

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

UNIVERSITÀ DEGLI STUDI DI FIRENZE

DIPARTIMENTO DI INFORMATICA
ELETTRONICA

Università degli Studi di Firenze
Dipartimento di Informatica
Elettronica

2021 2021 2021

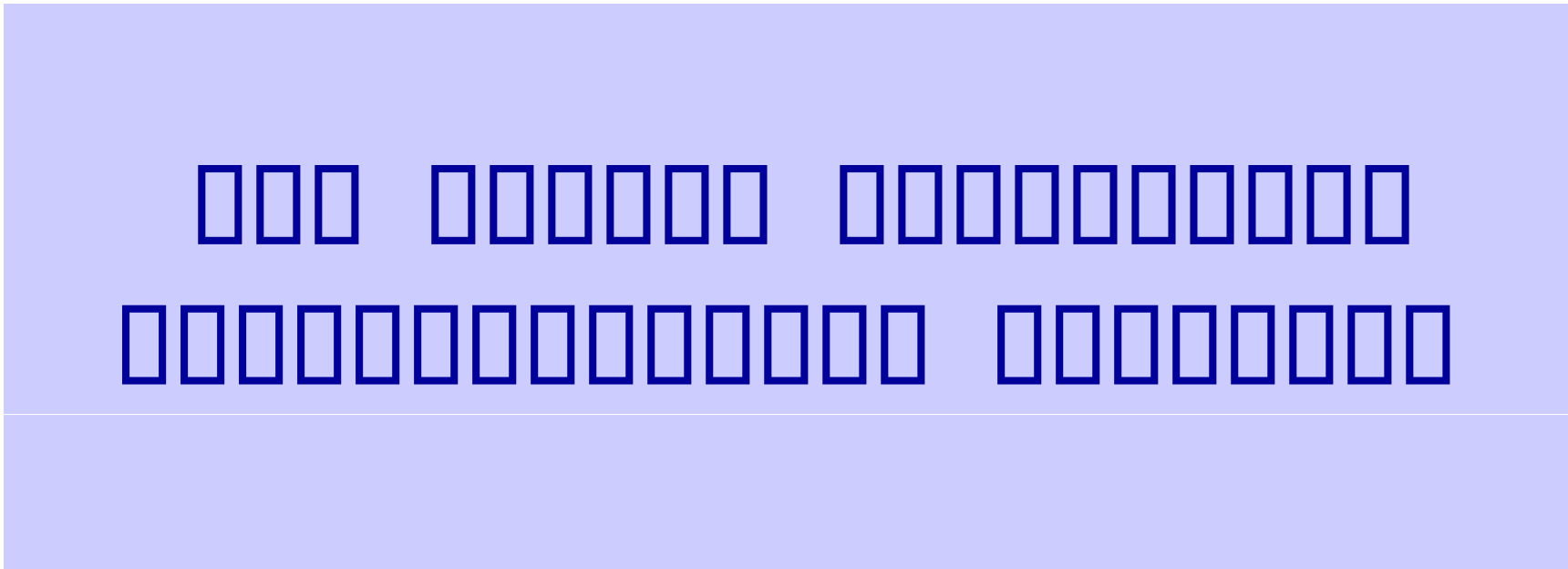
- 1. Dipartimento di Informatica, Università degli Studi di Firenze
- 2. Dipartimento di Informatica, Università degli Studi di Firenze
- 3. Dipartimento di Informatica, Università degli Studi di Firenze





Contents

- ▶ **Introduction**
 - **Security Assessment: A Brief History**
 - **Security Assessment: A Brief History (continued)**
- ▶ **Security Assessment: A Brief History**
 - **Security Assessment: A Brief History (continued)**
 - **Security Assessment: A Brief History (continued)**
- ▶ **Security Assessment: A Brief History**



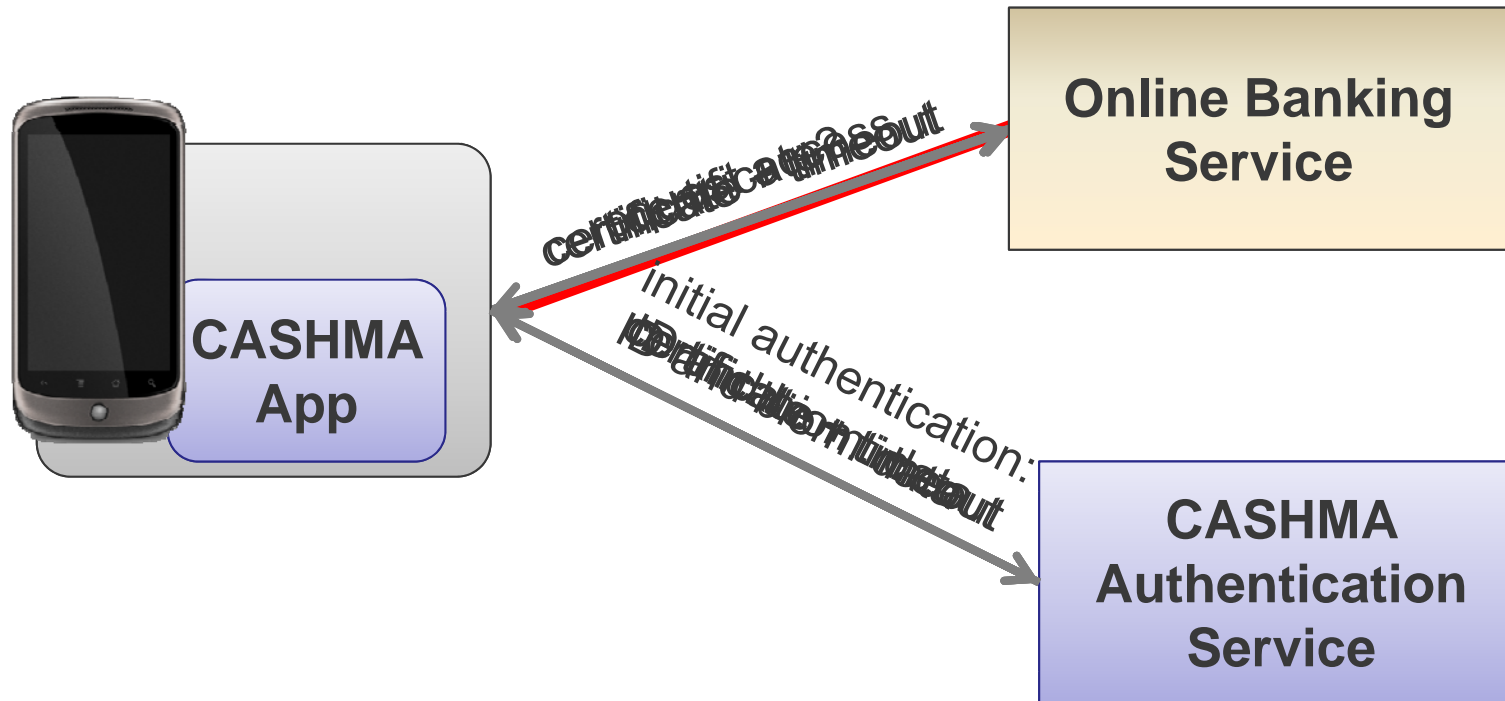


Context, motivations and objectives

- ▶ **Context** (Contexto) **Objectives** (Objectives) **Methodology** (Methodology) **Tools** (Tools) **Results** (Results) **Conclusions** (Conclusions)
- **Context** (Contexto) **Objectives** (Objectives) **Methodology** (Methodology) **Tools** (Tools) **Results** (Results) **Conclusions** (Conclusions)
- **Context** (Contexto) **Objectives** (Objectives) **Methodology** (Methodology) **Tools** (Tools) **Results** (Results) **Conclusions** (Conclusions)
- ▶ **Context** (Contexto) **Objectives** (Objectives) **Methodology** (Methodology) **Tools** (Tools) **Results** (Results) **Conclusions** (Conclusions)
- **Context** (Contexto) **Objectives** (Objectives) **Methodology** (Methodology) **Tools** (Tools) **Results** (Results) **Conclusions** (Conclusions)
- ▶ **Context** (Contexto) **Objectives** (Objectives) **Methodology** (Methodology) **Tools** (Tools) **Results** (Results) **Conclusions** (Conclusions)



Sample CASHMA scenario: online banking



► The user is notified of the certificate timeout and is prompted to re-authenticate. The user enters their credentials and the app sends them to the authentication service. The authentication service verifies the credentials and returns a new certificate to the app. The app then uses this certificate to access the online banking service.

– The user is notified of the certificate timeout and is prompted to re-authenticate. The user enters their credentials and the app sends them to the authentication service. The authentication service verifies the credentials and returns a new certificate to the app. The app then uses this certificate to access the online banking service.

– The user is notified of the certificate timeout and is prompted to re-authenticate. The user enters their credentials and the app sends them to the authentication service. The authentication service verifies the credentials and returns a new certificate to the app. The app then uses this certificate to access the online banking service.



Basics

□□□□□□□□□□. □ □□□□□□□ → □ □□□□□□□□□ □□□□□□

(□□□ □ □□□□□□□□ □□□□□□□□□□ □□)

▶ □□□□□ □□□□□ □□□□ □□□□ : □□□□□□□□□□□□ □□□□ □□□□
□□□□□ □ □□□□□ □□□□□ □□□□□

▶ □□□□□□□□□□ □□□□□ □□□□□ □(□□, □□): □□□□□□□□□□□□
□□□□ □□ □□ □□□□ □ □□□□ □□□ □□□□□□□□□□□□□□ □□
□□□□□□□□□□ □□□□□□□□□□□□ □□□ □□□ □□□□ □□□□
□□□□□□□□□□ □□ □□□□□□□□□□

▶ □□□□ □□□□□ □□□□□ □(□, □): □□□□□ □□ □□□ □□□□□
□ □□ □□□□ □

▶ □□□□□□ □□□□□ □□□□□ □□□□□(□, □): □□□□□□ □□□□□
□□ □□□□ □ □□□ □□□□ □ □□ □□□ □□□□□□ □□
□□□□□□□□□□ □ □□□□□□□□□□□□□□□□□□□□□



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

Initial trust value α_0

$$\alpha(\alpha_0, \alpha_0) = 1 - \beta(\alpha_0)$$

► $\alpha(\alpha_0, \alpha_1) = \alpha(\alpha_0, \alpha_0) \cdot \alpha^{-\beta \cdot \Delta t}$

$$\alpha(\alpha_0, \alpha_0) = \alpha(\alpha_0, \alpha_{0-1}) \cdot \alpha^{-\beta \cdot \Delta t}$$

Trust value at time t_i is calculated iteratively based on the previous trust value and the observed behavior of the subsystem.

∇ : Trust value at time t_i is calculated based on the previous trust value and the observed behavior of the subsystem.

∇ : Trust value at time t_i is calculated based on the previous trust value and the observed behavior of the subsystem.



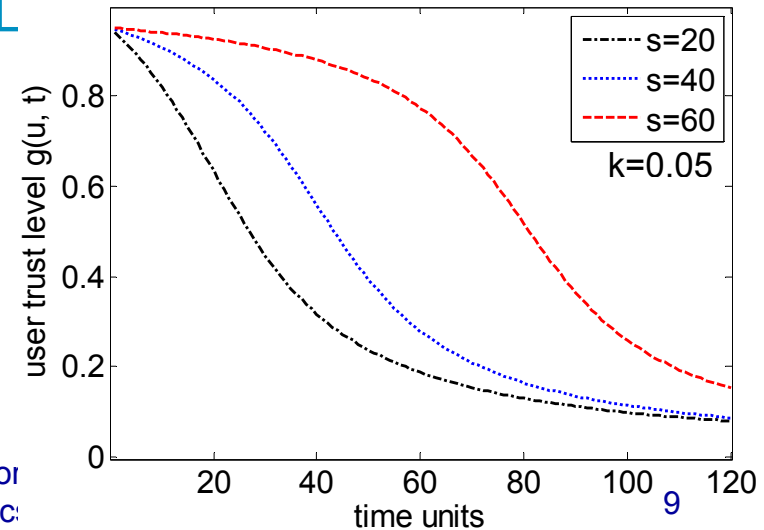
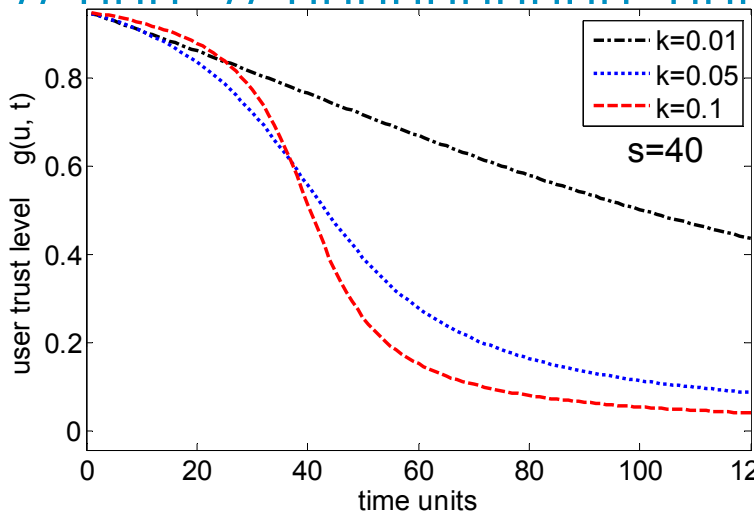
$g(u, t_i)$: trust in the user

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

Δt_i represents the time interval between t_{i-1} and t_i .

$\text{trust}(u, t_{i-1})$ represents the trust level at the previous time step.

The graph shows the evolution of the trust level $g(u, t)$ over time units.





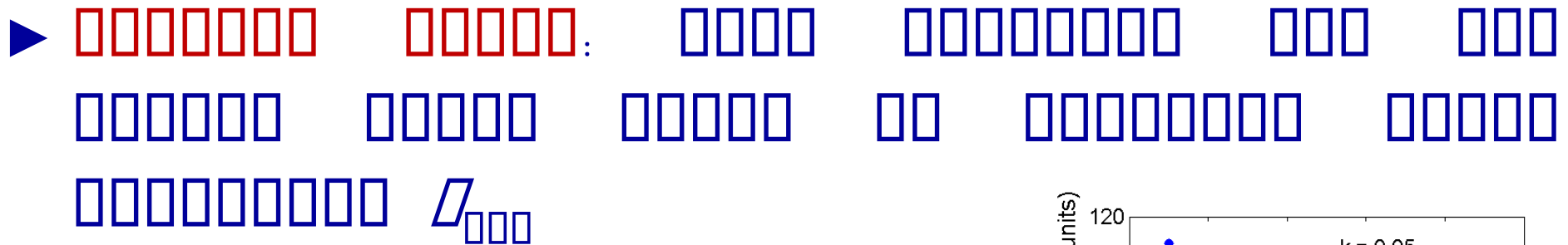
g(u, t_i): global trust level

T_i: timeout

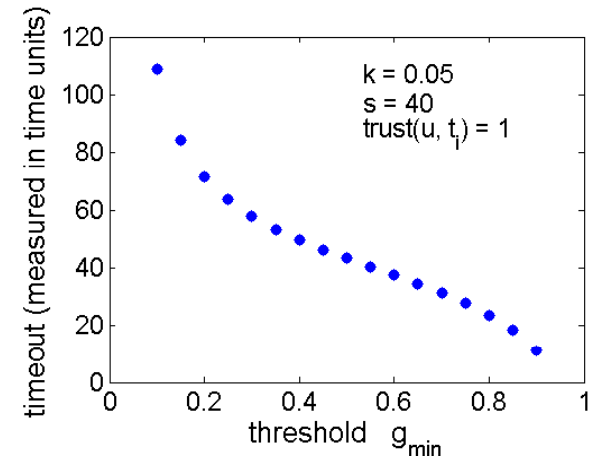
$$trust(u, t_0) = 1 - \prod_{k=1..n} (1 - m(S_k, t_0))$$

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

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



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

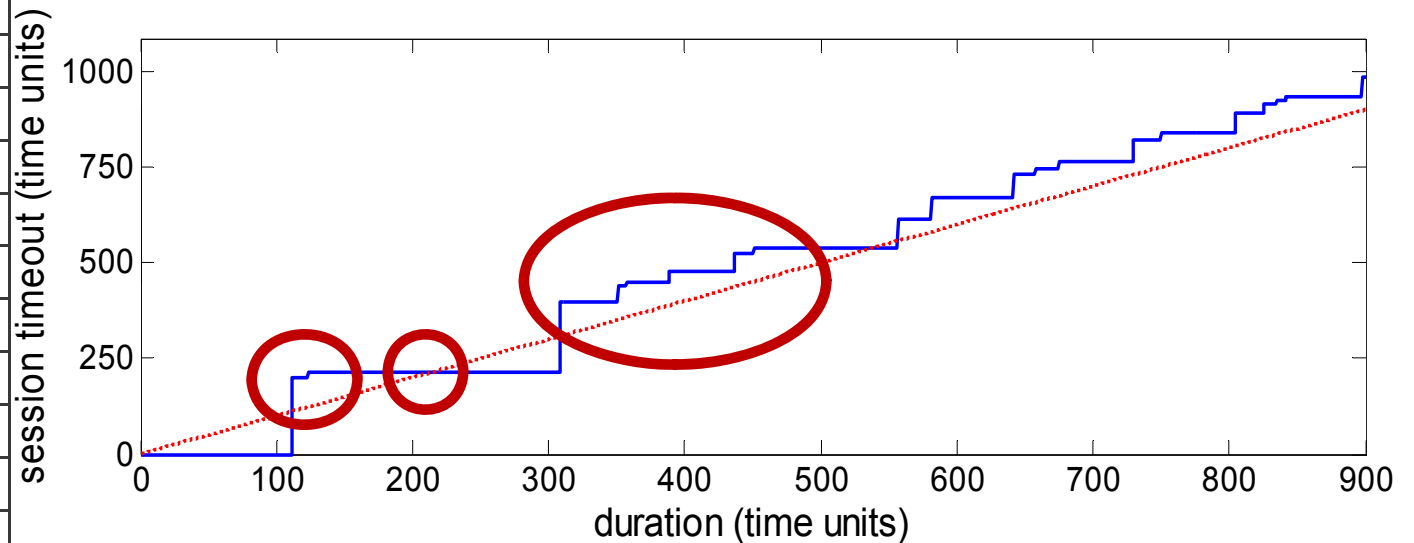
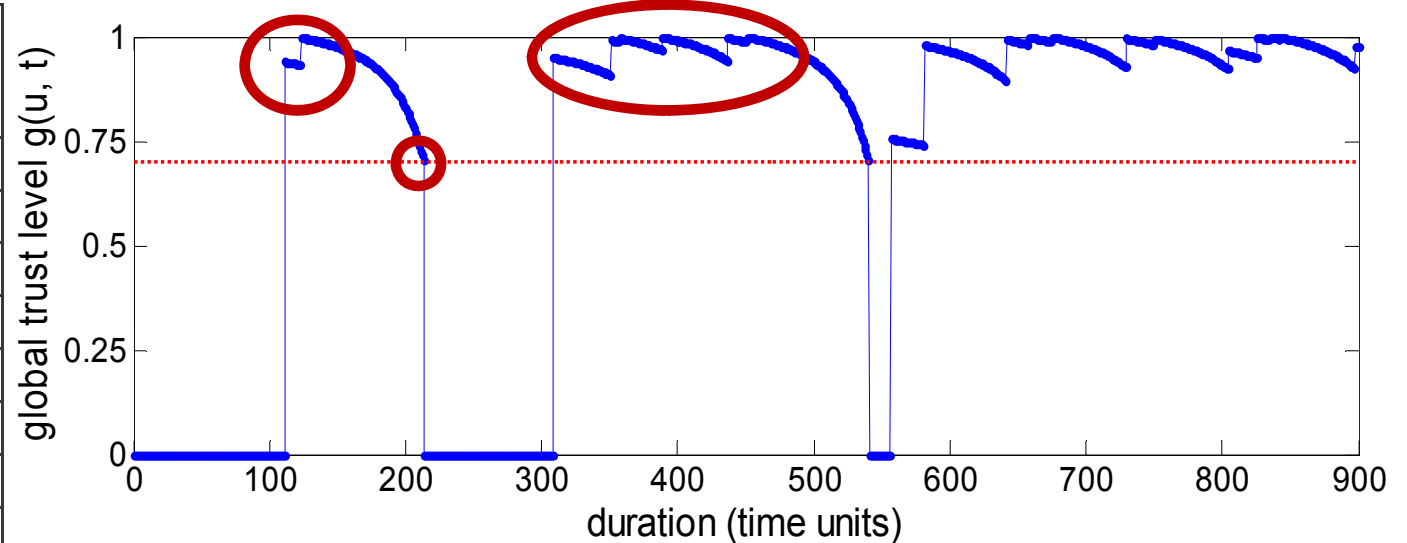




Exemplary runs

$g_{\min} = 0.7$ $k=0.05$ $s=100$

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. **ADversary View Security Evaluation (ADVISE)**

- **ADversary View Security Evaluation (ADVISE): ADVISE**
ADVISE, ADVISE ADVISE, ADVISE, ADV ADVISE

2. **ADversary View Security Evaluation: ADV ADV ADV ADV ADV**
ADVISE ADVISE, ADVISE ADVISE ADV ADVISE
ADVISE, ADV ADVISE:

- **ADVISE, ADVISE, ADVISE ADVISE**

► **ADV ADVISE ADVISE ADV ADVISE**
ADVISE ADV ADV ADVISE ADVISE, ADV

E. LeMay, M.D. Ford, K. Keefe, W.H. Sanders, G. Muenchke, "Model-based Security Metrics Using ADversary View Security Evaluation (ADVISE)". QUEST 2011: 191-200



Definition of the adversaries

► **Adverse Organization** **Technology Master Individual** **Generic (malicious) individual** **Insider** (OOO)

Access **Limits** **Resources** **Skill-Hack** **Skill-Spoofing** **Visibility**

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

► : , ,

#1: 2 .

#2: 3 .

#3 3 .
A. Ceccarelli



Attackers description

▶ **Attacker 1** (Low):
Access to one counterfeit biometric sample (voice)

– **Attacker 2** (Medium):

- access to one counterfeit biometric sample (voice)

– **Attacker 3** (High):

- access to two counterfeit biometric samples (voice + face)

– **Attacker 4** (Very High):

- knowledge of some system details

– **Attacker 5** (Expert):

▶ **Attacker 6** (Expert):

$P_{\text{acc}}(\text{acc})$ $P_{\text{acc}}(\text{acc})$ $P_{\text{acc}}(\text{acc})$ $P_{\text{acc}}(\text{acc})$ $P_{\text{acc}}(\text{acc})$

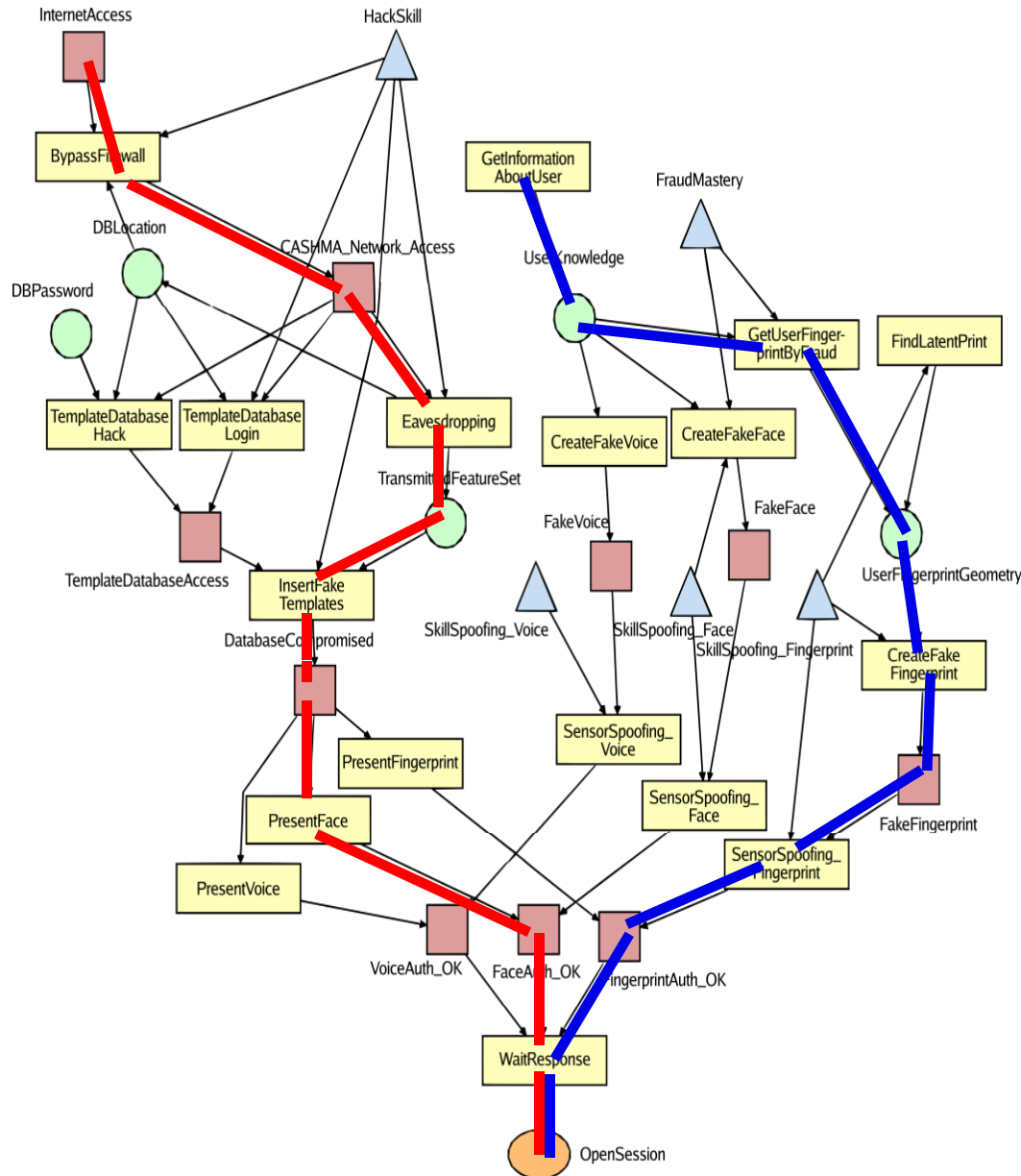


Attackers description - parameters

		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 □□□□□□ □□□□

10 □□□□□□ □□□□□□□

5 □□□□□□□□□□ □□□□□

5 □□□□□□ □□□□□□

18 □□□□□□ □□□□□□

□□□□□□ □□□□□□:

- □□□□ 1

- □□□□ 2

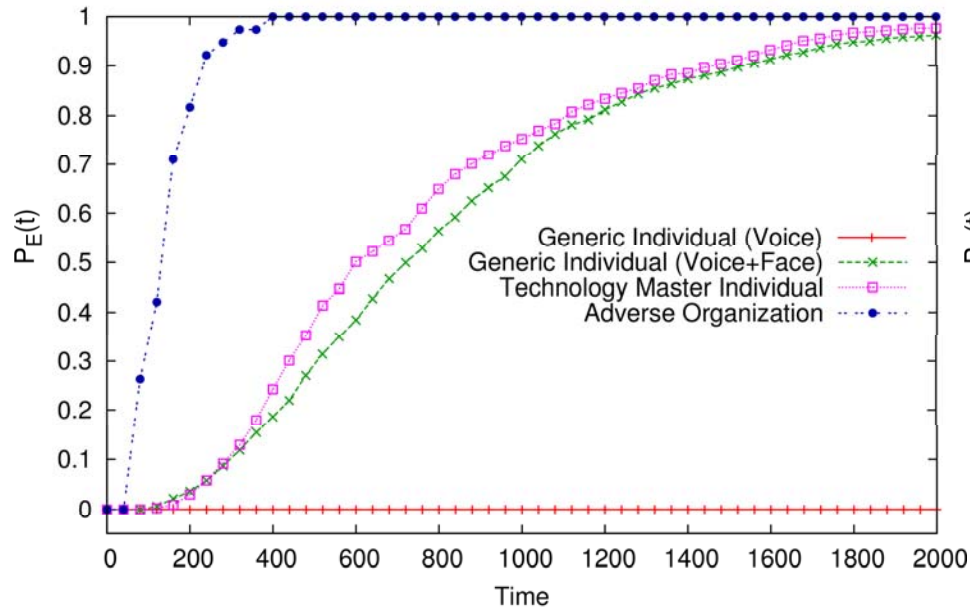


Evaluation and Results - 1

□□□□□□□□

#1

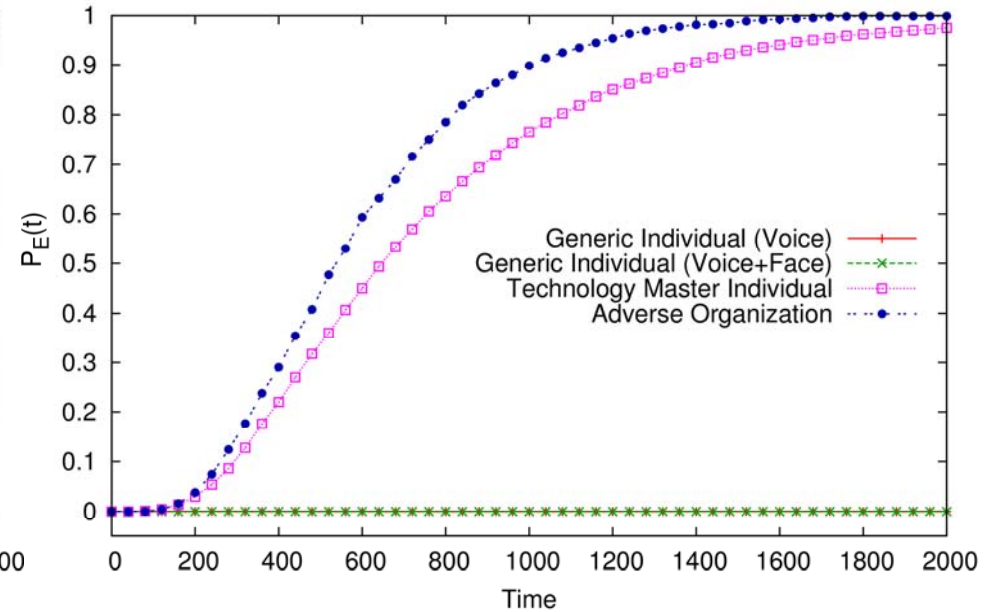
Probability that, at time t, the attacker has been successfully authenticated
Authentication requires 2 biometric traits



□□□□□□□□

#2

Probability that, at time t, the attacker has been successfully authenticated
Authentication requires 3 biometric traits



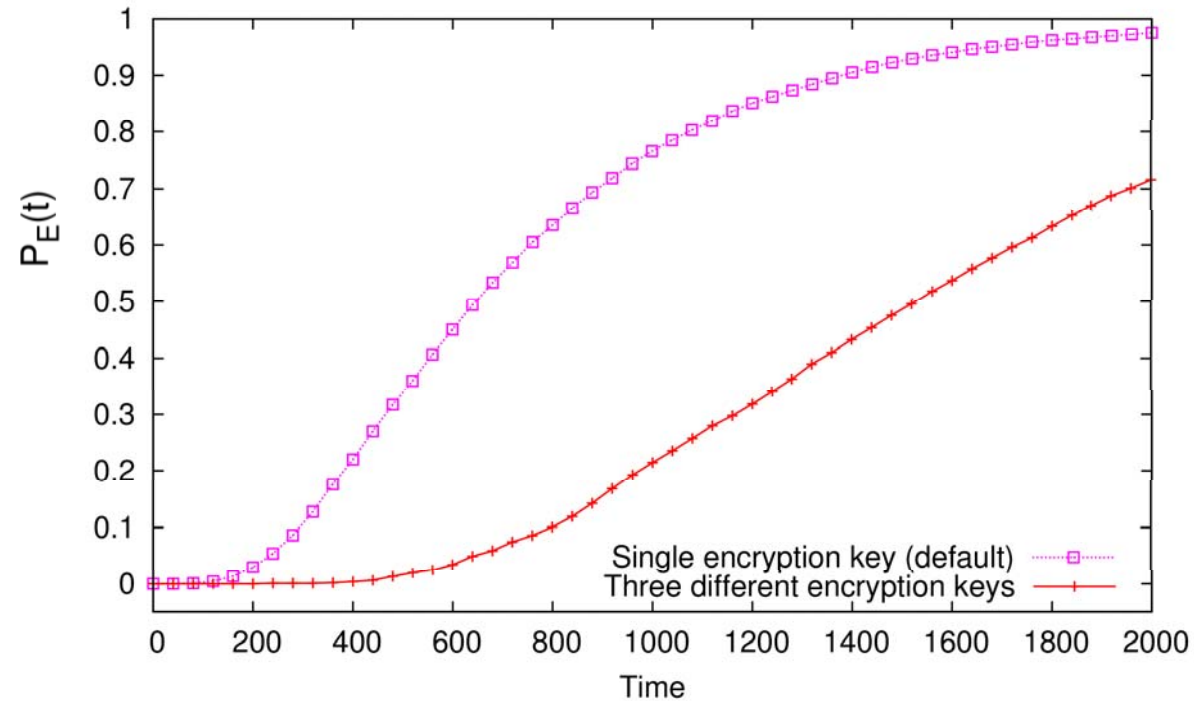
#1 □□□□ □□□□□□□□□□□□□□□□ □□□□□□□□ □□□□ □□□ □□ □□□ □□□□□
 □□□□□□□□□□ □□□□□□□□ □□□□□□□□ □□□□ □□□□□□□□□□□□ □□□□□ □
 □□□□□□ □□□□□□□□□□□□ □□□□

#2: □□□□ □□□□□□□□□□□□□□ □□□□□□□□ □□□ □□□ □□□□□□□□□□
 □□□□□□□□□□ □□□□□□□□ □□□□□□□□ □□□□ □□□□□□□□□□□□ □□□□□ □
 □□□□□□ □□□□□□□□□□□□ □□□□



Evaluation and Results - 2

Probability that, at time t , the attacker has been successfully authenticated
 "Technology Master Individual" adversary profile
 Authentication requires 3 biometric traits



Scenario #3 (Attacker uses a default encryption key)

- The attacker uses a default encryption key to authenticate. The probability of successful authentication is significantly higher than when three different encryption keys are used.



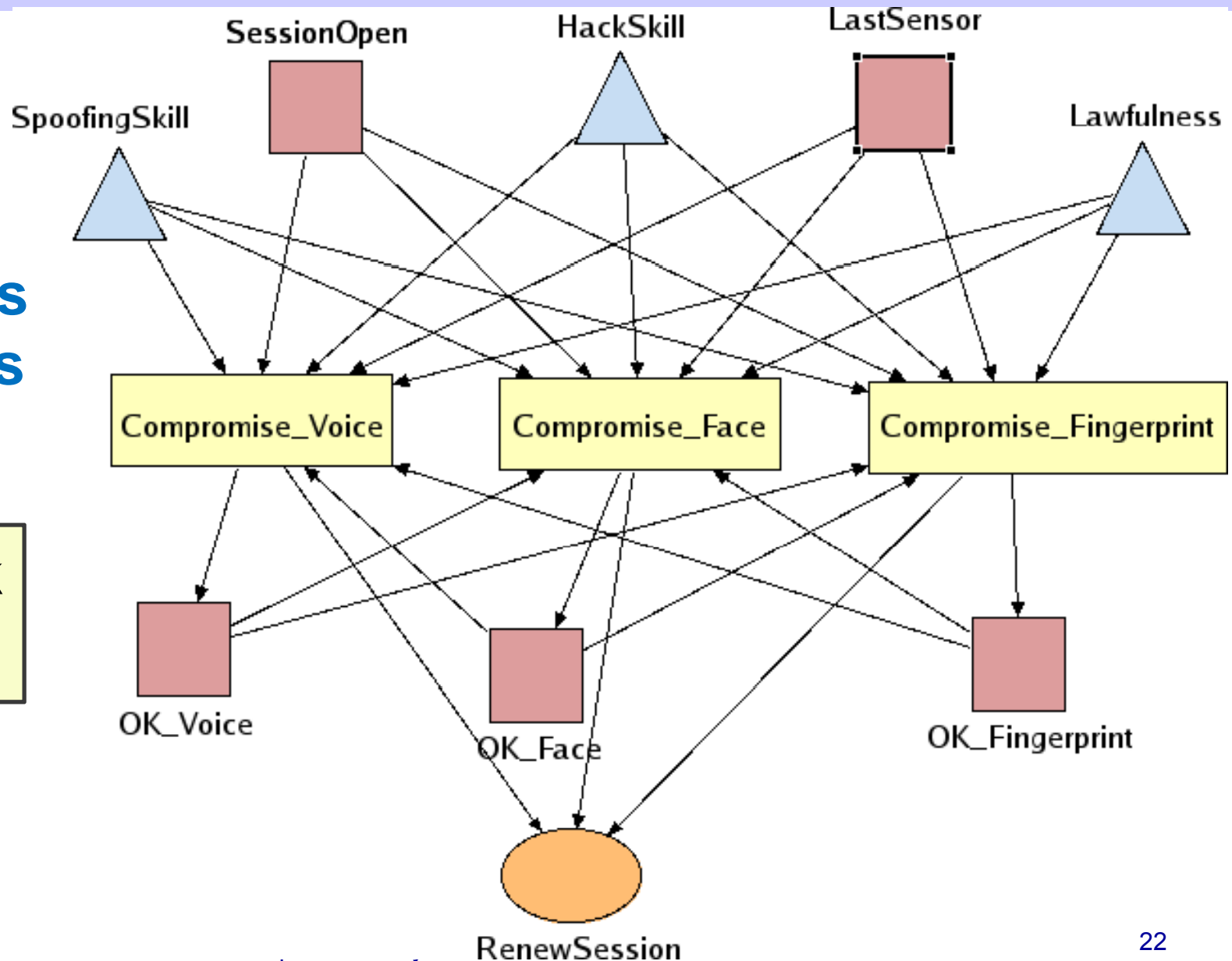
Attack Execution Graph

3 skills

6 access domains

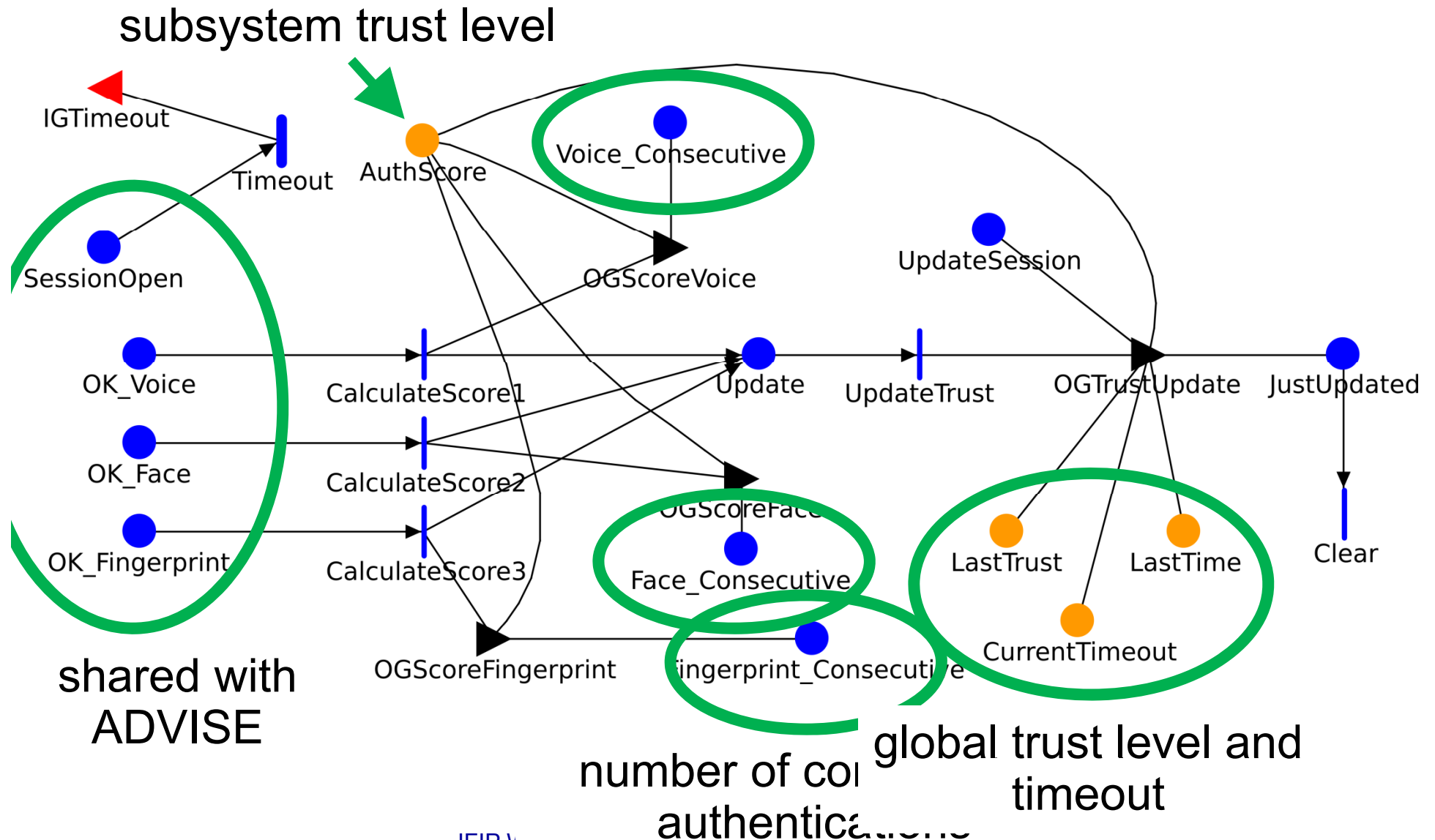
3 attack steps

1 goal





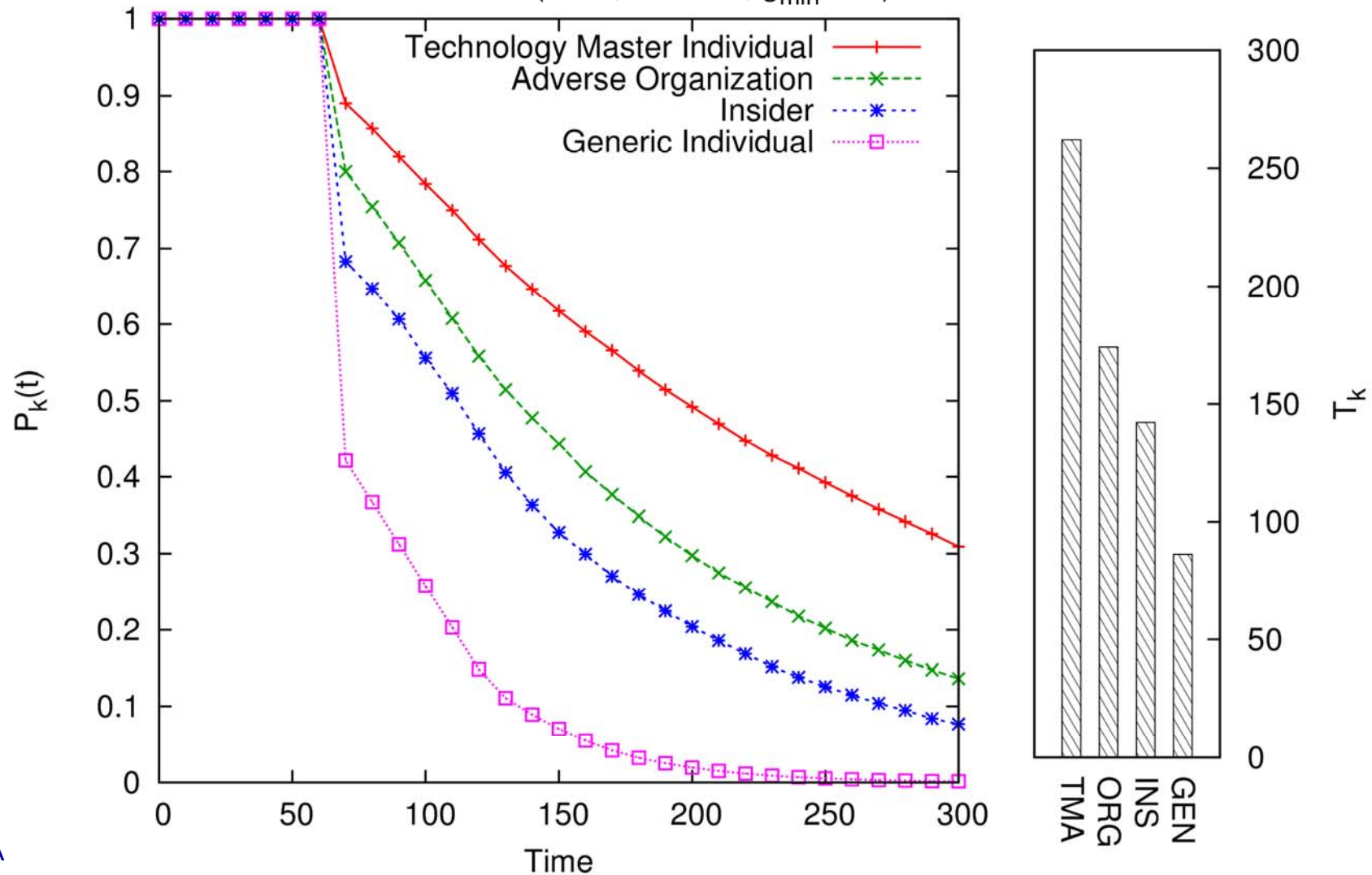
SAN model of the continuous authentication protocol





Effectiveness for different attackers

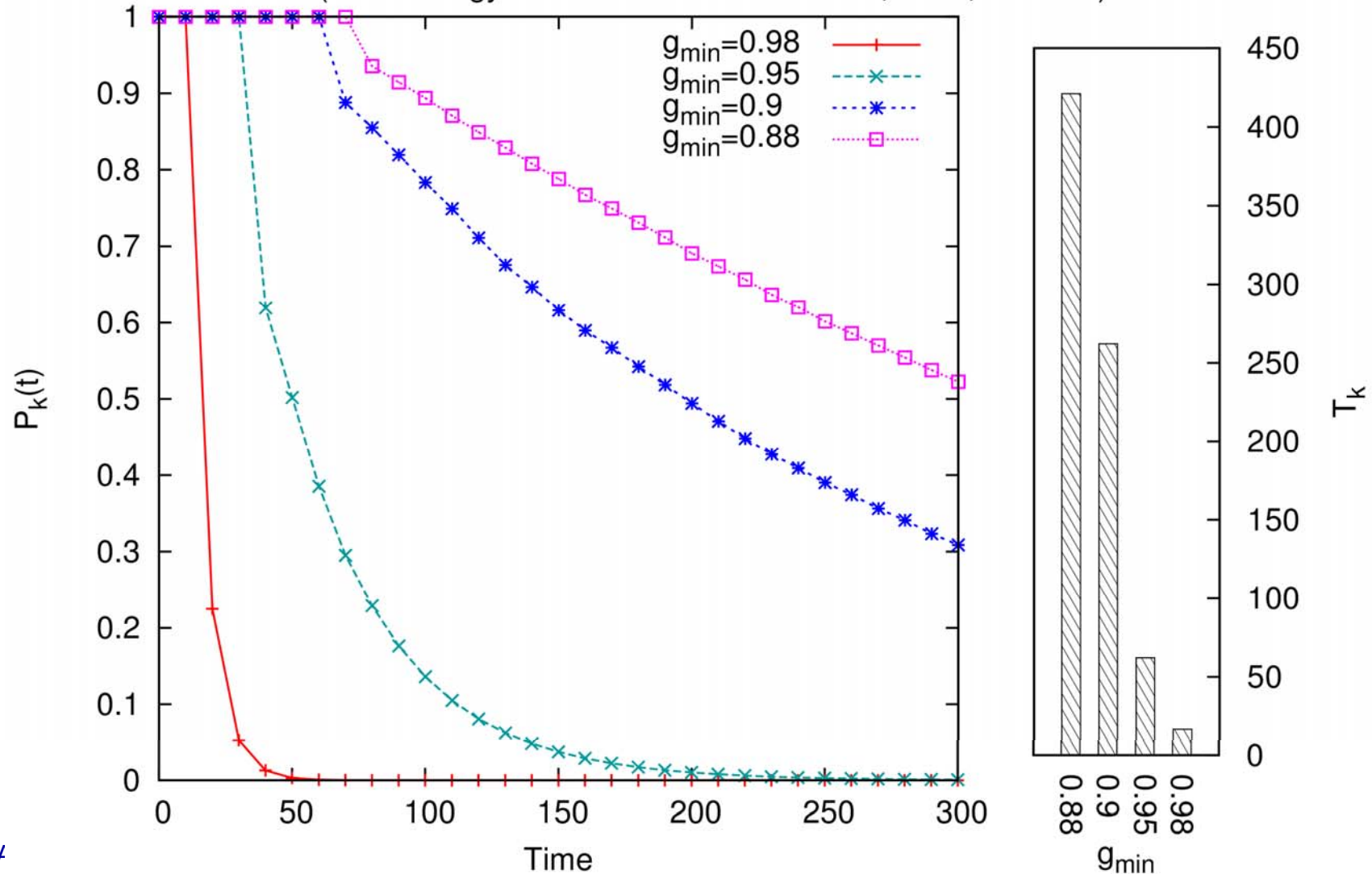
[Left] Probability that the attacker is able to keep the session alive until time t
[Right] Mean time for which the attacker is able to keep the session alive
($s=90$, $k=0.003$, $g_{\min}=0.9$)





Effectiveness of tuning thresholds on TMA attacker

[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
("Technology Master Individual" attacker, $s=90$, $k=0.003$)





Conclusions



Conclusions

► **Security assessment** is a **complex** and **ongoing** process that involves **multiple** stakeholders and **continuous** communication and collaboration.

► **Security assessment** is a **holistic** process that covers the **entire** system, from **requirements** to **implementation** and **operation**.
Security assessment 4.0

– **Security assessment** is a **continuous** process that evolves over time as the system and its environment change. It involves **regular** updates and re-assessments to ensure the system remains secure.

– **Security assessment** is a **holistic** process that covers the **entire** system, from **requirements** to **implementation** and **operation**.
Security assessment 8.4

► **Security assessment**:



References

► G. De Santis, G. De Santis, G. De Santis, G. De Santis, G. De Santis, G. De Santis, G. De Santis, G. De Santis, "The Security Assessment Metrics and Methods (SAMM) Framework: A Review of the State of the Art". In Proceedings of the 2012 IEEE Conference on Systems, Man, and Cybernetics (SMC), 2012, pp. 201–206.

► G. De Santis, G. De Santis, G. De Santis, G. De Santis, G. De Santis, G. De Santis, G. De Santis, G. De Santis, "The Security Assessment Metrics and Methods (SAMM) Framework: A Review of the State of the Art". In Proceedings of the 2012 IEEE Conference on Systems, Man, and Cybernetics (SMC), 2012, pp. 201–206.

► G. De Santis, G. De Santis, G. De Santis, G. De Santis, G. De Santis, G. De Santis, G. De Santis, G. De Santis, "The Security Assessment Metrics and Methods (SAMM) Framework: A Review of the State of the Art". In Proceedings of the 2012 IEEE Conference on Systems, Man, and Cybernetics (SMC), 2012, pp. 201–206.

