Design and security assessment of a protocol for continuous user identity verification

[redacted]

[redacted]

Università [redacted]

[redacted]

[redacted]

[redacted]

[redacted]

[redacted]

Contents

- [illegible]
  - [illegible]
- [illegible]
  - [illegible]
  - [illegible]
- [illegible]

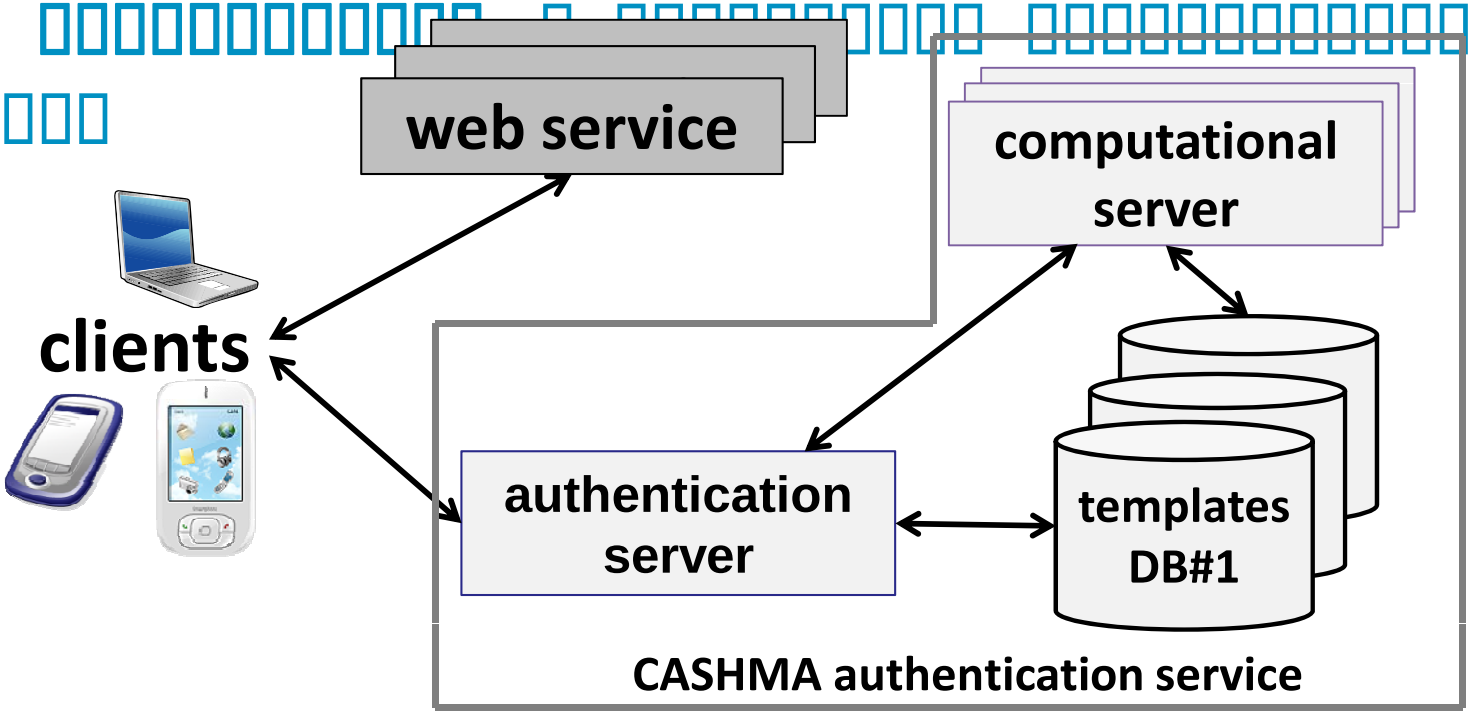
[illegible]

Context, motivations and objectives

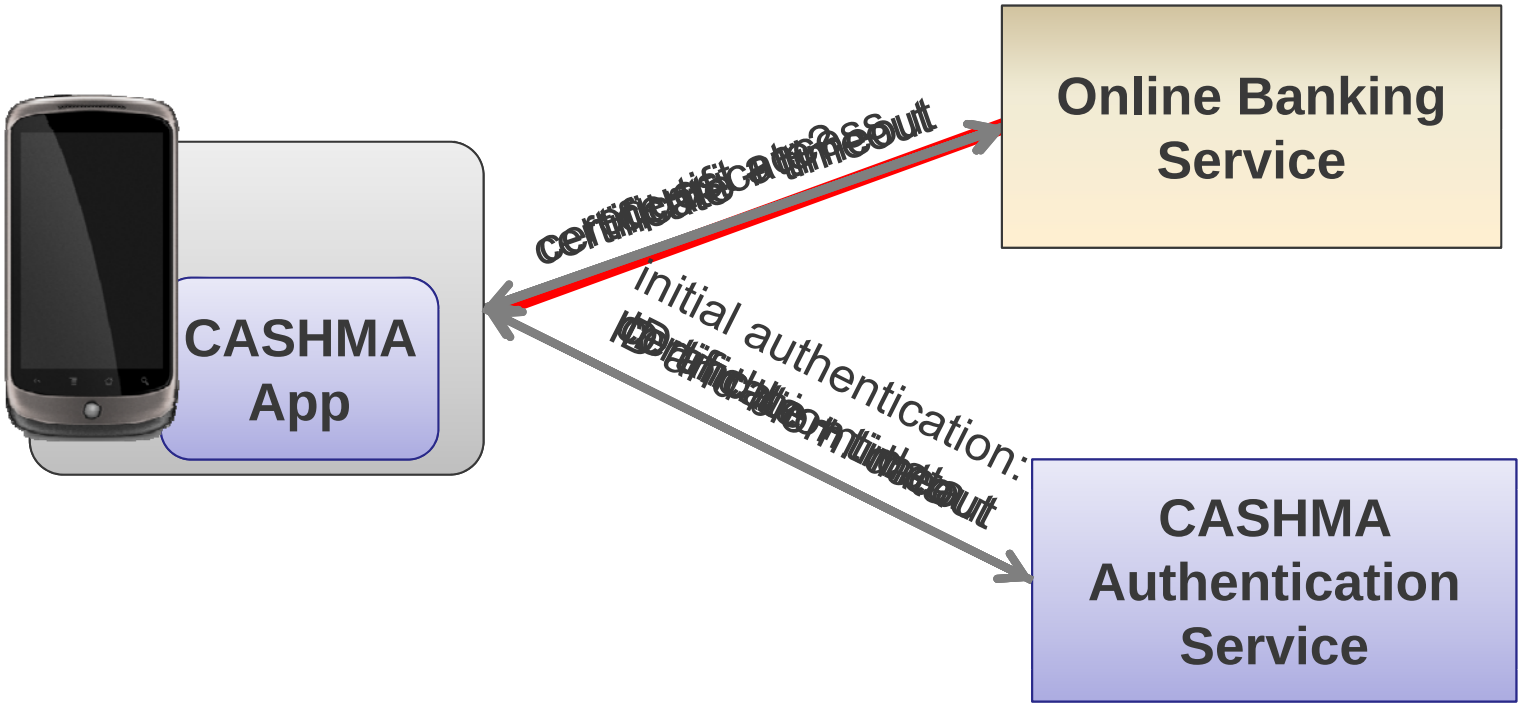
- [illegible]
  - [illegible]
  - [illegible]
- [illegible]
  - [illegible]
- [illegible]

The CASHMA system

- [illegible]
- [illegible]



Sample CASHMA scenario: online banking



- [illegible]
  - [illegible]
  - [illegible] *[illegible]* [illegible]

Basics

- [illegible]
- [illegible]
- [illegible]
- [illegible]
- [illegible]

$m(S_k, t_i)$: trust in the subsystem S_k at time t_i

[illegible] [illegible] [illegible] t_0

$$[illegible](t_i, t_0) = 1 - [illegible](t_i)$$

- [illegible] [illegible] [illegible] [illegible] [illegible] [illegible] [illegible], [illegible] [illegible] [illegible] [illegible] [illegible]

$$[illegible](t_i, t_i) = [illegible](t_i, t_{i-1}) \cdot [illegible]^{-[illegible]\cdot[illegible]}$$

[illegible] [illegible] $[illegible]^{-[illegible]\cdot[illegible]}$ [illegible] [illegible] [illegible] [illegible] [illegible] [illegible] [illegible] [illegible] [illegible] [illegible] [illegible]

- [illegible]: [illegible] [illegible] [illegible] [illegible] [illegible] [illegible] [illegible] [illegible] [illegible]
- [illegible]: [illegible] [illegible] [illegible]

g(u, t_i): trust in the user

- □□ □□□□ □□□□ □□□□□□□ □□□□□□□□□□
  □□□□□□□□□□□□□□□, □□□□□ □□ □□□ □□□□ □□□□□□□□□

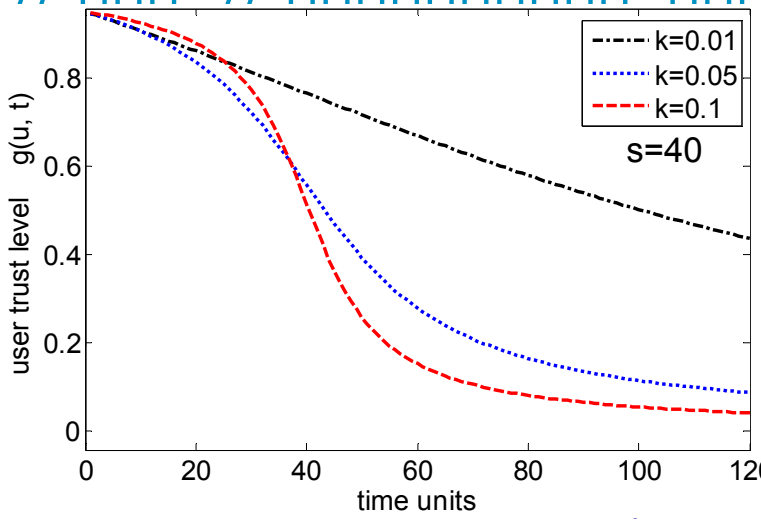
$$g(u, t_0) = 1 \qquad g(u, t_i) = \frac{\left(-\arctan\left((\Delta t_i - s)\cdot k\right) + \frac{\pi}{2}\right)\cdot trust(u, t_{i-1})}{\left(-\arctan(-s\cdot k) + \frac{\pi}{2}\right)}$$

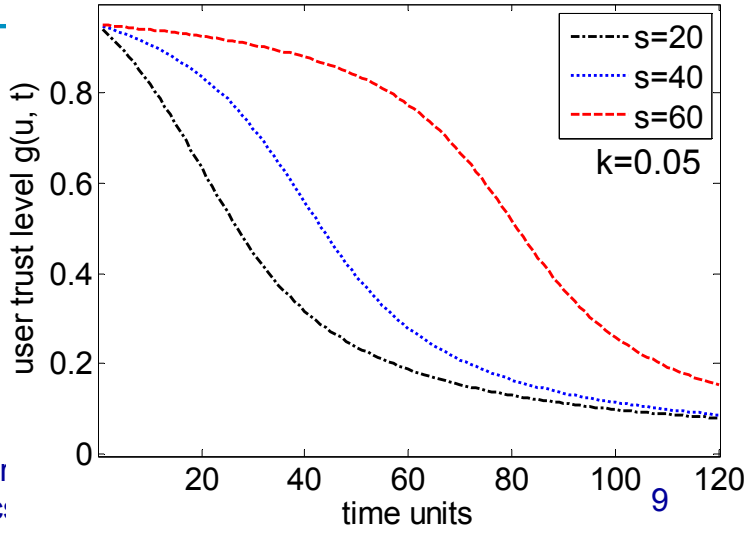
Δt_i □□□□ □□□□□ □□□□ □□□□□□□□□□□□

$trust(t_{i-1})$ □□□□□□ □□□□□ □□□□□ □□□□□□□□ □□ □□□

□□□□□□□□ □□□□□□□□□

□ □□□ □ □□□□□□□□□□ □□□□ □□□□ □□□





g(u, t_i): global trust level
T_i: timeout

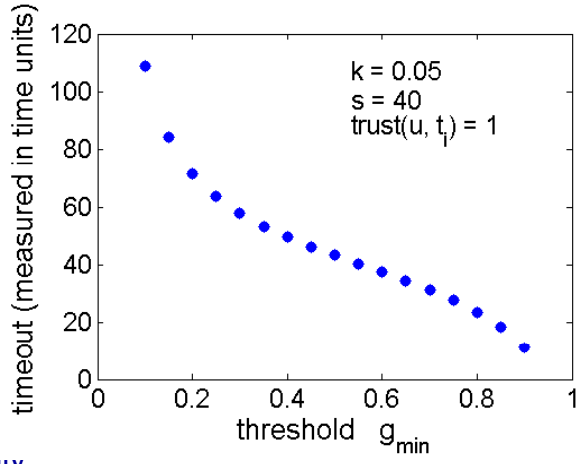
$$trust(u, t_0) = 1 - \prod_{k=1..n}(1 - m(S_k, t_0))$$

OR-rule from L. Hong et al., “Can Multibiometrics Improve Performance?,” *Proc. AutoID’99*, Summit, NJ, pp. 59–64, 1999.

$$trust(u, t_i) = g(u, t_i) + (1 - g(u, t_i)) \cdot m(S_k, t_i)$$

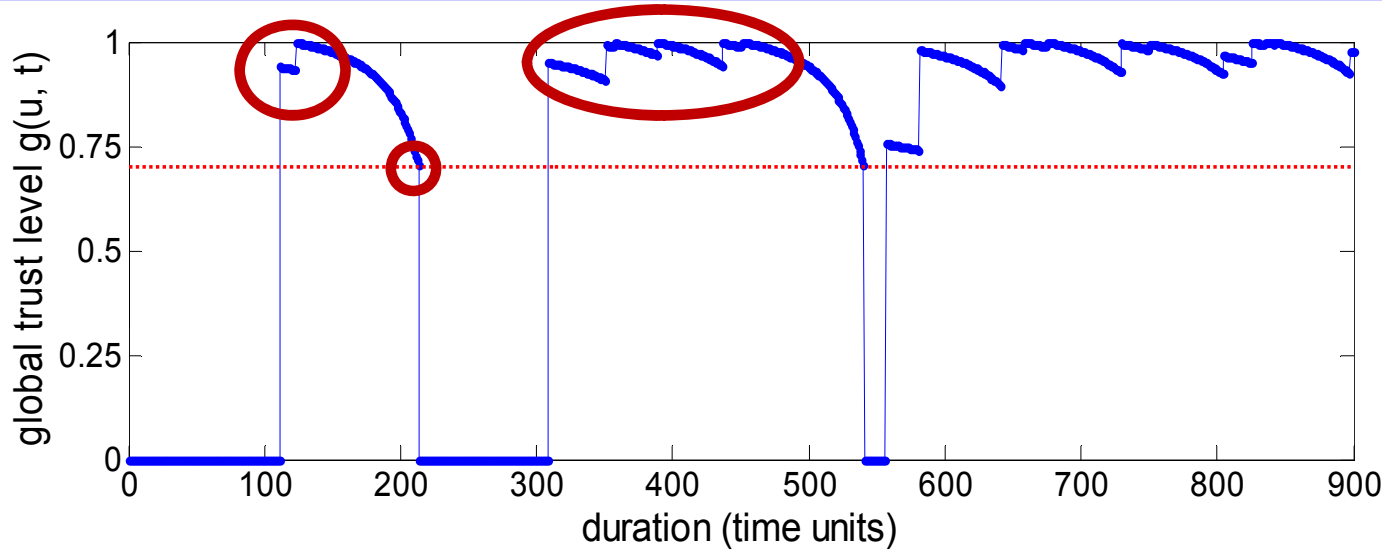
- [illegible]:

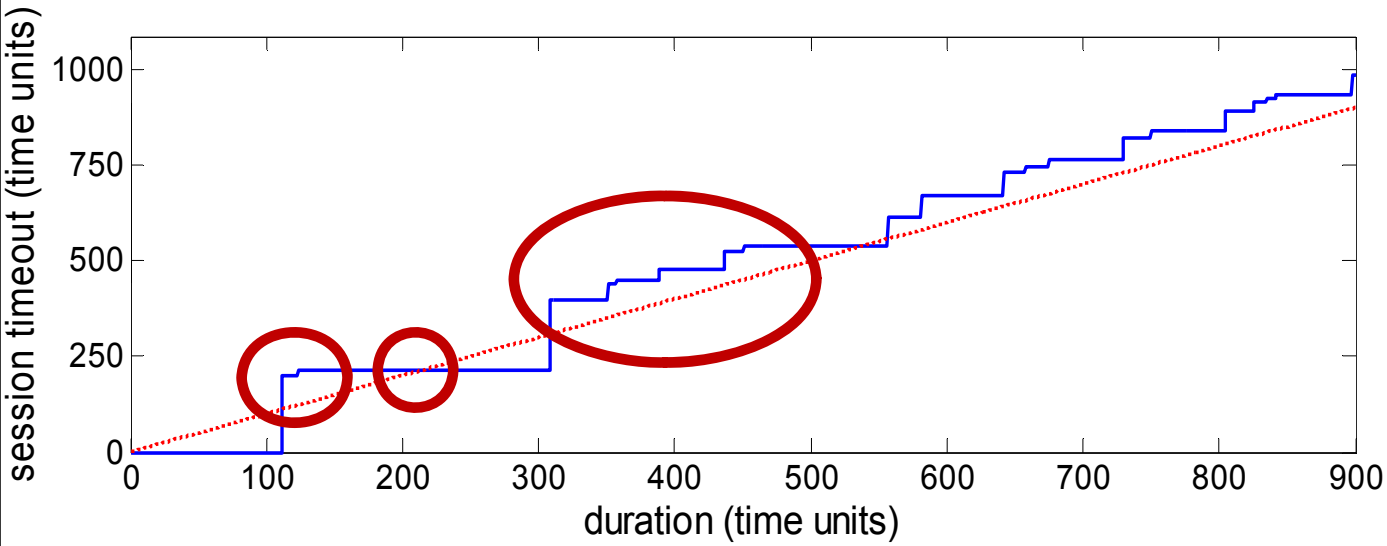
$$T_i = \tan\left(\frac{\left(g_{min} \cdot \left(\arctan(-s \cdot k) - \frac{\pi}{2}\right)\right)}{trust(u, t_i)} + \frac{\pi}{2}\right) \cdot \frac{1}{k} + s$$



Exemplary runs
g_{min} = 0.7 k=0.05 s=100

Biometric trait	Time instant	FMR
Voice	112	00.06
Fingerprint	124	00.03
Face	309	00.05
Keystroke	351	00.08
Keystroke	358	00.08
Fingerprint	389	00.03
Face	437	00.05
Fingerprint	451	00.03
Fingerprint	557	00.03
Keystroke	582	00.08
Voice	642	00.06
Fingerprint	658	00.03
Voice	675	00.06
Face	730	00.05
Face	750	00.05
Face	805	00.05
Fingerprint	826	00.03
Voice	835	00.06
Keystroke	842	00.08
Keystroke	898	00.08





Assessment: security modelling

ADversary VIew Security Evaluation - ADVISE

1. [illegible] [illegible] [illegible] (ADVISE)
   - [illegible] [illegible] [illegible] [illegible]: [illegible] [illegible], [illegible] [illegible], [illegible], [illegible]
2. [illegible]: [illegible] [illegible] [illegible] [illegible], [illegible] [illegible], [illegible]
   - [illegible], [illegible], [illegible]

▶ [illegible] [illegible] [illegible] [illegible] [illegible] [illegible] [illegible] *[illegible]*, [illegible] [illegible]

E. LeMay, M.D. Ford, K. Keefe, W.H. Sanders, C. Muehrcke, "Model-based Security Metrics Using ADversary VIew Security Evaluation (ADVISE)". QEST 2011: 191-200

Definition of the adversaries

- [illegible] [illegible] [illegible] [illegible] [illegible] (TAL) [illegible] [illegible]

T. Casey, "Threat Agent Library Helps Identify Information Security Risks", White Paper, Intel Corporation, 2007.

	Adverse Organization	Technology Master Individual	Generic (malicious) individual	Insider
Access	external	external	external	internal
Limits	extra-legal	extra-legal	extra-legal	extra-legal
Resources	government	moderate	individual	organization
Skill-Hack	operational	adept	none to minimal	none to minimal
Skill-Spoofing	operational	none	none to minimal	none to minimal
Visibility	covert	clandestine	overt or clandestine	clandestine

Evaluation of the initial authentication - scenario

- [illegible]: [illegible], [illegible], [illegible]

[illegible]:

#1: [illegible] 2 [illegible].
[illegible] [illegible] [illegible] [illegible] [illegible]

#2: [illegible] 3 [illegible].
[illegible] [illegible] [illegible] [illegible] [illegible]

#3: [illegible] 3 [illegible].

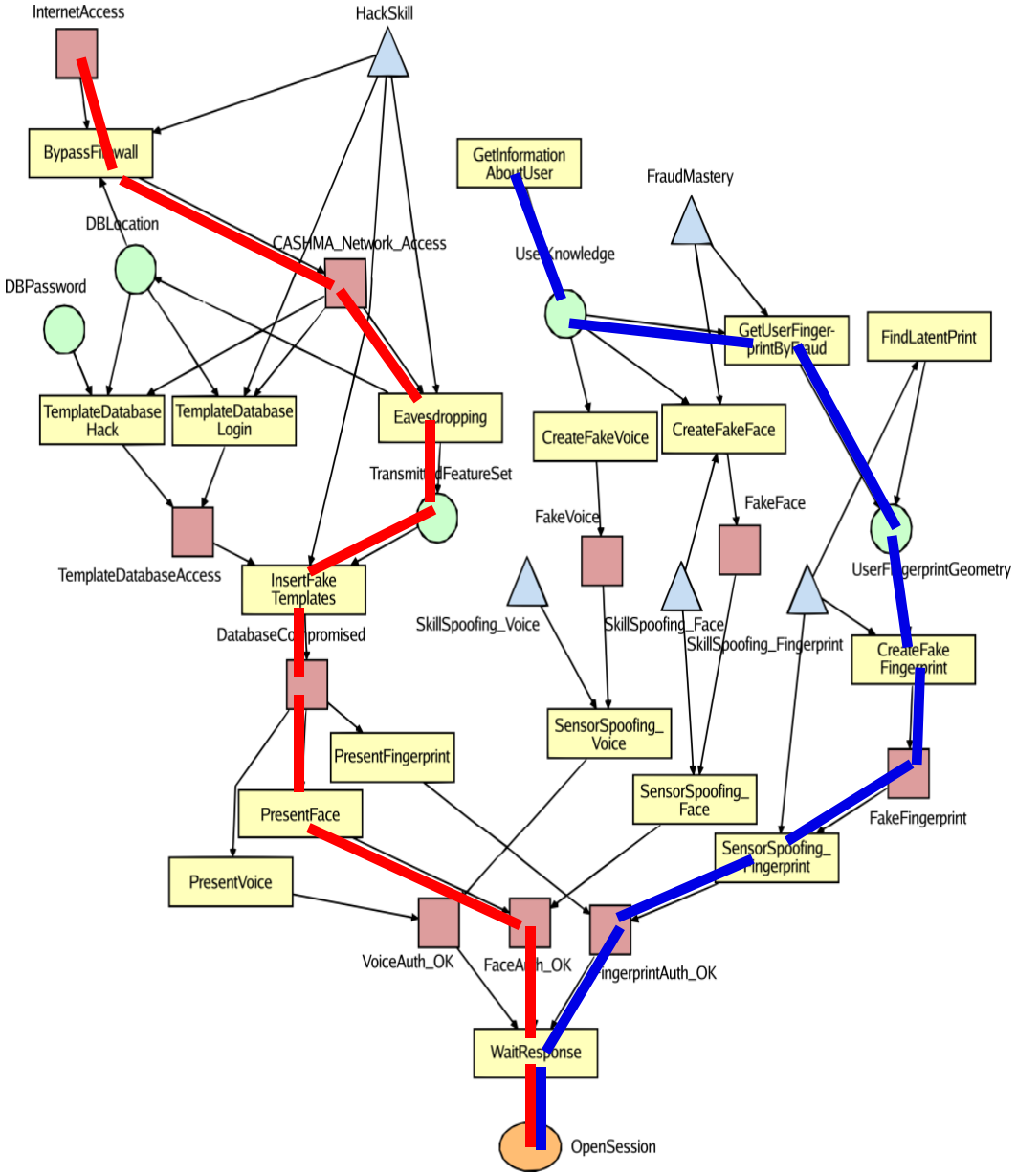
Attackers description

- [illegible]
  - [illegible]: [illegible]
    - access to one counterfeit biometric sample (voice)
  - [illegible]: [illegible] + [illegible]
    - access to two counterfeit biometric samples (voice + face)
  - [illegible]
    - knowledge of some system details
  - [illegible]
- [illegible]:
  - [illegible]

Attackers description - parameters

		Generic Individual (**face**)	Generic Individual (**face + voice**)	Technology Master Individual	Adverse Organization
attack skills	SkillSpoofing_Voice	1000	1000	200	600
	SkillSpoofing_Face	200	900	200	600
	SkillSpoofing_Fingerprint	200	200	200	600
	FraudMastery	200	200	200	600
	HackSkill	200	200	800	600
initial access domains	FakeVoice	Y	Y	N	N
	FakeFace	N	Y	N	N
	FakeFingerprint	N	N	N	N
	DatabaseLocation	N	N	Y	N
policies	WeightCost	0.3	0.3	0.25	0.05
	WeightDetection	0.3	0.3	0.25	0.05
	WeightPayoff	0.4	0.4	0.5	0.9
	PlanningHorizon	7	7	7	7

ADVISE Attack Execution Graph



1 [illegible]

10 [illegible]

5 [illegible]

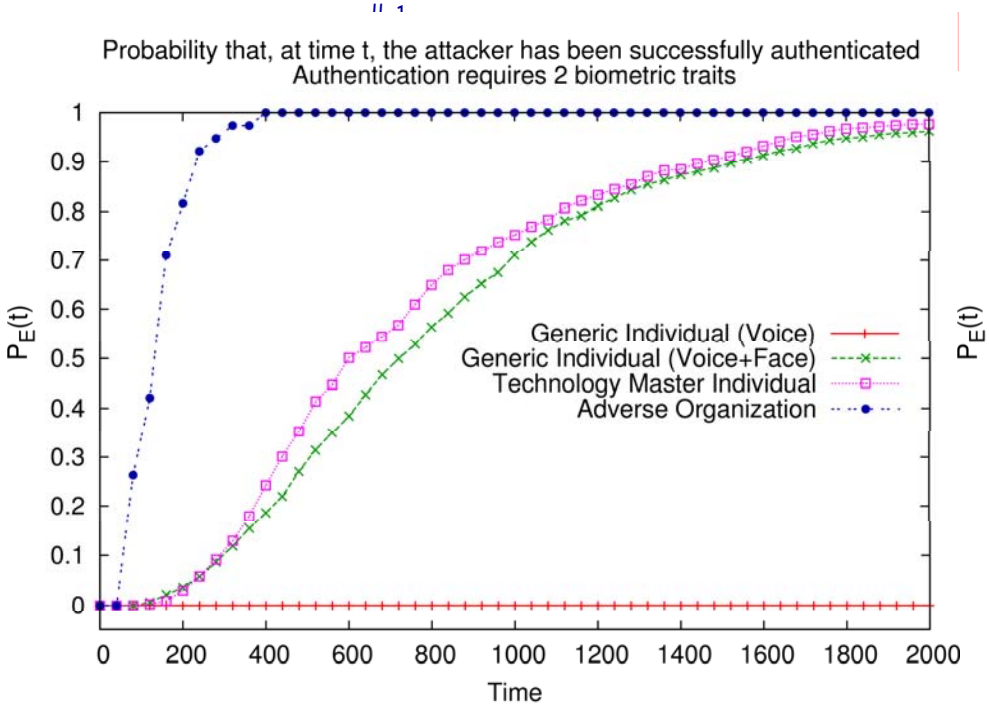
5 [illegible]

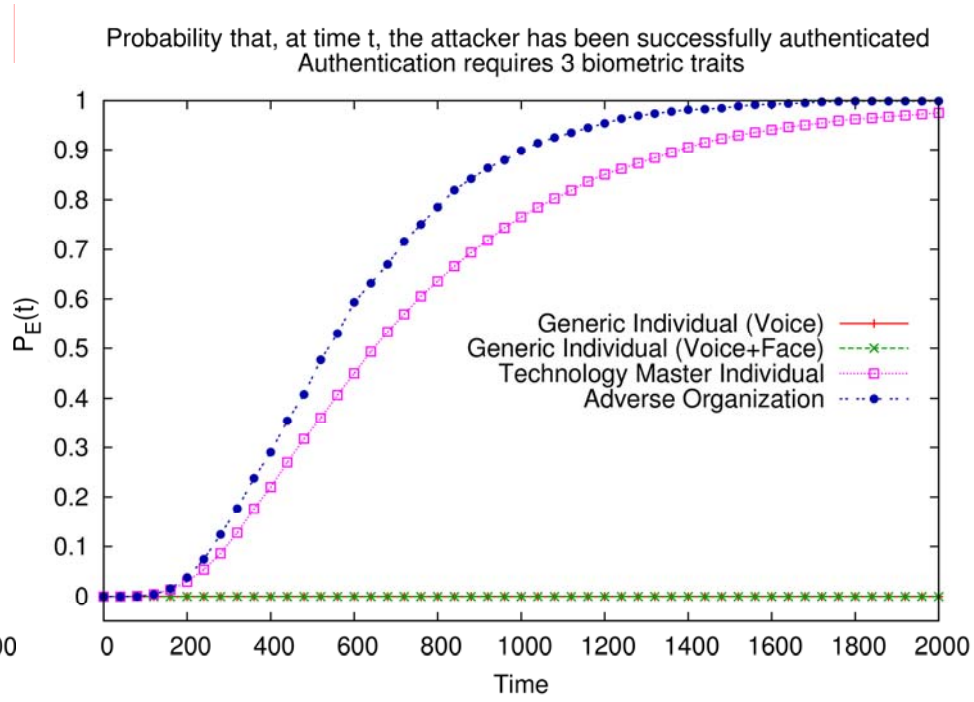
18 [illegible]

[illegible]:

- [illegible] 1
- [illegible] 2

Evaluation and Results - 1

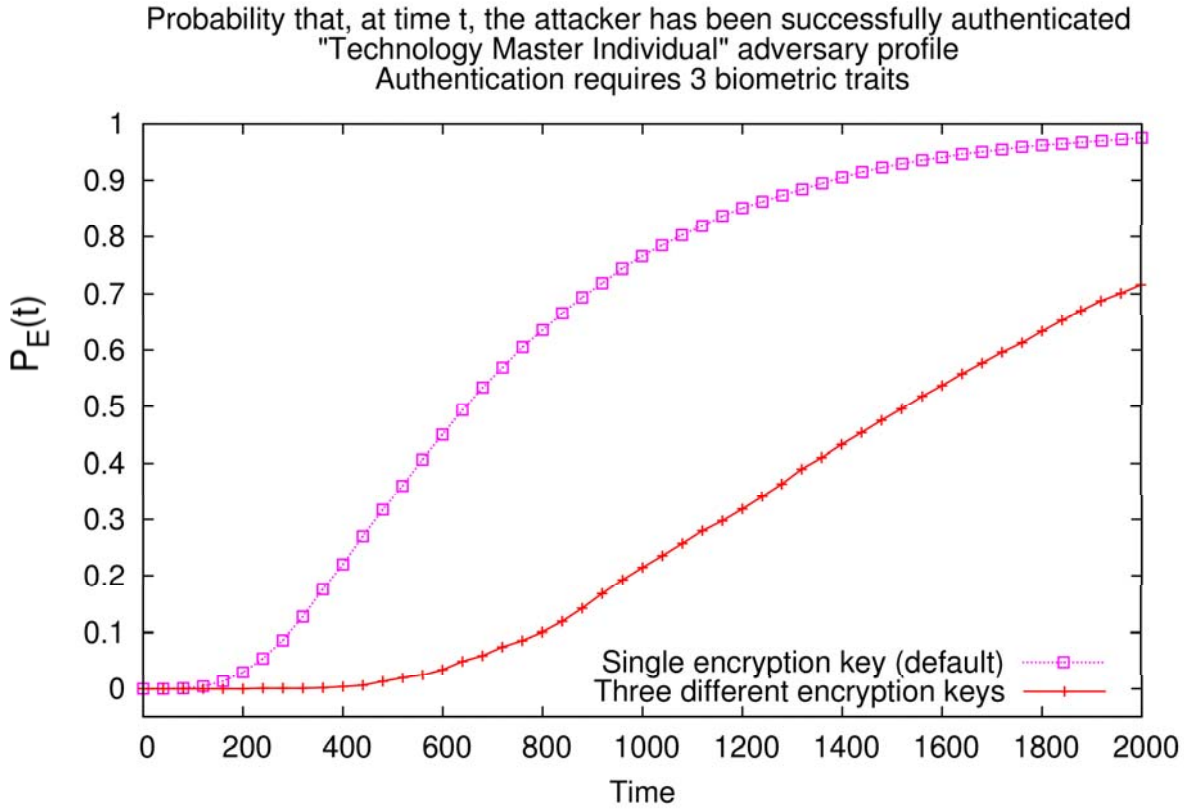




#1 [illegible]

#2: [illegible]

Evaluation and Results - 2



[illegible] #3 ([illegible])

- [illegible]

Evaluation of the continuous authentication - scenario

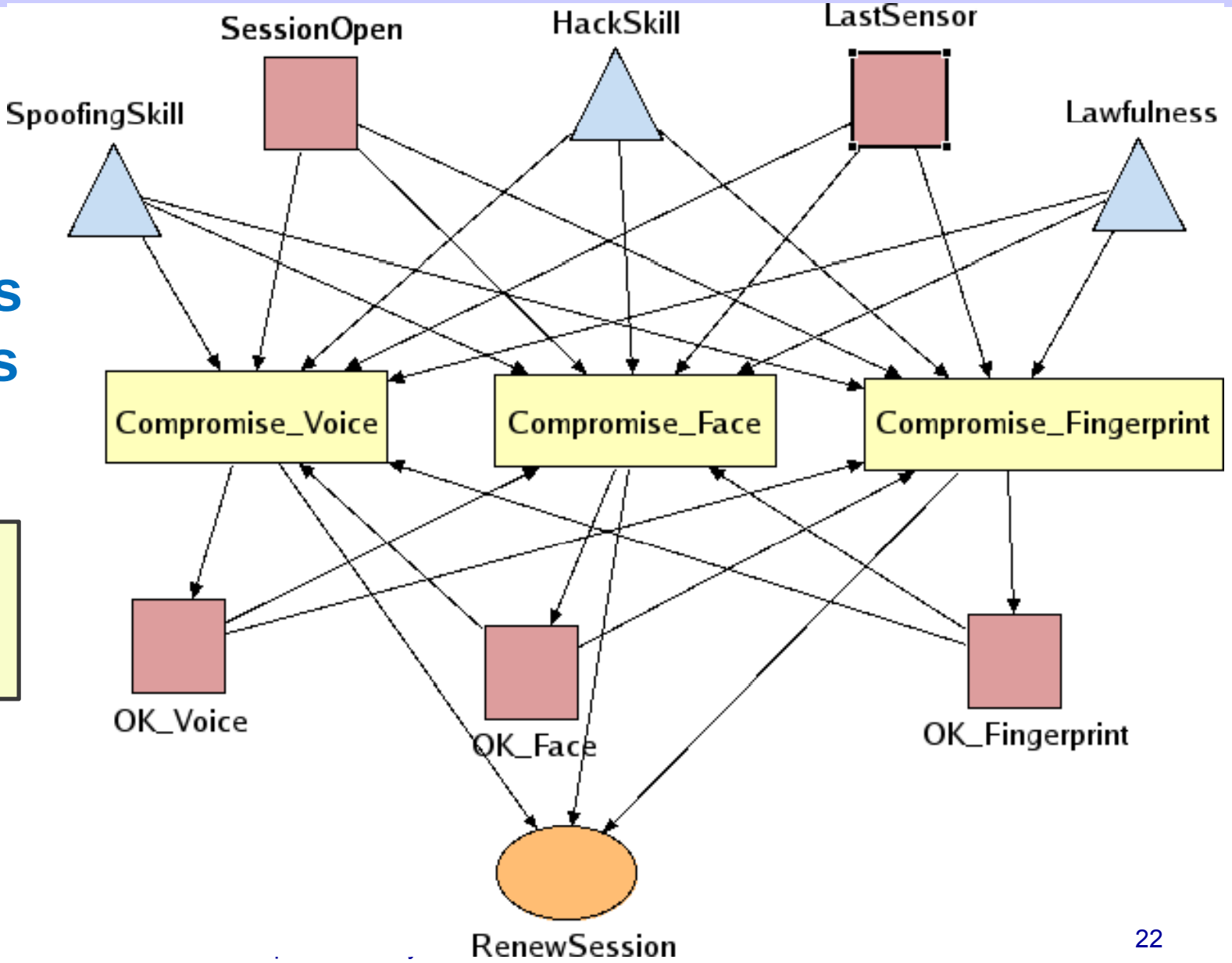
Attack Execution Graph

3 skills

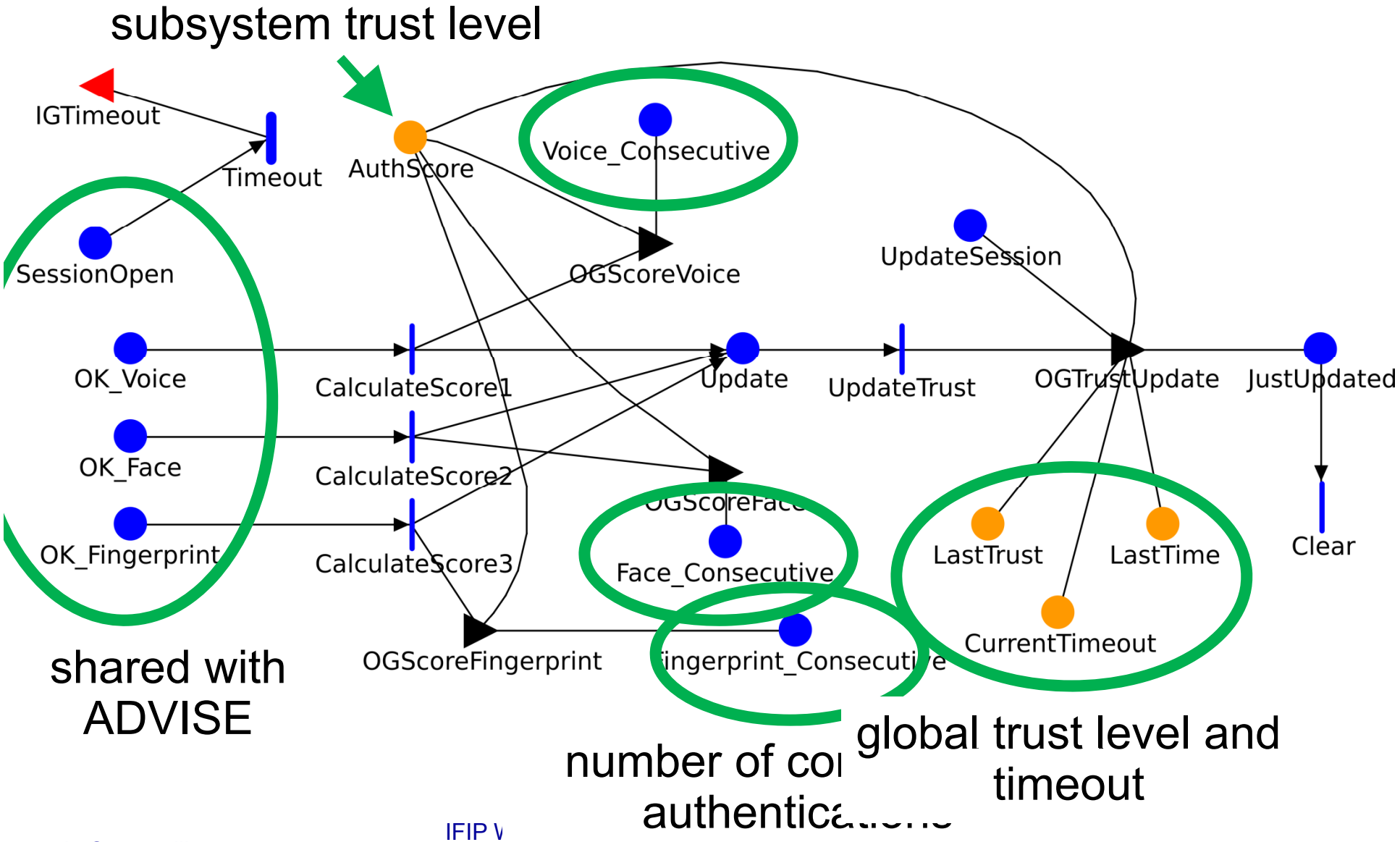
6 access domains

3 attack steps

1 goal

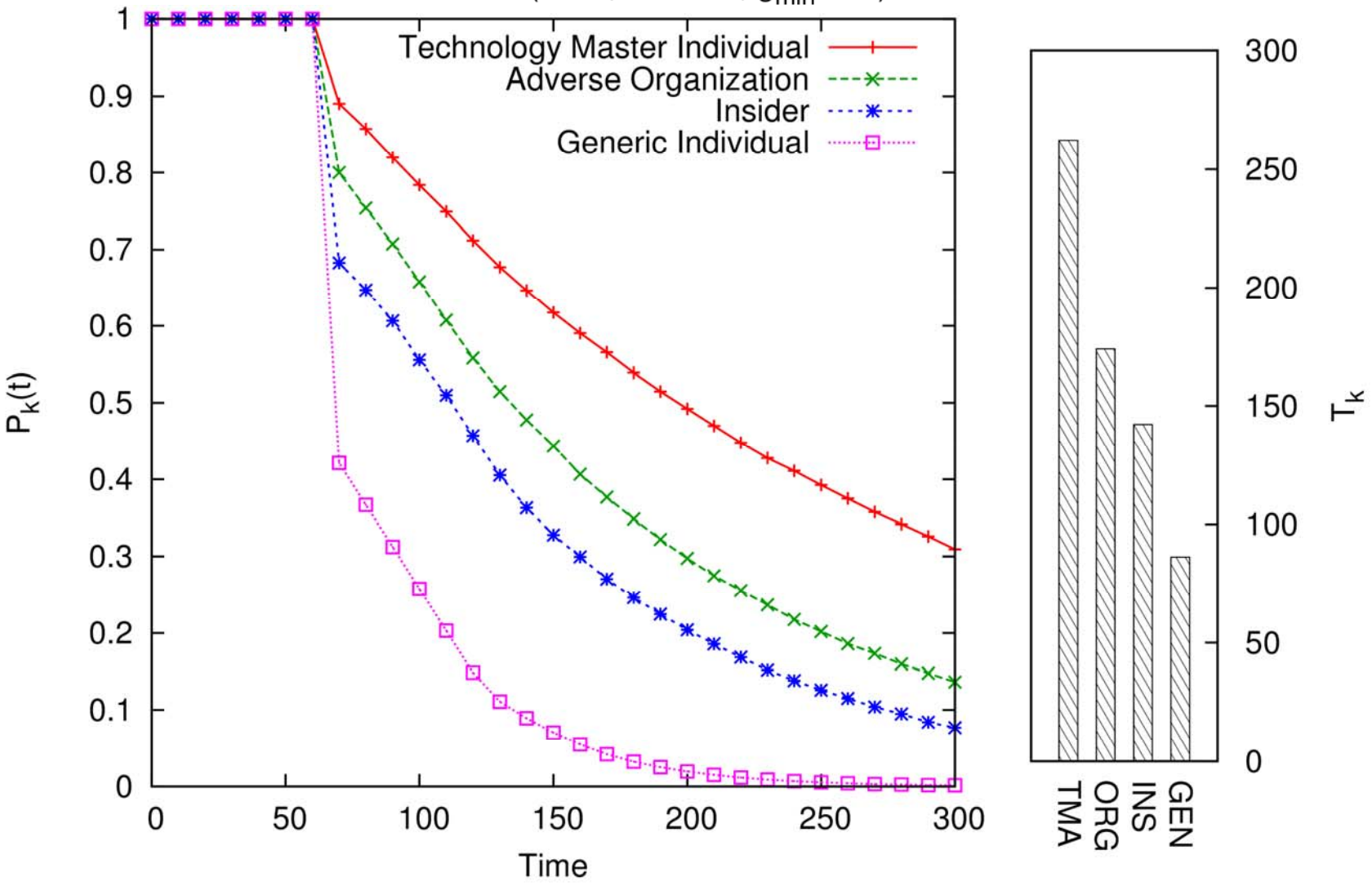


SAN model of the continuous authentication protocol



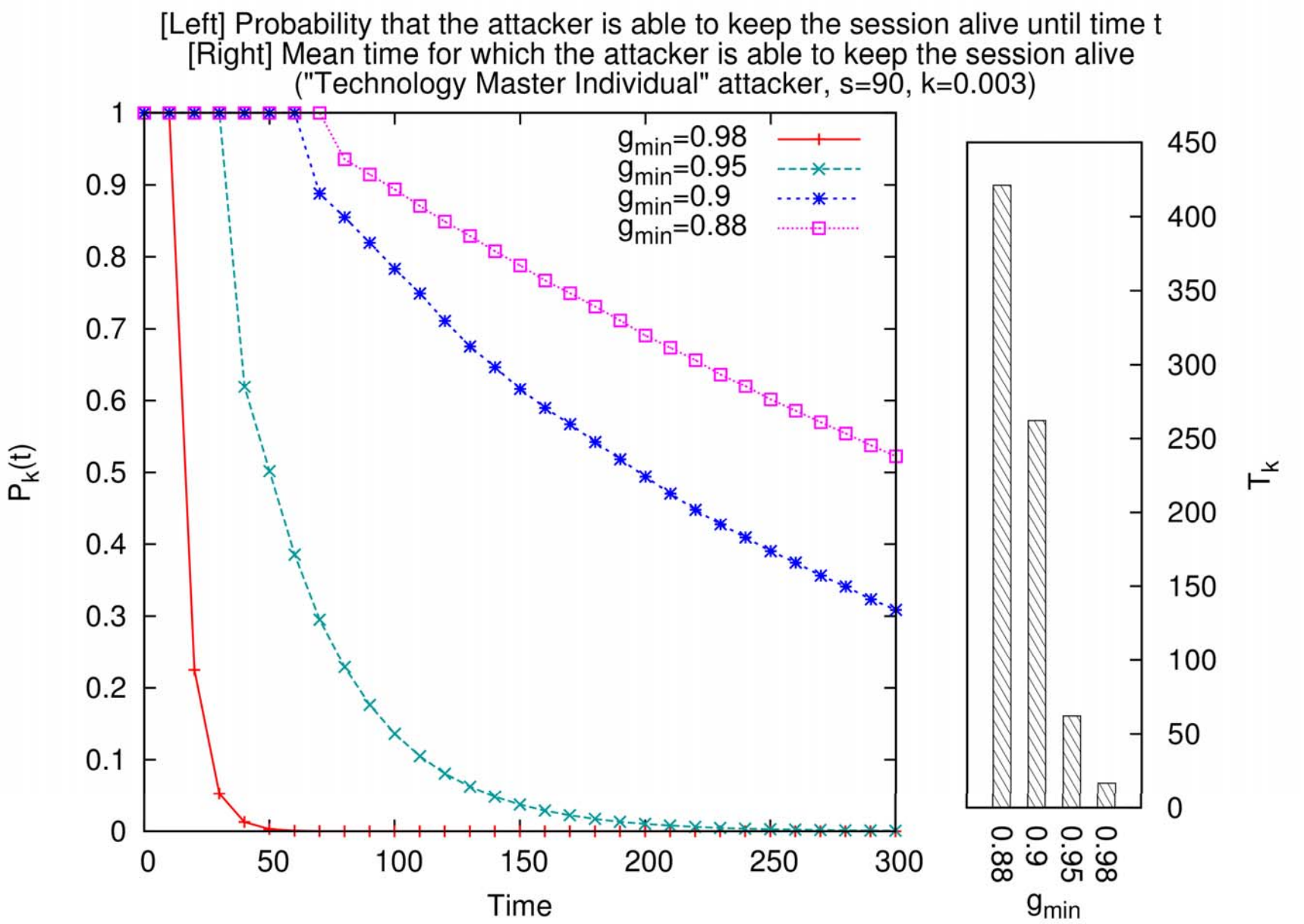
Effectiveness for different attackers

[Left] Probability that the attacker is able to keep the session alive until time t
[Right] Mean time for which the attacker is able to keep the session alive
(s=90, k=0.003, g_{min}=0.9)



A

Effectiveness of tuning thresholds on TMA attacker



Conclusions

Conclusions

- [illegible]
- [illegible] 4.0.
  - [illegible] 0 [illegible], [illegible], [illegible]
  - [illegible] 6 [illegible] 8.4
- [illegible]:

References

- [illegible]
- [illegible] 2012 , [illegible]. 201–206.
- [illegible]

THANK YOU
for your attention