OPERATIONAL EFFICIENCY IN OBFUSCATION

SECURITY THREATS
TECHNIQUES PROS & CONS

list
ceatech

cnrs Pré-GDR Sécurité Informatique

SECURIY THREATS

Man-at-the-end WITH - WITHOUT full control on the machine.

Sun Tzu and Niccolo Machiavelli, *Art of war*

DYNAMIC S.T	STATIC S.T
WITH debug and tracing Encryption is not enough, obfuscation or secure execution is needed	**WITHOUT** debug and tracing (local conditions make it cumbersome)

list
ceatech

Pré-GDR Sécurité Informatique

One good question to have:
Is that man in bad company? (or in love with Ida)

SOLUTIONS (360°)

ENCRYPTION, OBFUSCATION, TRUSTED EXECUTION

SW PROTECTION	WITHOUT DEBUG	WITH DEBUG 	STRATEGIES 	OPERATIONAL CONSTRAINTS
ENCRYPTION	**1**	**0**	"Make sure he can not debug..." Anti-dump. 	Key transfer and protection
OBFUSCATION	**RATIO**		Overload Semantic dillution	Selective process Performance Safety?
TRUSTED EXECTION ENVIRONMENT	**1**	**1**	Enlarge TCB to useful code	Vendor specific APIs

list
ceatech

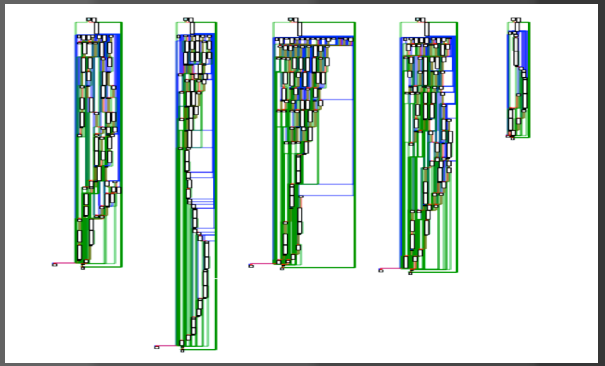
cnrs Pré-GDR Sécurité Informatique

SOLUTIONS (360° SOTA)

FOCUS ON OBFUSCATION

STRATEGIES:

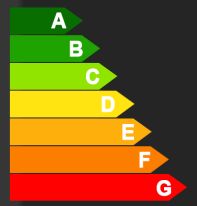
1. REMOVAL OF ALL SEMANTICS AND DEBUG DATA
2. OVERLOAD ATTACKER...AT A GIVEN PERFORMANCE "BUDGET"



MEANS:

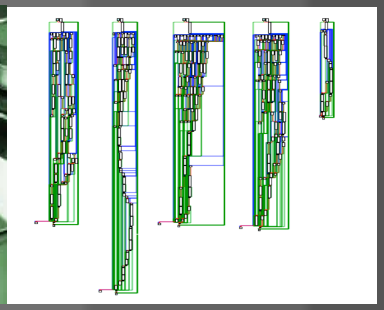
1. CODE EXPANSION (VERTICAL AXIS EXPANSION)
2. GRAPH COMPLEXITY (HORIZONTAL AXIS EXPANSION).

CONSTRAINT: PERFORMANCE



SOLUTIONS (360° SOTA)

FOCUS ON OBFUSCATION



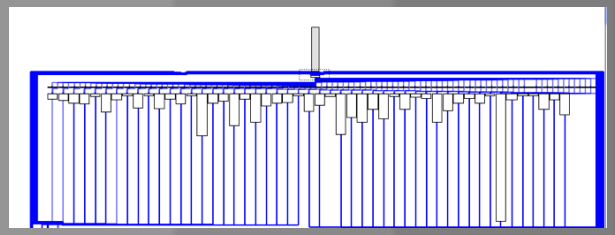
1. VARIABILITY
2. GRANULARITY

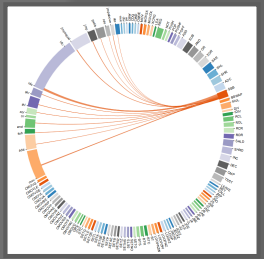
Worst case scenario. Deplete your own resources ...

Limited resources: Know which place to protect... and concentrate defense there ...

SOLUTIONS (360° SOTA)

VARIABILITY, GRANULARITY AND WORKFLOW





BESIDE SEMANTICS-BASED OBFUSCATION, WHATEVER TECHNIQUES (CFG FLATTENING, INSTRUCTION EMULATION, OPAQUE PREDICATE, ...) CAN BE ESTIMATED BY QUANTITY OF EXECUTED INSTRUCTIONS.

PREFERABLBY, VARIABILITY SHALL BE:

- AUTOMATICALLY GENERATED
- PROVEN TO BE SAFE (>>BUILT-IN CORRECTNESS TEST)
- APPLIED AT THE LOWEST GRAIN

SOLUTIONS (360° SOTA)

OBFUSCATION INDUSTRIAL BLOCKING POINTS

a) WHICH FUNCTION TO PROTECT? WHERE IT IS HIDDEN...
b) PERFORMANCE-CRITICAL FUNCTIONS ARE...
c) RUNTIME TEST FEEDBACK LOOP
d) FRICTION ON WORKBENCH, WORKFLOW AND WORKLOAD.
e) SAFETY ASSURANCE?

SOLUTIONS (360°)

FOCUS ON TRUSTED EXECUTION

1. Deterministic security by Hardware managed memory page encryption. No country for Ida.
2. Security and performance are no more bound.
3. Strong research for CLOUD processing, super hot topics today.
4. Unchanged (marginal changes) on source code

Limiting Factors

a) Hardware bound technique
b) Complex workflow (source level changes requested)

list
cea tech

Pré-GDR Sécurité Informatique

TAKE AWAYS

✓Know your ennemy (intent and means) as well as yourself (resources, places to defend)
✓Obfuscation is linked to Performance…and preparation.
✓Appeal for automatic *no-brainer-by-default* solution that provides both static and dynamic resilience to attacks.
✓TEE is a strong concept to consider today.
✓Safety and security shall be joined (uncovered area of work).

list
ceatech

cnrs Pré-GDR Sécurité Informatique

THANKS TO

CEA LIST

CNRS –PRÉ-GDR SÉCURITÉ INFORMATIQUE

QUESTIONS?