SILK-TV

Secret Information Leakage from Keystroke Timing Videos

September 3rd, 2018 *ESORICS 2018 - Barcelona*

Kiran Balagani*, Mauro Conti§, Paolo Gasti*, Martin Georgiev+, Tristan Gurtler*, ***Daniele Lain***§, Charissa Miller*, Kendall Molas*, Nikita Samarin+, Eugen Saraci§, Gene Tsudik+, Lynn Wu*

** New York Institute of Technology*
USA

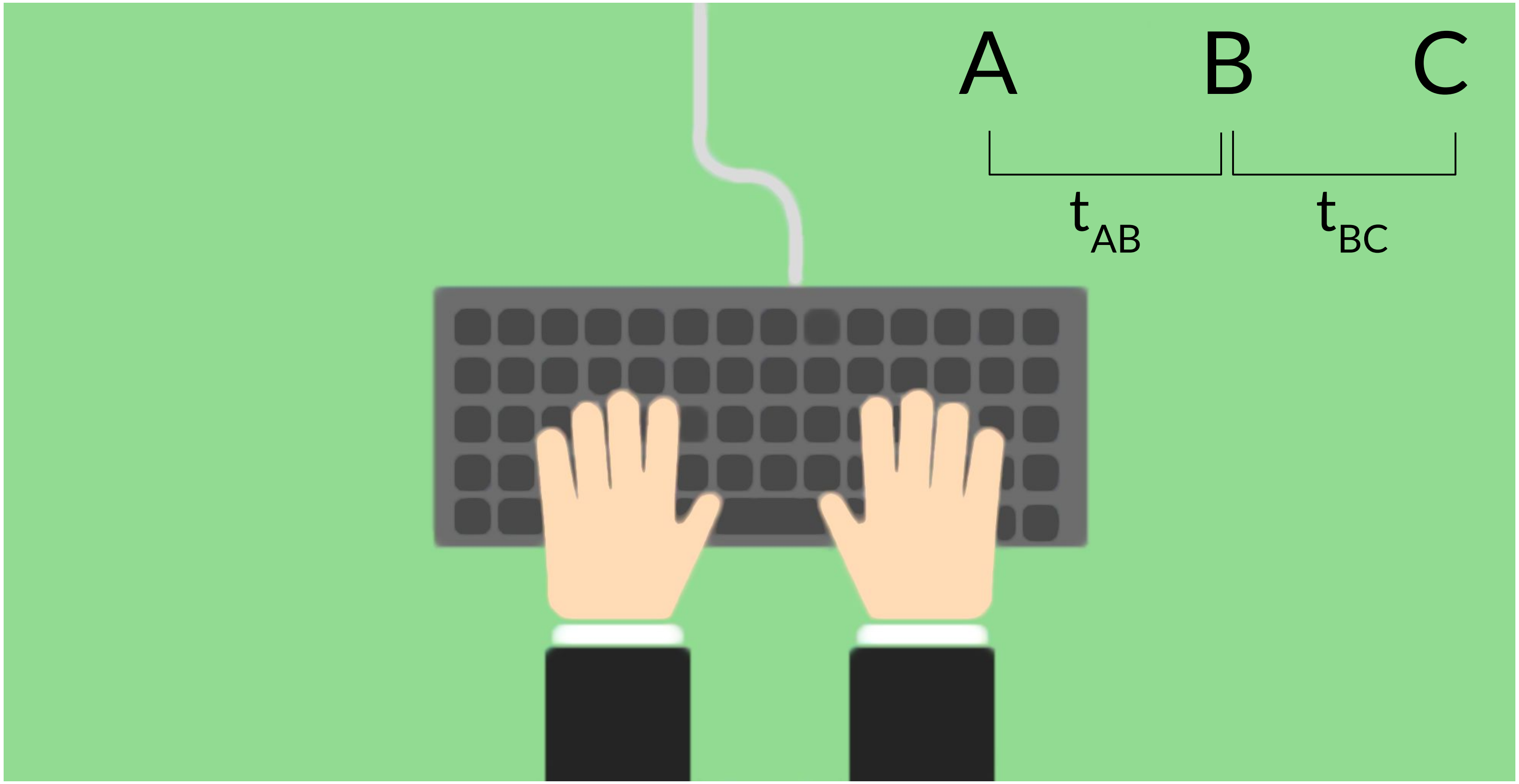
§ University of Padua
Italy

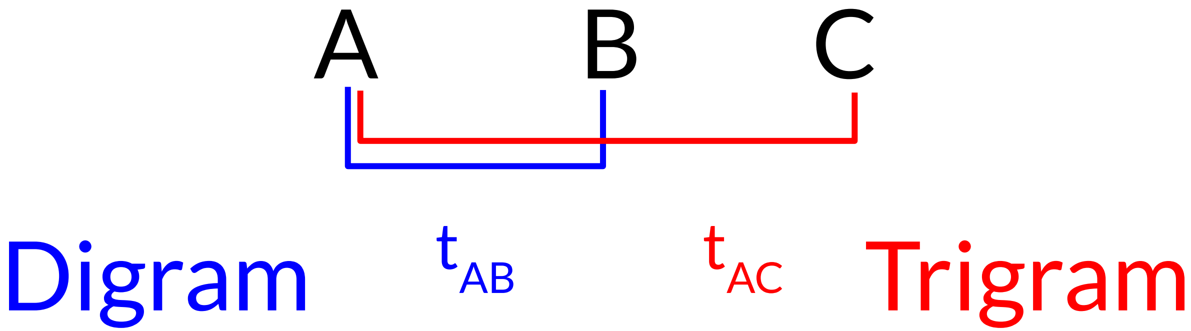
+ University of California, Irvine
USA

A

A
B

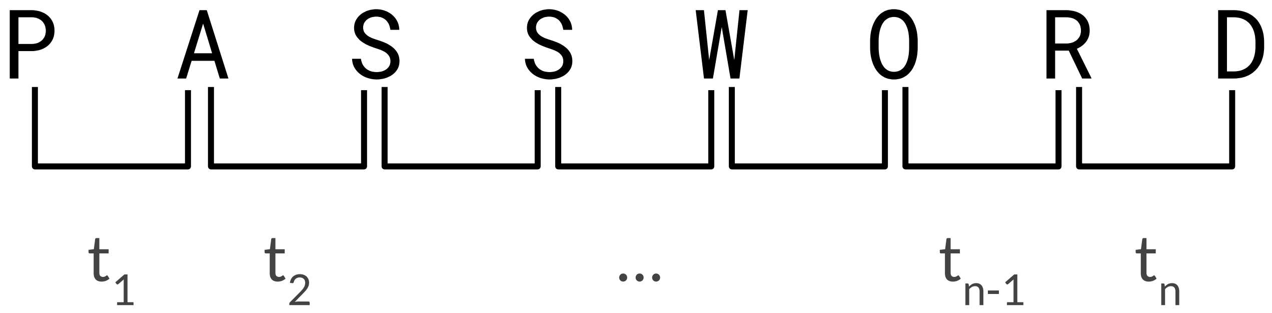
A
B
C


A
B
C
t_{AB}
t_{BC}



A B C

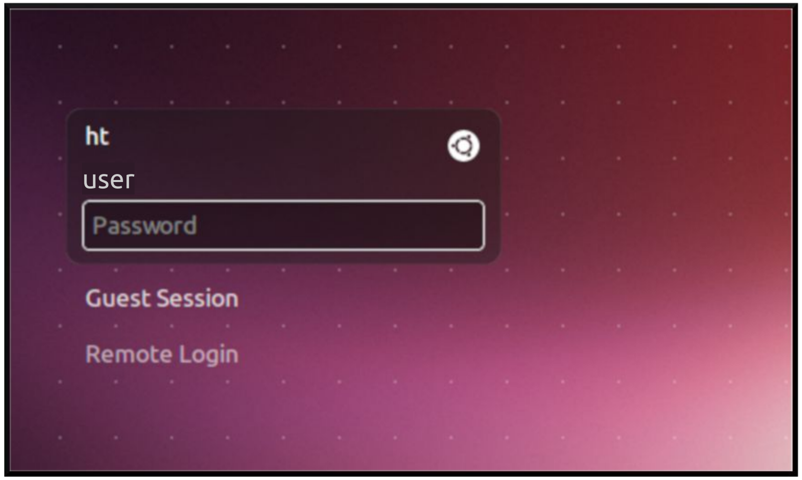
Digram t_{AB} t_{AC} Trigram



P A S S W O R D

t_1 t_2 … t_{n-1} t_n

- Inter-keystroke times as a personal *signature*
- Used as biometric in authentication systems



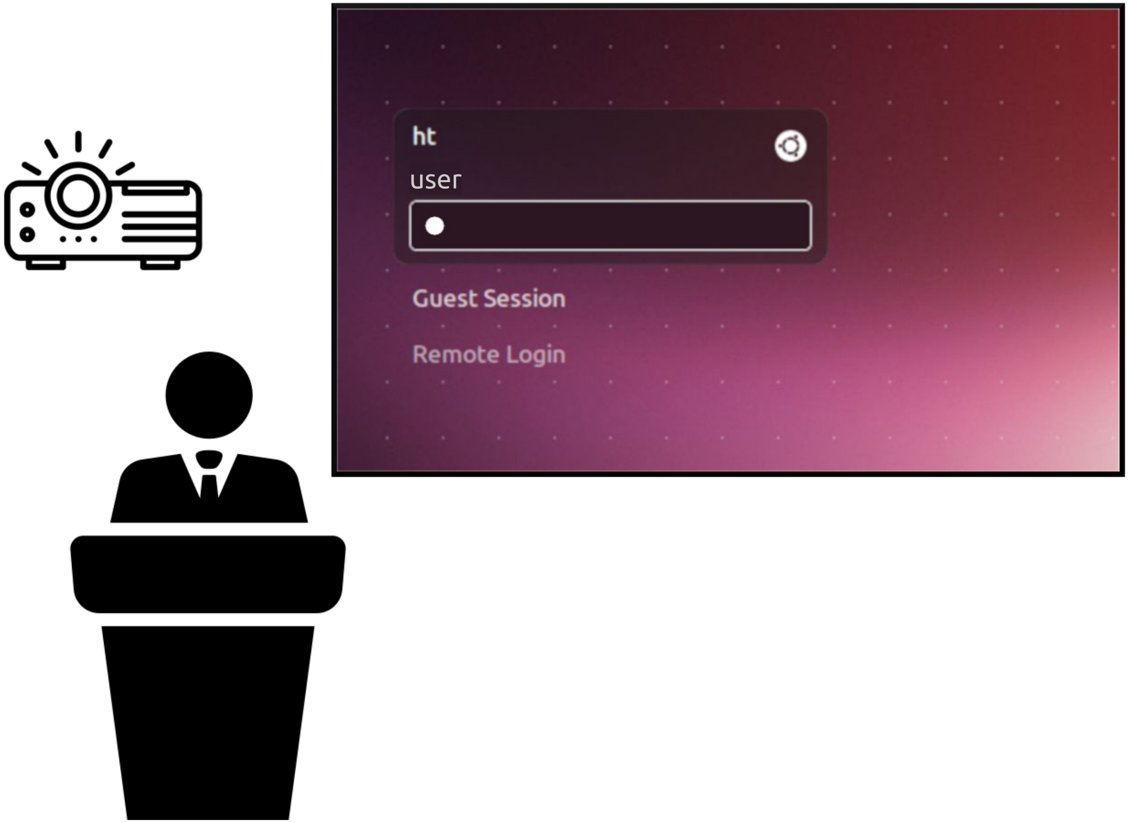
ht

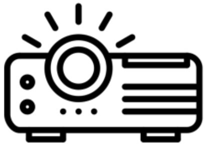
user

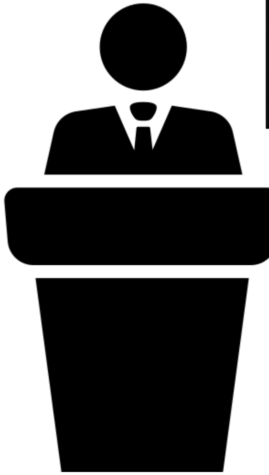
Password

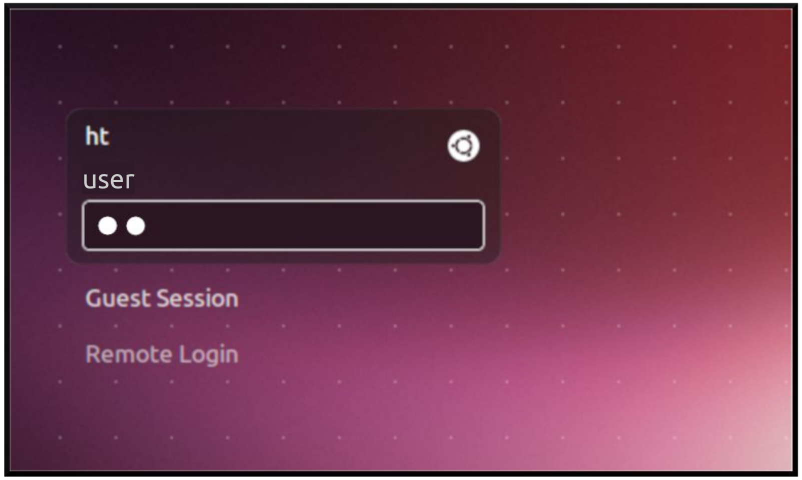
Guest Session

Remote Login


ht
user
●
Guest Session
Remote Login







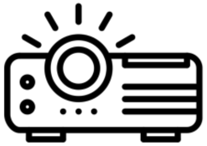
ht

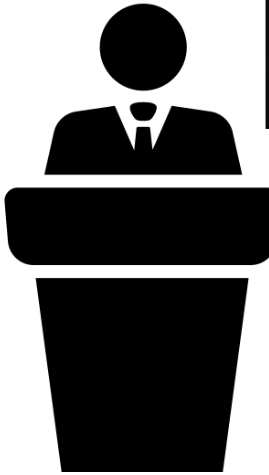
user

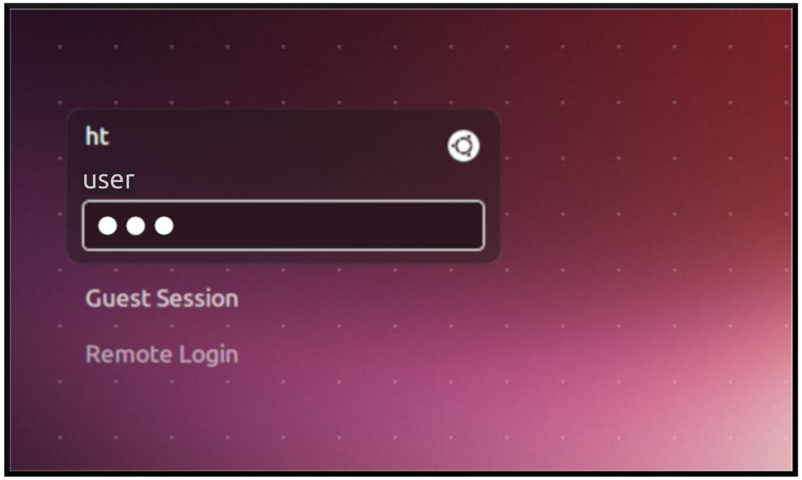
●●

Guest Session

Remote Login







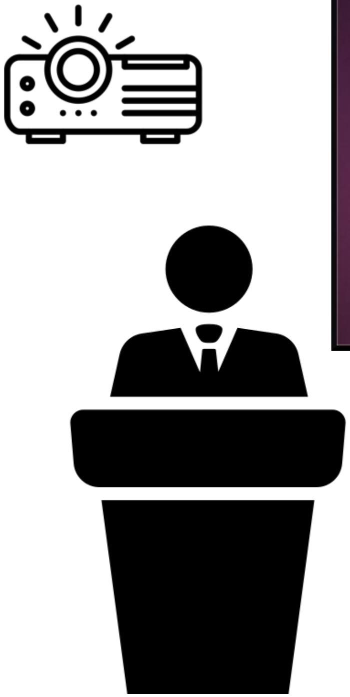
ht

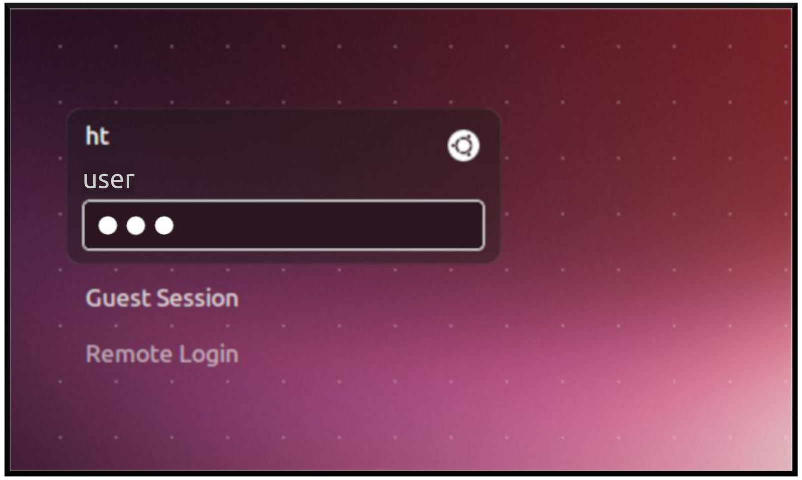
user

●●●

Guest Session

Remote Login





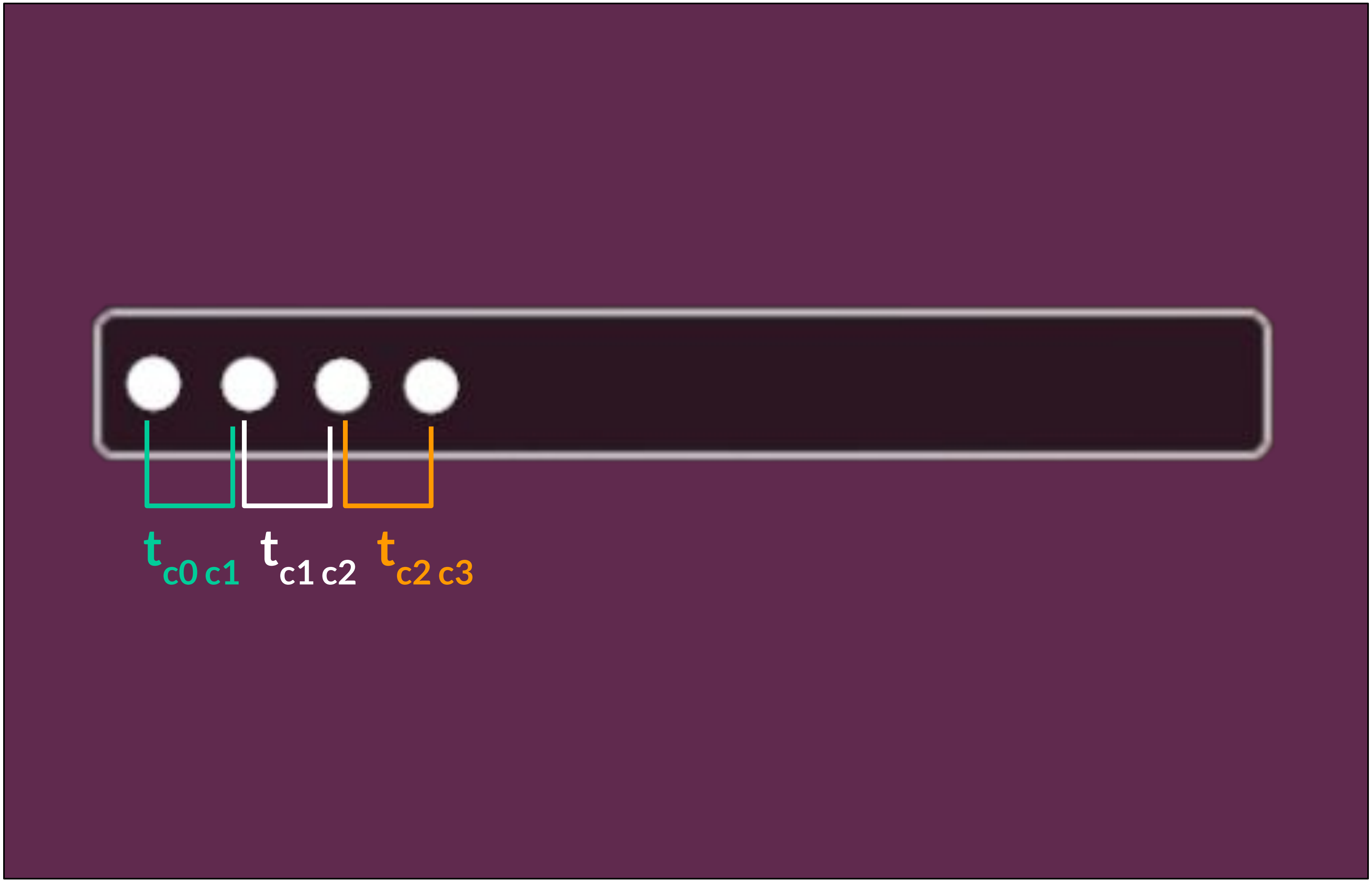
ht

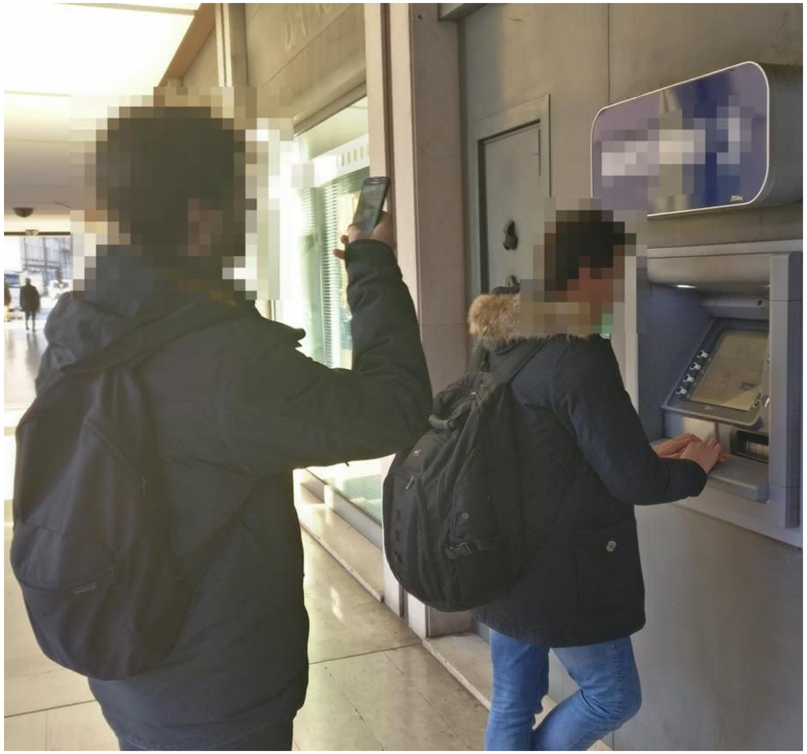
user

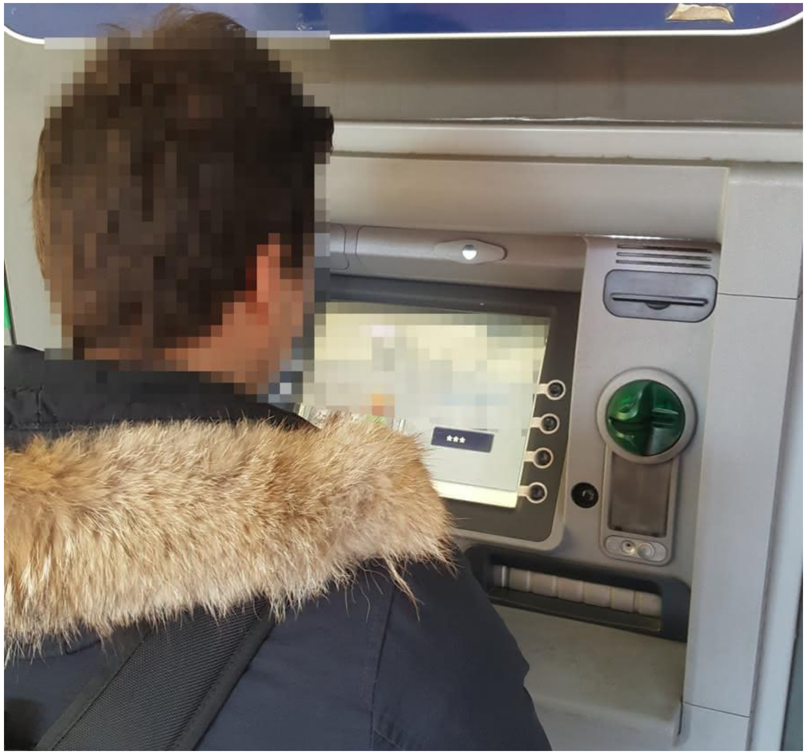
●●●

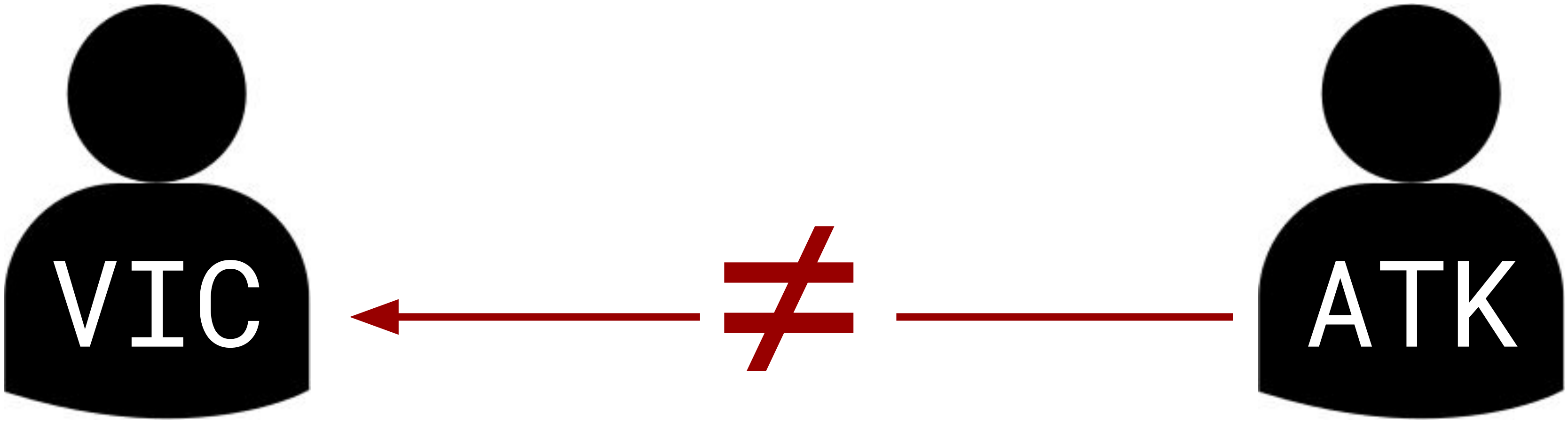
Guest Session

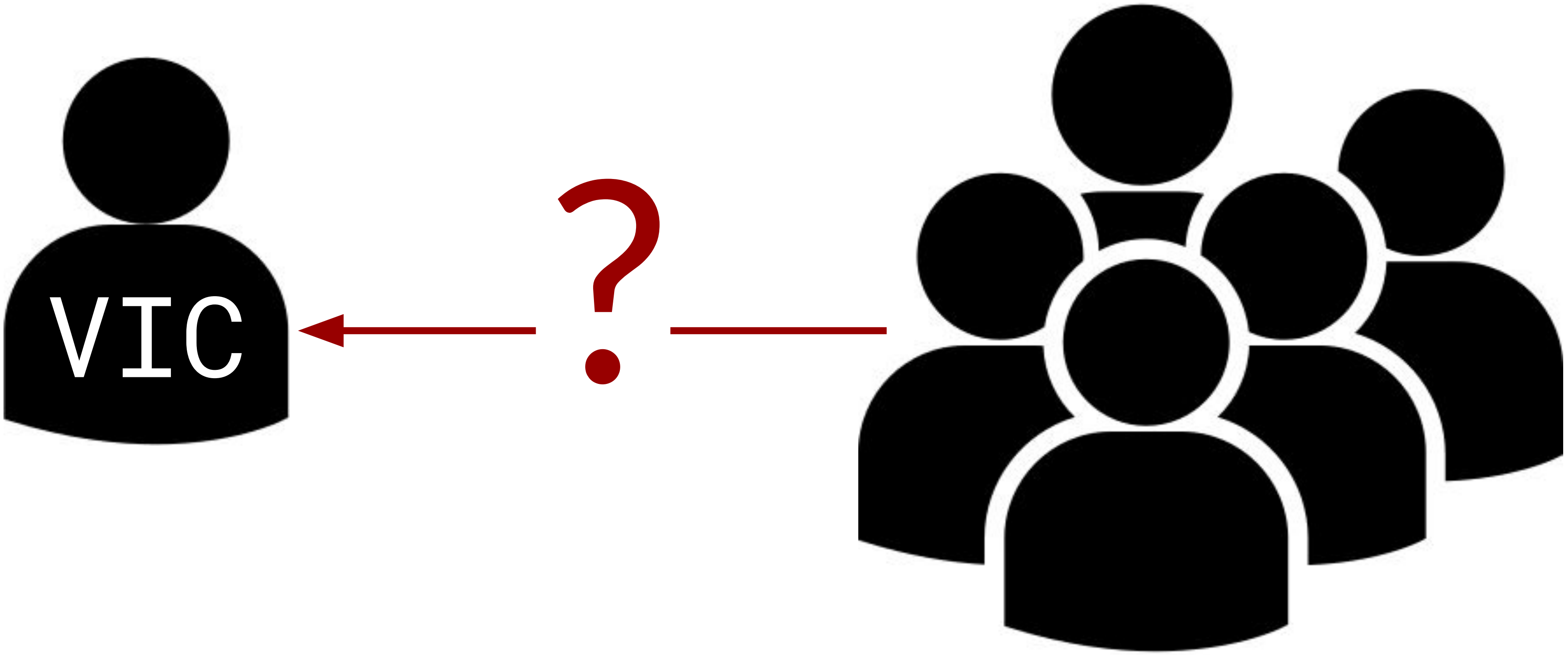
Remote Login


$t_{c0\ c1}$
$t_{c1\ c2}$
$t_{c2\ c3}$





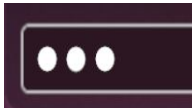

VIC
≠
ATK


VIC
?

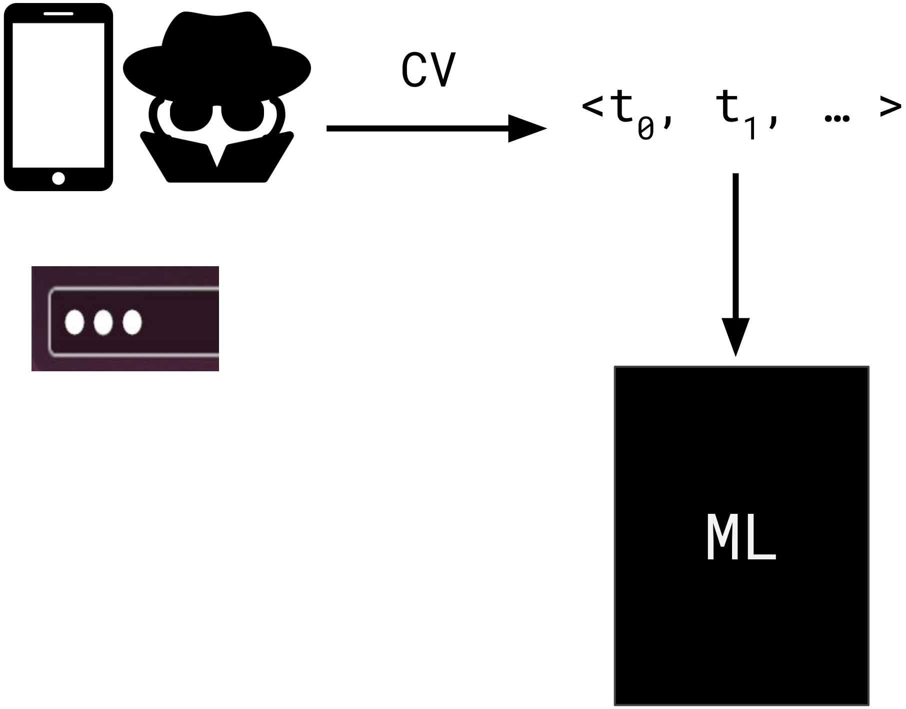
Contributions

- Quantify information leakage of on-screen keystroke feedback
- Novel attack: *SILK-TV*
  - *Uses public datasets only from multiple sources ("population data")*
  - *Machine Learning to guess typed text (passwords and PINs)*

SILK-TV



SILK-TV

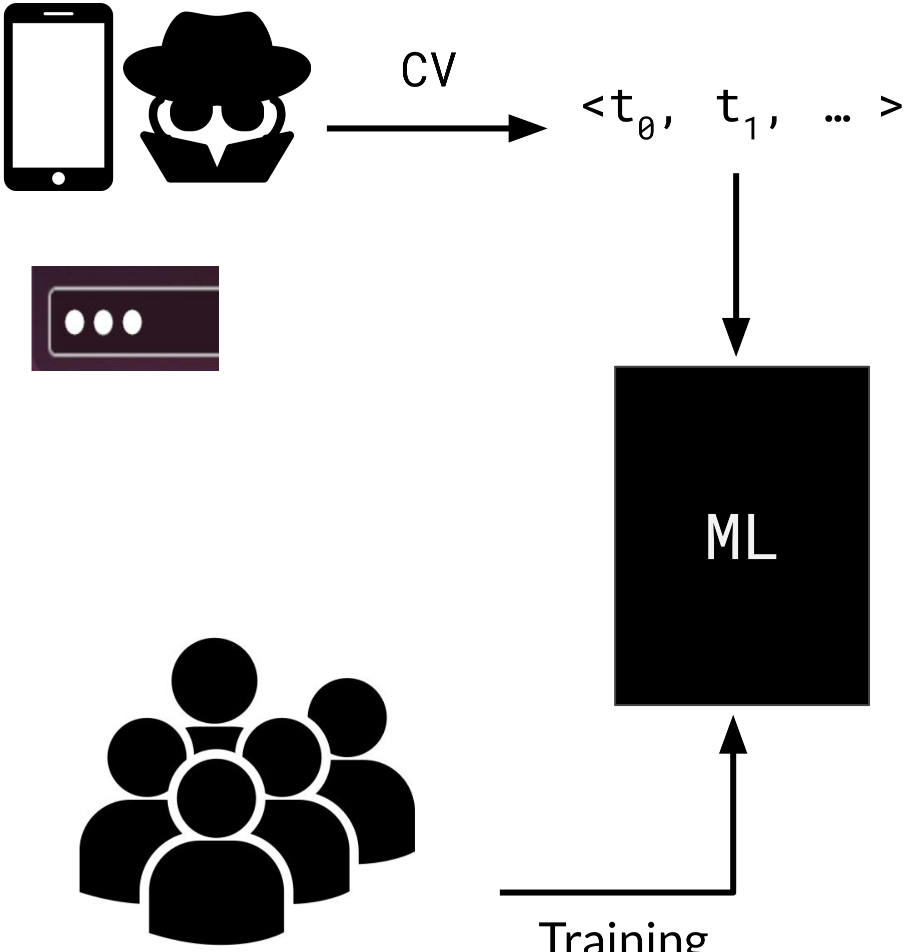


CV

$<t_0, t_1, … >$

ML

SILK-TV



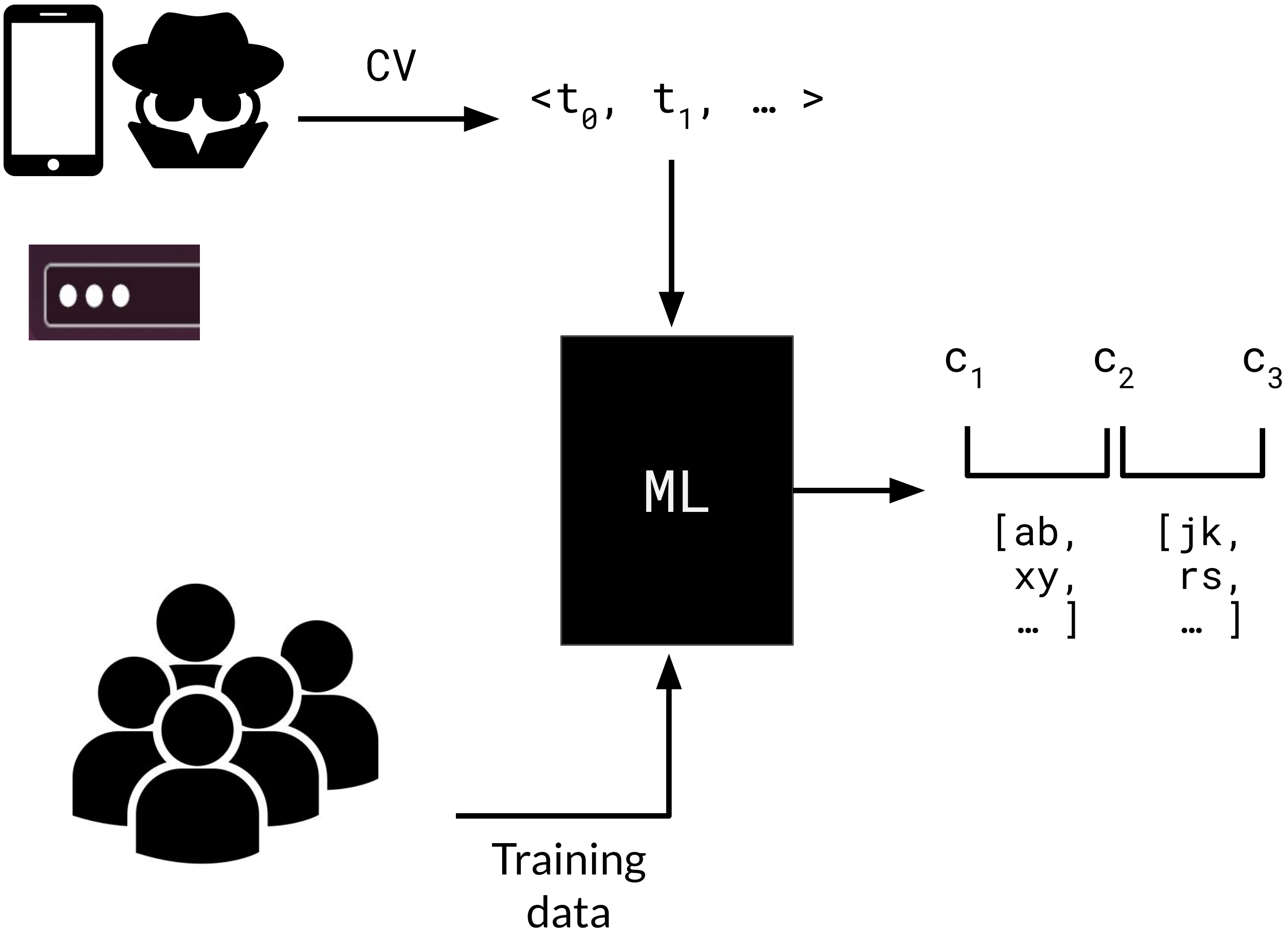
CV

$<t_0,\ t_1,\ \dots >$

ML

Training data

SILK-TV



CV

$<t_0, t_1, \ldots >$

ML

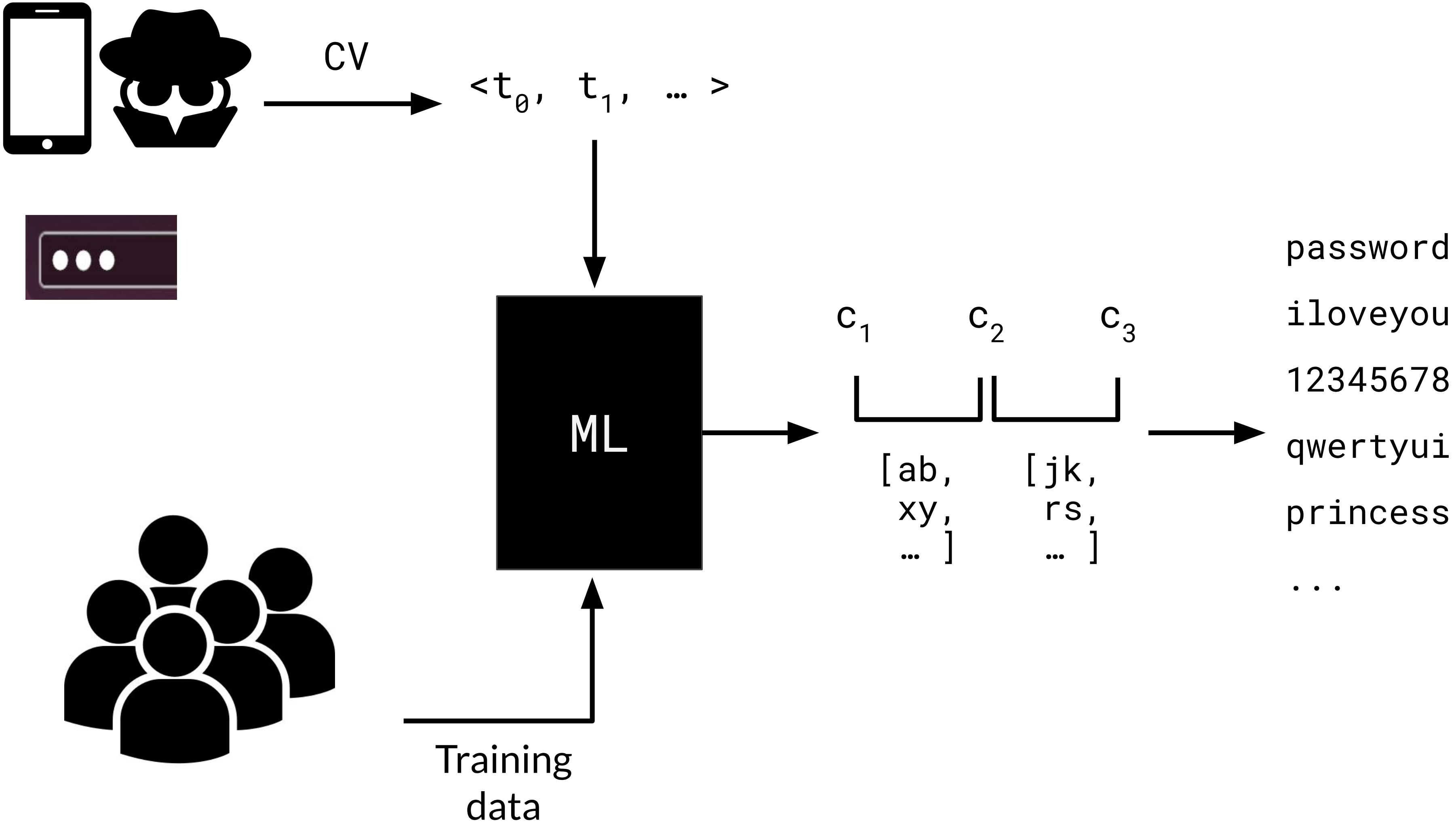
c_1 c_2 c_3

[ab, xy, …]

[jk, rs, …]

Training data

SILK-TV



CV

$\langle t_0, t_1, \ldots \rangle$

ML

Training data

c_1 c_2 c_3

[ab, xy, …] [jk, rs, …]

password

iloveyou

12345678

qwertyui

princess

...

Data Collection

- Passwords
  - Data from **projector** and **laptop screen** @ 60Hz
  - Recorded with a smartphone
  - 62 users - 3 times each pwd - *touch* typing on keyboard
  - `jillie02, william1, 123brian, lamondre`

- PINs
  - Data from **screen** @ 60Hz
  - Recorded with a videocamera
  - 22 users for 3 sessions - 12 times each PIN - on a ATM numpad
  - 15 selected PINs

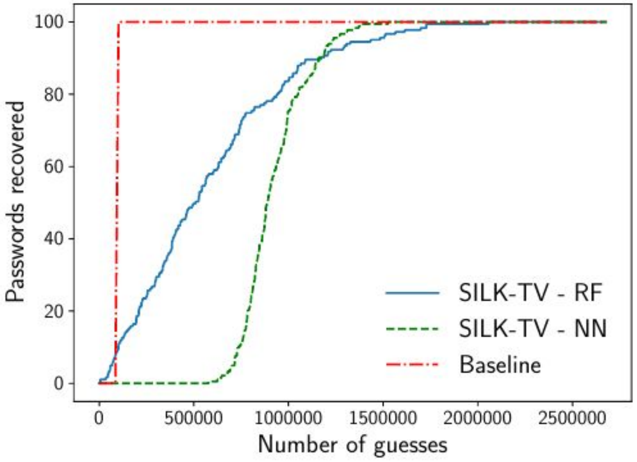
Evaluation - Passwords

- Baseline: password list sorted by frequency
  - “Best” strategy for a zero-information attacker

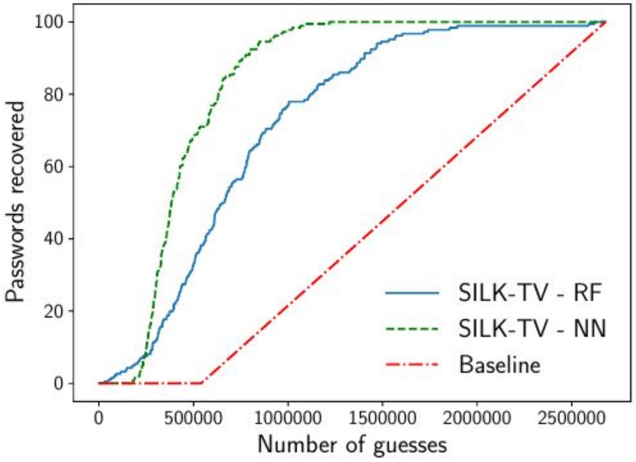
`123brian`	-	93,874th	
`jillie02`	-	1,753,571st	
`lamondre`	-	397,213rd	
`william1`	-	187th	← *very frequent password*

- Evaluation scenarios
  - *“Single shot”*
  - *“Multiple recordings”* (e.g., professor at lectures)

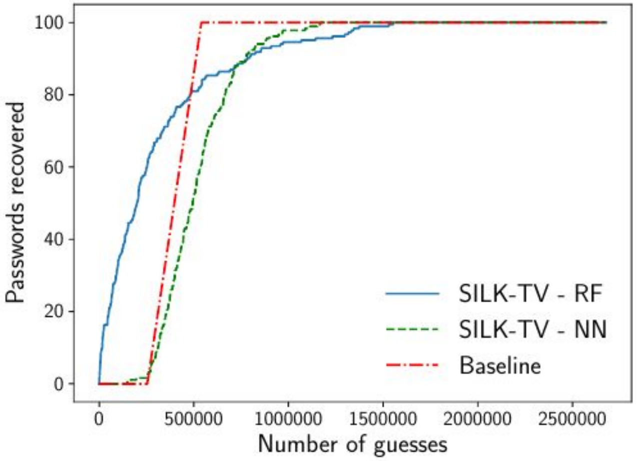
Password - “Single Shot” results



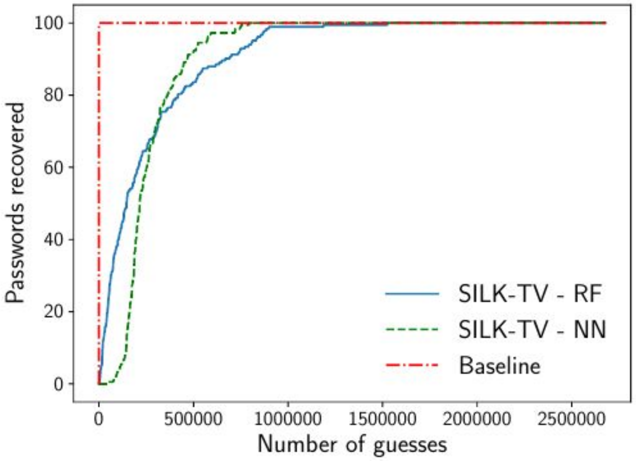
(a) `123brian` (183 auth. attempts).



(b) `jillie02` (186 auth. attempts).

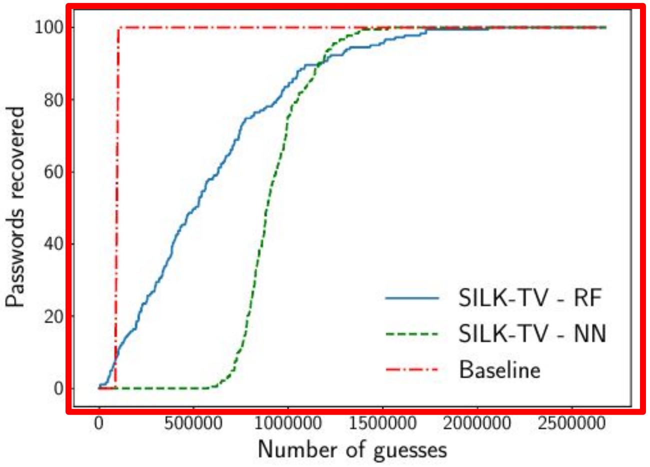


(c) `lamondre` (184 auth. attempts).

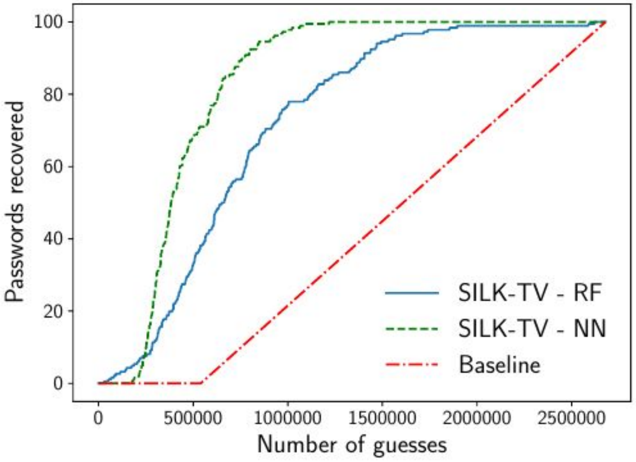


(d) `william1` (183 auth. attempts).

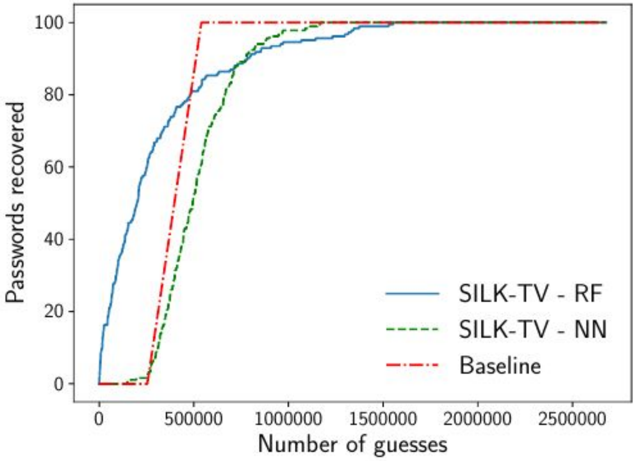
Password - “Single Shot” results



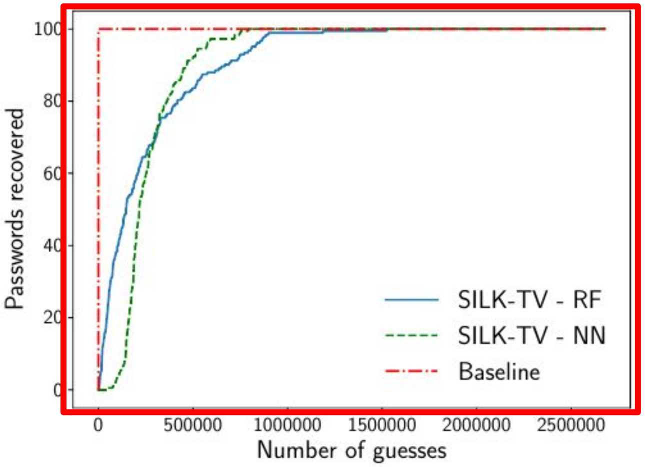
(a) `123brian` (183 auth. attempts).



(b) `jillie02` (186 auth. attempts).

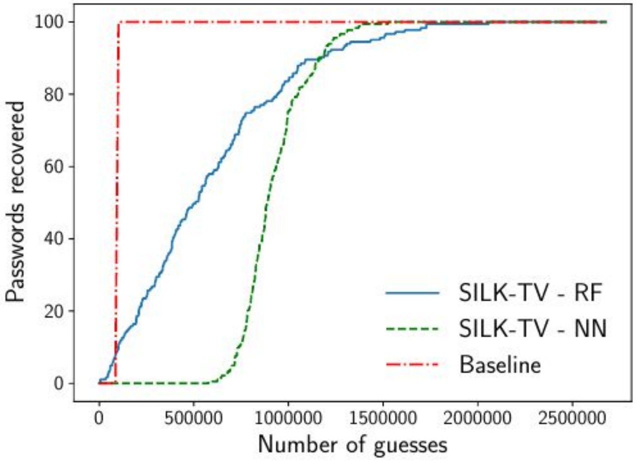


(c) `lamondre` (184 auth. attempts).

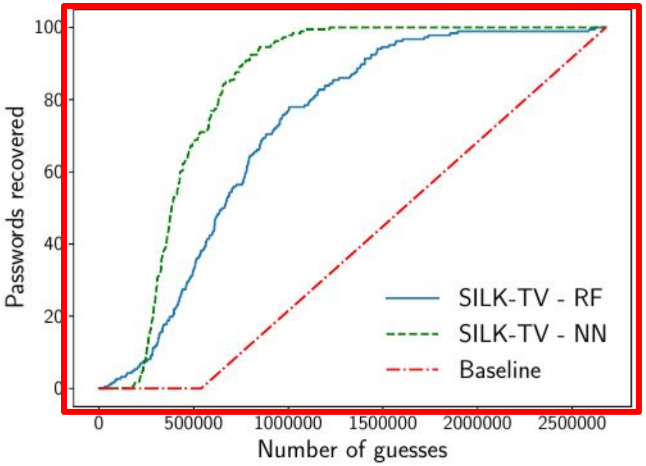


(d) `william1` (183 auth. attempts).

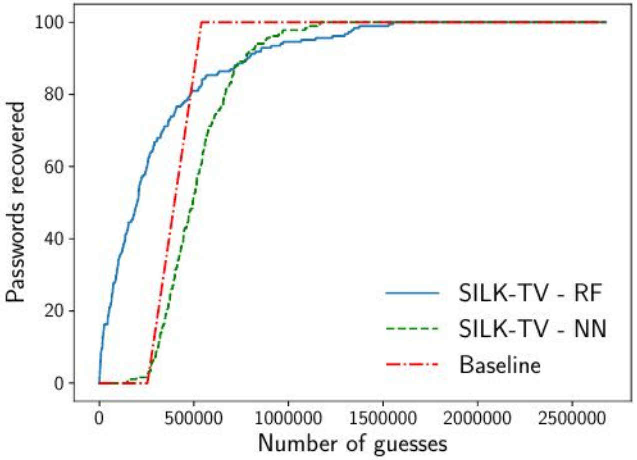
Password - “Single Shot” results



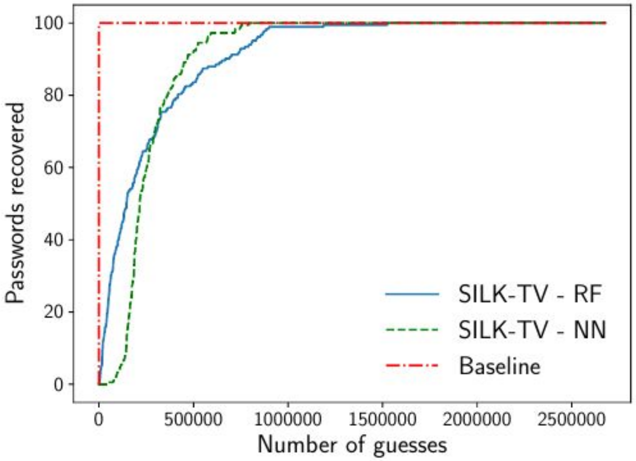
(a) **123brian** (183 auth. attempts).



(b) **jillie02** (186 auth. attempts).

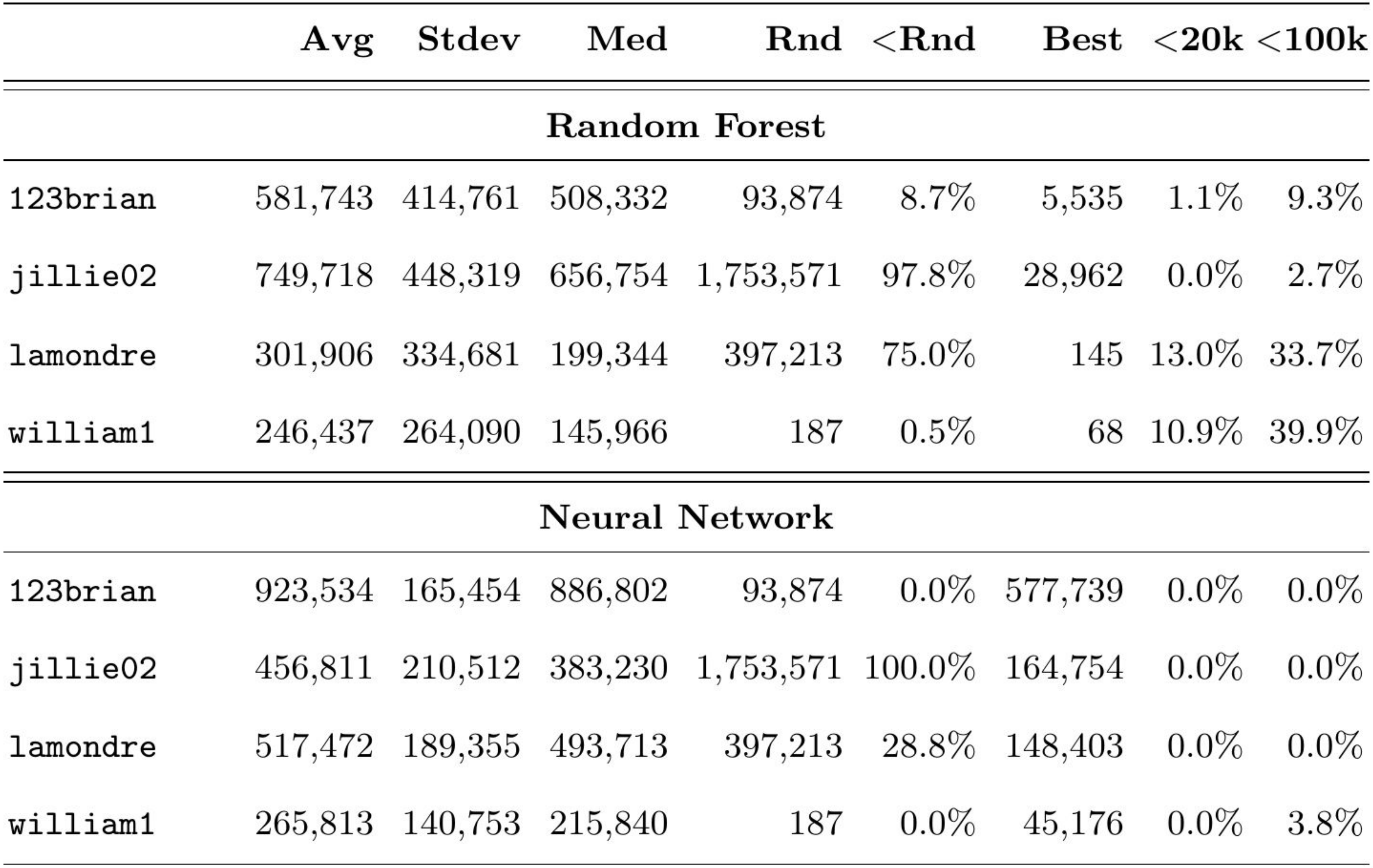


(c) **lamondre** (184 auth. attempts).



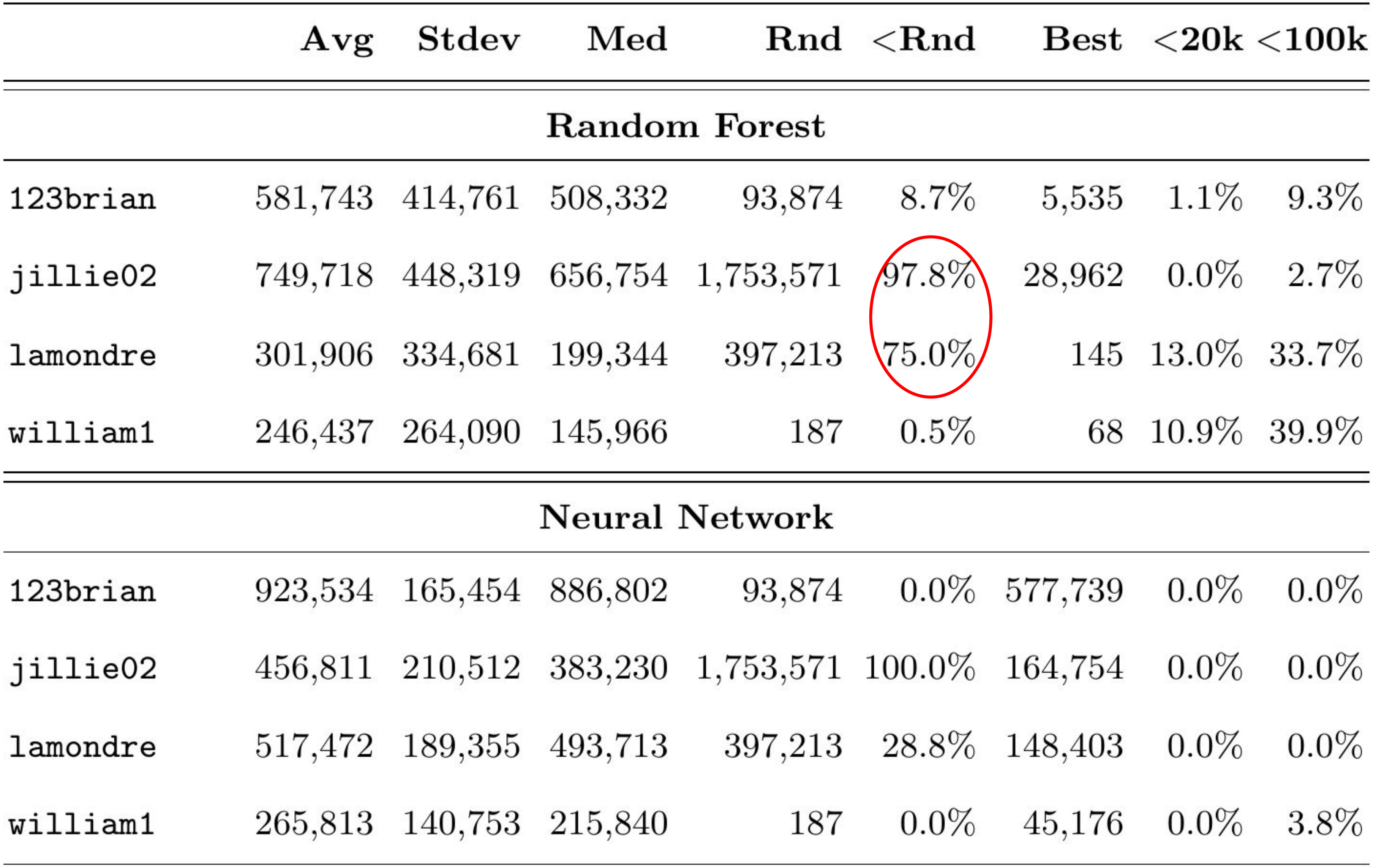
(d) **william1** (183 auth. attempts).

Password - “Single Shot” results



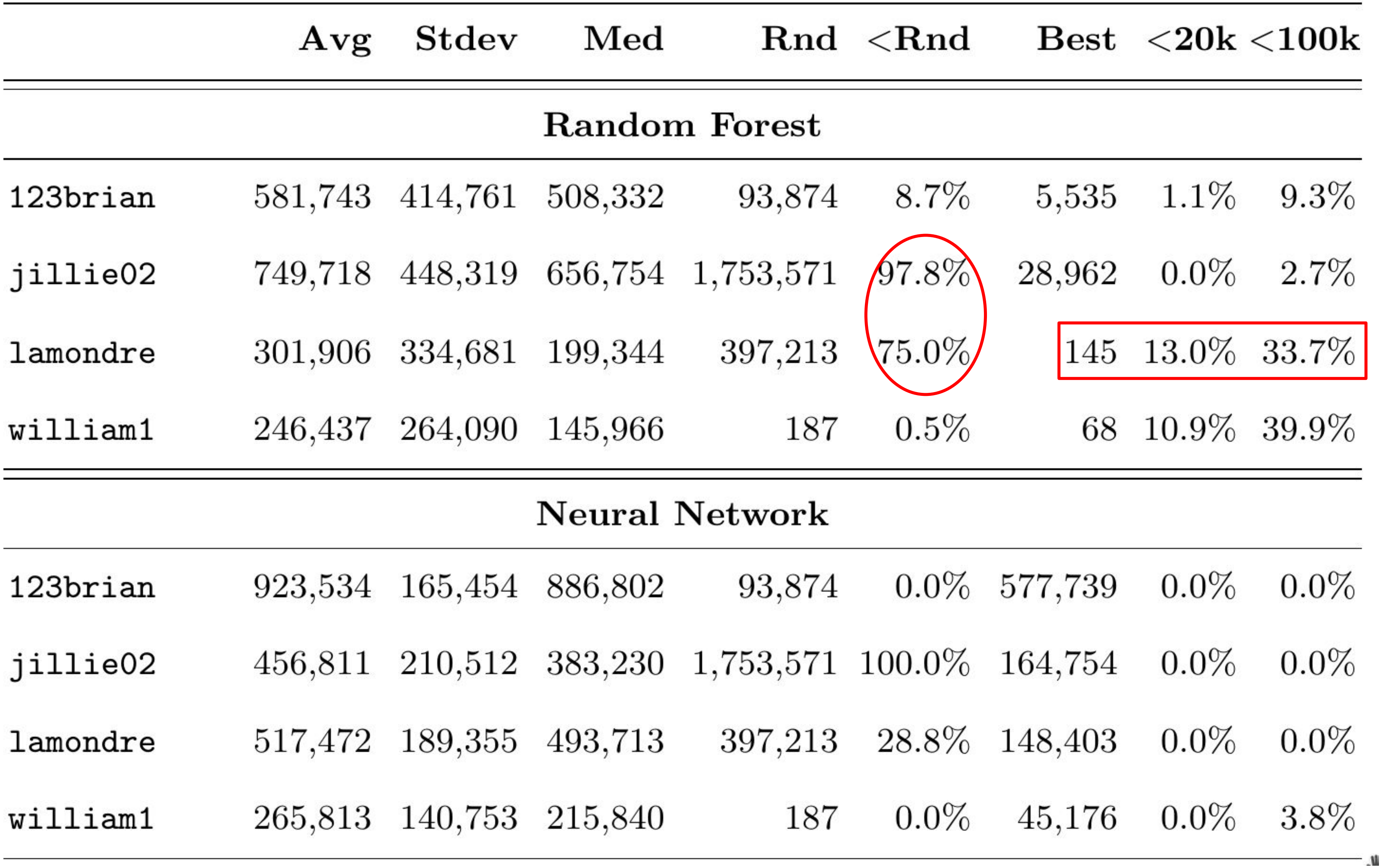
	Avg	Stdev	Med	Rnd	<Rnd	Best	<20k	<100k
Random Forest								
123brian	581,743	414,761	508,332	93,874	8.7%	5,535	1.1%	9.3%
jillie02	749,718	448,319	656,754	1,753,571	97.8%	28,962	0.0%	2.7%
lamondre	301,906	334,681	199,344	397,213	75.0%	145	13.0%	33.7%
william1	246,437	264,090	145,966	187	0.5%	68	10.9%	39.9%
Neural Network								
123brian	923,534	165,454	886,802	93,874	0.0%	577,739	0.0%	0.0%
jillie02	456,811	210,512	383,230	1,753,571	100.0%	164,754	0.0%	0.0%
lamondre	517,472	189,355	493,713	397,213	28.8%	148,403	0.0%	0.0%
william1	265,813	140,753	215,840	187	0.0%	45,176	0.0%	3.8%

Password - “Single Shot” results



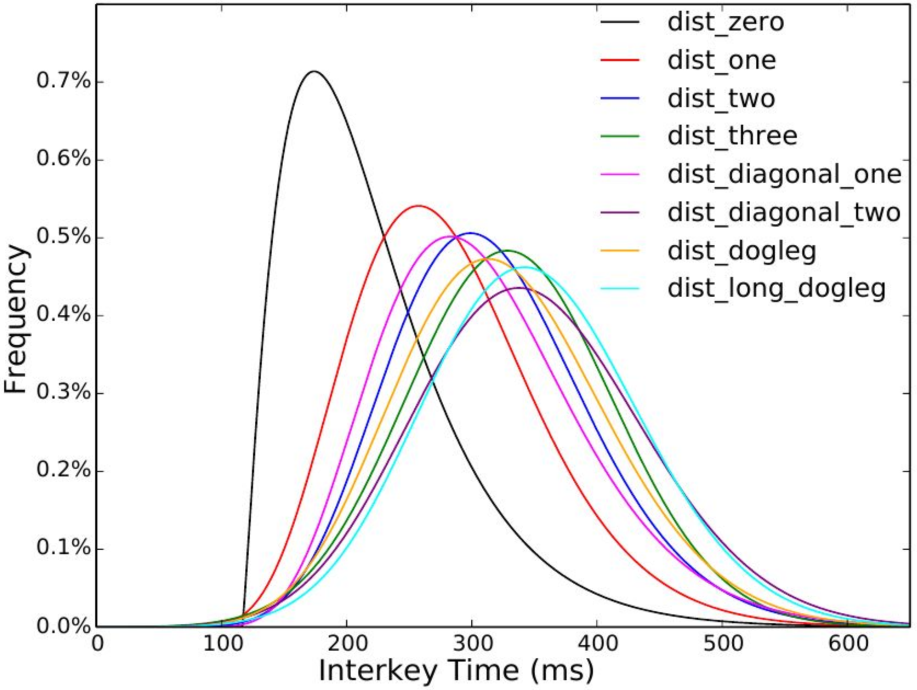
	Avg	Stdev	Med	Rnd	<Rnd	Best	<20k	<100k
Random Forest								
123brian	581,743	414,761	508,332	93,874	8.7%	5,535	1.1%	9.3%
jillie02	749,718	448,319	656,754	1,753,571	97.8%	28,962	0.0%	2.7%
lamondre	301,906	334,681	199,344	397,213	75.0%	145	13.0%	33.7%
william1	246,437	264,090	145,966	187	0.5%	68	10.9%	39.9%
Neural Network								
123brian	923,534	165,454	886,802	93,874	0.0%	577,739	0.0%	0.0%
jillie02	456,811	210,512	383,230	1,753,571	100.0%	164,754	0.0%	0.0%
lamondre	517,472	189,355	493,713	397,213	28.8%	148,403	0.0%	0.0%
william1	265,813	140,753	215,840	187	0.0%	45,176	0.0%	3.8%

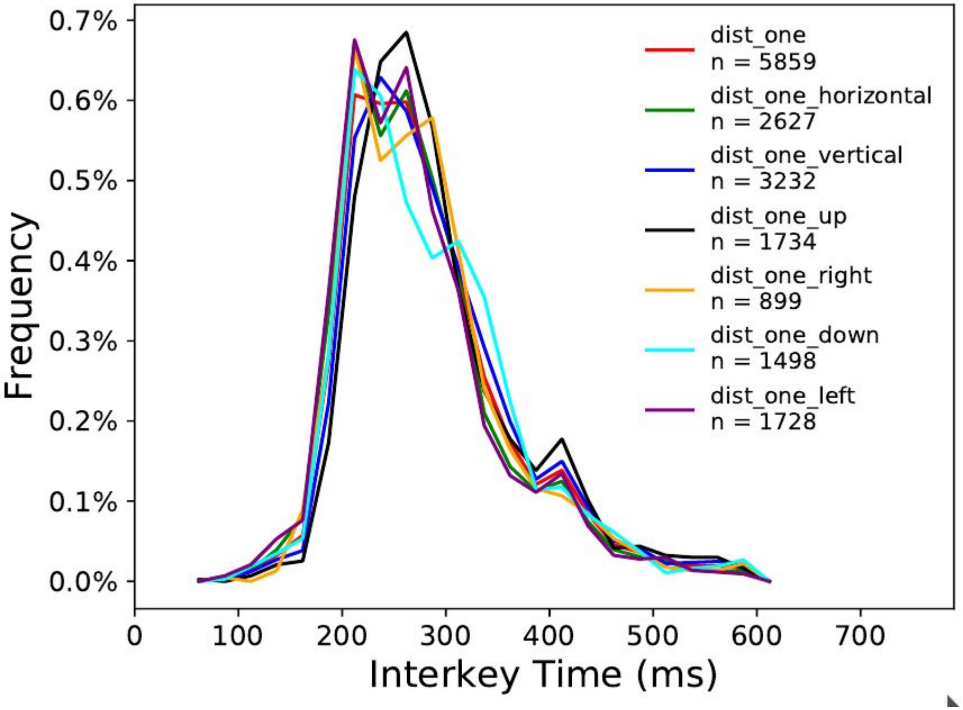
Password - “Single Shot” results



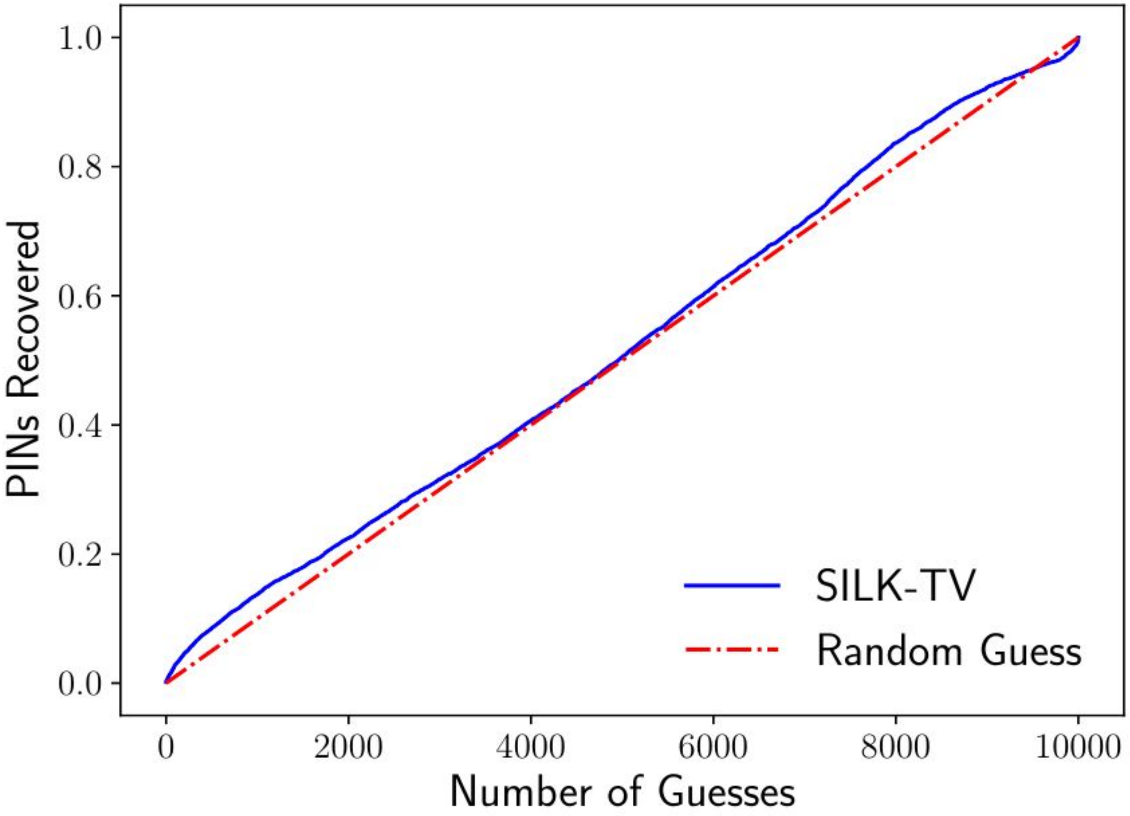
	Avg	Stdev	Med	Rnd	<Rnd	Best	<20k	<100k
Random Forest								
123brian	581,743	414,761	508,332	93,874	8.7%	5,535	1.1%	9.3%
jillie02	749,718	448,319	656,754	1,753,571	97.8%	28,962	0.0%	2.7%
lamondre	301,906	334,681	199,344	397,213	75.0%	145	13.0%	33.7%
william1	246,437	264,090	145,966	187	0.5%	68	10.9%	39.9%
Neural Network								
123brian	923,534	165,454	886,802	93,874	0.0%	577,739	0.0%	0.0%
jillie02	456,811	210,512	383,230	1,753,571	100.0%	164,754	0.0%	0.0%
lamondre	517,472	189,355	493,713	397,213	28.8%	148,403	0.0%	0.0%
william1	265,813	140,753	215,840	187	0.0%	45,176	0.0%	3.8%

PIN - Results


dist_zero
dist_one
dist_two
dist_three
dist_diagonal_one
dist_diagonal_two
dist_dogleg
dist_long_dogleg
Frequency
0.0%
0.1%
0.2%
0.3%
0.4%
0.5%
0.6%
0.7%
0
100
200
300
400
500
600
Interkey Time (ms)


dist_one
n = 5859
dist_one_horizontal
n = 2627
dist_one_vertical
n = 3232
dist_one_up
n = 1734
dist_one_right
n = 899
dist_one_down
n = 1498
dist_one_left
n = 1728
Frequency
0.0%
0.1%
0.2%
0.3%
0.4%
0.5%
0.6%
0.7%
0
100
200
300
400
500
600
700
Interkey Time (ms)

PIN - Results


PINs Recovered
0.0
0.2
0.4
0.6
0.8
1.0
Number of Guesses
0
2000
4000
6000
8000
10000
SILK-TV
Random Guess

Conclusions

- Timing information from videos is **accurate**
- Password masking leak timing → useful information
  - Reduces number of attempts
  - More useful on **uncommon** passwords!
- PIN masking looks safe

SILK-TV

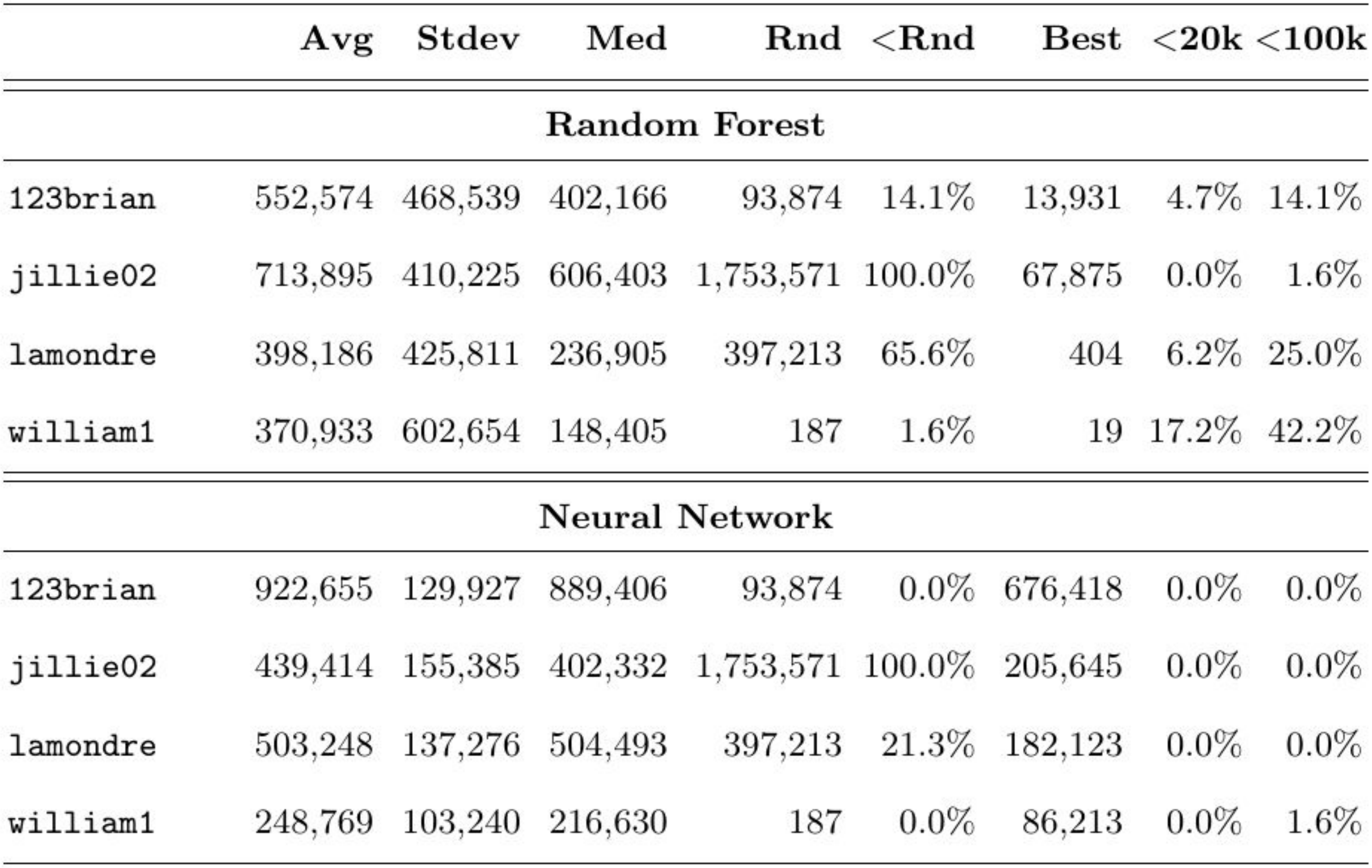
Secret Information Leakage from Keystroke Timing Videos

Daniele Lain

ETH Zurich

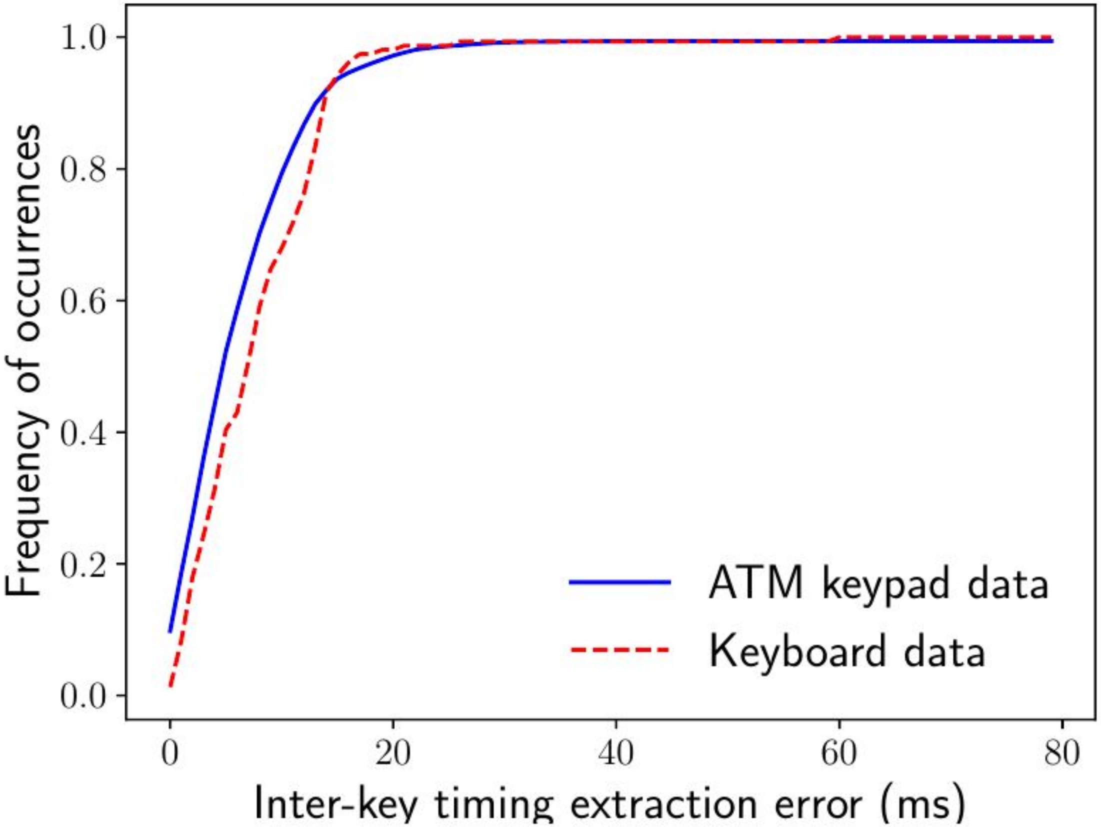
daniele.lain@inf.ethz.ch

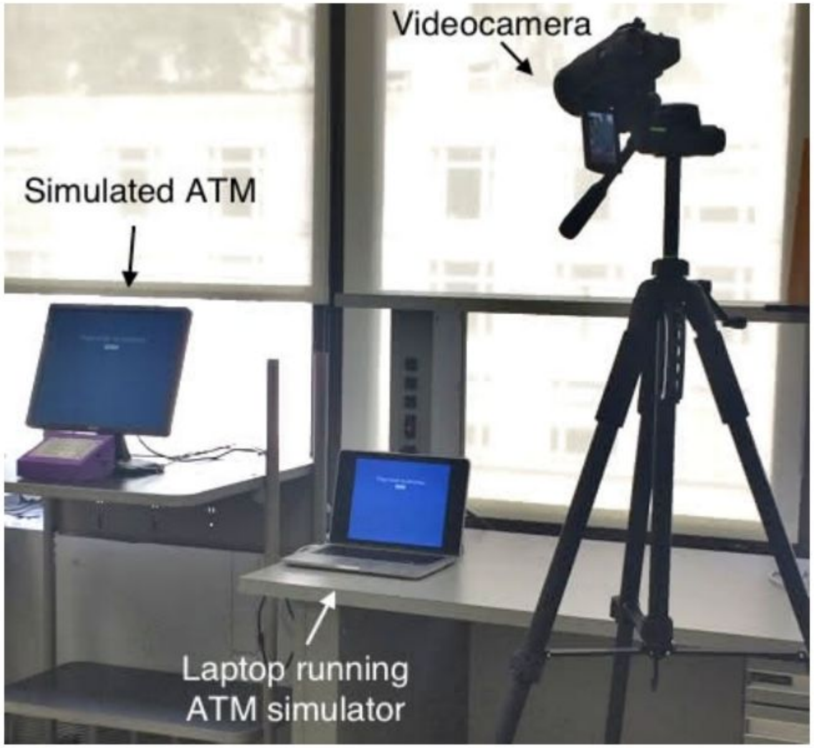
Passwords - "Multiple Recordings"

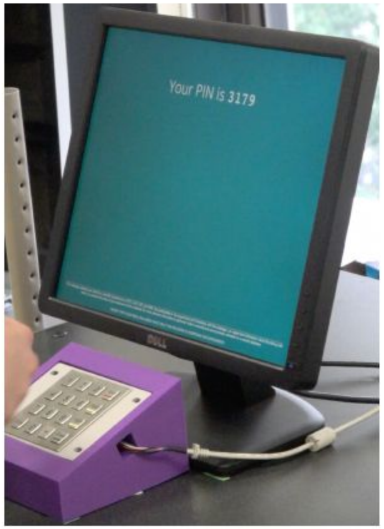


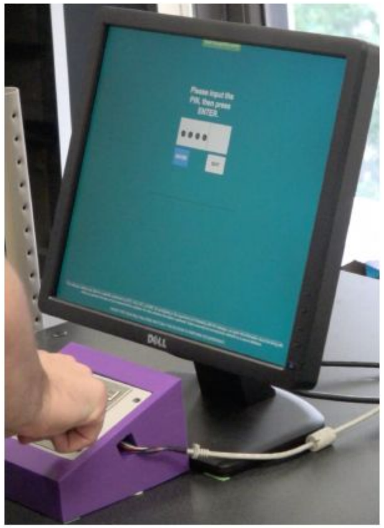
	Avg	Stdev	Med	Rnd	<Rnd	Best	<20k	<100k
			Random Forest					
123brian	552,574	468,539	402,166	93,874	14.1%	13,931	4.7%	14.1%
jillie02	713,895	410,225	606,403	1,753,571	100.0%	67,875	0.0%	1.6%
lamondre	398,186	425,811	236,905	397,213	65.6%	404	6.2%	25.0%
william1	370,933	602,654	148,405	187	1.6%	19	17.2%	42.2%
			Neural Network					
123brian	922,655	129,927	889,406	93,874	0.0%	676,418	0.0%	0.0%
jillie02	439,414	155,385	402,332	1,753,571	100.0%	205,645	0.0%	0.0%
lamondre	503,248	137,276	504,493	397,213	21.3%	182,123	0.0%	0.0%
william1	248,769	103,240	216,630	187	0.0%	86,213	0.0%	1.6%

Video information extraction




Videocamera
Simulated ATM
Laptop running
ATM simulator


Your PIN is 3179


Please input the PIN, then press ENTER.