Reliable Biometrics for Digital Authentication

Protecting Your Hard Earned Cash After Compromise

Netizens

[1]Cyber Security
Computer Science
University of Hertfordshire

April 2016

Contents

Introduction

Current Issues

Generalisation

Tackling the Issues

Future Work

Wrapping Up

Overview

Considering authentication methods within the financial industry we look to propose how systems may be improved to better protect customers from fraudulent use. The proposed method uses **statistical data unique to the user** to increase the security of a connection.

Objectives

- Current issues
- Generalise the problem
- Tackling the issue
- Future works

Bank Fraud

"*Thieves drain our bank accounts of more than 300 million pounds every year*" - BBC Watchdog, Online [2]


[1]

Bank Data

"*Globally, 22 data records were lost or stolen every second in 2015*" - Gemalto, Online [3]


[1]

Card, Chip & Pin

- Compromised details
- Shared accounts
- Fake claims to bank compromise


[1]

[1]

Online

- Stolen details
- Unauthorised usage
- Identifying compromisers (that could stand up in court)

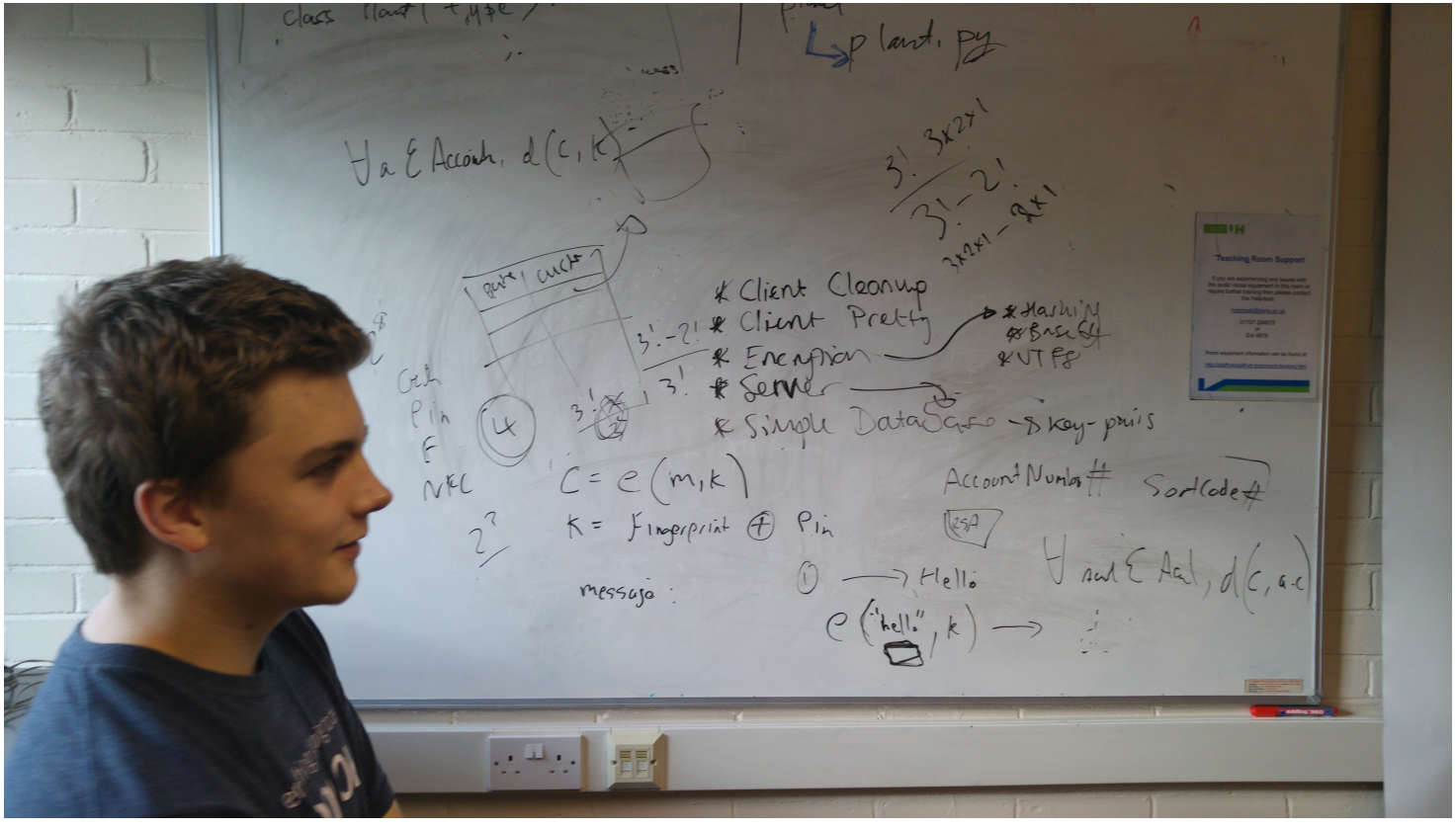

[1]


[1]

What is the issue here?

Non-repudiation

The act of associating actions with an individual.

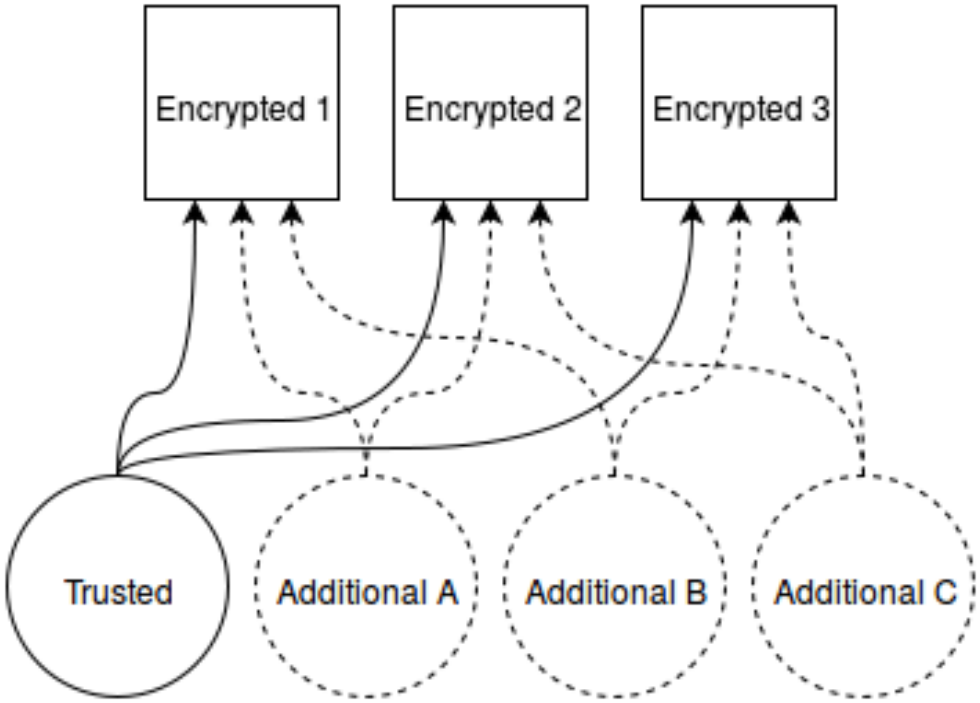


What does this mean?

- Asking “questions” only the user will be able to reply with
- Uniqueness of reply - we’re not robots!

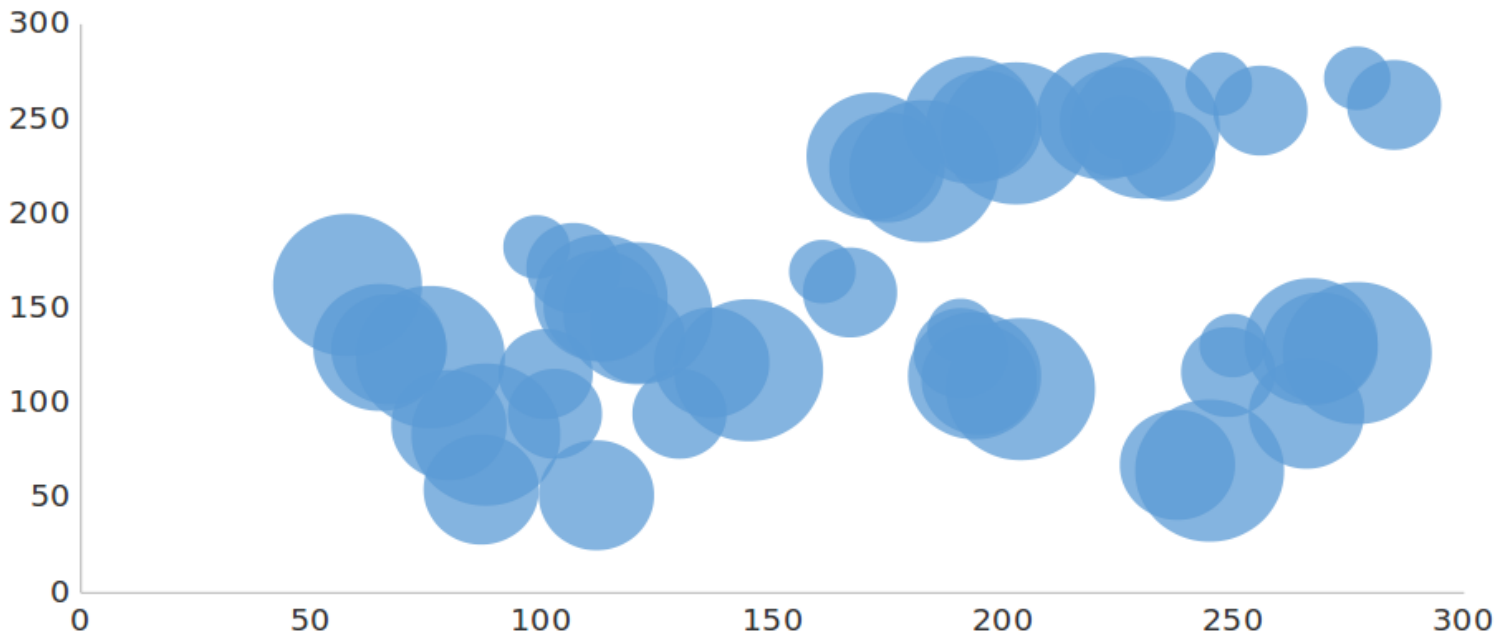
Main Algorithm

Multi-pillar trust, relying on current proven methods and building up security for reduced risk.



Fingerprints

Researching methods of reliable storage and recall of fingerprints stored in a hash.



Others

- **Voice Recognition** - Recognising patterns in different words
- **Facial Expression** - Looking at the uniqueness in expressions
- **Gestures** - A challenge-response check

Most biometrics will work!

Passwords

- Less to remember as information is part of you
- Potential for faster authentication
- Solves the problem of longer and more complicated passwords
- Failures in methods are supported by other pillars
- Robustness increases with number of methods used
- Not predictable for a hacker
- Hashes mean that personal information isn't stored on the server

Santander - Rán-Lock

We were short-listed to present at Santander Big Ideas.

- 500 teams registered
- 80 teams submitted
- 13 selected for finals

What we have

- Demonstration of how the overall algorithm works
- Example of how users will integrate with the system

6. Future Work

What Next?

We need reliable hashes!

- **Fingerprints** - Good starting point given the amount of data available.
- **More biometrics** - The more options the better, a lot aren't ready yet for reliable hashing.
- **Testing** - We want to field test the idea with a larger audience.

Thank You!

Any questions?

References I

Wiki Commons.
Emoji.
[Accessed 04-2016] Google - https://code.google.com/p/noto/, *Apache License 2.0: http://tinyurl.com/h8kzup7*

BBC Watchdog.
Bank Fraud: Easy to be a victim - hard to get your money back?.
[Accessed 04-2016] http://tinyurl.com/glrbl9k.

Gemalto.
2016 The Year Data Breaches Got Personal.
[Accessed 04-2016] http://tinyurl.com/h7vduvk.