Strengthening applets on legacy SIM cards with singularization, a new Moving Target Defense strategy

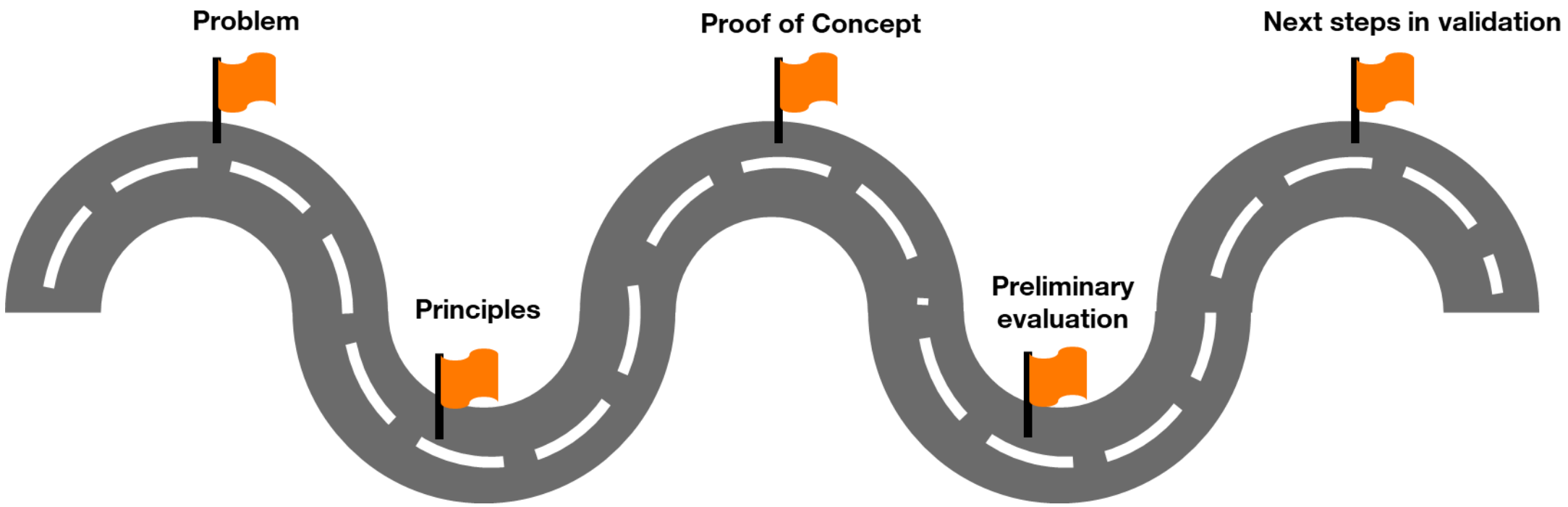
Chrystel Gaber, Jean-Philippe Wary

28/05/2025

AMTD 2025

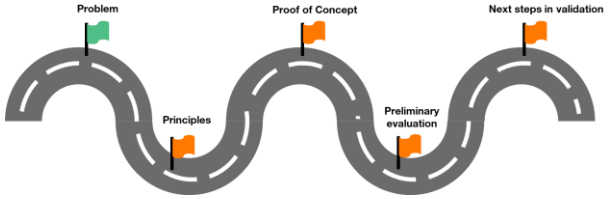
https://www.manufacturedelongchamp.com/collection/kintsugi

Outline



Orange Restricted

Problem



CyberSecurity Act Assurance Levels

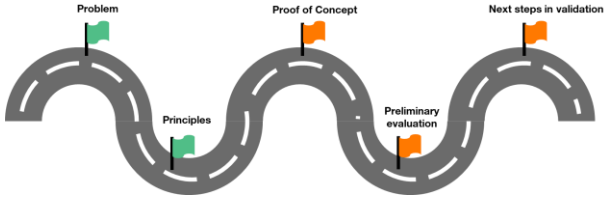
HIGH		SUBSTANTIAL	BASIC
eSIM	NFC SIMs	Legacy SIMs	

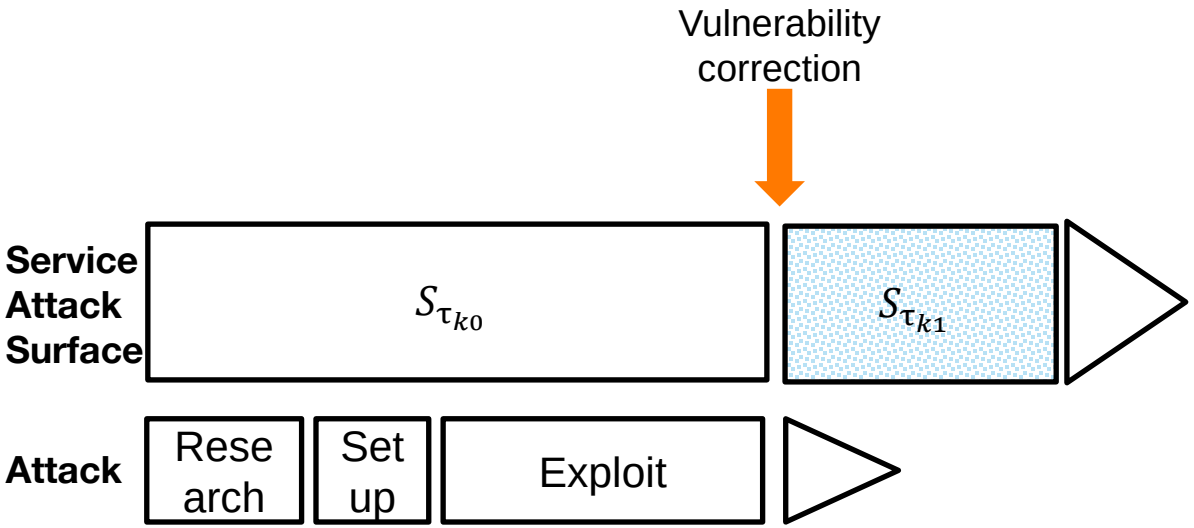
Estimated : 100 million SIMs in Europe for Orange
Estimated cost to replace : 1.5 billion euros
« Natural » roll out estimated in the next 10 years

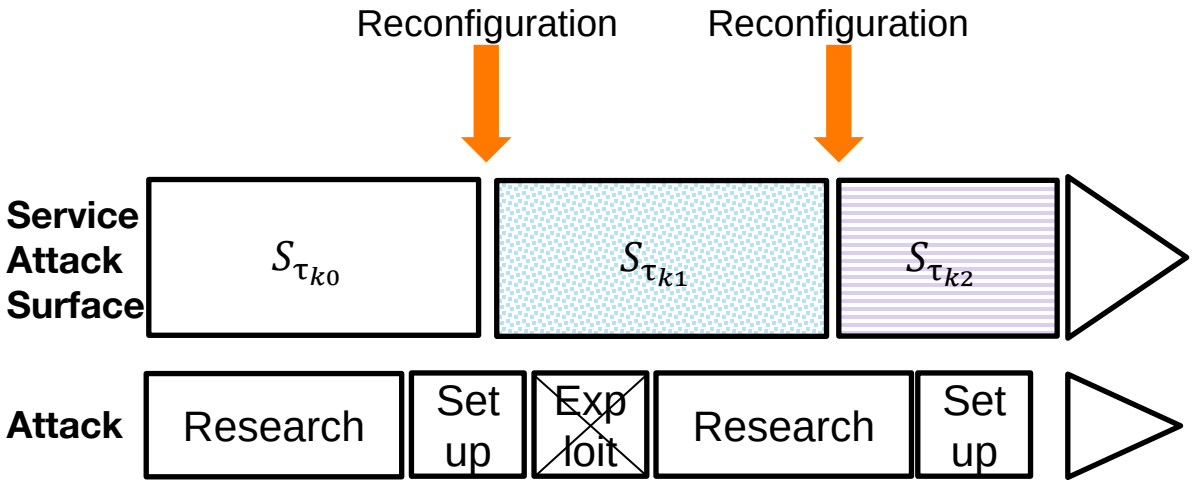
Incompatibility between **assurance levels** required by **use cases** (e.g. identity) & level offered by **legacy SIMs**

Orange Restricted

Principles: Moving Target Defense





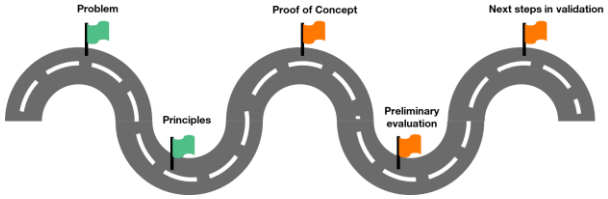


Without MTD
The attack is successful until next patch
Some pain, big gain

With MTD
Attacks are prevented if reconfiguration time < time to attack
Big pain, no gain

Orange Restricted

Principles: Singularization



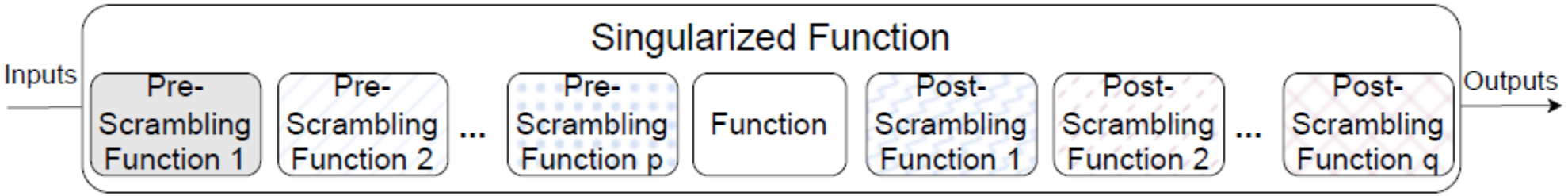
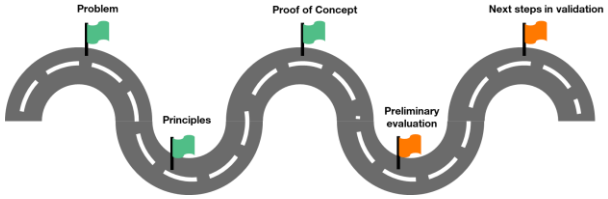


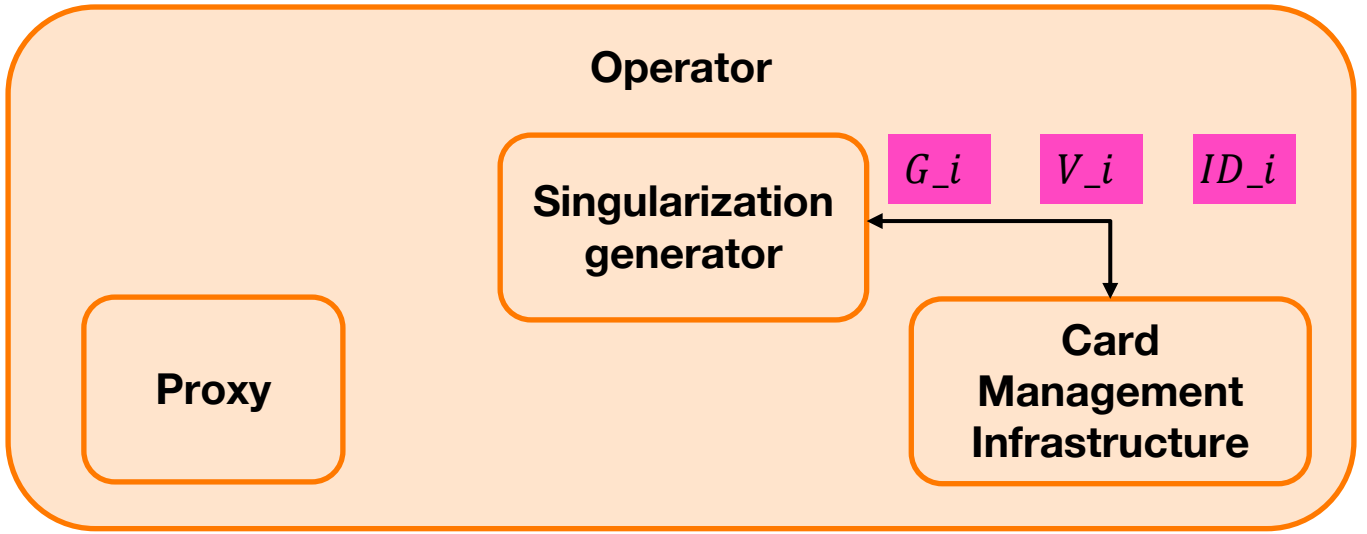
Fig. 1. Singularized Function

The functionality of the code is singularized for each target

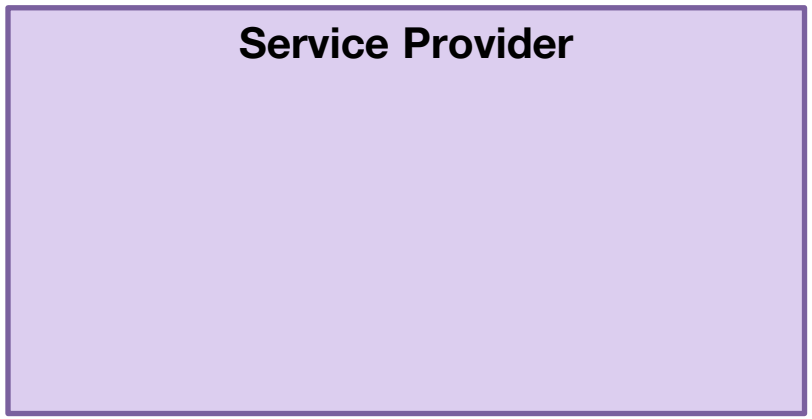
Orange Restricted

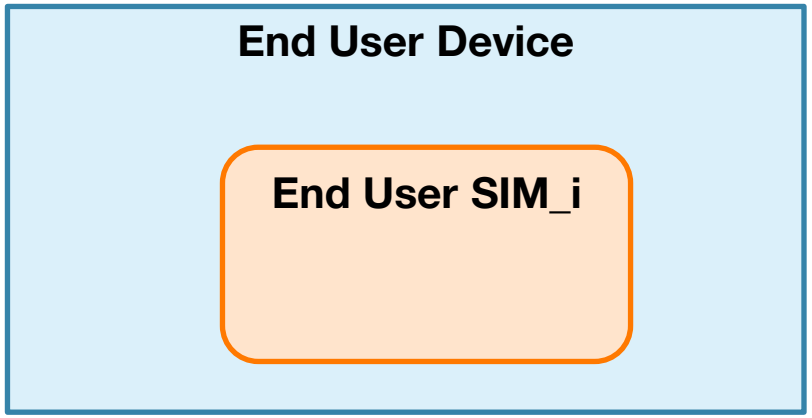
Proof of concept : step 1





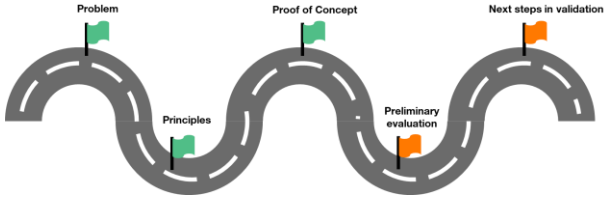
Generate singularized function G & counterpart V

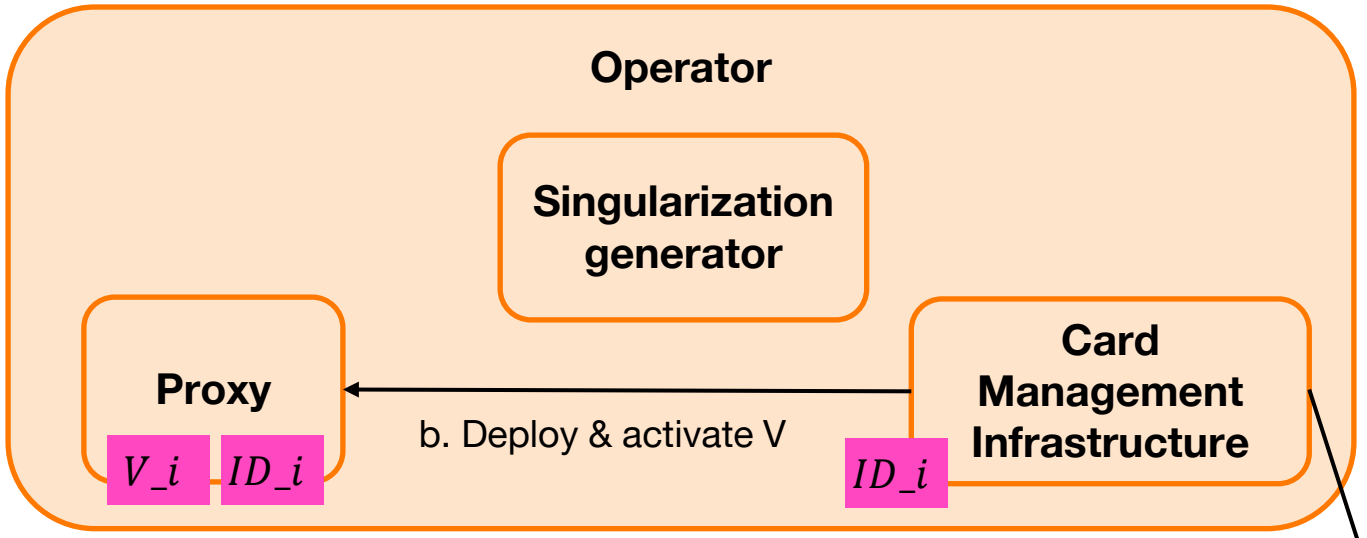




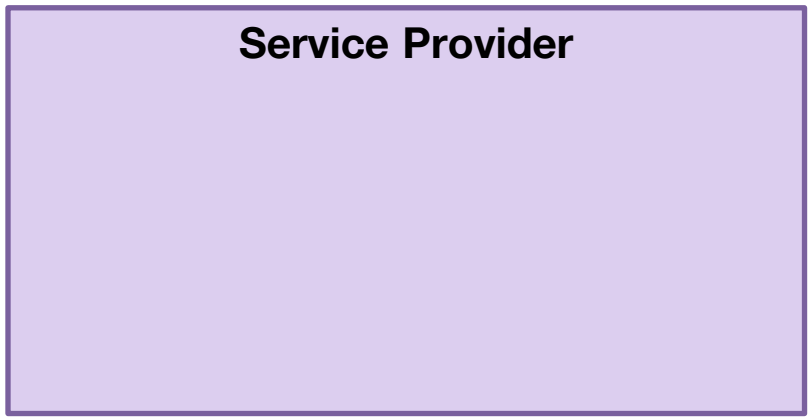
Orange Restricted

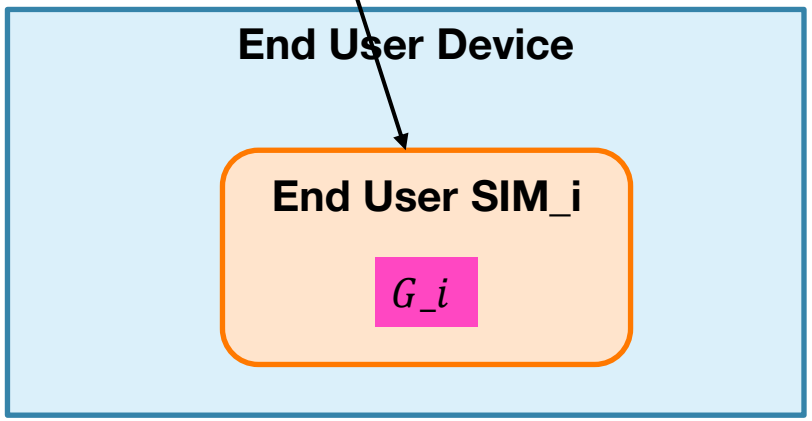
Proof of concept : step 2





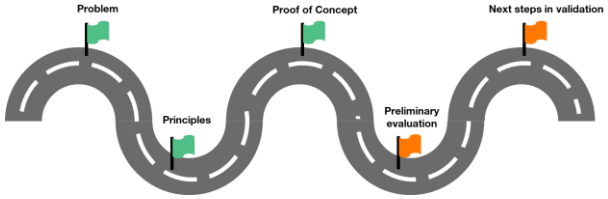
a. Deploy & activate G

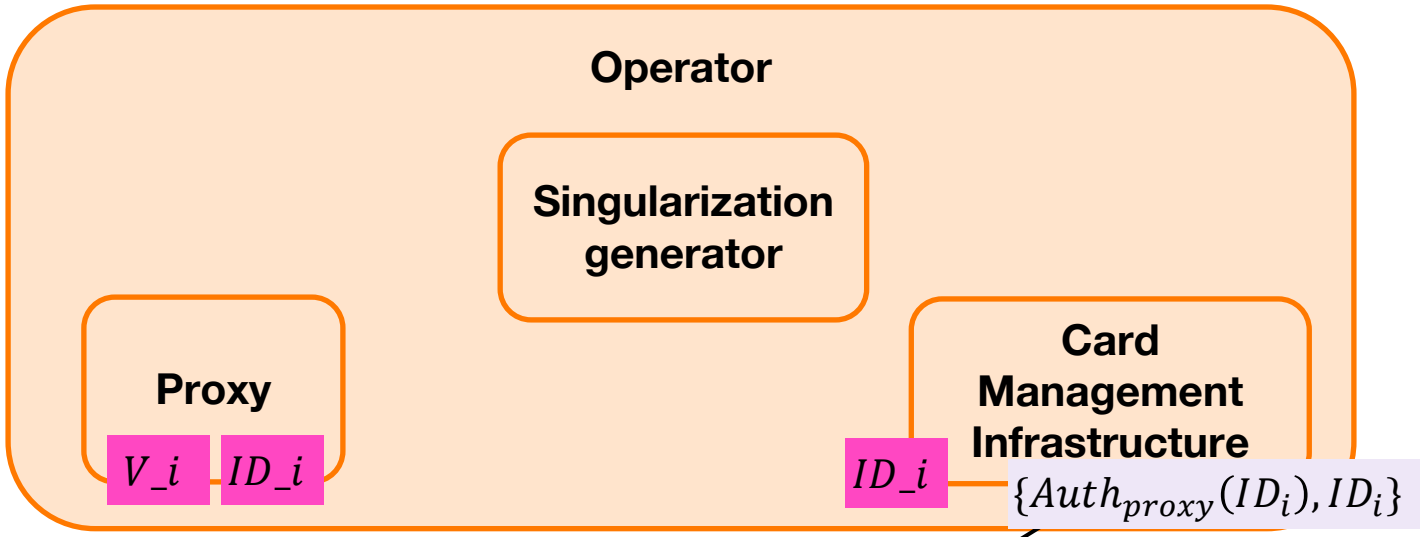




Orange Restricted

Proof of concept : step 3





Authorize use of singularization service

Service Provider

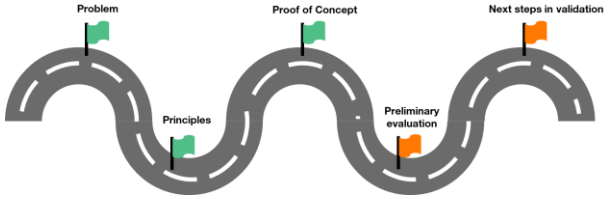
End User Device

End User SIM_i

G_i

Orange Restricted

Proof of concept : step 4



Operator

Singularization generator

Proxy

V_i ID_i

Card Management Infrastructure

Service Provider

$\{Auth_{proxy}(ID_i), ID_i\}$

End User proves legitimacy to access online resource provided by Service Provider

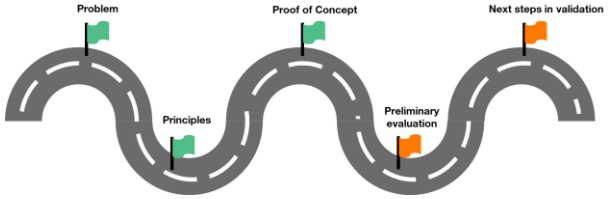
End User Device

End User SIM_i

G_i

Orange Restricted

Proof of concept : attacker model & assumptions



Operator

Singularization generator

Proxy

V_i ID_i

Card Management Infrastructure

Attacker does not control:
- Operator
- Service Provider
- SIM Operating System

Attacker cannot use impersonate Service Provider

Channel to deploy G_i does not leak any information

Service Provider

$\{Auth_{proxy}(ID_i), ID_i\}$

End User Device

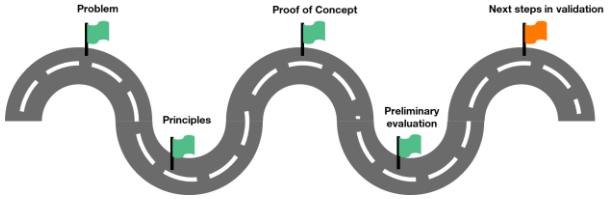
End User SIM_i

G_i

Attacker has physical control of Device :
- Has high expertise
- Has high-end equipment
- Intercepts SIM inputs and outputs
- Modifies SIM inputs
- Measures power consumption
- Has the capacity to inject faults

Orange Restricted

Preliminary evaluation: methodology



- Fault injection with physical attacks: Laser & electromagnetic impulses
- Naive programmation without any software countermeasure

Deck A:
- Chip A
- Manufacturer 1

End User SIM_Ai
End User SIM_Ai
End User SIM_Ai

AES | *NVM read /write* | *Singularized AES_i*

Deck B:
- Chip B
- Manufacturer 1

End User SIM_Ai
End User SIM_Ai
End User SIM_Ai

AES | *NVM read /write* | *Singularized AES_i*

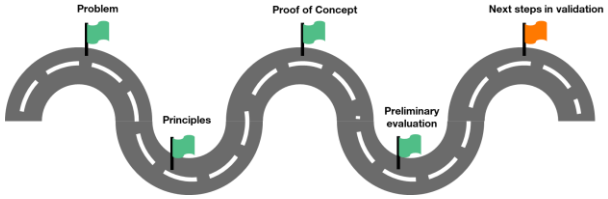
Deck C:
- Chip C
- Manufacturer 2

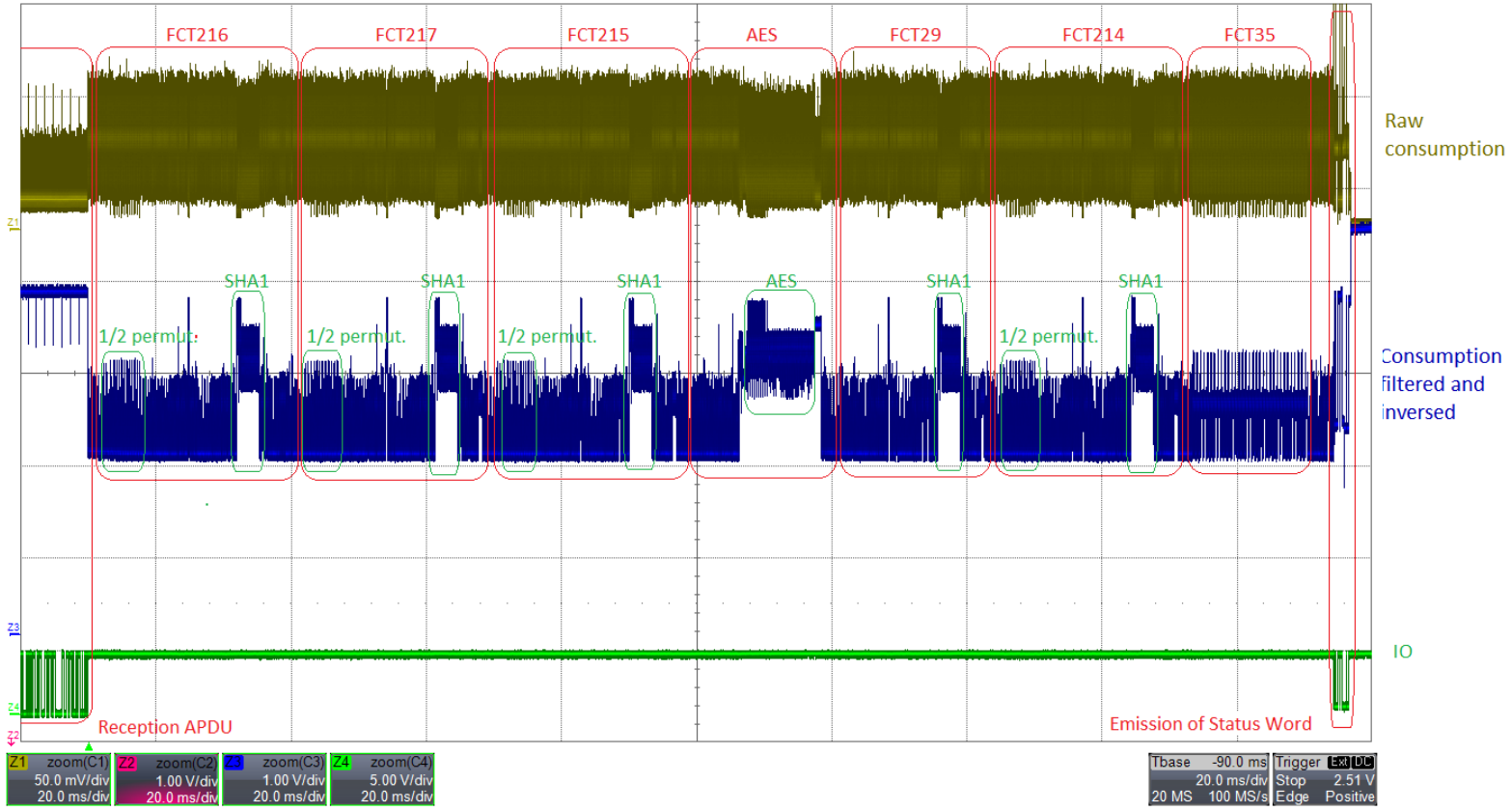
End User SIM_Ai
End User SIM_Ai
End User SIM_Ai

AES | *NVM read /write* | *Singularized AES_i*

Orange Restricted

Preliminary evaluation: observations





Raw consumption

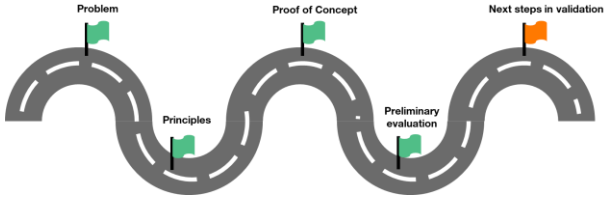
Consumption filtered and inversed

IO

The form of functions can be recognized, independantly from chip & manufacturer. Consistent with SOTA [Lashermes2024]

Orange Restricted

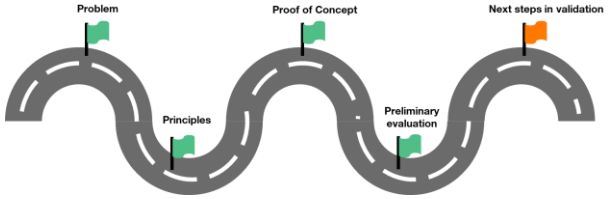
Preliminary evaluation: scrambling functions



Scrambling function
Order 0 - XOR
Order 1 – Circular permutation
Order 2 – Feistel networks
Order 3 – Arithmetic in base 65537

Orange Restricted

Preliminary evaluation: Time To Find Key (TTFK)

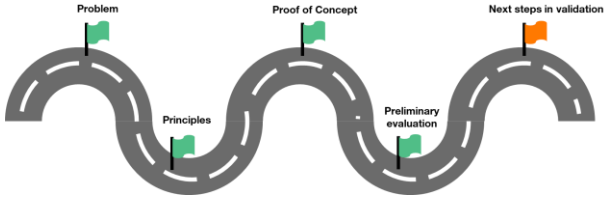


Scrambling function	TTFK white box (Deck A & B)	TTFK black box (Deck C)
Card preparation	2 days	=
AES without singularization	1 week	~
Order 0 - XOR	Few days, complex because proprietary implementation	~
Order 1 – Circular permutation	1 week	~
Order 2 – Feistel networks	2 weeks, double fault required	~
Order 3 – Arithmetic in base 65537	NA	Not achieved within 2 weeks

Complexity orders are confirmed
Proprietary implementation adds noise that makes attack more complex

Orange Restricted

Preliminary evaluation: Attack quotation (CC) AES deck A

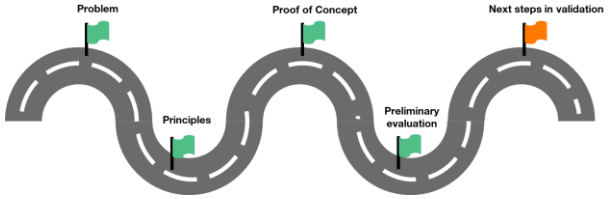


Criteria	Comments	Identification	Exploitation
Elapsed Time	< 1 month to identify attack < 1 jour pour la reproduire	2	4
Expertise	Expertise level required to create & reproduce attack	5	2
Knowledge of TOE	Restricted	2	0
Access to TOE	< 10 cards to identify & reproduce attack	0	0
Equipment	High-end oscilloscope	3	4
Open Samples / known secrets	Restricted	2	NA
Sous-total		14	10
Total		24	

Range of values*	TOE resistant to attackers with attack potential of:
0-15	No rating
16-20	Basic
21-24	Enhanced-Basic
25-30	Moderate
31 and above	High

Orange Restricted

Preliminary evaluation: Attack quotation (CC) singularized AES deck A



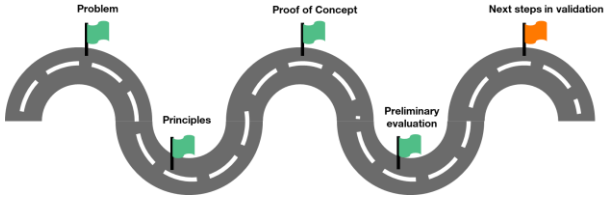
Estimated as only half of secrets were retrieved

Criteria	Comments	Identification	Exploitation
Elapsed Time	< 1 month to identify attack < 1 jour pour la reproduire	5	4
Expertise	Expertise level required to create & reproduce attack	5	2
Knowledge of TOE	Restricted	2	0
Access to TOE	< 10 cards to identify & reproduce attack	0	0
Equipment	High-end oscilloscope	3	4
Open Samples / known secrets	Restricted	2	NA
Sous-total		17	10
Total		27	

Range of values*	TOE resistant to attackers with attack potential of:
0-15	No rating
16-20	Basic
21-24	Enhanced-Basic
25-30	Moderate
31 and above	High

Orange Restricted

Preliminary evaluation: Attack quotation (CC) singularized AES production scenario



Criteria	Comments	Identification	Exploitation
Elapsed Time	< 1 month to identify attack < 1 jour pour la reproduire	5	4
Expertise	Expertise level required to create & reproduce attack	5	2
Knowledge of TOE	Sensitive	4	0
Access to TOE	< 10 cards to identify & reproduce attack	0	0
Equipment	High-end oscilloscope	3	4
Open Samples / known secrets	Sensitive	5	NA
Sous-total		22	10
Total		32	

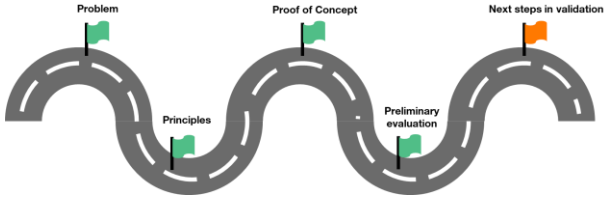
Added software countermeasures

More restrictive management of samples & documentations

Range of values*	TOE resistant to attackers with attack potential of:
0-15	No rating
16-20	Basic
21-24	Enhanced-Basic
25-30	Moderate
31 and above	High

Orange Restricted

Preliminary evaluation: Attack quotation (CC) singularized AES production scenario



Criteria	Comments	Identification	Exploitation
Elapsed Time	< 1 month to identify attack < 1 jour pour la reproduire	5	4
Expertise	Expertise level required to create & reproduce attack	5	2
Knowledge of TOE	Sensitive	4	0
Access to TOE	< 10 cards to identify & reproduce attack	0	0
Equipment	High-end oscilloscope	3	4
Open Samples / known secrets	Sensitive	5	NA
Sous-total		22	10
Total		32	

Added software countermeasures

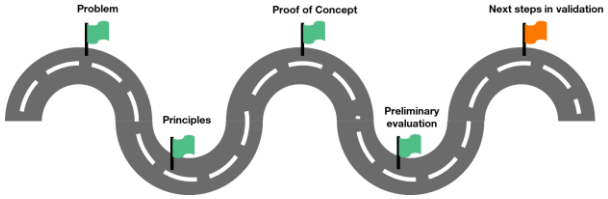
More restrictive management of samples & documentations

31 and above	High

The approach has potential to achieve higher levels of assurance

Orange Restricted

Preliminary evaluation: Costs & unpredictability



Estimated cost to deploy a function of 0.5MB on 100 million devices with each 1 SIM

1. 10 millions € to deploy a singularized function of size 0.5MB on entire SIM flet
2. 1.5 billions € to fully replace legacy SIM fleet immediately

Unpredictability

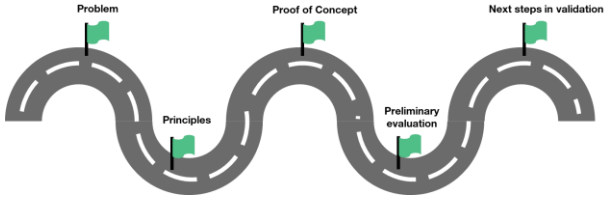
1. $(n \cdot m)^k$ number of sequences that can be formed with n functions chosen among in a catalog of k functions with an average of m parameters
2. $P(C) = (n \cdot m)^{-k}$ probability to select one particular sequence, if each combination has the same probability of being selected

- Unpredictability is achieved if $P(C) = (n \cdot m)^{-k} \ll 0$

From an industrial point of view, the proposal is very promising depending on the cost to maintain a catalogue & reconfiguration which ensure unpredictability

Orange Restricted

Next steps : advanced evaluation



Preliminary evaluation is promising but:

- depends on some parameters (e.g. reconfiguration rate, catalogue dimensions & renewal rate)
- not formal enough

Challenge : MTD approaches are rarely evaluated in the literature, there is no methodology to our knowledge

Next steps :

1. Validate formally singularization approach
2. Determine optimal parameters to minimize defender's costs & maximize attacker's costs

Orange Restricted

References

[Lashermes2024] *"Generic SCARE: reverse engineering without knowing the algorithm nor the machine"*, Journal of cryptography engineering, 2024

[Gaber2024] *" Position Paper: Strengthening Applets on Legacy SIM Cards with Singularization, a New Moving Target Defense Strategy"*, Mobile, Secure, and Programmable Networking, 2024

Orange Restricted

Thank you