OPERATIONAL EFFICIENCY IN OBFUSCATION
SECURITY THREATS
TECHNIQUES PROS & CONS
SECURITY THREATS

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

Sun Tzu and Niccolo Machiavelli, *Art of War*

<table>
<thead>
<tr>
<th>DYNAMIC S.T</th>
<th>STATIC S.T</th>
</tr>
</thead>
</table>
| **WITH** debug and tracing  
Encryption is not enough, obfuscation or secure execution is needed | **WITHOUT** debug and tracing  
(local conditions make it cumbersome) |

One good question to have:
Is that man in bad company? (or in love with Ida)
<table>
<thead>
<tr>
<th>SW PROTECTION</th>
<th>WITHOUT DEBUG</th>
<th>WITH DEBUG</th>
<th>STRATEGIES</th>
<th>OPERATIONAL CONSTRAINTS</th>
</tr>
</thead>
<tbody>
<tr>
<td>ENCRYPTION</td>
<td>1</td>
<td>0</td>
<td>&quot;Make sure he cannot debug...&quot; Anti-dump.</td>
<td>Key transfer and protection</td>
</tr>
<tr>
<td>OBFUSCATION</td>
<td>Ratio</td>
<td></td>
<td>Overload Semantic dilution</td>
<td>Selective process Performance Safety?</td>
</tr>
<tr>
<td>TRUSTED EXECTION ENVIRONMENT</td>
<td>1</td>
<td>1</td>
<td>Enlarge TCB to useful code</td>
<td>Vendor specific APIs</td>
</tr>
</tbody>
</table>
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
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 ...
BESIDE SEMANTICS-BASED OBFUSCATION, WHATEVER TECHNIQUES (CFG FLATTENING, INSTRUCTION EMULATION, OPAQUE PREDICATE, ...) CAN BE ESTIMATED BY QUANTITY OF EXECUTED INSTRUCTIONS.

PREFERABLY, 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)
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).
THANKS TO
CEA LIST
CNRS –PRÉ-GDR SÉCURITÉ INFORMATIQUE

QUESTIONS?