



TURBINE Security Assessment: How to Build Trust

Koen Simoens
K.U.Leuven – COSIC

TURBINE Final Workshop
Brussels, 17-18 January 2011

Sidecar Recipe



Ingredients for a Sidecar	Quantities for one drink
Cognac	2 oz Cognac
Cointreau	1/2 oz Cointreau
Lemon Juice	1 oz Lemon Juice

Blending Instructions

1) In a shaker half-filled with ice cubes, combine all of the ingredients. 2) Shake well. 3) Strain into a cocktail glass.

Serving Glass

Cocktail glass

Nutrition Facts (per 4.6 oz serving)

Calories (kcal)	117	Fiber	0.1 g
Energy (kj)	492	Sugars	9.7 g
Fats	0 g	Cholesterol	-
Carbohydrates	11.3 g	Sodium	0 mg
Protein	0.1 g	Alcohol	12 g

The Crypto-Biometrics Cocktail

- Headline of today:
 - *How Research Can Combine Biometrics, Cryptographic and Architecture for Trusted Identities*
- Template Protection Recipe
 - Put **biometrics** in your cocktail shaker
 - Pour **architecture** over it
 - Top some **crypto**-flavor (carefully)
 - **Shake** vigorously (do not stir)
 - Garnish with a cherry and serve with a **straw**



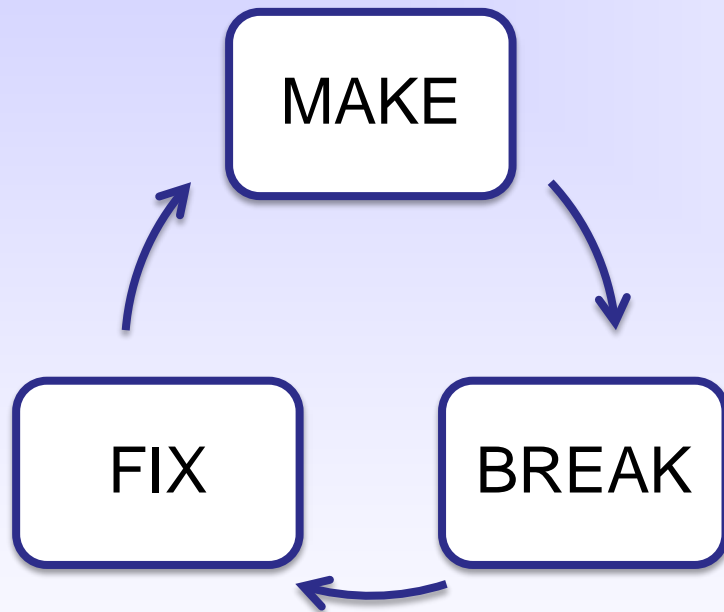
This Talk

- Reflection on TURBINE security analysis
- How to build trust
- Some results and conclusions
- Outlook (where to go next)



How to Build Trust

How to *BUILD* trust



- **Self-assessment**
 - Too often missing
 - Requires change in mindset
 - Prove security (rarely possible)
- **Independent** evaluation
 - Cf. biometric performance testing
 - Scrutiny of the scientific community
- Advancing progress in the field
 - I make, I break, I fix, you break, you fix, I break, I fix, I make, they break...

The Assessment Process

- Threat analysis and risk assessment
 - Security requirements (attack resistance)
 - Impact motivates what to analyze
- Evaluation Phases
 - **Theoretical** verification of requirements
 - Come up with attacks
 - **Practical** experiments and testing
 - Verify attacks, countermeasures, real data
 - Early feedback to developers
 - Process updates and fixes
- Received 7 “submissions” (5 initial, 2 fixes)

Terminology Pitfall

- On the use of the word “trust”
 - **What is trust?** How do you define trust?
 - An abundance of books and articles on trust
 - Reliance, assurance, confidence... (emotional)
- Translate into “**can be measured**”
 - Need numbers (we often fail...)
 - That can be compared with each other
 - Or with some threshold



Results and Conclusions

What To Test?

- 7 submitted template protection **methods**
 - Not just template-level (PI algorithms)
 - Advanced protocols (cf. Julien Bringer's Talk)
- Goals of template-level protection
 - One-way transformation: **irreversibility**
 - Diversification: **unlinkability** and revocability
 - Evaluate properties based on fundamental principles
- Goals of advanced protocols
 - Prevent access to biometric data
 - Provide **additional properties** (e.g. anonymity)
 - Challenge **trust assumptions**

Error-Correcting Codes Constructions

- First analysis of constructions based on error-correcting codes (fuzzy commitment,...)

- **Linkability/reversibility** issues

- *Simoens et al., "Privacy weaknesses in biometric sketches," IEEE Symp. SP2009*

- Given the best code and 12.5% noise-tolerance

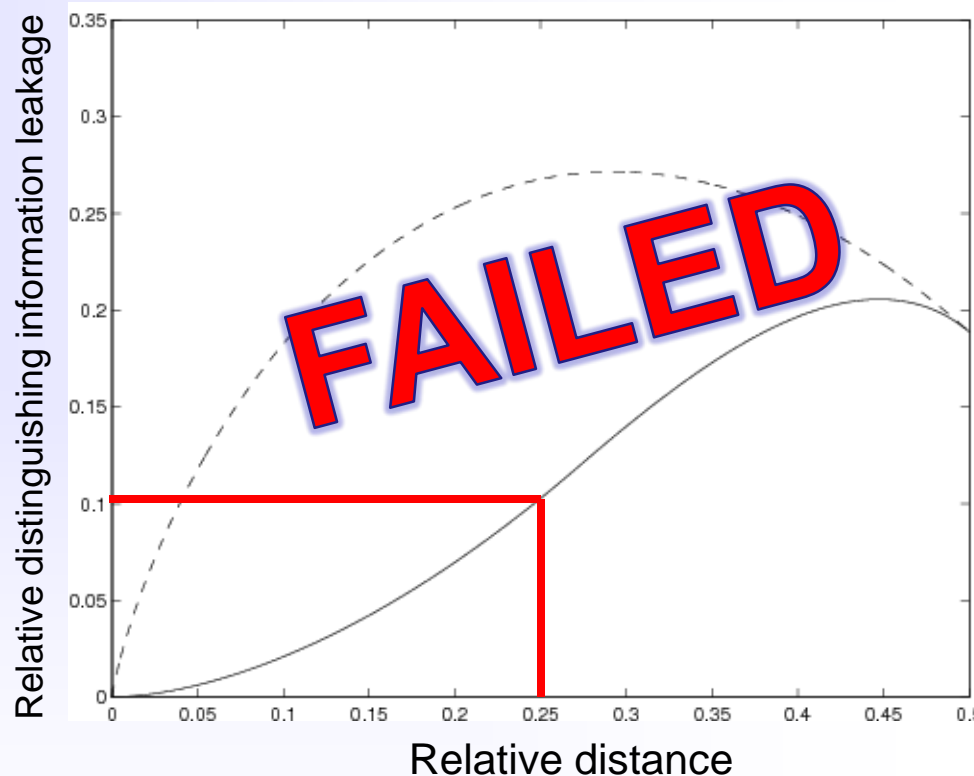
- At least 10% of the bits distinguishing information leakage

- Rudimentary assumptions

- **Fix proposed**

- *Kalkbrenner et al., "Preventing the decodability attack based on the modeling in a fuzzy commitment scheme," IEEE Tr. Inf. For. & Sec. 2010*

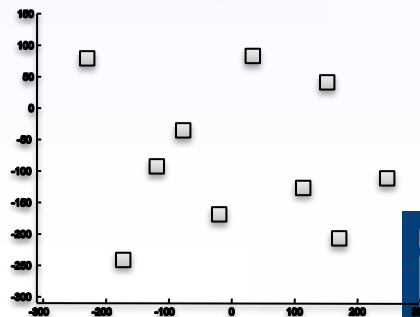
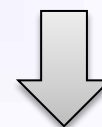
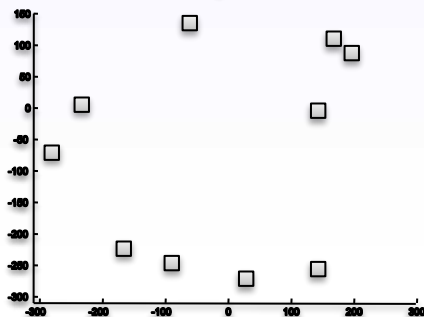
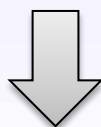
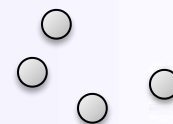
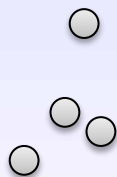
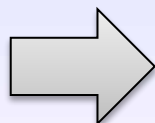
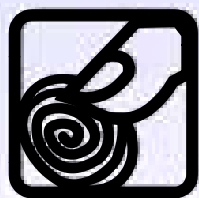
PASSED



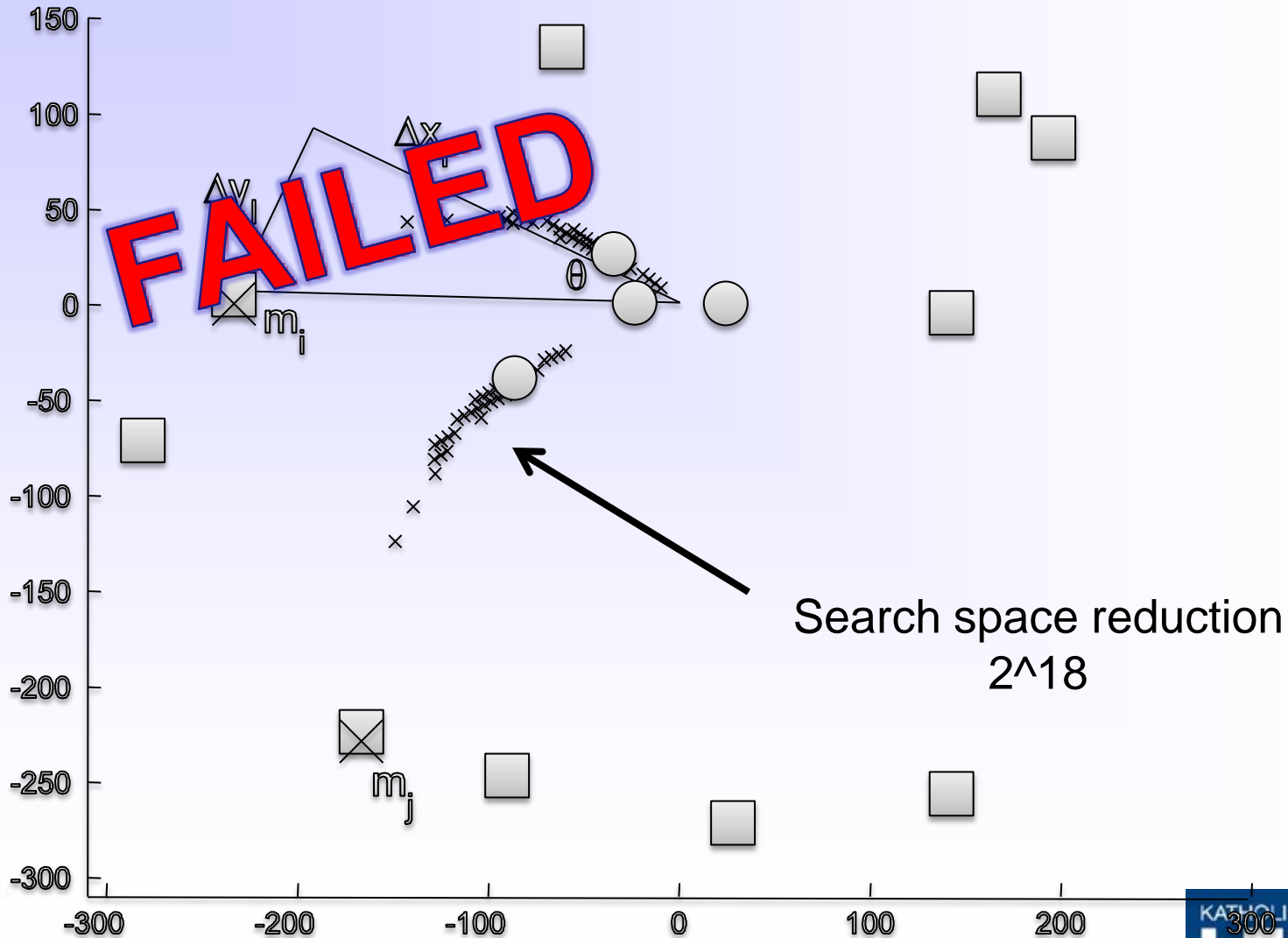
— lower bound
 - - - upper bound

Geometric Vicinity Transformation

- **Estimated complexity** : find short cut
 - » *Simoens et al., "Reversing protected minutiae vicinities," BTAS 2010*
- Regression attack on
 - » *Bian et al., "Parameterized geometric alignment for minutiae-based fingerprint template," BTAS 2009*
- Vicinity methods **lack inherent complexity**



Geometric Vicinity Transformation

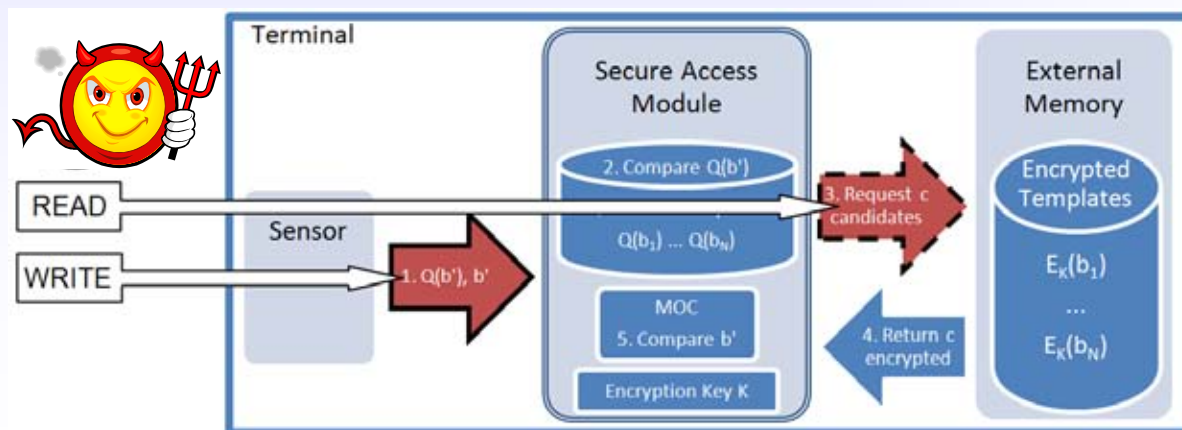


Some Thoughts

- Both attacks produce **numbers**
 - Try the attacks => e.g. time complexity, average success probabilities
 - Get your hands dirty (use real data, simulations)
- But how do you **compare security**?
 - Construction based on error-correcting codes
 - With geometrical transformations
 - What is reversibility for one versus the other?
 - Leaking minutia positions or bits?
- Sometimes you **fix, sometimes** you don't
- Many different required **skills**: #1 = creativity
- **The straw matters**
 - Security testing complements performance testing

Protocol : SAC Terminal

- Major case to analyze
 - Potentially high impact on breach (runway access)
 - Potentially high loss of biometric data (database)
- Attack scenarios **challenge assumptions**
- Secure hardware component : **blackbox**
 - » *Bringer et al., "Blackbox security of biometrics (invited paper)," IIH-MSP 2010*

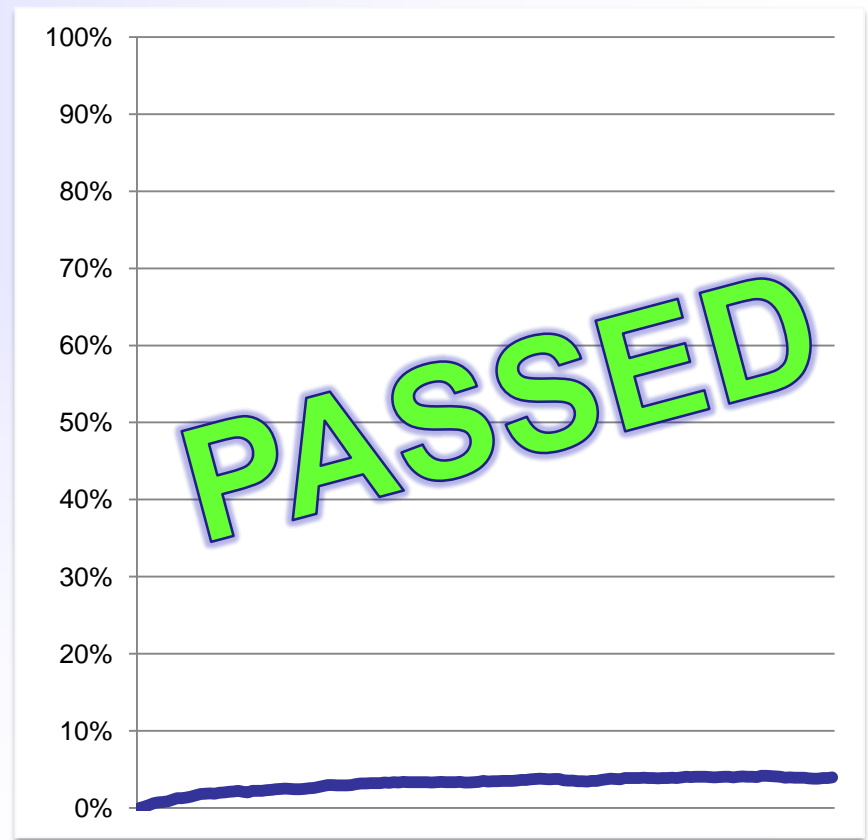


Try It With Real Data: Make-Break-Fix:

First version:
quantized database leaked



Countermeasures and new quantization
scheme (talk V. Despiegel)



Top Crypto-Flavors Carefully

- Extension of **blackbox model** to other works
 - Distributed authentication protocols
 - A number of schemes broken when defined in the malicious adversary model
 - » *Simoens et al., “Analysis of biometric authentication protocols in the blackbox model,” arXiv:1101.2569*
- **Beware** of homomorphic encryption
 - Matching on encrypted data (popular)
 - Malleable : other people can do things too

Other Protection Methods

- **Group Signature** protocol

- (cf Julien Bringer's talk)
- Secure, relying on specific assumptions

PASSED

- **Diversified random projection**

- Substantial inversion and linkability issues
 - » *Yang et al., "Renewable Minutiae Templates with Tunable Size and Security. Pattern Recognition," ICPR 2010*

FAILED

- **Dynamic random projection**

- Fix for the previous method
- Using a dynamic input-dependent method to assemble projection matrices
 - » *Yang et al., "Dynamic random projection for biometric template protection," BTAS2010*

PASSED



Outlook

Bloody Minutiae Twist



Ingredients	Quantities
ECC	Binary [n,k,d] code
One-way function	256-bit hash function
Permutation	Size n permutation matrix

Blending Instructions
Enroll: 1) Permute sample. 2) Add random codeword. 3) Hash codeword...

Serving
Use for X, do not use for ?

Properties			
Best known full rev. attack	Code search	Avg. complexity	2^k
Best know link. attack	?		
Biometric performance	123		?
	?		?
	?		?

INCOMPLETE



What's Next

- **NIST Project** – Award 60NANB10D217
 - *Developing Metrics for a Benchmarking-Framework to Rank Biometric Template Protection*
 - Continuation of the TURBINE evaluation
 - Gjøvik University College
 - Katholieke Universiteit Leuven
 - Consensus on issues and challenges
 - But what are the actual nutrition facts?
 - How to measure and compare?
 - Missing **properties** ?
- Results coming soon

Conclusion

- TURBINE helped making progress
 - By breaking, fixing and learning
- There are open issues (future work)
- Remember
 - It is not the same as cryptography
 - It is not the same as biometrics
 - It is not the same as protocols
- It is a cocktail!

Thank You



Gin Face
Tequila Iris
Iris Colada
Gait on the Beach



koen.simoens@esat.kuleuven.be

FP7 Integrated Project TURBINE (TrUsted Revocable Biometric IdeNtitiEs)