



Responsibility and Tangible Security: **Towards a Theory of User Acceptance** **of Security Tokens**

Payne, Jenkinson, Stajano, Sasse, & Spencer

pico

Pico Team

Current Members:

- **Frank Stajano (Principal Investigator)**
- David Llewellyn-Jones (Research Associate)

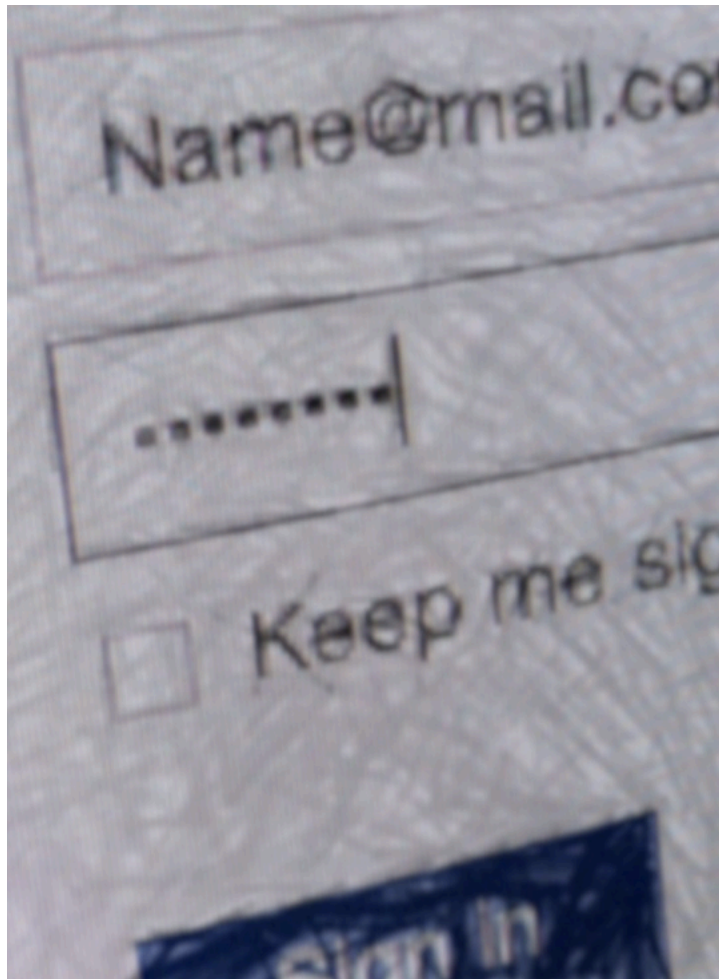
Past Members:

- Chris Warrington (now with Google)
- Quentin Safford-Fraser (now on the Endeavour Project at University of Cambridge the Computer Lab)
- Max Spencer (now at the Guardian)
- Jeunese Payne (now at Africa's Voices)
- Graeme Jenkinson (now on the CADETS project at the University of Cambridge Computer Lab)

Agenda

- **Passwords**
- **Background to Pico**
- **Approach**
- **Analysis**
- **The Grounded Theory**
- **Conclusions**

Passwords



- Coping strategies (reusing, storing, etc.)
- Alternative password types (passphrases, graphical passwords, etc.)
- Password managers
- FIDO
- Two-factor authentication
- Purely token-based schemes

Agenda

- Passwords
- Background to Pico
- Approach
- Analysis
- The Grounded Theory
- Conclusions

Pico (Stajano, 2011)

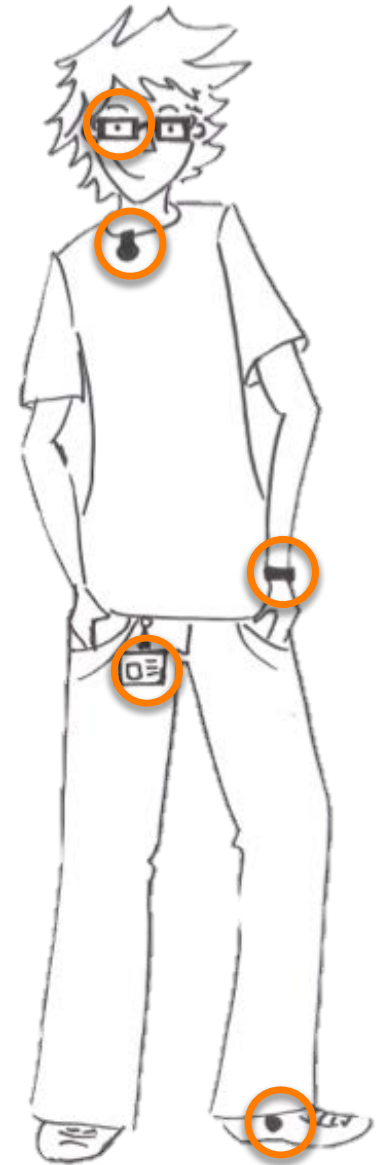
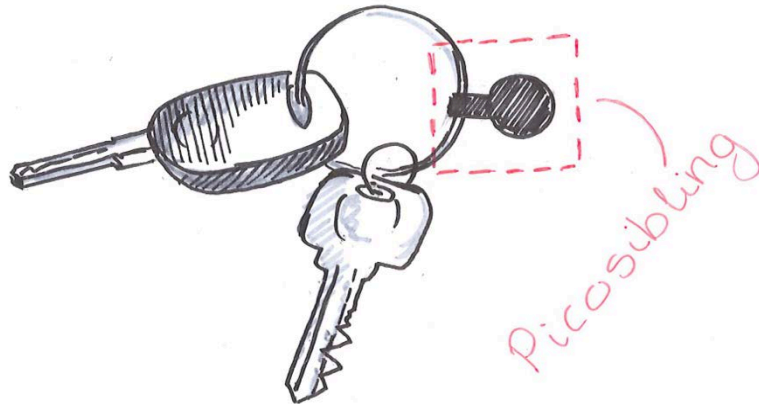
Pico = Small, dedicated device; ~~Passwords~~ → Scan a QR code

Usability benefits: Memory, Effort, Scalability

Security benefits: Continuous authentication; Resistant to guessing, phishing, and key-logging; **Theft-resistant**



Picosiblings



- It locks itself!
- Detects how close it is to its **Picosiblings**
- Smaller devices you carry with you
- Collection → only need some

What explains the acceptability of a token-based authentication mechanism, such as Pico?

Agenda

- Passwords
- Background to Pico
- Approach
- Analysis
- Results
- Conclusions

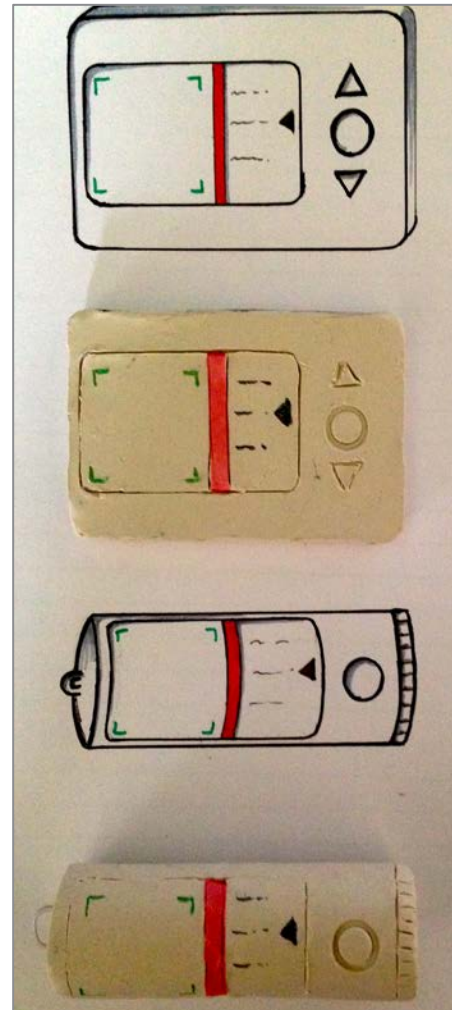
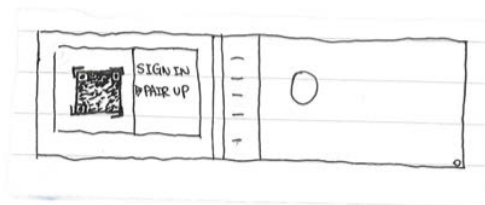
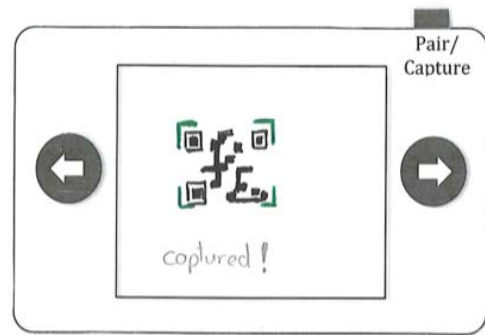
Approach: Overview

Data obtained from **semi-structured interviews** in which participants interacted with low-fidelity prototypes

Data analysed using **Grounded Theory** (Glaser & Strauss, 1967; Strauss & Corbin, 1998)

Approach: Low Fidelity Prototypes (1)

- a. Paper designs
- b. Re-design
- c. Plasticine
- d. Polymorph



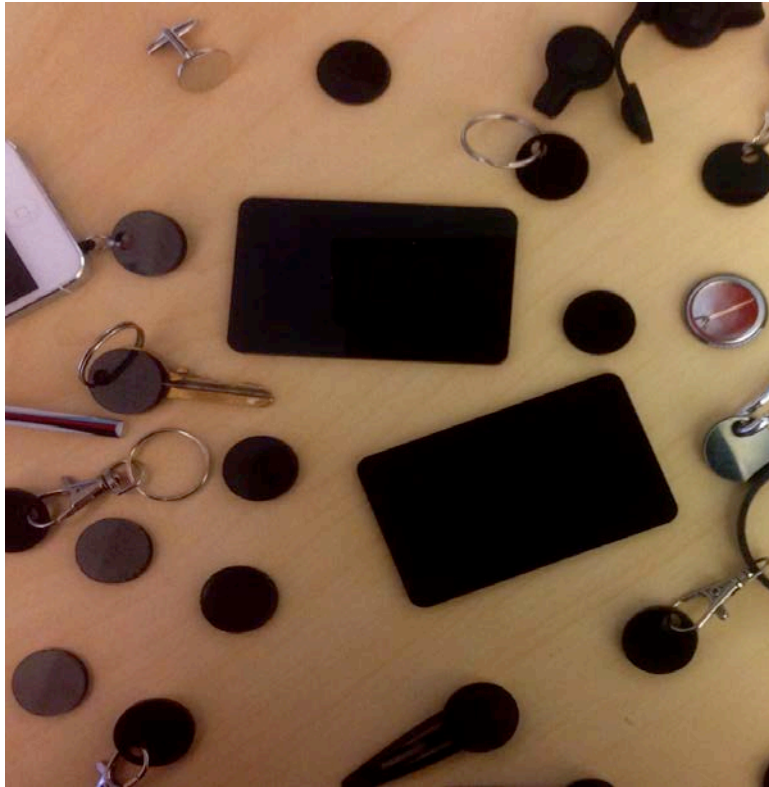
Students involved:

T. Brouwer, K. Phatpanichot,
R. Dorrity, G. Liang, J. Luo,
E. J. Kay-Coles

Approach: Low Fidelity Prototypes (2)

**Pilot Study of Picosiblings:
Everyday and makeshift items**

**Main Interview Study: Uniform
items and more options**



Approach: Semi-Structured Interviews



- **Pilot** Phase: Open and axial coding of first 6 interviews
- **Main** Phase: Open, axial, and selective coding of 16 interviews
- **Expanding**: Testing the fit of the data in the final model from an additional 4 interviews → **20 interviews**

Approach: Participants

The range (count and percentages) of participant occupations

	Count (Percentage)
Accounting (female)	1 (5%)
Engineering (male)	1 (5%)
Military (male)	1 (5%)
Admin/Clerical (male)	1 (5%)
Publishing (female)	1 (5%)
Translating (female)	1 (5%)
Software Developer (male)	1 (5%)
Homemaker (female)	1 (5%)
Unemployed:	
Software Engineer (male)	1 (5%)
Product Designer (female)	1 (5%)
Research:	
Physics (male)	1 (5%)
Neuronal development (male)	1 (5%)
Cancer (female)	1 (5%)
No Occupation given (female)	1 (5%)
Student (undisclosed subject) (male)	1 (5%)
Education (teaching assistant) (1 male, 1 female)	2 (10%)
Post-grad student:	
Sustainable Energy (female)	1 (5%)
Computer Science (1 male; 1 female)	2 (10%)

Gender:

10 male, 10 female

Age:

20-57 years

(mean = 30.5)

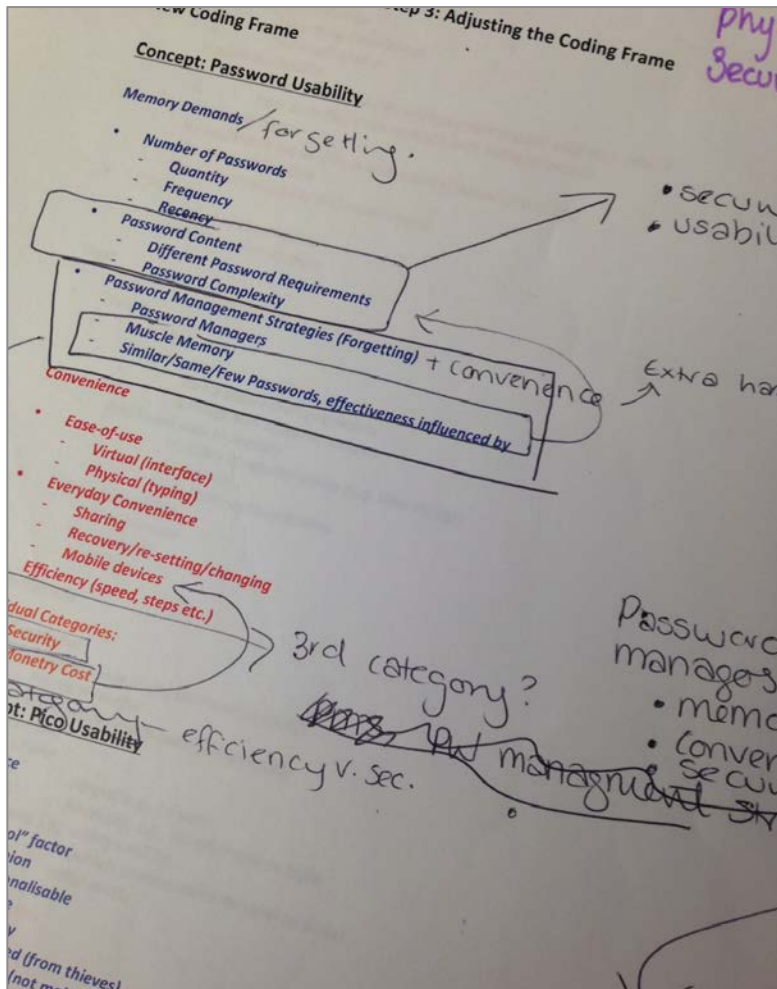
Occupation:

See table

Agenda

- Passwords
- Background to Pico
- Approach
- **Analysis**
- **The Grounded Theory**
- **Conclusions**

Open Coding

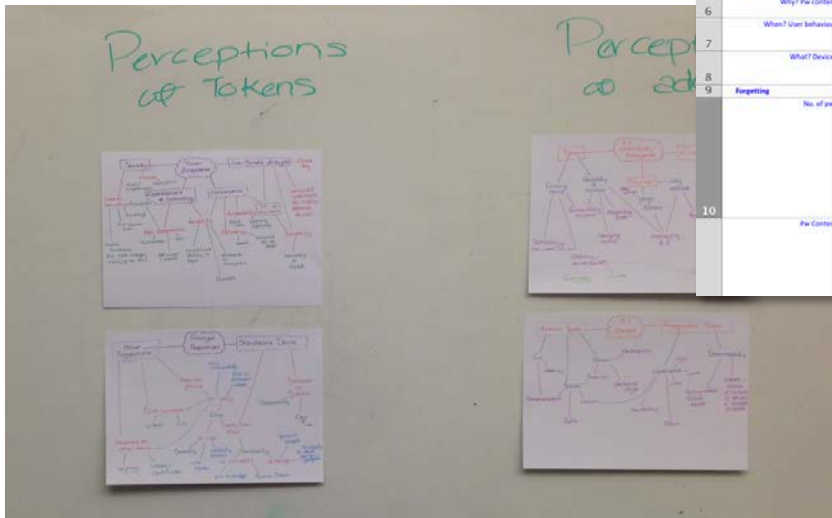


Reducing the data into codes

- Trial open-coding (interviews 1-6):
 - Double-coding
 - Blind-coding)
- Open-coding proper (interviews 1-16):
 - “Memoing”
 - Developing a coding frame

Axial Coding

Grouping codes into conceptual categories that reflect relationships



1	2	3	4	5	6	7	8	9	10
Concept/Password Usability Category Label (the phenomenon)	Description	Properties (the context in which the phenomena are embedded)	Dimensions (metrical or categorical values)	Examples					
Password Policy/Complexity (Security Requirements)				"I find them [passwords] a bit of a nightmare to be fair, to be quite honest, many different passwords, and obviously there's so many different to access or, you know, use frequently, and it does become quite a pain and up writing them down somewhere obvious and it obviously the subject doesn't like it." "Some do insist on a mixture don't they? Again, it					
Typing	Password entry errors due to typing inaccuracy			"I honestly mistype my password at work 20 times a day because it's very long."					
Why? Pw context	The impact of content of passwords on the ability to type them	1. Characters; 2. Length	1. (M) level of complexity; 2. (M) short-long	"... half the time I don't even remember the characters in my password my fingers go, and I have to actually pretend I've got a keyboard in front of me just not forgetting. The reason I mistype is because I'm typing					
When? User behaviour	The impact of user abilities to type passwords accurately and with efficiency	Speed of typing	1. (M) slow-fast; 2. (C) yes-no	"I don't really log into things on my phone and I guess typing it, like, time and the password everytime..." see comment above about how keyboard is above of the user;					
What? Devices	The impact of particular devices on the ability to type passwords	1. mobile devices; 2. traditional keyboards (muscle memory)	1. (C) issue with typing? Yes/No 2. reliance on muscle memory? Yes/No	"I'm useless at remembering passwords";					
Forgetting	Difficulty remembering passwords			"I hate the fact that you have so many passwords that you have to store online and buy anything from any website without registering for it up a password for the website"; "I have a number of accounts it's so I really used a strong password for everything. And if something you have to change your password"; "Yeah, we stick to two password same one..."; "I always use the same password. Probably sometimes number"; "Problematic... because I have 3 or 4 different passwords"; using pw in] On the whole, okay, because they tend to be quite complicated very good at remembering passwords. I don't know, maybe that's better"; "I have a different password for different things but they're longer and I find it harder to remember them all";					
No. of pws	The issues associated with the number of unique passwords users are asked to remember	1. Few pws; 2. Proliferation of accounts and pws; 3. Pw uniqueness	All (C) 1. Yes/No; 2. Problem? Yes/No; 3. Same -> Similar -> Unique	"When they need special characters it's a bit difficult to remember, characters... Lower case letters and numbers are okay"; "I guess it's you've got more restrictions in that password"; "I've got all these passwords now to try and make them secure, like 'Must contain upper characters, numbers...' - all like that"; "I know that you have to use numbers, and capital letters"; "And they all have different criteria of have different passwords"; "Different criteria [are the main] problem"					
Pw context	The issues associated with the unique passwords users are asked to create and remember	1. Pw requirements; 2. Policy inconsistency							

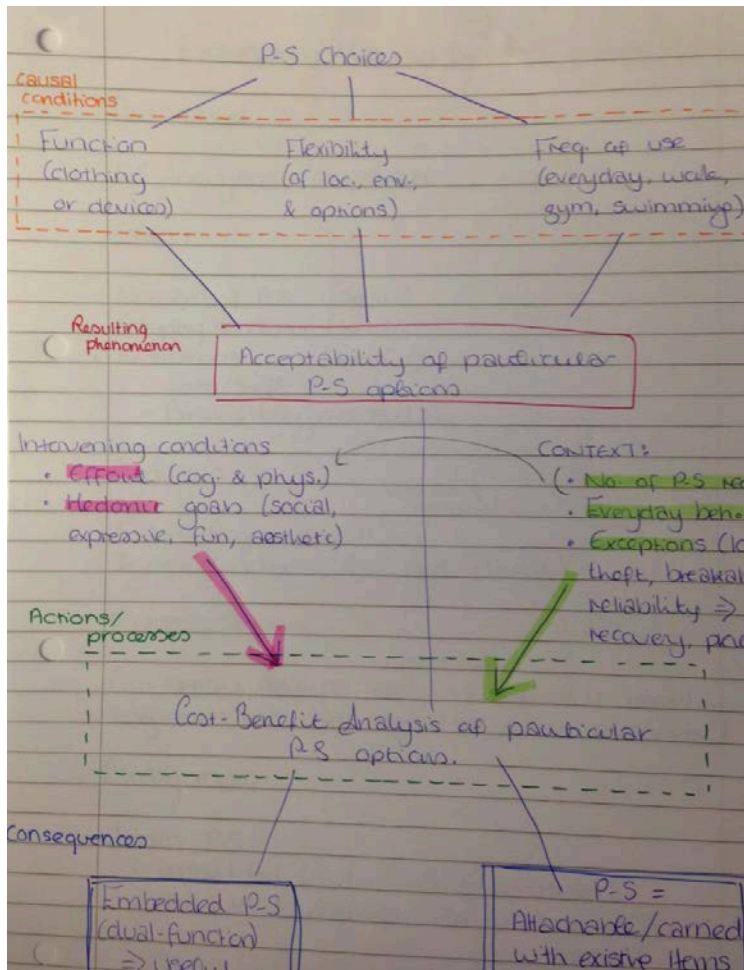
Axial Coding: Pico Token

Convenience	Prototype Preferences	Trustworthiness
1. Efficiency (effort & time)	1. Familiarity (of concept & design)	1. Reliability (uninterrupted use)
2. Deployment (widely adopted)	2. Easy to carry, hold, and use (shape, size, & button functions)	2. Security (misuse, loss, & theft)
3. Something to carry (vs. dual-purpose or app)		

Axial Coding: Picosiblings

Hedonic Concerns	Utilitarian Concerns	Routine Use
1. Self-presentation (personal style)	1. Dual-purpose (e.g. a watch)	1. Day-to-day (fixed or frequent)
2. Personalisation (novelty, fun, & creativity)	2. Practical Convenience (e.g. a key-ring)	2. Exceptions (loss & theft)
	3. Flexibility (e.g. a sticker)	

Selective Coding



Interpretation of codes in terms of an underlying **process**

- Integration of axial codes
- Refining the theory
- Developing a story line to demonstrate the theory

Selective Coding: Inconvenience

“I like the card kind of idea, kind of because you can maybe put it with other secure... with your bank card”

Selective Coding: Risk Perception

“Is there a way to do, like, a time thing on them? ... I guess it just makes it even more secure ... because it changes all the time”

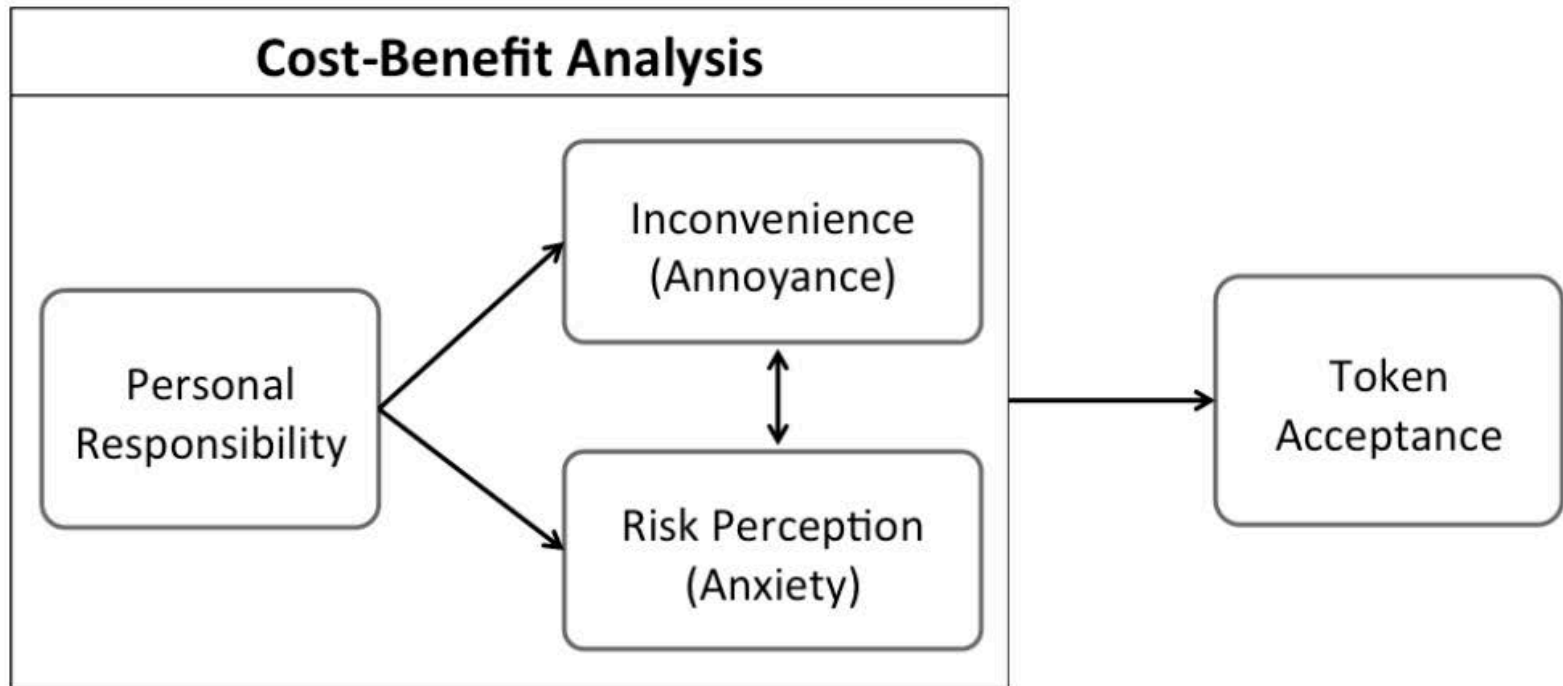
Selective Coding: Responsibility

“The worry would be obviously if you lost one and then you went to your access point and then realised that you lost one: where would you always keep the spares?... You wouldn’t want to carry too many things”

Agenda

- Passwords
- Background to Pico
- Approach
- Analysis
- **The Grounded Theory**
- **Conclusions**

The Grounded Theory

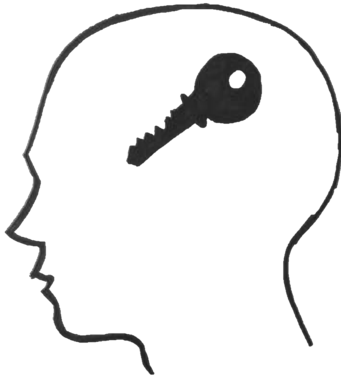


Agenda

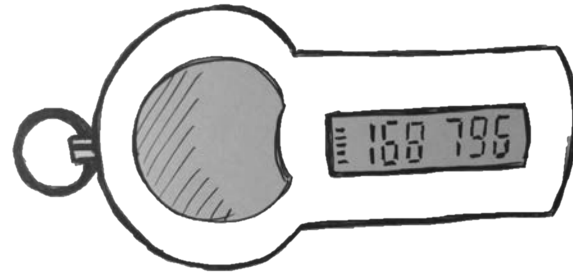
- Passwords
- Background to Pico
- Approach
- Analysis
- The Grounded Theory
- **Conclusions**

Conclusions

Passwords → Abstract



Tokens → Tangible



Tangible security increases perceived responsibility for:

- a. Mitigating security risks
- b. Managing physical item

= anxiety-provoking and inconvenient

Conclusions

Three key challenges:

1. Reducing annoyance (associated with inconvenience) and anxiety (associated with risk)
2. Avoiding system failures (reliability issues)
3. Aligning mental models of Pico with how it actually works

Questions?