What is the name of my dog[1]: on not so secret answers to security questions

Bart Preneel

COSIC, K.U.Leuven

[1] I don’t own a dog

Information classification?

- Sensitive – secret - top secret
- What is the question you really want an answer to?
- Simple: who are the reviewers who rejected my beautiful and elegant xxxcrypt submission introducing the first *efficient* and *provably secure* lattice-based homomorphic multiparty quantum identity-based computation with a tight reduction of the shortest path between Nice and Monaco?

If you really want to know

- Hack the conference review system
- But this is hard: for a security conference we use a multi-level secure machine with threshold-based multi-factor authentication with zero-knowledge identification (in a smart card), location based verification (in a smart phone), biometrics (iris, no fingerprint) and phishing detection

If you really want to know

- Hack the conference review system
- But this is hard: for a security conference we use a multi-level secure machine with threshold-based multi-factor authentication with zero-knowledge identification (in a smart card), location based verification (in a smart phone), biometrics (iris, no fingerprint) and phishing detection
- No, wait a minute, we actually use passwords
- And what if someone forgets his/her password?

If you really want to know

- Hack the conference review system
- But this is hard: for a security conference we use a multi-level secure machine with threshold-based multi-factor authentication with zero-knowledge identification (in a smart card), location based verification (in a smart phone), biometrics (iris, no fingerprint) and phishing detection
- No, wait a minute, we actually use passwords
- And what if someone forgets his/her password?
- That never happens
- Wait a minute, even cryptographers forget passwords

If you really want to know

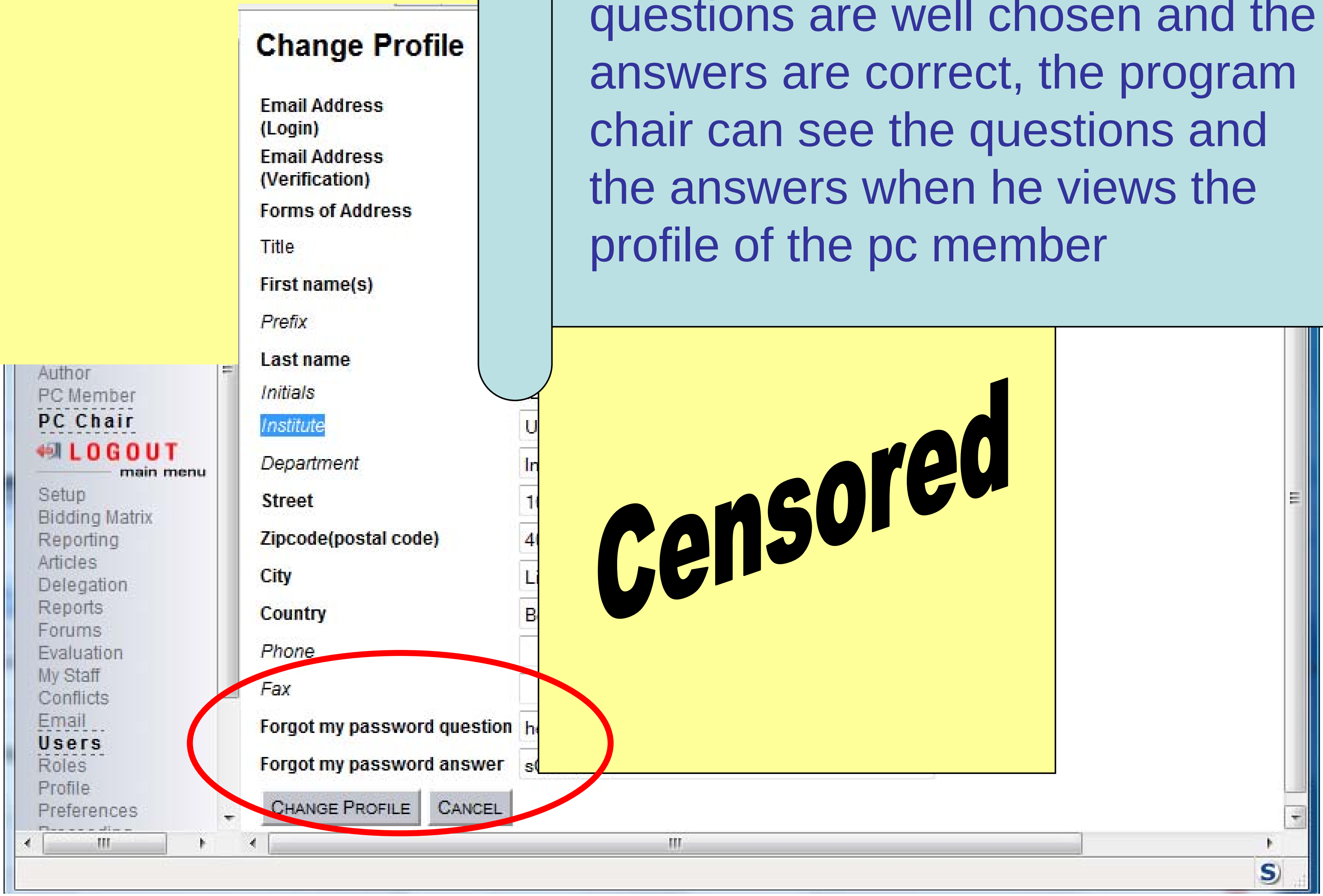
- Since Clipper (key escrow) has been sunk in 1994, we use a security question

If you really want to know

- Since Clipper (key escrow) has been sunk in 1994, we use a security question
- Example: what is the name of my dog? Answer could be: Tekkie/Tawny/Snoopy
- Enhanced security feature: user can choose his/her own question

If you really want to know

- Since Clipper (key escrow) has been sunk in 1994, we use a security question
- Example: what is the name of my dog? Answer: Tekkie
- Enhanced security feature: user can choose his/her own question
- This feature is provided by a conference review system offered by a publisher



Change Profile

Email Address (Login)	
Email Address (Verification)	
Forms of Address	
Title	
First name(s)	
Prefix	
Last name	
Initials	
Institute	U
Department	In
Street	1(
Zipcode(postal code)	4(
City	Li
Country	B
Phone	
Fax	
Forgot my password question	h(
Forgot my password answer	s(

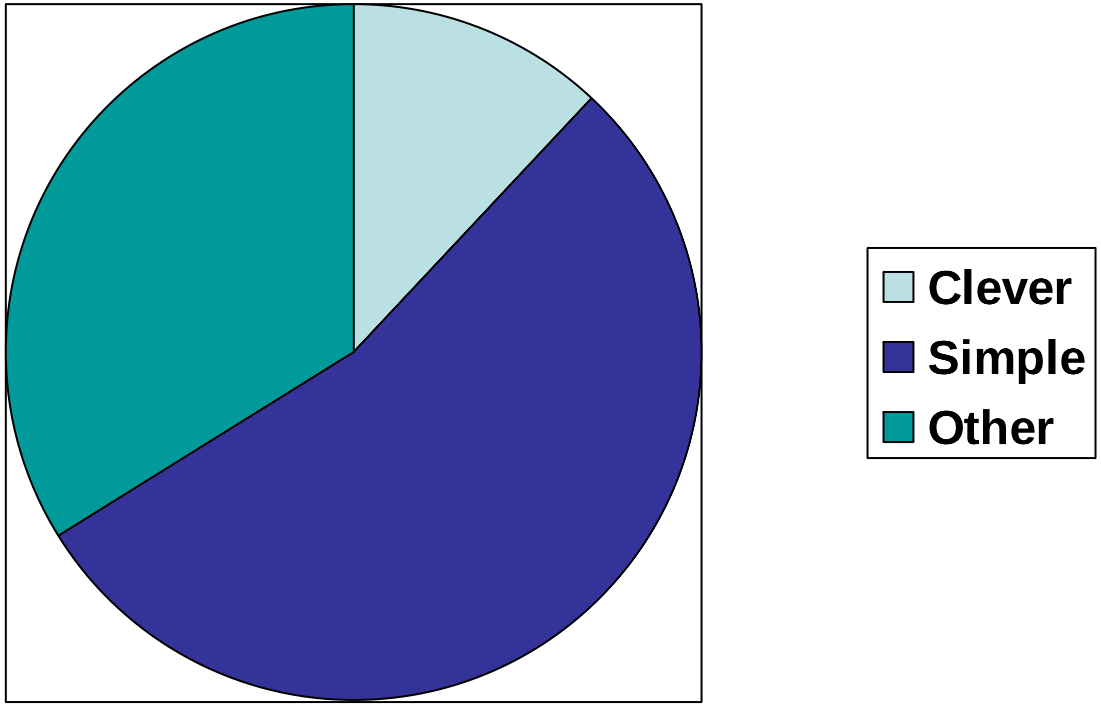
Censored

In order to make sure that these questions are well chosen and the answers are correct, the program chair can see the questions and the answers when he views the profile of the pc member

How to respond

- the privacy advocate: should I really see this data?
- the cryptographer: perhaps this has security implications
- the scientist: great, this is valuable empirical data

The results: 50 security experts



Clever (12%)

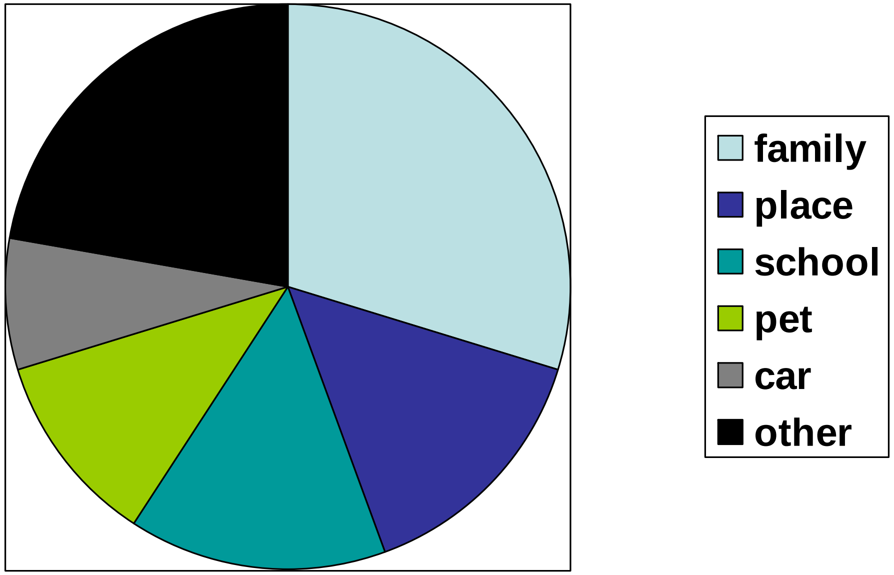
- Question = script or string
- Answer = output of script or function of string

Clever (12%)

- Question = script or string
- Answer = output of script or function of string

Simple (54%)

- entropy is low
- answer easy to find: “what is the name of my oldest son”



Variant (6%)

- Question = “the question”
- Answer = “a question”

Variant (6%)

- Question = “the question”
- Answer = “a question”

Answer = question (28%)

- 4%: 1 character: “7” or “+”
- 6%: negation: “no” “n/a” “none”
- 6%: a simple word: “qwerty”
- 12%: a phrase or question: “what is the question?”

In some cases the phrase or word may be a password hint, which could be used to help a password cracker

More research is needed…

The good news

as far as I can tell the security question is not used in any way

the password is just sent (in clear) to the email address of the pc member

so why is this information collected?

- to sell it?
- to support academic research into security questions?

Ask for help with my research

- I am fascinated by the question how cryptographers choose security questions
- Please send your favorite security questions and answers to bart.preneel(AT)esat.kuleuven.be
- If you send 20$ to my PayPal account, I will send you a detailed security analysis of your question
- You can trust me: I have hired a lawyer to write an 80-page security policy[1] which will someday be reviewed by the ethics board of my university

[1] This security policy will be updated monthly to reflect changes in the regulatory environment. Additional disclaimers my be added at any time[2]

[2] Disclaimer: there may be some disclaimers in my security policy[1]