

FC 2010

**Shoulder-Surfing Safe Login in a
Partially Observable Attacker
Model (Short Paper)**

Toni Perković

joint work with

Mario Čagalj and Nitesh Saxena

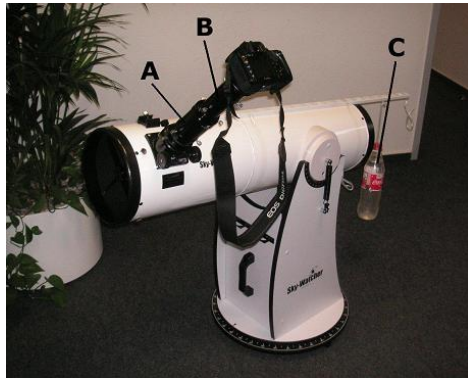
University of Split, Croatia

27/01/2009

Introduction

- Classical PIN-entry methods (via keyboards, keypads and alike) are all vulnerable to observation attacks

Oakland - [Backes2008]



- Designing a usable cognitive PIN-entry method secure against eavesdroppers is truly challenging:
 - SAT solver attacks [Golle07]
 - Side channel timing attacks

Introduction

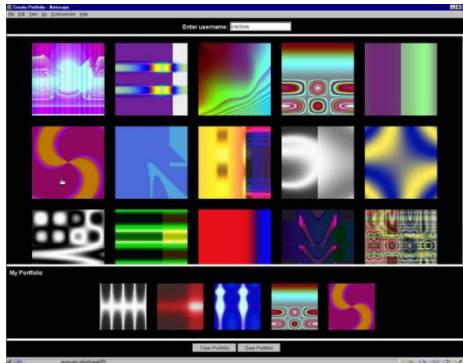
- We roughly divide PIN-entry methods in two classes based on information available to a passive adversary:
 - **Fully observable model:** the adversary observes the entire input and output of a PIN-entry procedure (the attacker observes challenge and response values)
 - **Partially observable model:** the adversary can only partially observe the input or output

Fully observable model

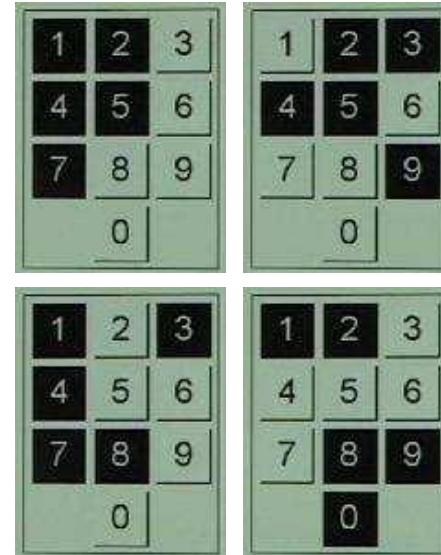
Passfaces



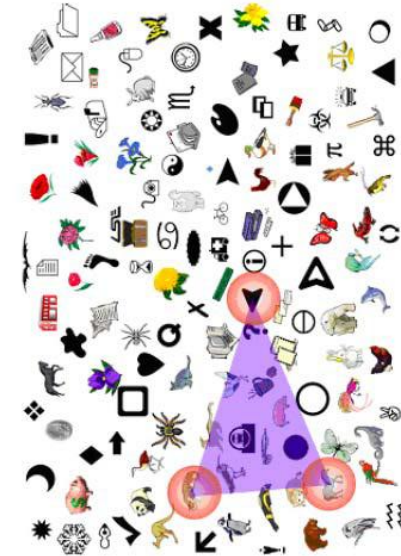
Deja Vu



[Roth04]



[Sobrado02]



(i) Short authentication time

- Broken after a single authentication

(ii) Long authentication time

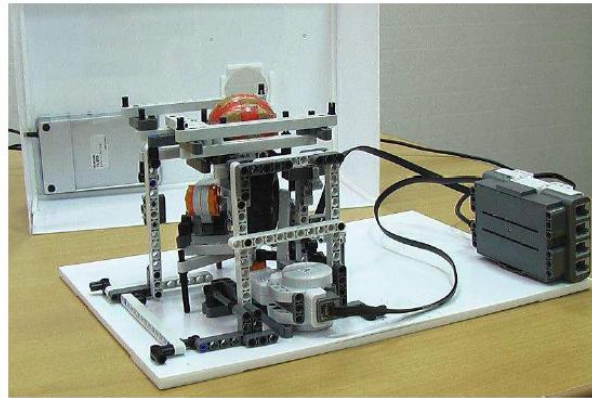
- Mentally demanding
- Broken after several successful authentications

Partially observable model

- The adversary can only partially observe the input and/or output
- He/she does not have an access to challenge values
- Authentication Using Tactile Feedback [Kuber06]
- Undercover [Sasamoto08]



(a) Outside view



(b) Inside view



- Requires new hardware (price), mentally demanding

Usability and Design Requirements

- **User friendly** - low login error rates and fast authentication times
- **Cost-efficient** - cheap to implement, integrate it with existing systems
- **Secure** – resistant to keyloggers, passive attacks (camera recording)

Our paper

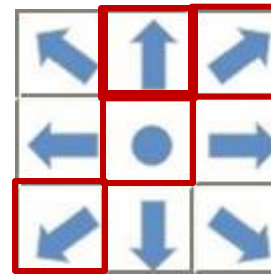
- Modulo 10 (Mod10) [Hill99]
 - mentally demanding (older persons)
 - has never been studied before
 - Example: PIN = 4 6 5 4
 - challenge = 7
 - response = $4+7 \bmod 10 = 1$
- Our solution:
 - Simple Table Lookup (STL)
 - Mod10-table
 - graphical based authentication methods based on table lookups
 - our goal is to compare these methods with Mod10

Simple Table Lookup (STL)

- STL components

9	7	8	9	7
3	1	2	3	1
6	4	5	6	4
9	7	8	9	7
3	1	2	3	1

(a) STL table



(b) Response buttons



(c) Protected channel

- Example: PIN = 4 6 5 4 8
(5 digit pin)

PIN	4	6	5	4	8
Challenge values	9	6	2	1	6
User's response	↙	○	↑↑	↑↑	↗

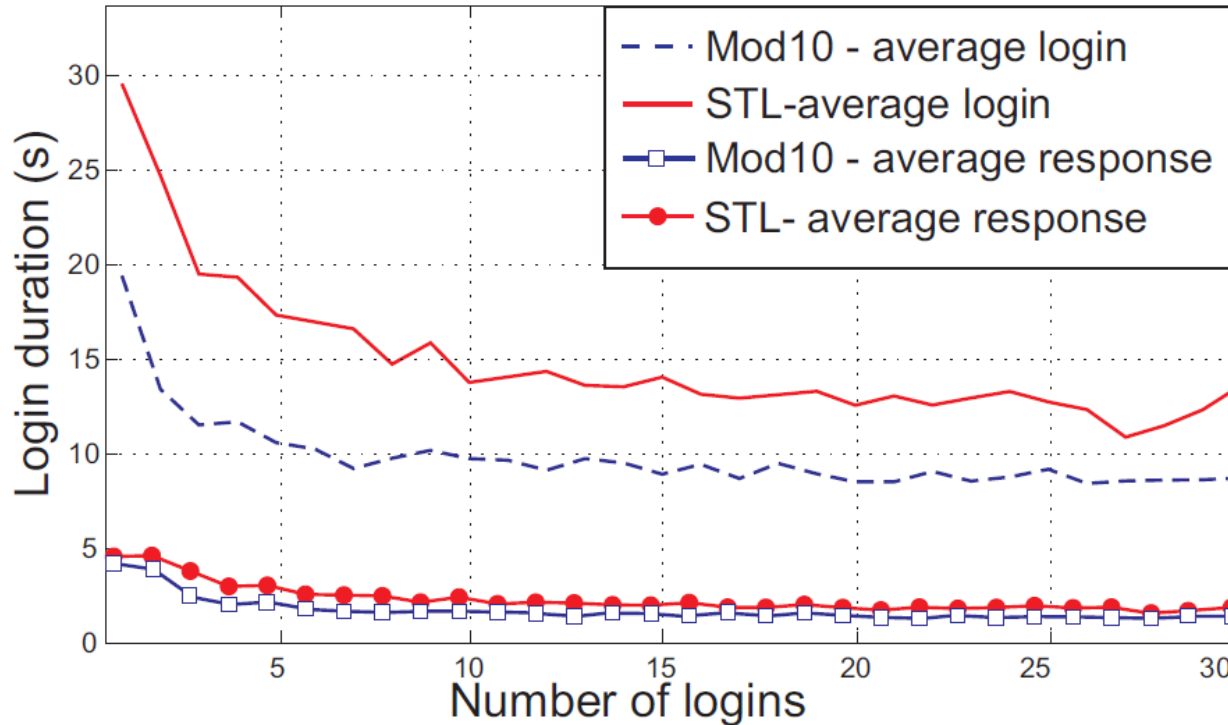
Usability evaluation – STL vs Mod10

Age			Male / female	
18-25	26-40	>40	Male	Female
18	2	0	13	7

- Each study took 90 minutes per user (30 min. per method)
- Users would take half an hour between the tested methods
- **Training phase:** 5 successful logins per method
- **Authentication phase:** 30 successful logins per method

Usability evaluation – STL vs Mod10

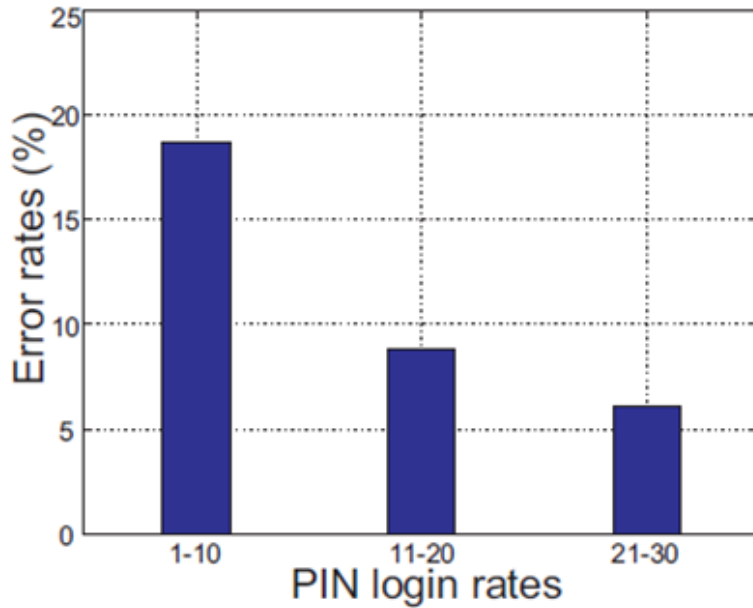
- Average login time



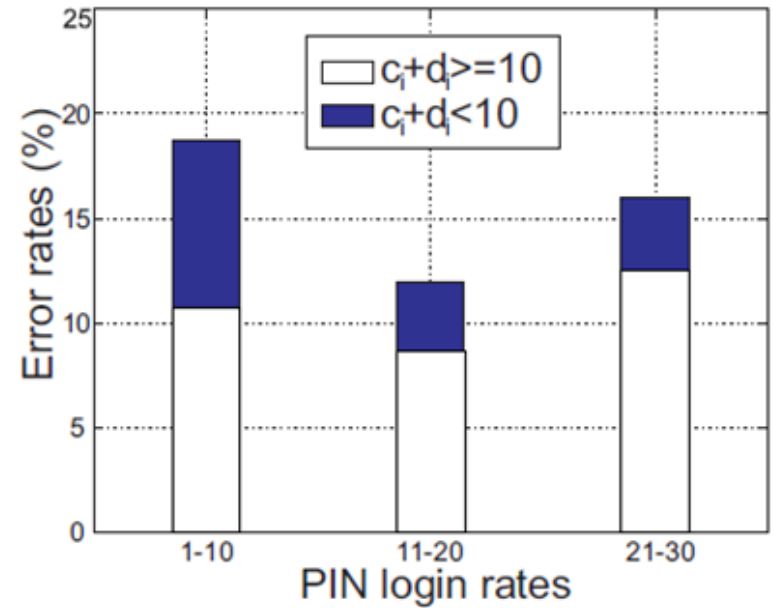
- The average login times are 12.5 and 9.5 seconds for STL and Mod10, respectively.
- The average login time per PIN digit was is 2.25 and 1.8 seconds for STL and Mod10, respectively.

Usability evaluation – STL vs Mod10

- Error rates



STL

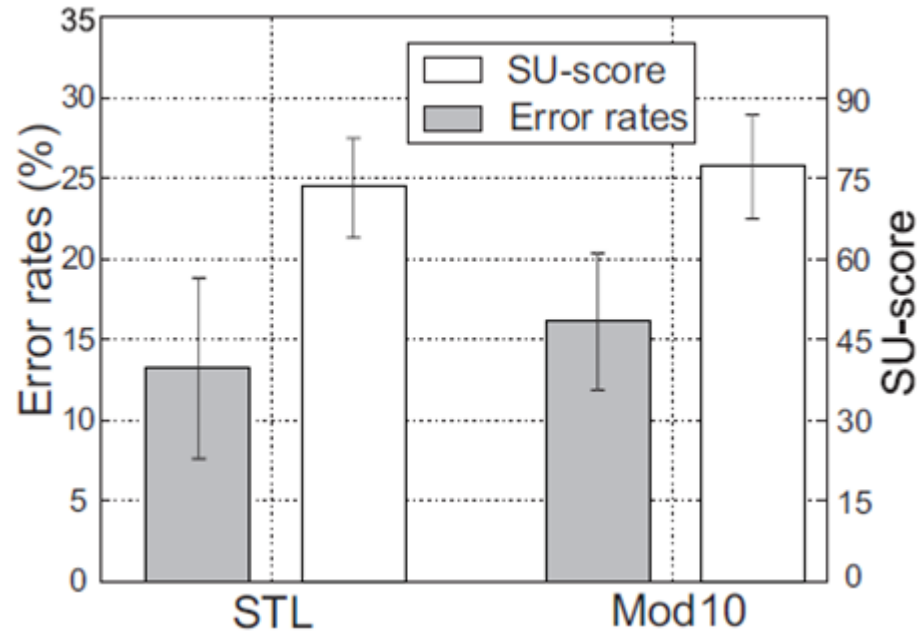


Mod10

- The major source of errors with the Mod10 method are cases in which the sum of the challenge and the respective PIN digit exceeds 10

Usability evaluation – STL vs Mod10

- SU-score



- The average SU-score for STL and Mod10 is 73 and 78 (out of 100)
 - due to the shorter login time

	Using					Feel secure				
	5	4	3	2	1	5	4	3	2	1
STL	10	4	6	0	0	11	5	4	0	0
Mod10	9	4	7	0	0	9	9	2	0	0

Mod10 vs Mod10-table

- Modulo 10 (Mod10) [Hill99]
- Mod10-table
- Example: PIN = 4 6 5 4

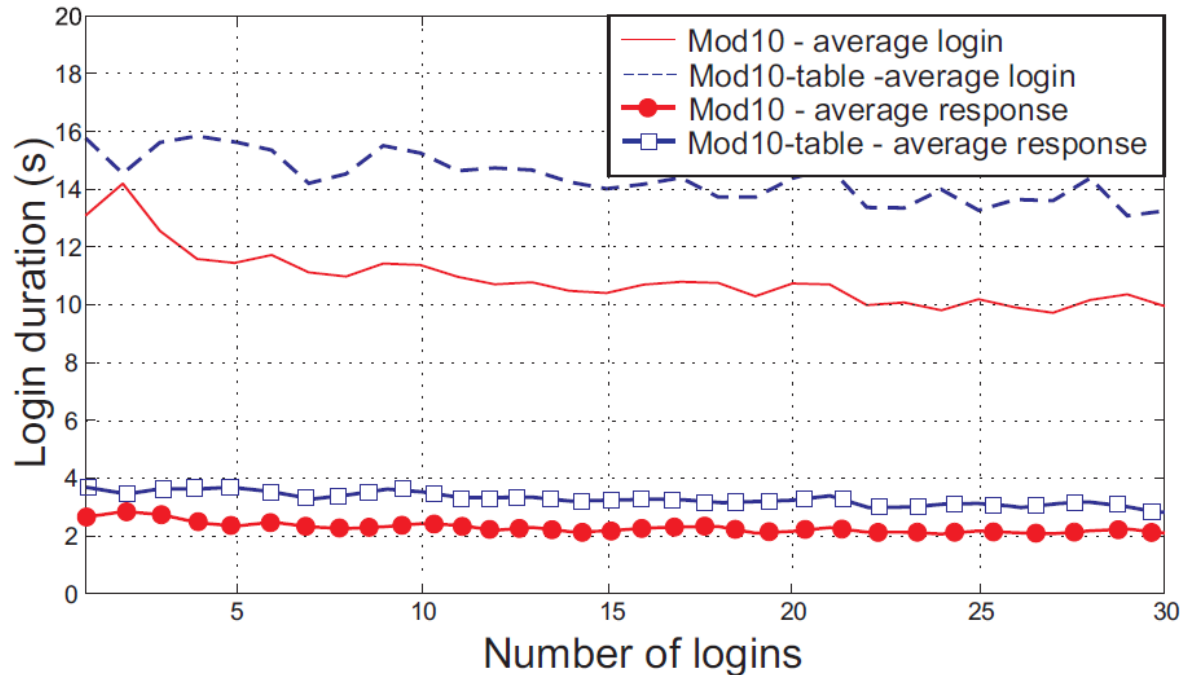
	0	1	2	3	4	5	6	7	8	9
0	0	1	2	3	4	5	6	7	8	9
1	9	0	1	2	3	4	5	6	7	8
2	8	9	0	1	2	3	4	5	6	7
3	7	8	9	0	1	2	3	4	5	6
4	6	7	8	9	0	1	2	3	4	5
5	5	6	7	8	9	0	1	2	3	4
6	4	5	6	7	8	9	0	1	2	3
7	3	4	5	6	7	8	9	0	1	2
8	2	3	4	5	6	7	8	9	0	1
9	1	2	3	4	5	6	7	8	9	0

challenge = 7
response = 1

Usability evaluation – Mod10 vs Mod10-table

- Average login time

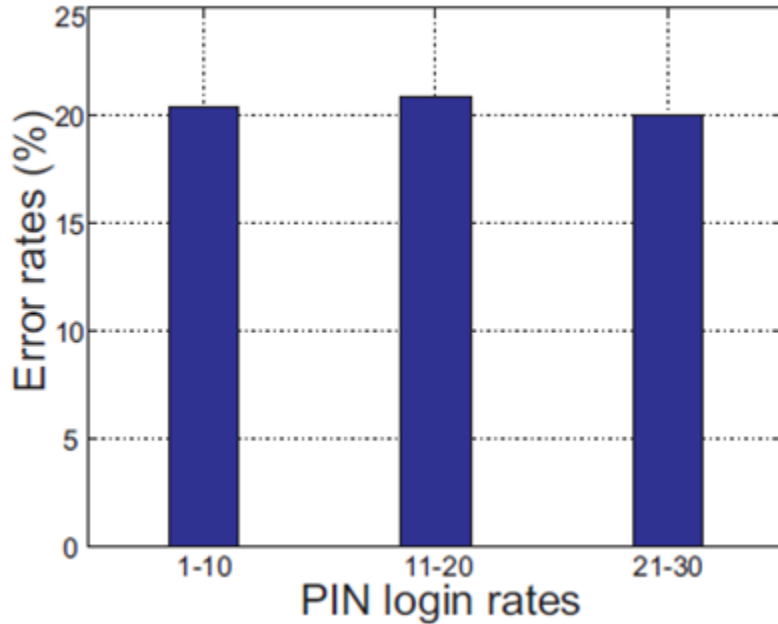
Age			Male / female	
18-25	26-40	>40	Male	Female
22	8	8	26	12



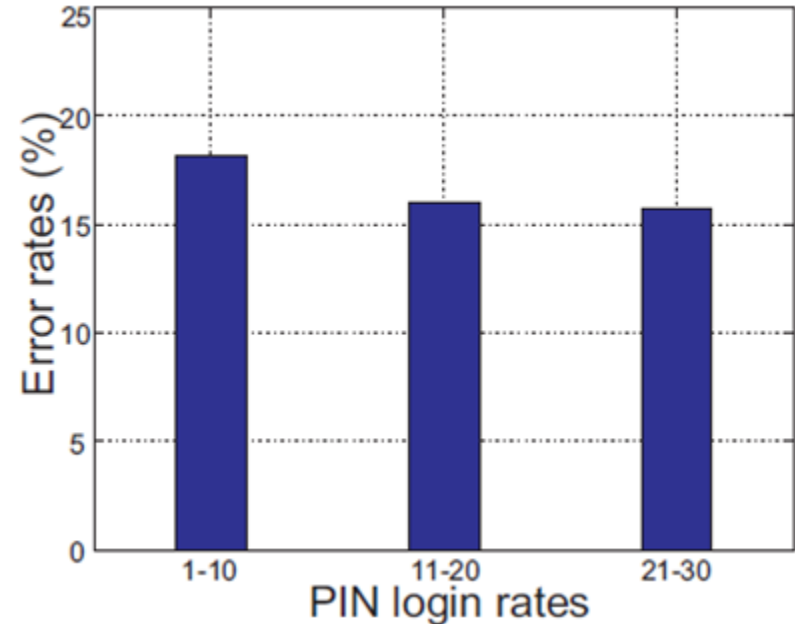
- The average login times are 10 and 12.5 seconds for Mod10 and Mod10-table, respectively.
- The average login time per PIN digit was 2 and 2.7 seconds for Mod10 and Mod10-table, respectively.

Usability evaluation – Mod10 vs Mod10-table

- Error rates



Mod10



Mod10-table

- The users achieved higher error rates with Mod10 method

Usability evaluation – Mod10 vs Mod10-table

- SU-score



- The average SU-score for Mod10 and Mod10-table is 78 and 72 (out of 100) – due to the shorter login time
- Older participants tend to use Mod10-table

	Using					Feel secure					Prefer			
	5	4	3	2	1	5	4	3	2	1	18-25	26-40	>40	All
Mod10	11	10	13	3	1	14	12	4	4	4	19	6	4	29
Mod10-table	9	7	12	6	4	16	13	9	2	3	3	2	4	9

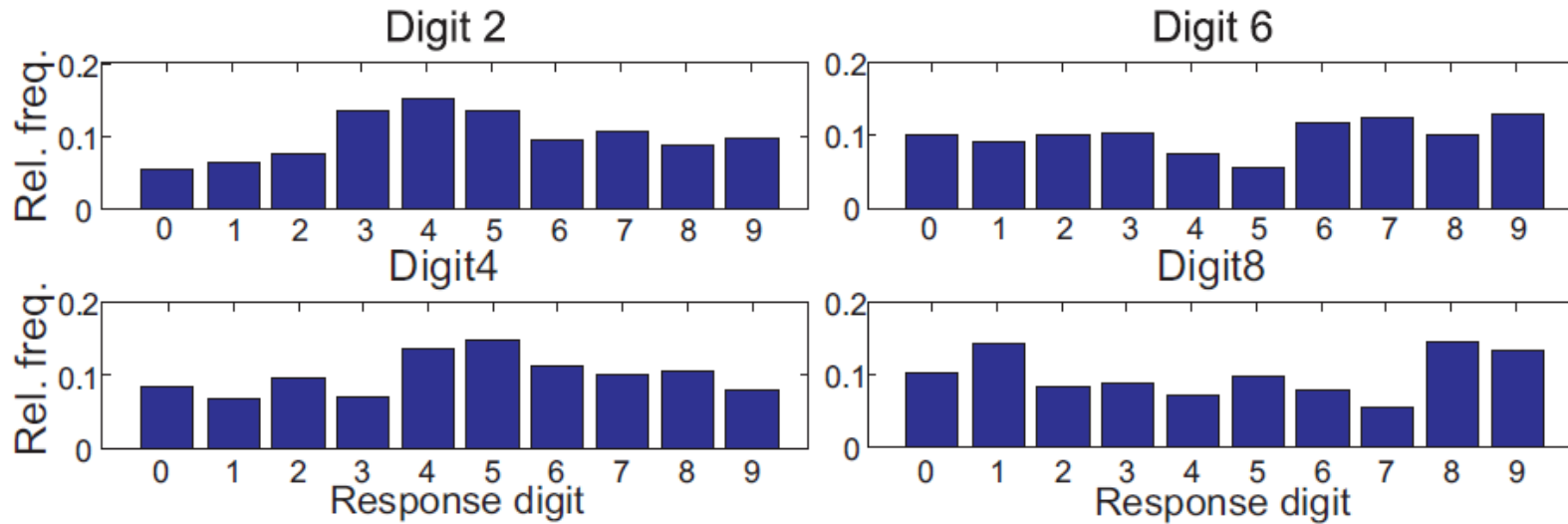
Security analysis

- Camera Recording (Passive) Adversary
- Mod10, STL and Mod10-table PIN-entry schemes implement the one-time pad paradigm
- Example:

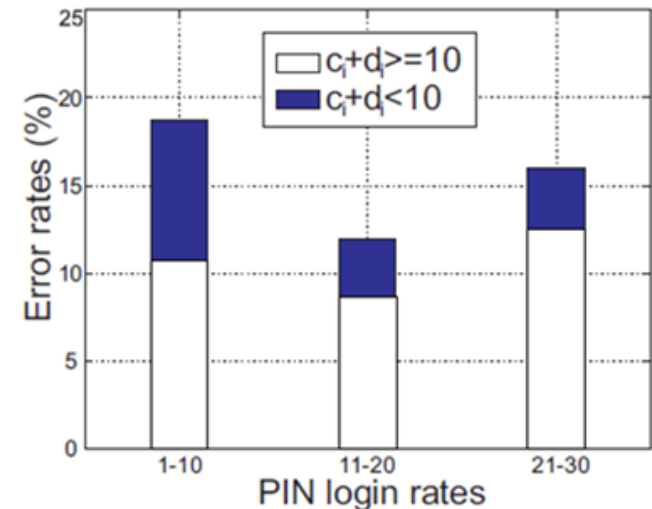
PIN	4	6	5	4	8
Challenge values	9	6	2	1	6
User's response	↙	○	↑	↑	↗

- The probability of guessing the correct PIN: 9^{-5}
- Side channel attack

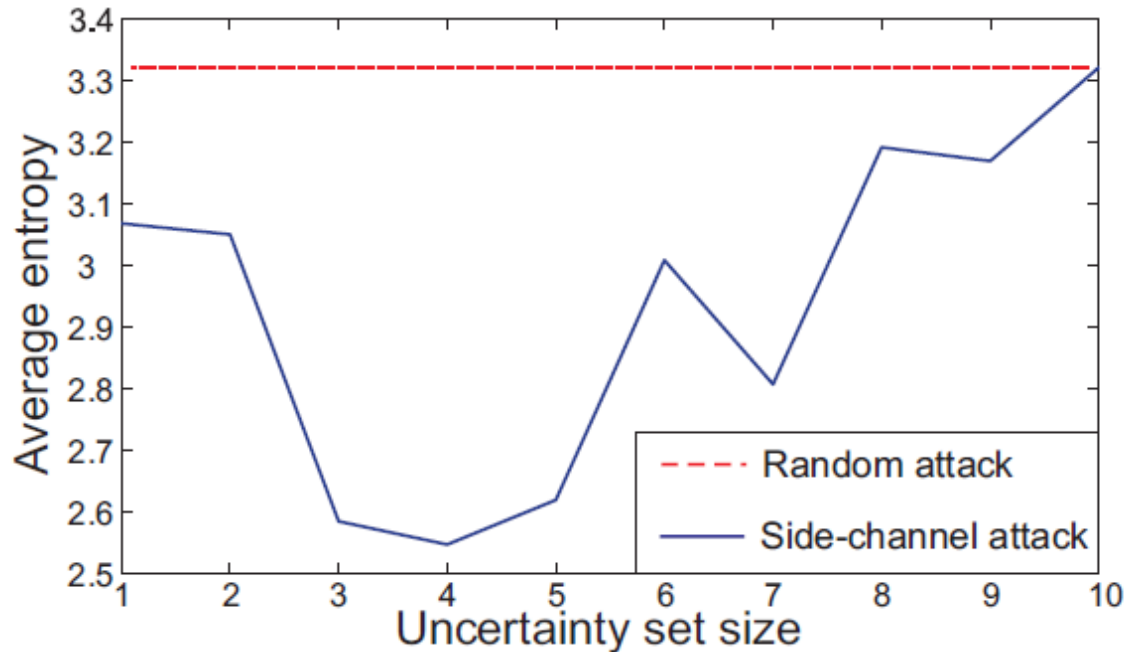
Side-Channel Timing Attack on Mod10



- The major source of errors are the cases when the sum of two numbers exceeds 10
- We recorded 30 successful logins and calculated the response time taken for a given PIN digit
- Easy additions (PIN digit with 0, 1 and 2) have shortest response times
- We applied standardized pattern matching techniques (k-nearest neighbor)



Side-Channel Timing Attack on Mod10

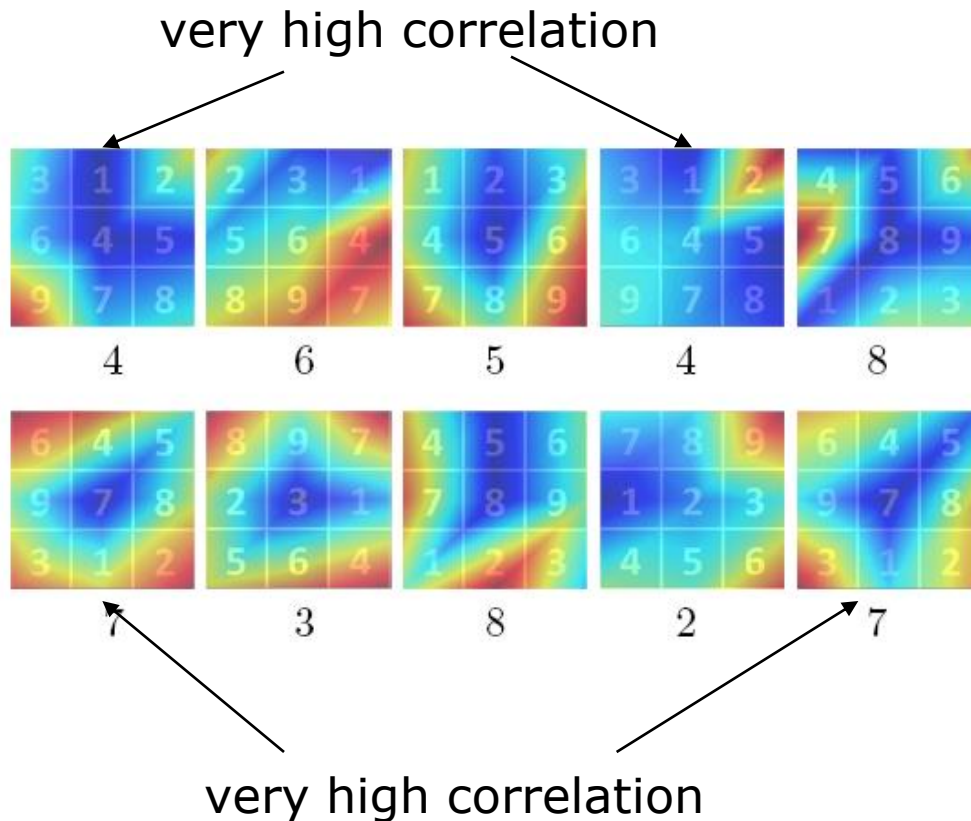


- We reduced the entropy of the PIN digit from $\log_2 10 = 3.3$ bits to **2.55!** bits

$$H(d) = r(k) \log_2 \frac{k}{r(k)} + (1 - r(k)) \log_2 \frac{10 - k}{1 - r(k)}$$

Security analysis

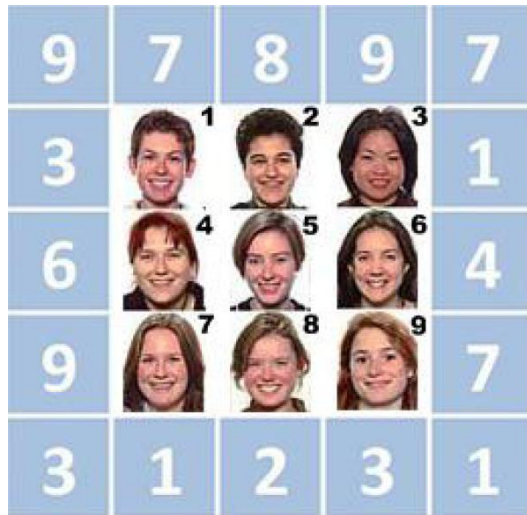
- Side-Channel Timing Attack on STL



- Attacker can record the user's response time
- Benefits from reaction time
- Patterns showing different response times by two users with PINs: 46548 and 73827
- Security factor reduces from 9^5 to 9^4
- Solution: we can apply random delay in STL challenge-response procedure

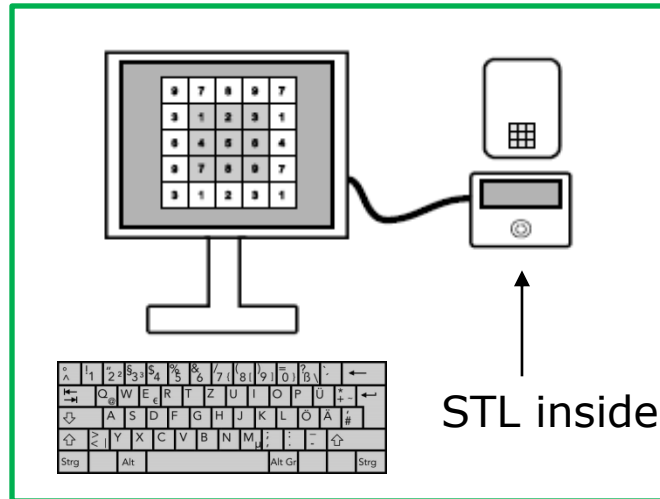
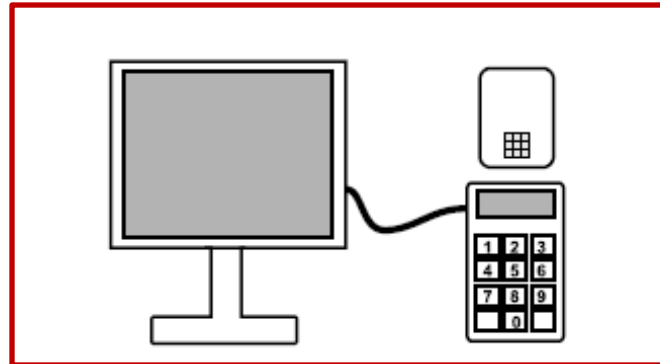
STL applications

STL Integrated with Graphical Passwords

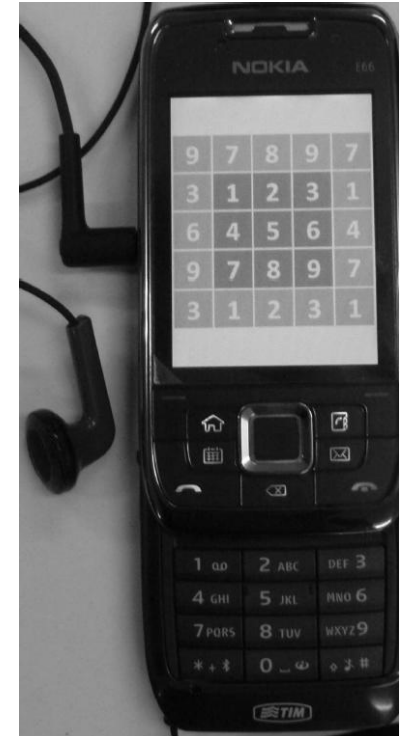


Passfaces

Internet banking



Mobile Phones



- STL reduces the cost of the card reader

Conclusion

- We presented two cognitive authentication schemes (STL and Mod10-table) that require no math
- STL can be easily adapted to work with graphical passwords – Passfaces
- We performed a user study of these schemes and a Mod10 scheme that requires elementary math (addition mod 10)
- It is very easy to learn and use - small average login times achieved
- STL integration into systems like Internet banking and mobile phones
- We revealed the attack on Mod10 and STL

Side-Channel Timing Attacks on cognitive authentication schemes has to be seriously considered