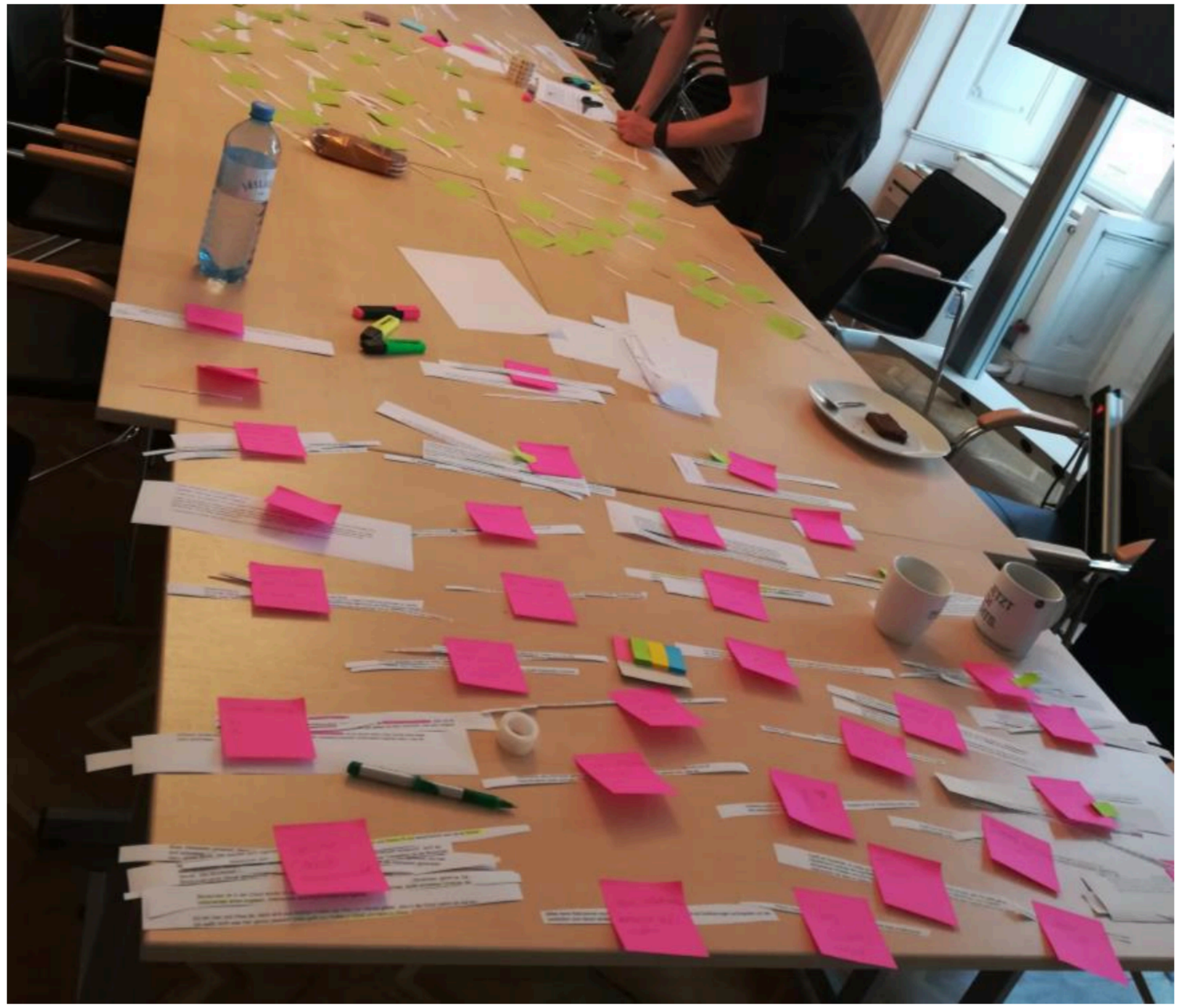
collection of qualitative data (interviews, observations, drawings, card-sorting tasks…)





A methodological approach to elicit mental models

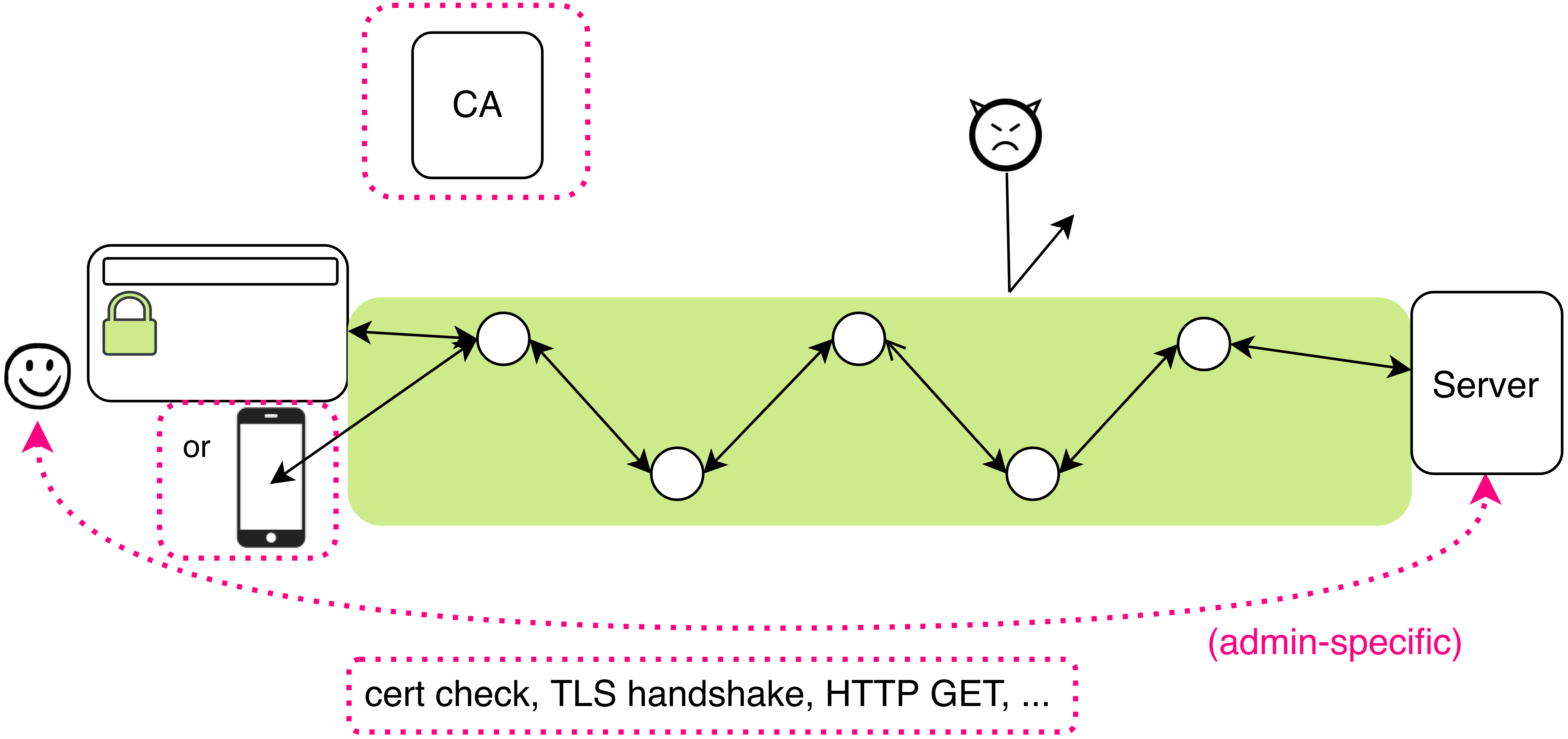
“coding” (process making ***unstructured*** data ***structured***)



goal: construct a **theory/model**

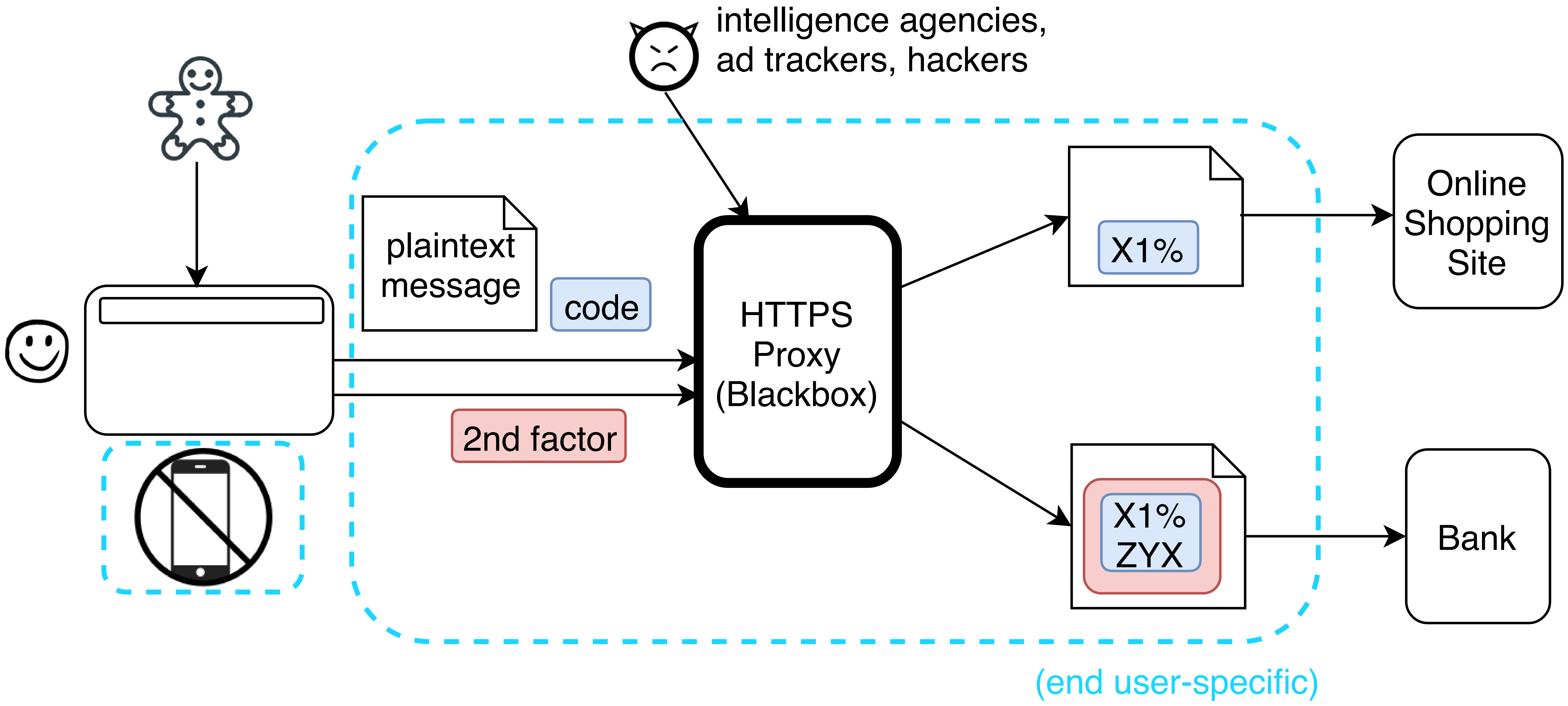
Example mental models

- the best case mental models of HTTPS



Example mental models

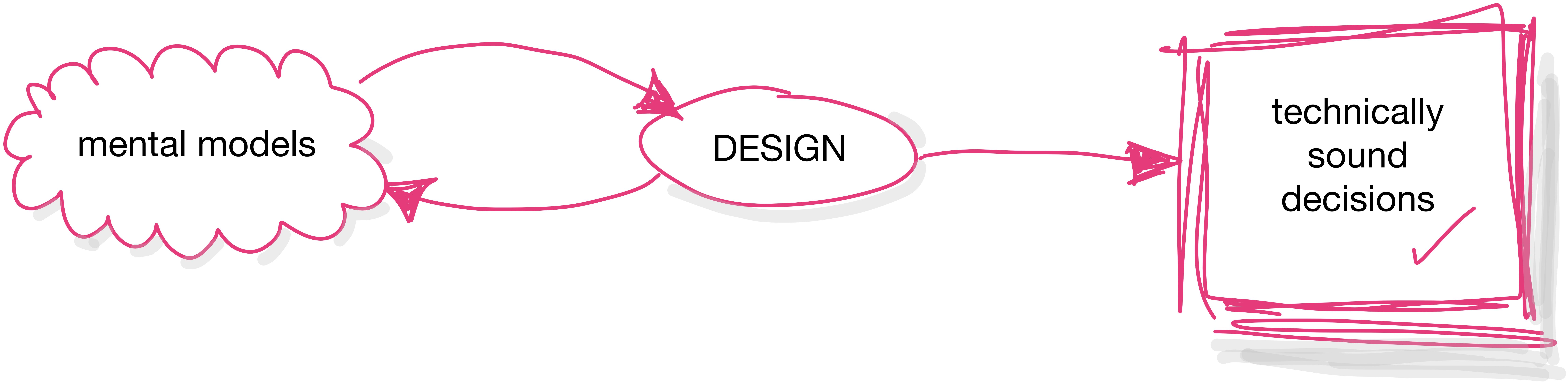
- the worst case mental model of HTTPS



Design and mental models

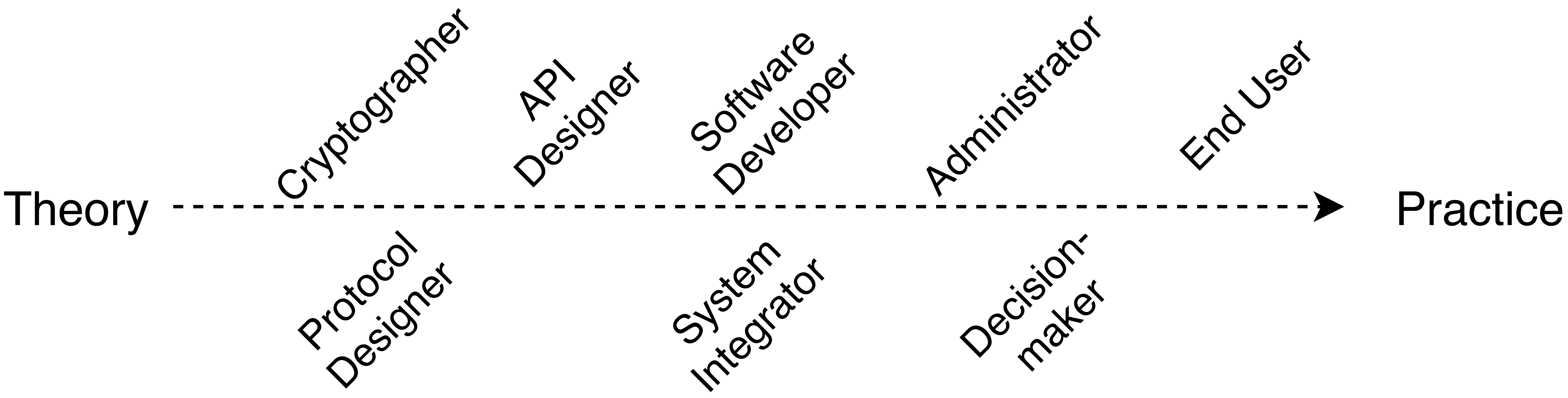
- In our HTTPS study, we found that **end user mental models are more conceptual while administrator mental models are more protocol-based.**
- In our cryptocurrency study **we discovered a tool bias.**

The interplay of design and mental models



- design informs mental models
- also **APIs, CLIs and metaphors shape mental models**

Ultimately, all security vulnerabilities are caused by humans



- we must **stop making implicit assumptions about users**, even if they are experts
- and design security technology that is better tied to their needs and values

Summary and references

- Empirical work can help to understand the users needs and inform the design of security technology
- All artifacts that users ineract with have an impact on user mental models and the users' decision-making

- Selected recent works:
  - Krombholz et al.,"If HTTPS Were Secure, I Wouldn't Need 2FA" - End User and Administrator Mental Models of HTTPS (IEEE S&P'19)
  - Mai et al., User Mental Models of Cryptocurrency Systems - A Grounded Theory Approach (SOUPS'20)
  - Fassl et al., Exploring User-Centered Security Design for Usable Authentication Ceremonies (CHI'21)