



How typing characteristics differ from one application to another

Hafez Barghouthi

Introduction

- Authentication
- Biometrics.
- Keystroke Dynamics.



Authentication

- One of the most important things before giving a person access to any resource is to identify or authenticate him\her first.
- By authentication we mean verifying a claimed identity.
- By identification we mean establishing an identity.



Authentication Parties

- The authenticator (legitimate user).
- The verifier.
- The attacker(imposter).

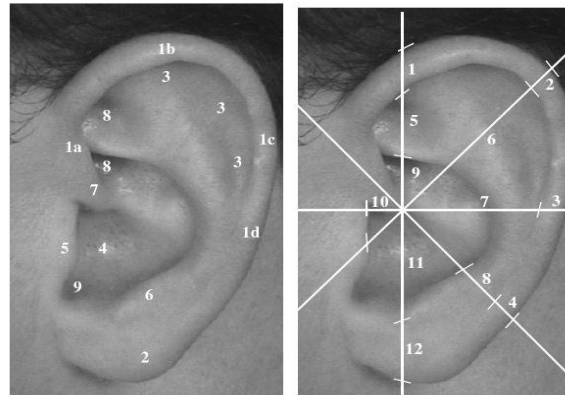
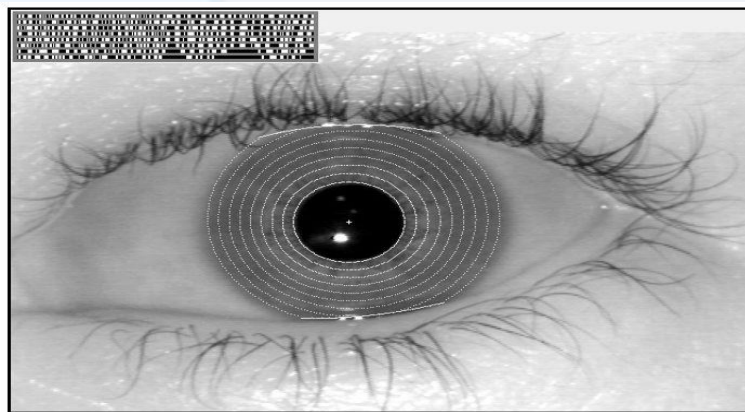


Authentication Factors

- Know: something only you remember.
- Have: something only you possess.
- Are: some biometric property.
- Combinations (Multiple factors).

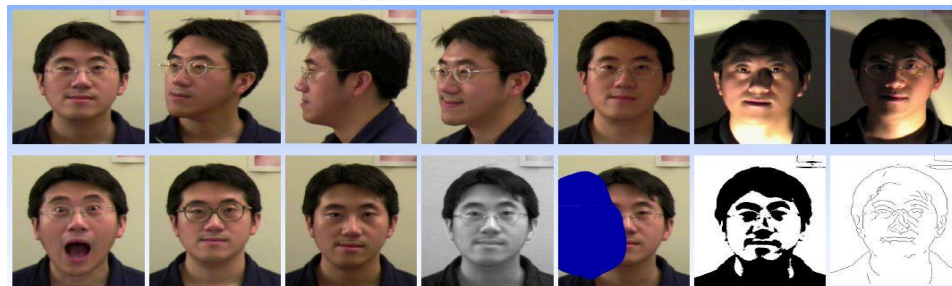
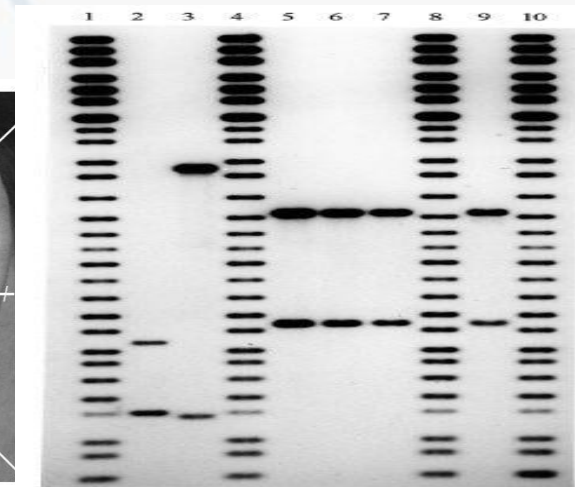
Biometrics (Are)-1

- Physiological (static) : Features that are physically related to a person for example iris, fingerprints and retina.



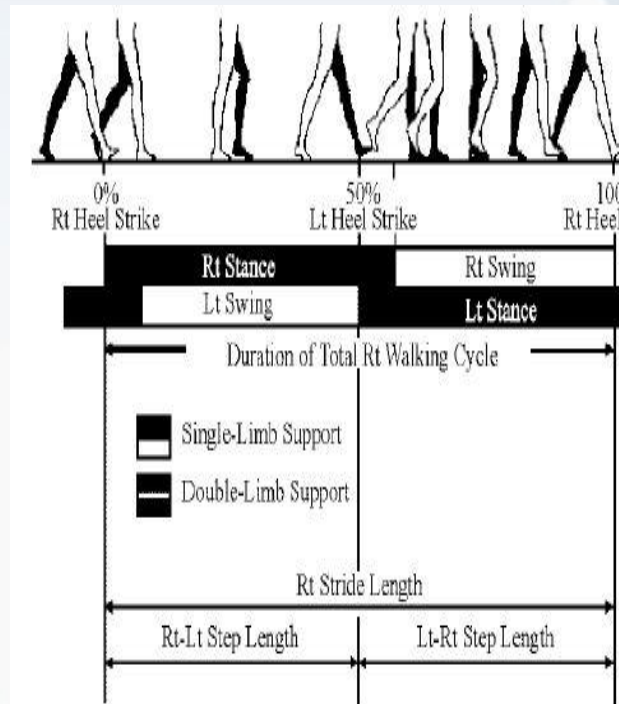
(a) Anatomy.

(b) Measurements.



Biometrics (Are)-2

- Behavioral (dynamic): features that people have learned to do. Gait, signatures, and keystroke dynamics



Keystroke dynamics

- Keystroke dynamics is the process of analyzing the way a user types on a keyboard and identify him based on his habitual typing rhythm
- A user's typing pattern may be unique because similar neuro-physiological factors that make written signatures unique are also exhibited here
- Keystroke dynamics is a behavioral biometric
- Natural choice for computer login and network security



History

Brief History of Keystroke Biometrics

SRI International
develops first
hardware-based
implementation

Technology found
to comply with
NIST Computer
Security Act of
1987

*Technology
embedded into
consumer products
from cell phones to
home security*

WW-II

1979

1984

1988

2000

2001

Military Intelligence
identifies the "Fist
of the Sender"
method

National Bureau of
Standards study
finds technology to
be 98% effective

FSTC/IBG
Comparative
testing program
verifies keystroke
technology

- World War II
- Telegraph operators on many U.S. ships could recognize the sending operator
- "Fist of the Sender" the uniqueness in the keying rhythm (even of Morse-code), could distinguish one operator from another.

http://www.wsta.org/publications/articles/1003_article06.html

State Of Art-1 Features



- Keystroke dynamics is not what you type, but how you type
- Features commonly used to describe a user's typing pattern are
 - Latencies between successive keystrokes (the elapsed time between the release of the first key and the depression of the second).
 - Duration of each keystroke (How long is the key held down).
 - Finger placement.
 - Pressure applied on the keys .
 - Overall typing speed.
- For known regularly-typed strings (e.g., username and password), such features are quite consistent
- However, features are a function of the user and the environment

State Of Art-2

Static vs. Continuous



- In static verification, the keystrokes are analyzed only at specific times e.g., during login.
- Static approaches provide more robust user verification than simple passwords.
- But static methods do not provide continuous security –they cannot detect substitution of the user after the initial verification.
- Continuous verification monitors the user’s typing behavior throughout the session; can be used to detect uncharacteristic typing rhythm caused by say drowsiness.

Monrose and Rubin, “Keystroke dynamics as biometrics for authentication”, Future Generation Computer Systems 16 (2000), 351-359.

Problem description

- It is important to know if we can still depend on keystroke dynamics to authenticate people when they run different applications.

example Java Vs Chat on Msn

- Our target in this project is to investigate this problem, and try to assure the stability of keystroke dynamics techniques.

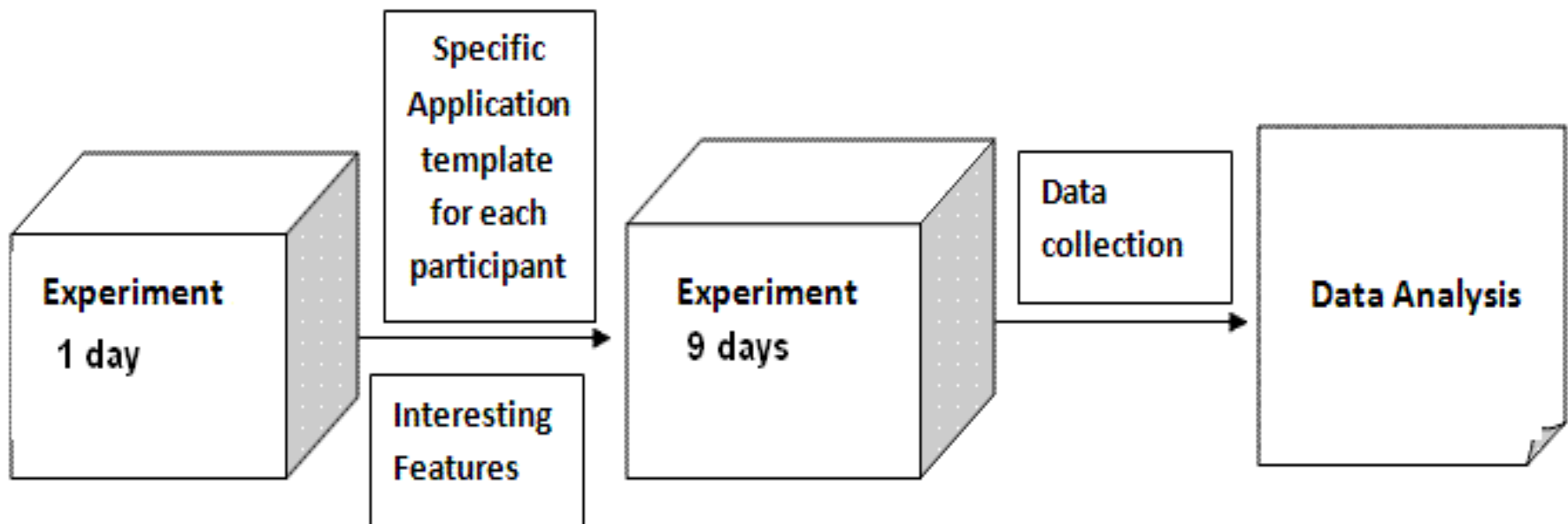
Justification, motivation and benefits

- keystroke Dynamics will strengthen the security of the system. Even after logging into the system, the user needs to know how to type.

Research Questions

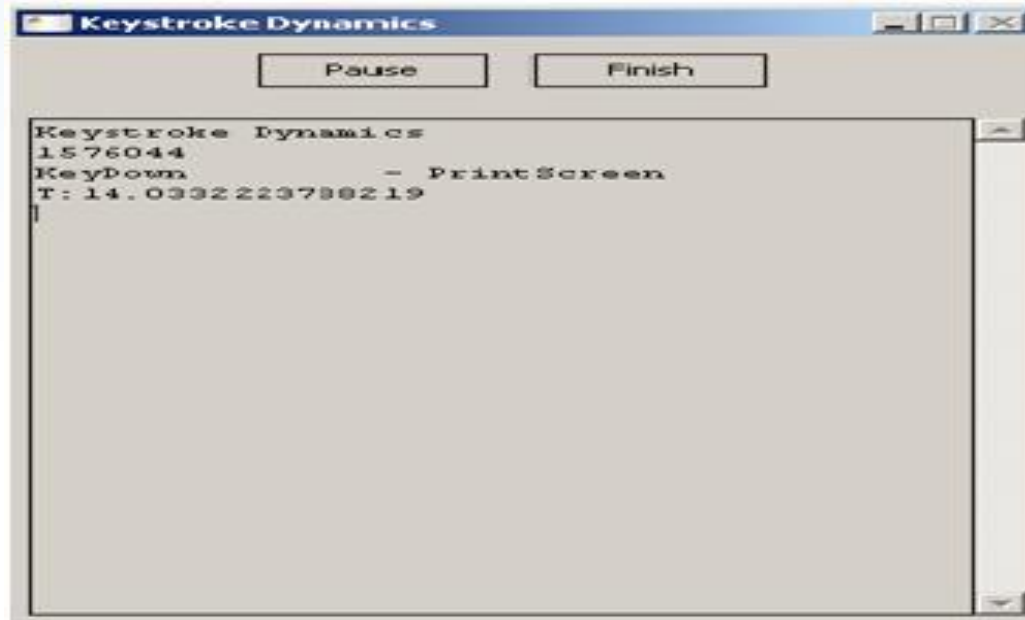
- How are typing characteristics different from one application to another and where are the similarities?.
- How we can benefit from the results of those differences and similarities to generate a reliable template to authenticate a user regardless which application is used?.
- Is it possible to authenticate a person based on one general template or we need a set of application dependent templates?.
- Is it possible to say that the typing characteristics in application X is more stable than in application Y?.

Choice of Methods

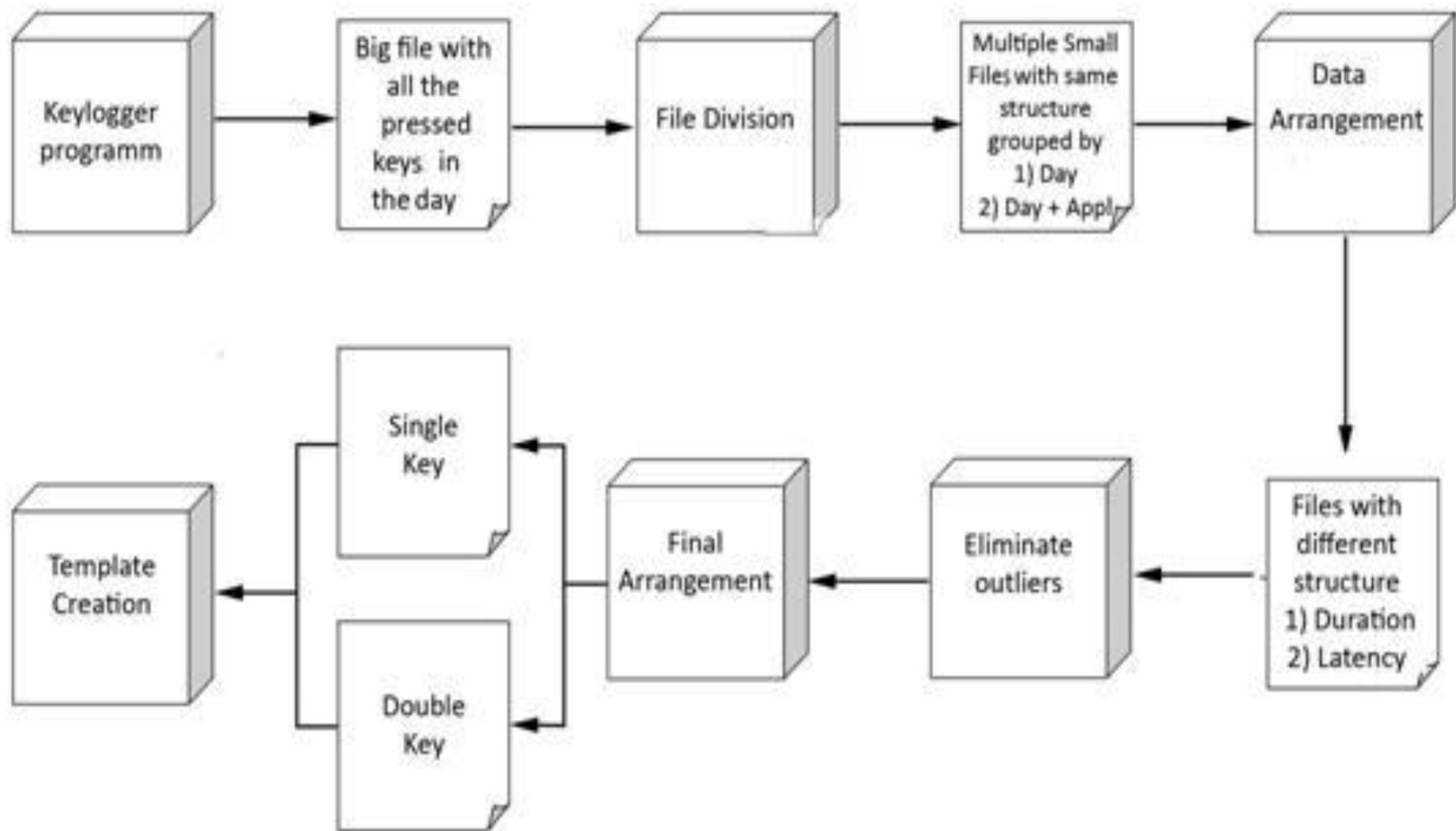


Experiment

- Collecting data
 - Keycondition KeyName Time App
- Program on c# . Net
- Participants 35, only 25 completed the Exp.



```
Keystroke Dynamics
1576044
KeyDown - PrintScreen
T: 14.0332223788219
```



Data analysis

- Analysis disregarding different applications
- Analysis considering different applications

Analysis disregarding different applications



- Template creation
- Procedure
- Distance metric
- Decision rule
- Analysis using different thresholds
- Penalty function

Template creation

- Interesting features (most common btw participants).
Back, Space, E, A, T, I, N, O, S,L, Comma and Period.
AT,NG, TH, HE, ME, AN, IC, IS, OF, TE, BE, CO, OR,
BY.
- 2 types of template
 - General Template: whole features
 - Personal Template: some features excluded according to
 - Occurence
 - Mean/Standar deviation



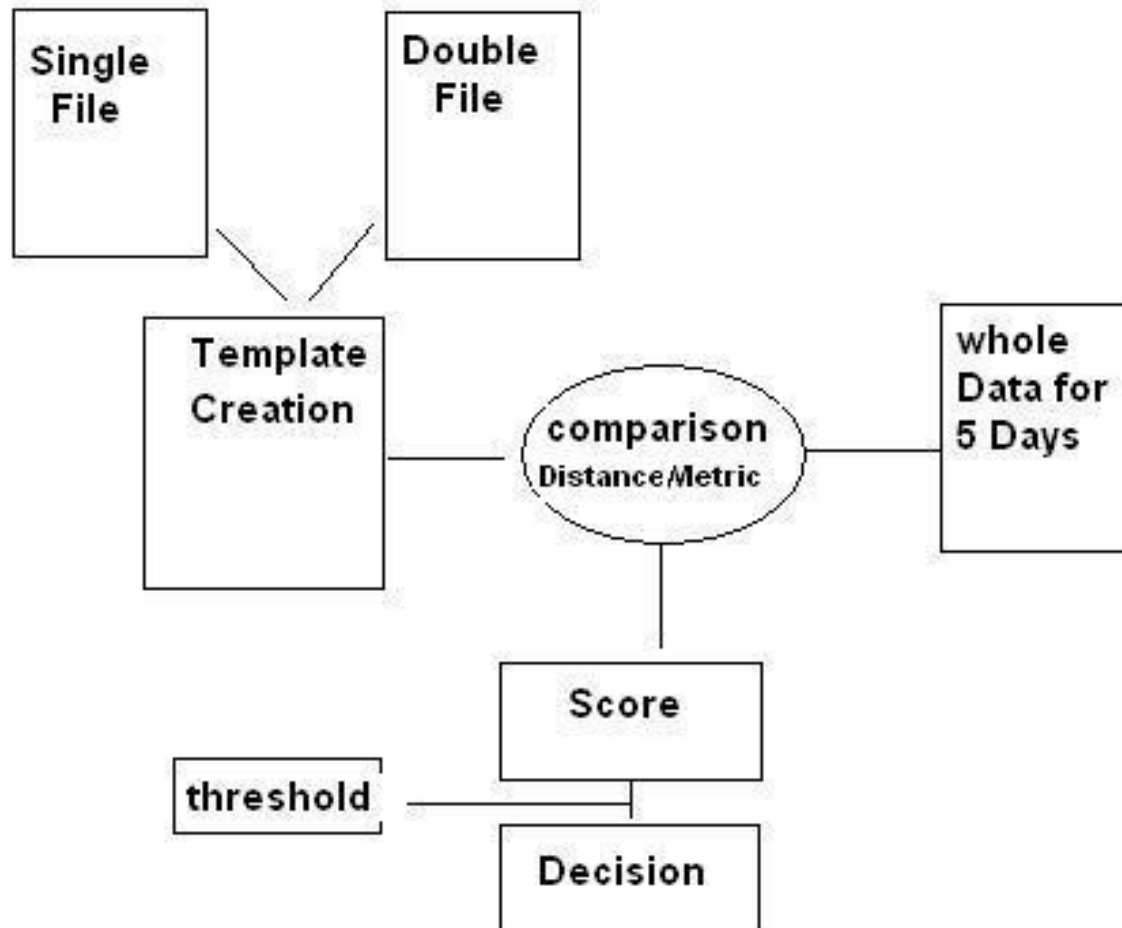
General Template

Feature	Dur mean 1st Key	Dur std 1st Key	Dur mean 2nd Key	Dur std 2nd Key	Latency mean	latency std	occur.
Space	0.08637580	0.01328496	X	X	x	X	1884
A	0.09000276	0.01615889	X	X	x	X	1451
I	0.07929272	0.01262098	X	X	x	X	1436
E	0.08230904	0.01348837	X	X	x	X	938
S	0.08313311	0.01454619	X	X	x	X	866
T	0.07853734	0.01329261	X	X	x	X	829
N	0.08163786	0.01490012	X	X	x	X	723
O	0.08061462	0.01668728	X	X	x	X	700
Back	0.07828552	0.03453691	X	X	x	X	633
L	0.08149716	0.01228543	X	X	x	X	317
OemPeriod	0.07346880	0.0172407	X	X	x	X	111
Oemcomma	0.08411327	0.011013509	X	X	x	X	98
AN	0.09203296	0.02295964	0.07565121	0.01639196	0.19993104	0.12558609	316
IS	0.07638905	0.01417211	0.07818376	0.01728256	0.18319768	0.12591701	281
ME	0.08338640	0.01349267	0.06650816	0.02535259	0.16544372	0.10750007	217
TE	0.06770484	0.01582099	0.07438959	0.01732062	0.18364483	0.08447577	214
OR	0.07472894	0.01528932	0.07166613	0.02260963	0.21820969	0.14488173	185
AT	0.08829169	0.02116809	0.06393712	0.01608110	0.22723099	0.11699529	180
NG	0.08352435	0.01185858	0.05745269	0.01626420	0.21217961	0.1472827	137
TH	0.07866979	0.01968767	0.07895768	0.01896588	0.27252661	0.16046803	130
BE	0.07752167	0.01643902	0.07890289	0.01921127	0.16378787	0.05837643	120
HE	0.07638126	0.01573692	0.08540163	0.02636182	0.16648760	0.08927590	95
OF	0.06862645	0.01082124	0.06874293	0.02191353	0.32288578	0.17615738	64
CO	0.08559011	0.02349451	0.09827384	0.03577344	0.19233384	0.11316296	53
BY	0.08159148	0.01364979	0.08049215	0.01429820	0.24434897	0.11784635	56
IC	0.07714354	0.01150201	0.07474248	0.01152103	0.48978481	0.14164011	52

Personal template

user\Features	Back	Space	E	A	T	I	N	O	S	L	Comma	Period
1	X	X	X	X	X	X	X	X	nc	X	X	X
2	X	X	X	X	X	X	X	X	X	X	X	X
3	nc	nc	X	X	X	X	X	X	X	X	X	nc
4	nc	X	X	X	X	X	X	X	X	X	X	X
5	X	X	X	X	X	X	X	nc	X	X	nc	X
6	X	X	X	X	X	X	X	X	X	X	X	X
7	nc	X	X	X	X	X	X	X	X	X	X	X
8	X	X	X	X	X	X	X	X	X	X	X	X
9	X	X	X	X	X	X	X	X	X	X	X	X
10	nc	X	X	X	X	X	X	X	X	X	X	X
11	X	X	X	X	X	X	X	X	X	X	X	X
12	nc	X	X	X	X	X	X	X	X	X	X	X
13	X	X	X	X	X	X	X	X	X	X	X	nc
14	nc	X	nc	X	X	X	X	nc	X	X	X	X
15	X	nc	X	X	X	X	X	X	X	X	X	X
16	nc	nc	nc	X	nc	nc	nc	nc	X	nc	nc	nc
17	nc	X	X	X	X	X	nc	X	X	X	X	nc
18	nc	X	nc	X	nc	X	nc	X	X	X	X	nc
19	nc	X	X	X	X	X	X	X	X	X	X	X
20	X	X	X	X	X	nc	X	X	X	X	X	X
21	nc	X	X	X	X	X	nc	X	X	X	X	nc
22	X	X	X	X	X	X	X	X	X	X	X	X
23	nc	X	X	X	X	X	X	X	X	X	X	nc
24	X	X	X	X	X	X	X	X	X	X	X	X
25	nc	nc	nc	nc	X	X	nc	nc	nc	nc	nc	nc

Procedure



Distance metric

- For single file

$$D = \left| \frac{t_K - \mu_K}{\sigma_K} \right|$$

k : Current Key.
 t_K : Duration time.
 μ_K : Mean from template.
 σ_K : Standard deviation from template.

- For Double file

$$D_{K1} = \left| \frac{t_{K1} - \mu_{K1}}{\sigma_{K1}} \right|$$

$$D_{K2} = \left| \frac{t_{K2} - \mu_{K2}}{\sigma_{K2}} \right|$$

$$D_L = \left| \frac{t_L - \mu_L}{\sigma_L} \right|$$

$$D = \frac{D_{K1} + D_{K2} + D_L}{3}$$

Where k_1 : First Key, k_2 : Second Key, L : is the latency, μ : Mean from template, σ : Standard deviation from template

Decision Rule

- A decision rule based on a predefined threshold is needed after applying the distance metric.
- Many decision rules could be applied.

$$\text{– Rule (1)} = \begin{cases} 0 & \text{if } D \leq T \\ 1 & \text{if } D > T \end{cases}$$

Where T is the predefined threshold and D is the distance.

$$\text{– Rule(2)} = \begin{cases} 0 & \text{if } D \leq T \\ D - T & \text{if } D > T \end{cases}$$

- Rule 2 is more realistic than Rule 1 since we have an idea of how bad the feature is typed.

Analysis using different thresholds



Threshold	FAR
0.5	7.04%
1.0	9.76%
1.5	12%

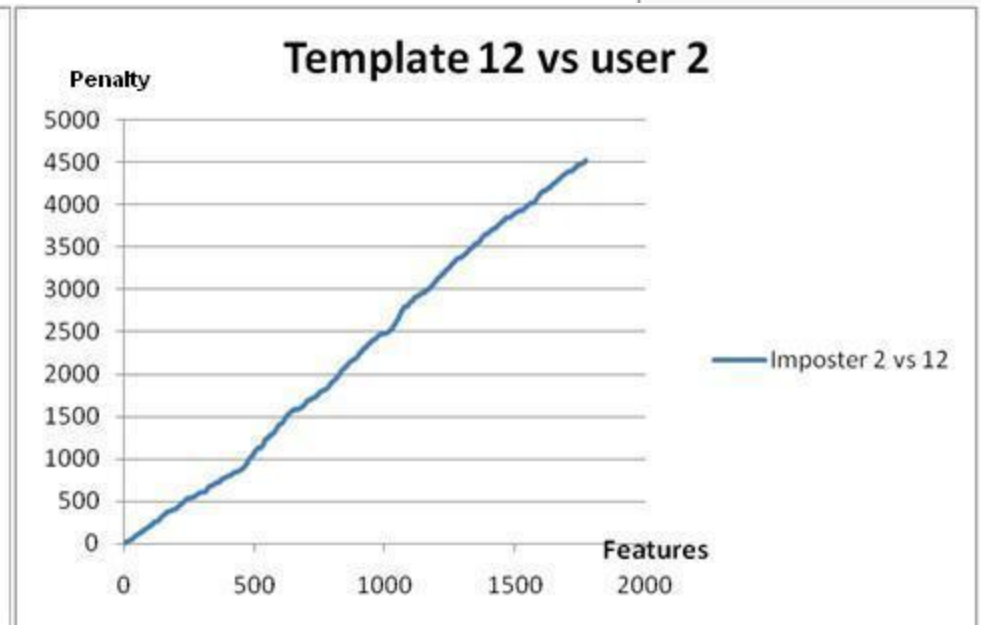
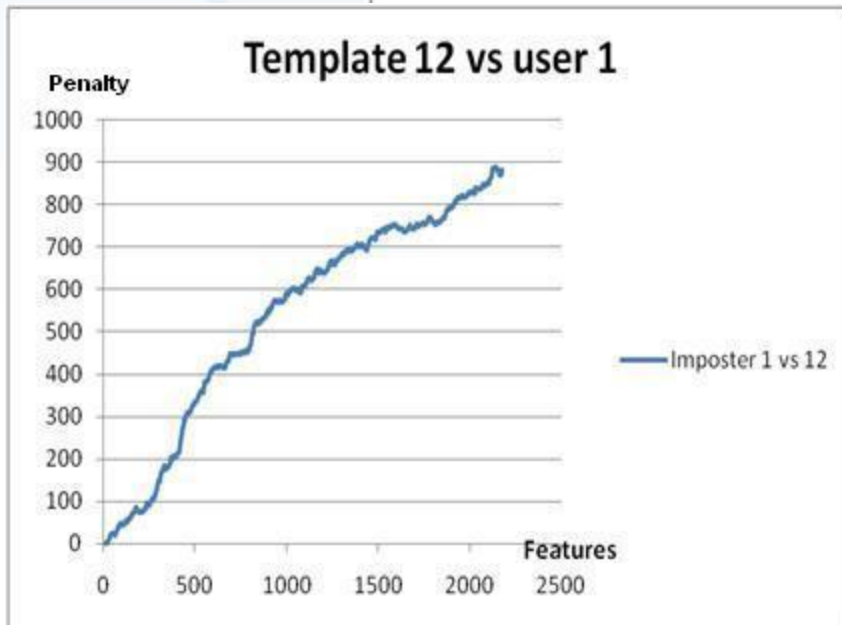
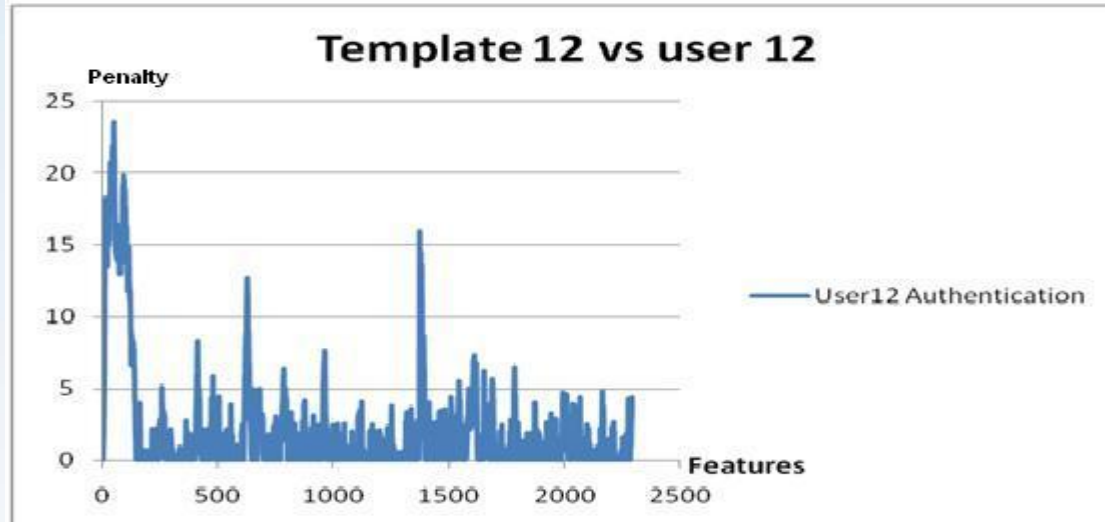
Penalty function

- Penalty (Feature) =

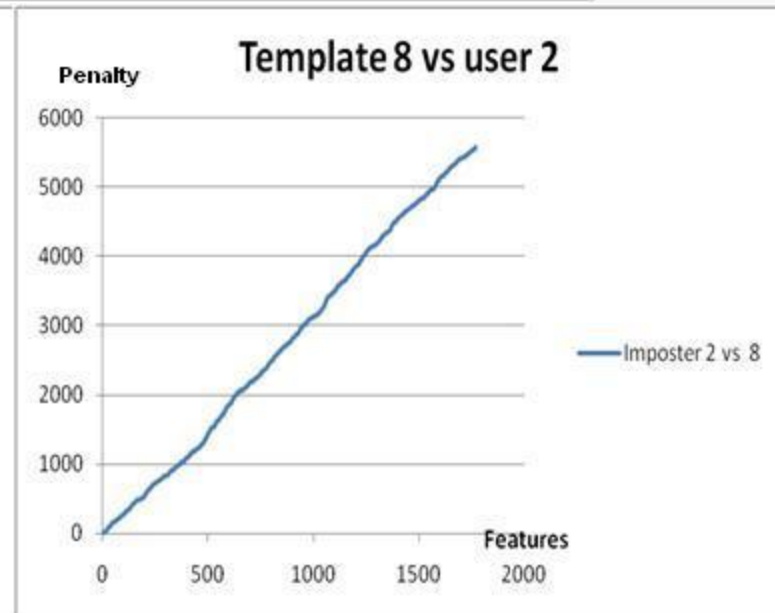
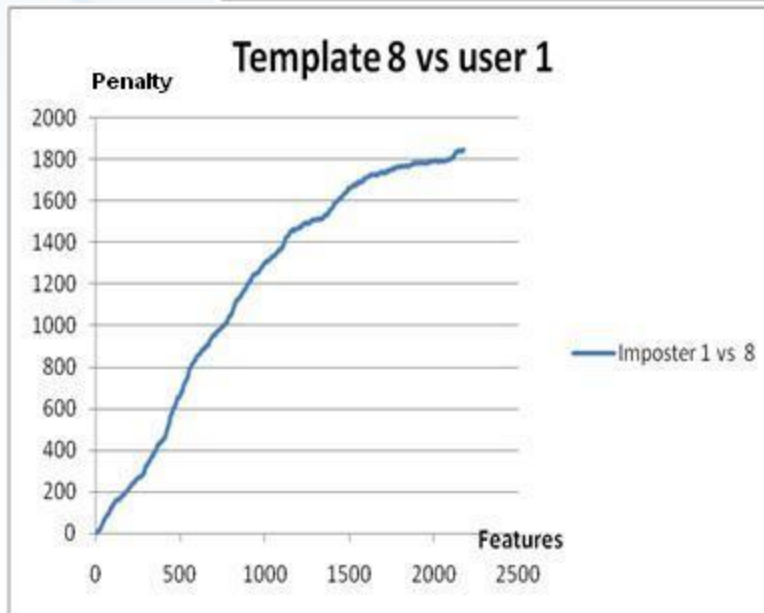
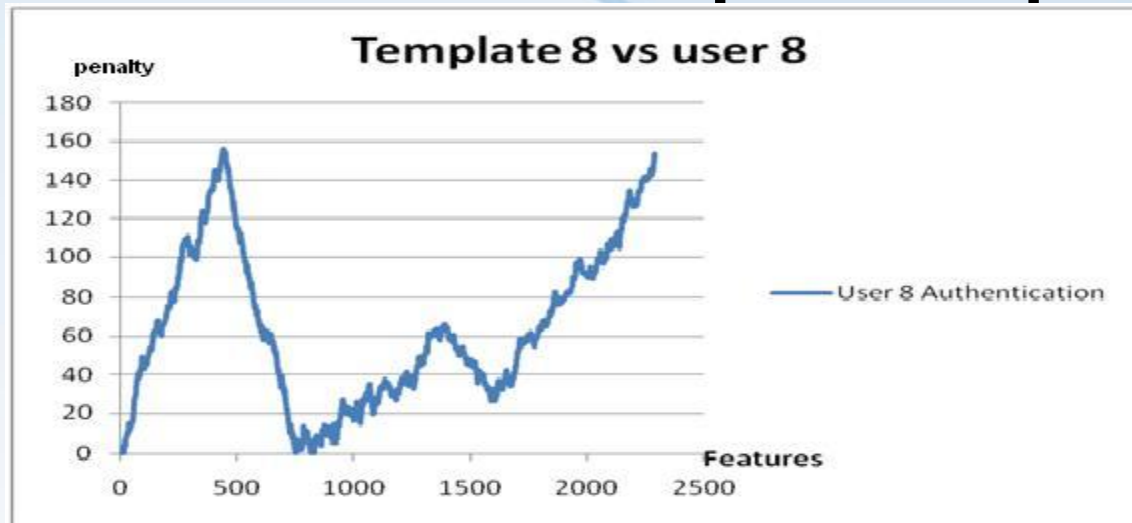
$$\begin{cases} 0 & \text{initial condition} \\ P + \text{Punishment} & \text{Mistake} \\ P - \text{Reward} & \text{Correct} \\ P + \alpha & \text{Not exist} \end{cases}$$

- P is penalty value , $P \geq 0$.
- Punishment: $D-T$, Reward: predefined value
- α small value = 0.01.

Very consistent participant



Non consistent participant



Analysis considering different applications



- Classification.
- Template creation.
- Analysis applying Penalty function.

classification

User/Application Group	Group X Text Editors	Group Y Browsers	Group Z Instant Messages
1	X	X	X
2	X	X	NA
3	X	X	X
4	NA	X	X
5	X	X	X
6	NA	X	X
7	NA	X	X
8	NA	X	X
9	X	X	X
10	X	X	X
11	X	X	X
12	NA	X	X
13	NA	X	X
14	X	X	X
15	NA	X	X
16	NA	X	X
17	NA	X	X
18	NA	X	X
19	NA	X	NA
20	X	X	NA
21	X	X	X
22	NA	X	X
23	NA	X	X
24	NA	X	X
25	X	X	X



Template Creation

- General and personal template still used
- Application based template
- Each user has 3 application based templates.

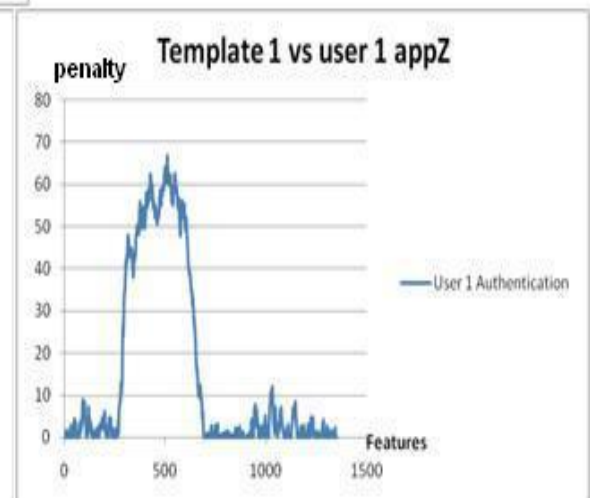
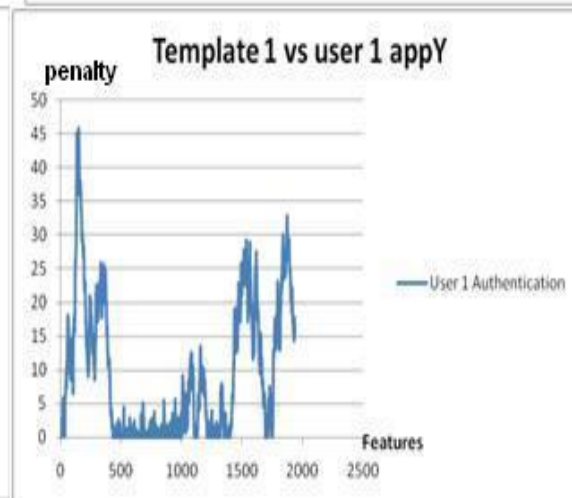
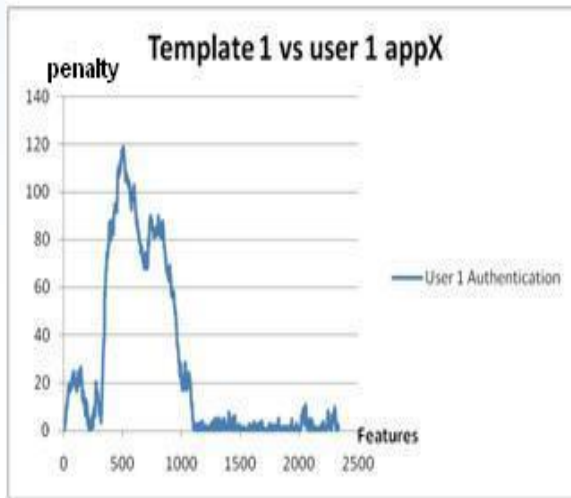
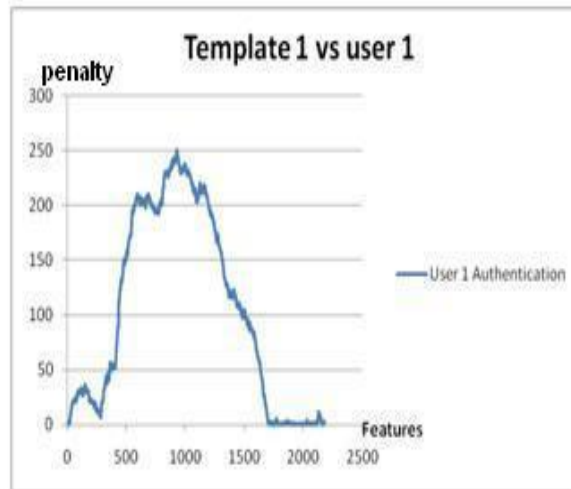


Penalty function+Rule 2 +T=0.5

- Since we got the best results using rule 2 and $T = 0.5$ we decide to use the same in this part.

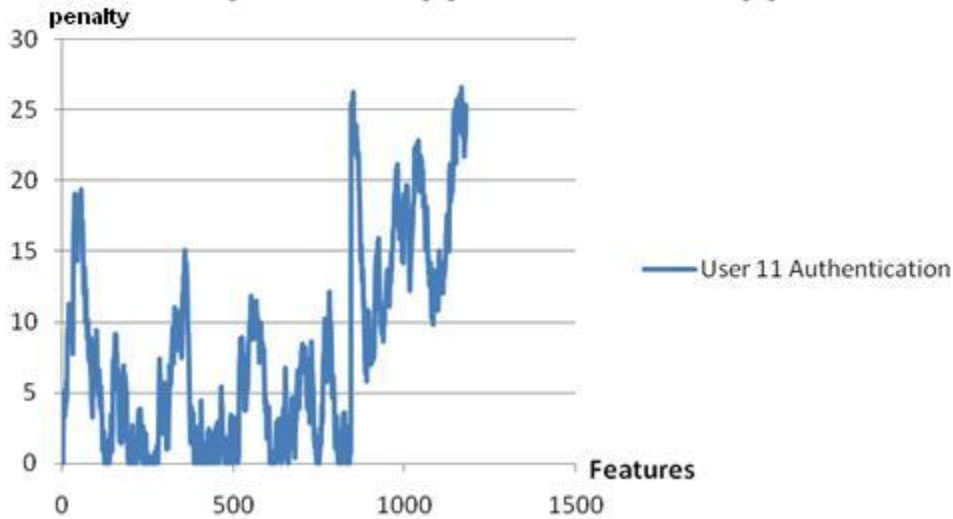
0	<i>initial condition</i>
$P + \text{Punishment}$	<i>Mistake</i>
$P - \text{Reward}$	<i>Correct</i>
$P + \alpha$	<i>Not exist</i>

Same application

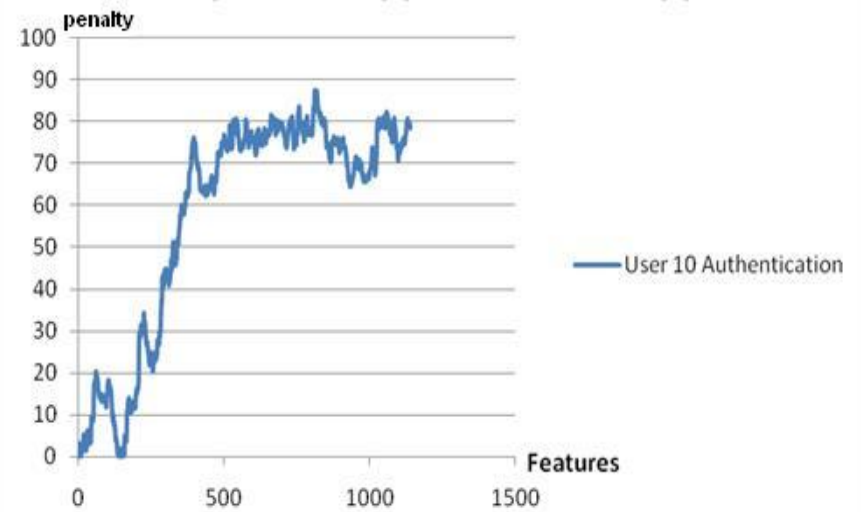


Different application

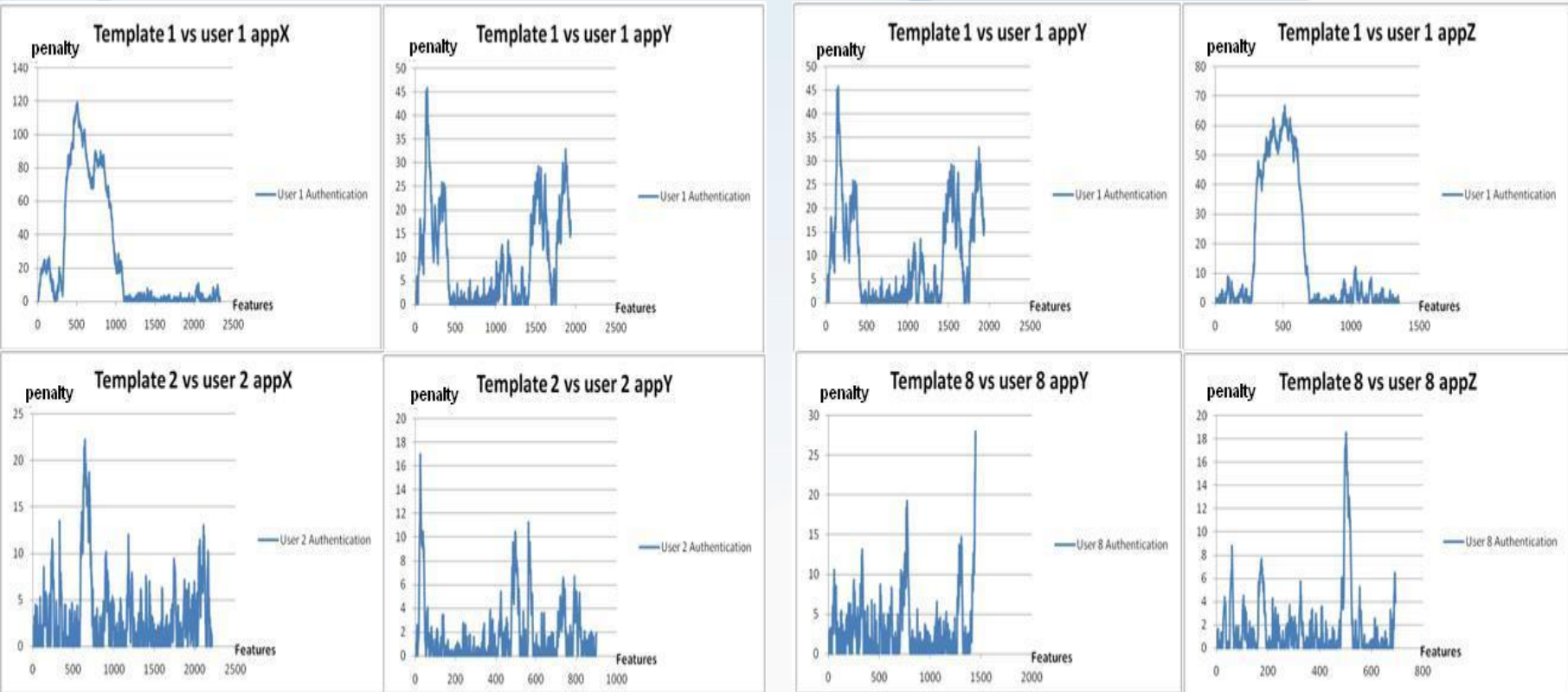
Template 11 appY vs user 11 appX



Template 10 appY vs user 10 appX



Application stability



Comparison 1 & 2

- Number of features before rejection
- Disregarding application.

DVT	1	2	3	4	5	6	7	8	9	10	11	12	13	14	15	16	17	18	19	20	21	22	23	24	25
1	0	128	291	204	158	147	246	65	42	273	143	108	255	408	277	97	260	229	187	101	313	171	306	226	89
2	76	0	79	60	279	117	109	14	11	121	53	46	97	93	111	37	84	60	175	278	71	45	68	88	87
3	200	117	0	174	138	107	208	115	117	232	162	138	212	259	186	50	316	198	126	100	282	186	232	195	131
4	292	118	418	0	160	163	329	99	131	236	291	295	433	474	380	54	498	203	160	99	321	223	309	421	100
5	54	182	66	48	0	103	99	32	33	83	46	39	85	64	99	47	71	47	110	196	52	39	51	78	179
6	103	291	121	97	329	0	212	54	51	232	82	78	176	140	218	60	139	82	329	206	104	69	97	149	108
7	226	146	395	323	190	176	0	90	117	374	245	247	517	357	535	78	453	168	208	116	267	192	243	481	142
8	228	138	178	159	155	141	205	0	70	233	118	121	150	322	293	48	224	261	183	105	150	167	210	100	98
9	161	104	316	192	145	106	219	78	0	170	296	138	297	203	220	79	406	166	114	98	200	176	183	268	131
10	204	214	180	114	228	159	180	116	55	0	90	92	148	261	235	85	161	137	227	162	170	91	169	150	161
11	186	113	365	213	142	122	251	92	175	208	0	161	362	257	188	184	481	214	144	100	252	197	215	250	51
12	469	115	621	591	152	149	353	137	147	306	352	0	553	731	377	194	705	283	159	96	529	320	511	449	58
13	151	147	205	167	224	173	311	67	81	144	164	127	0	192	304	73	279	122	167	120	161	116	152	300	92
14	232	130	228	160	155	136	195	105	79	217	139	127	219	0	180	103	232	188	169	107	230	128	214	173	100
15	224	181	255	182	214	185	296	104	75	412	145	144	287	247	0	81	272	156	246	133	209	140	199	263	179
16	84	142	86	61	165	100	102	48	36	120	56	50	98	98	110	0	89	72	125	125	78	53	75	85	194
17	178	139	444	211	175	149	356	89	123	291	237	171	401	253	271	69	0	179	166	115	246	193	209	326	92
18	264	96	313	170	116	106	168	154	106	194	174	128	212	336	181	82	285	0	125	81	329	199	294	163	128
19	145	316	112	106	377	233	202	67	51	223	86	86	192	166	181	79	139	89	0	227	114	69	114	149	89
20	65	271	73	54	314	113	99	37	34	97	52	43	90	70	118	158	79	53	140	0	58	44	57	89	131
21	417	85	382	193	118	116	190	195	88	178	167	145	243	386	214	74	343	546	122	74	0	238	401	207	170
22	374	95	511	250	127	109	222	165	127	206	239	176	285	429	247	108	428	420	123	82	515	0	418	250	324
23	291	133	302	223	160	152	266	124	96	266	164	169	280	368	316	74	304	209	190	105	298	170	0	249	213
24	127	166	194	141	257	198	333	62	87	226	147	105	298	167	329	82	233	108	155	144	125	104	122	0	200
25	137	116	180	124	144	117	171	73	80	138	106	94	153	173	170	61	174	117	134	101	150	96	136	153	0

Comparison 1 & 2 Means



user	disregarding	same	different
1	197	106	193
2	94	54	x
3	174	94	171
4	258	136	286
5	79	46	81
6	146	80	138
7	261	138	285
8	169	95	219
9	186	100	206
10	157	86	160
11	205	109	226
12	348	181	344
13	168	91	181
14	164	90	177
15	200	107	212
16	93	54	95
17	211	113	230
18	183	98	202
19	150	82	x
20	97	56	x
21	221	117	217
22	260	137	278
23	213	113	220
24	171	92	166
25	129	71	127

Conclusion

- Knowing application in advance is much better.
- No matter what application the user use still this user can be authenticated.
- More various applications are needed to generalize the previous point.
- Some applications show a higher stability than others.



Questions