

Keystroke dynamics

Can Attackers learn someone's
typing characteristics.

Presentation Outline

.Introduction

- Research question
- Keystroke dynamics

.Experiments

- Results

.Conclusion

Introduction

Biometric

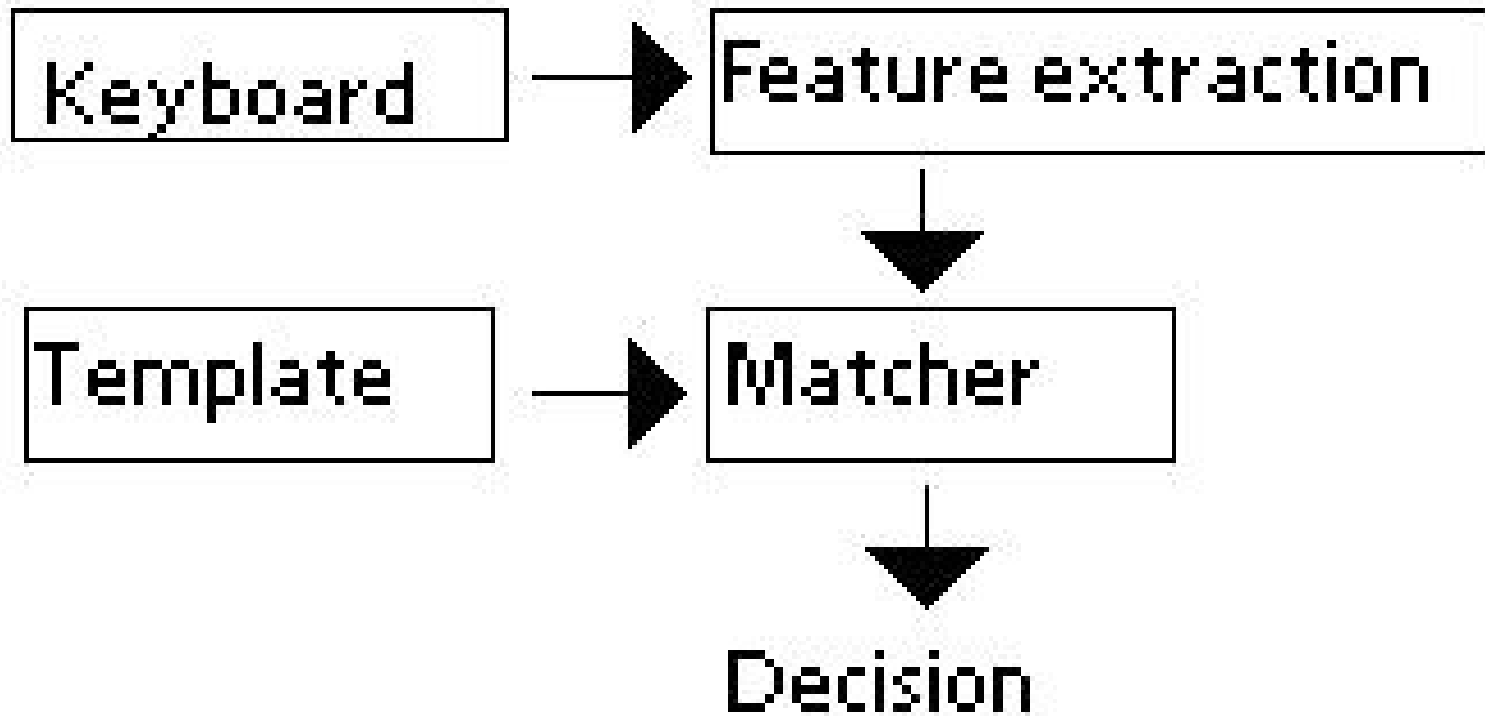
- Physiological
- Behavioral

Introduction

Keystroke dynamics

- Static authentication
- Dynamic authentication

Introduction



Research question

Question:

- Can attackers learn someone's typing features?

Keystroke dynamics

Timings:

- Duration
 - Key-down to key-up
- Latency
 - Key-up to key-down

Keystroke dynamics

Raw data:

KEY_DOWN	3.089985	P
KEY_UP	3.216883	P
KEY_DOWN	3.897391	D5
KEY_UP	3.982308	D5
KEY_DOWN	4.197313	U
KEY_UP	4.282212	U

Keystroke dynamics

Results:

P	0.126897	0,680507	5
5	0.084917	0,215004	U
U	0.084898	0,283323	X
X	0.097770		

Keystroke dynamics

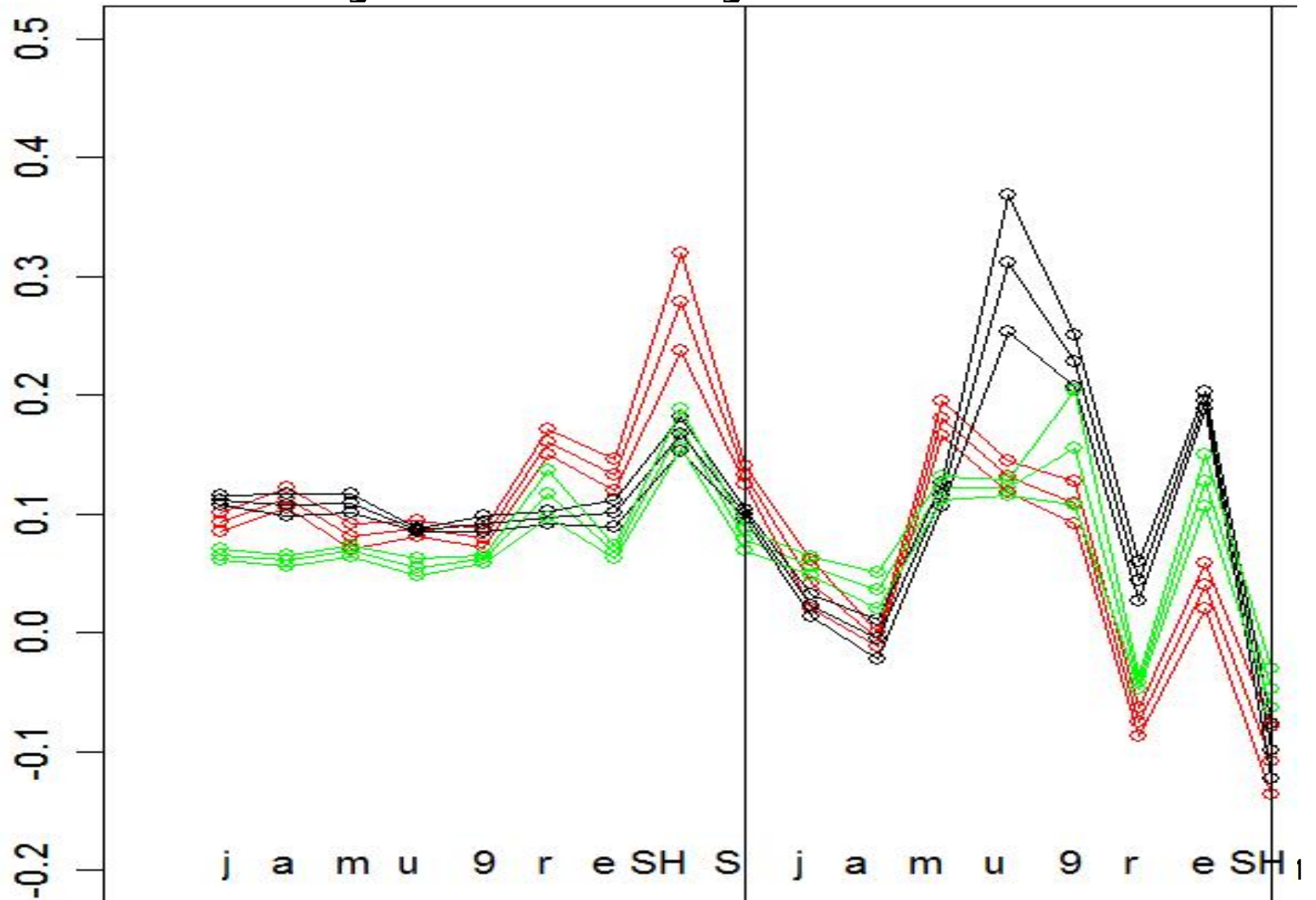
Average:

J	0.111769	0.023055
A	0.107431	-0.005695
M	0.108999	0.116150

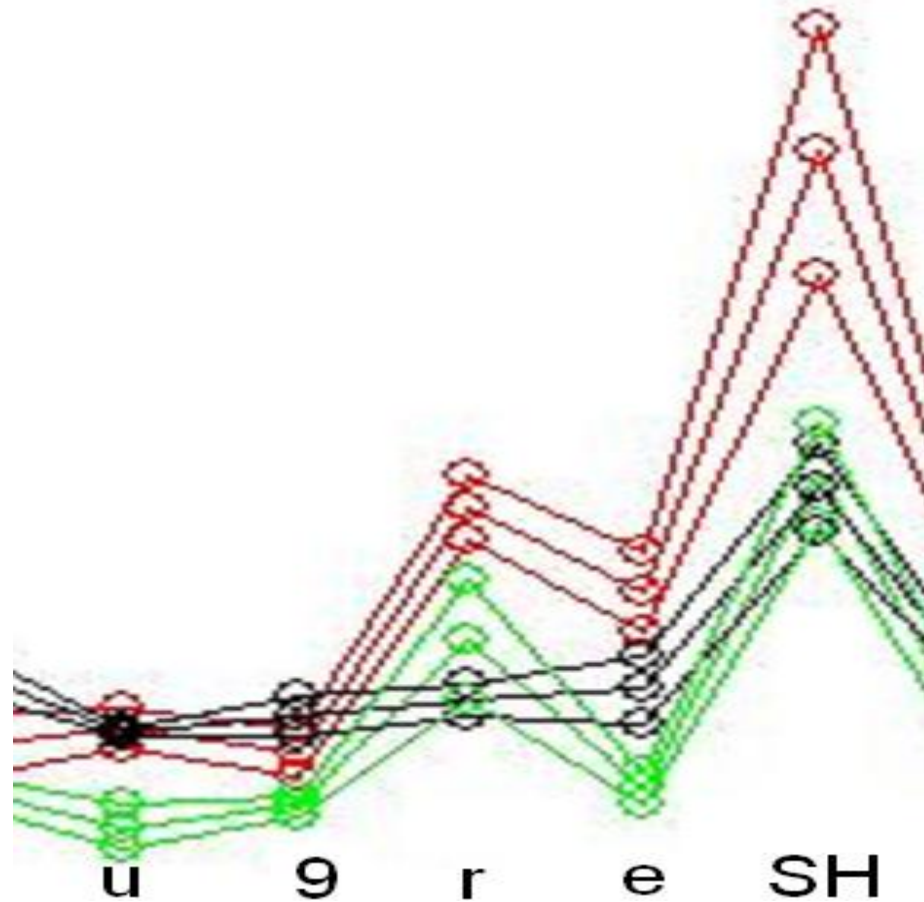
Standard deviation:

J	0.003556	0.009268
A	0.009771	0.017162
M	0.008285	0.009409

Keystroke dynamics



Keystroke dynamics



Experiments

Two experiments were conducted

- Authentication experiment
- Imitation experiment

Authentication Experiment

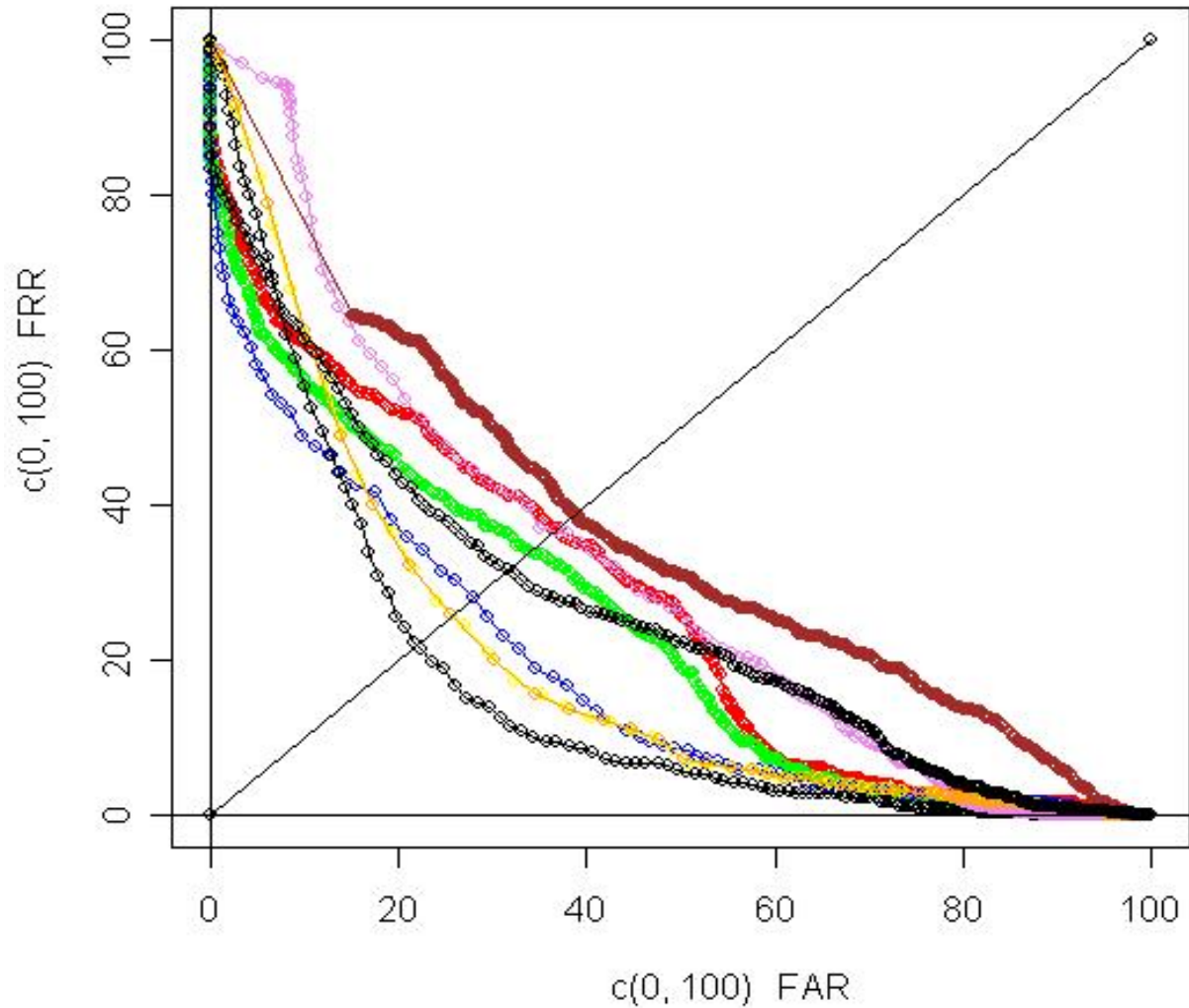
- 21 participants.
- Password: p5uxAc6emm
- Two months.
- Experiment on their own computers.
- 2000 passwords.
- 16.9 % misspellings.
- 1468 legitimate attempts.
- 32133 impostor attempts.

Authentication Experiment

- 14+ Distance metrics
- Equal Error Rate between <20% and 60%
- Best suited distance metric:
 - Manhattan city block distance metric with standard deviation.
 - 23% to 27%, depending on outlier removal.

ROC curve

ROC



Imitation experiment

- Time-series experiment design
 - Three treatments (programs)
 - Three groups
- 3 Victims
- 9 Attackers
- 3 Passwords
 - jamu9reS
 - bruf9Tr2
 - p7eneZuh

Imitation experiment

3 programs

- Accepted or not (Control)
- Score (Treatment 1)
- Score and Graph (Treatment 2)

Imitation experiment

Attack group	A	B	C
Victim			
I	P1 Prog3	P2 Prog2	P3 Prog1
II	P3 Prog2	P1 Prog1	P2 Prog3
III	P2 Prog1	P3 Prog3	P1 Prog2

- Managed to disrupt the learning curve.

Results

- Learning Curves.
 - Attackers learn quicker with most feedback.
- False acceptance rate.
 - Program one: 7.5%
 - Program two: 12.5%
 - Program three: 22%

Results

Regression analysis:

Formula $Y = \beta_0 e^{\beta_1 X} + \epsilon$

Results

	Estimate	Std. Error	t value	Pr(> t)
Intercept	4.722	0.063	75.34	< 2e-16
Number	-0.018	0.002	-7.64	1.17e-13
Program 2	-0.048	0.034	-1.39	0.165
Program 3	-0.097	0.034	-2.83	0.005
Victim 2	0.141	0.034	4.12	4.55e-05
Victim 3	0.518	0.034	15.09	< 2e-16
Attacker 2	0.037	0.066	0.56	0.573
Attacker 3	-0.249	0.063	-3.97	8.43e-05
Attacker 4	-0.366	0.062	-5.88	7.60e-09
Attacker 5	0.142	0.070	2.03	0.043
Attacker 6	0.174	0.067	2.61	0.009
Attacker 7	-0.113	0.064	-1.76	0.079
Attacker 8	-0.383	0.062	-6.19	1.30e-09
Attacker 9	0.953	0.065	14.68	< 2e-16
Password 2	-0.260	0.034	-7.57	1.90e-13
Password 3	-0.276	0.034	-8.02	7.76e-15

Results

Regression analysis:

- Program two is slightly better than program one.
- Program three is significantly better than program one. $p=0.0048$

Conclusion

- Keystroke dynamics works, but has a high EER in our experiments.
- The password is important.
- Attackers can learn someone's typing characteristics, with the proper tool and determination.
- A bigger experiment is needed to verify this.

Questions?

Program Three

