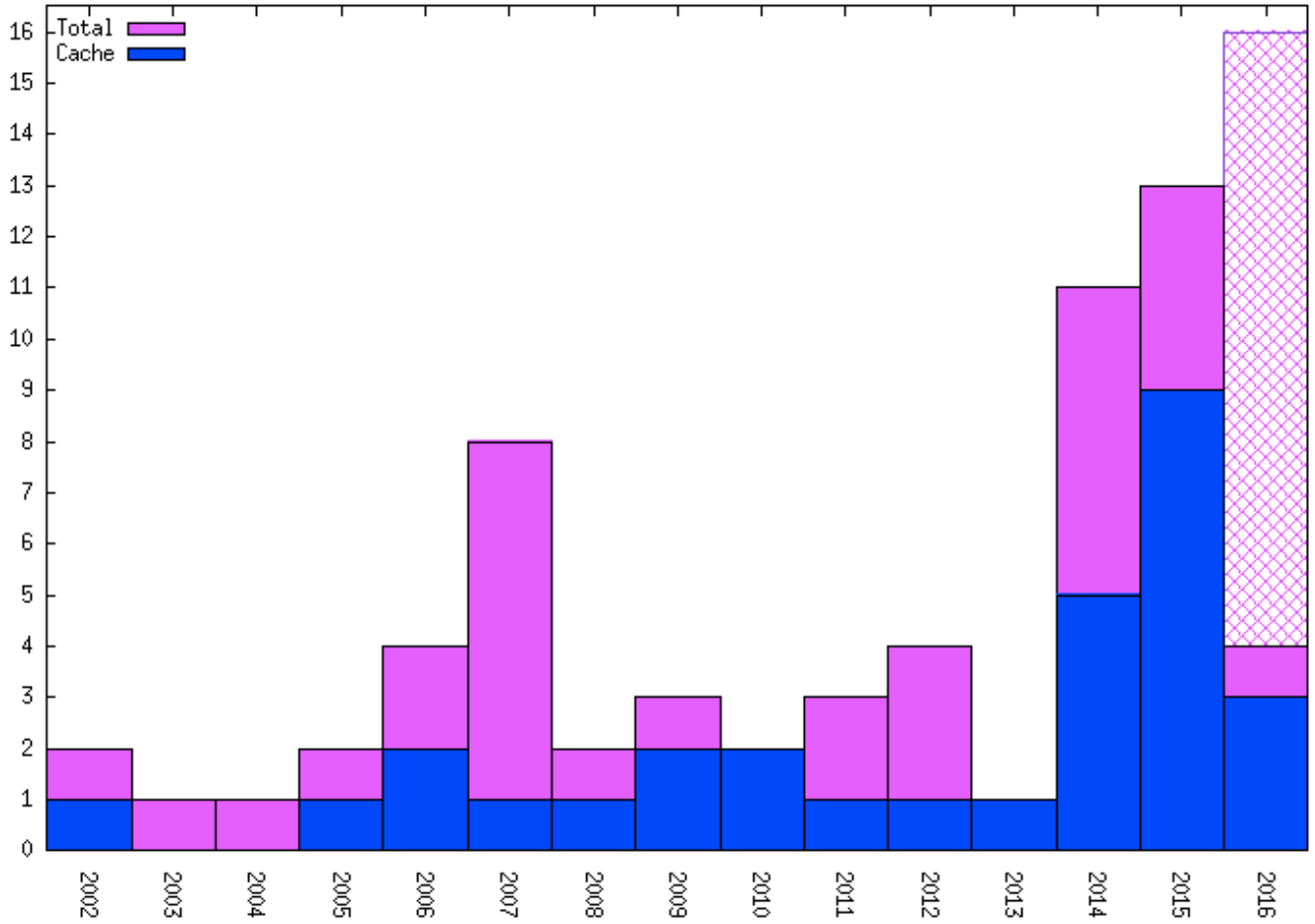
Reducing Piracy on the High Seas

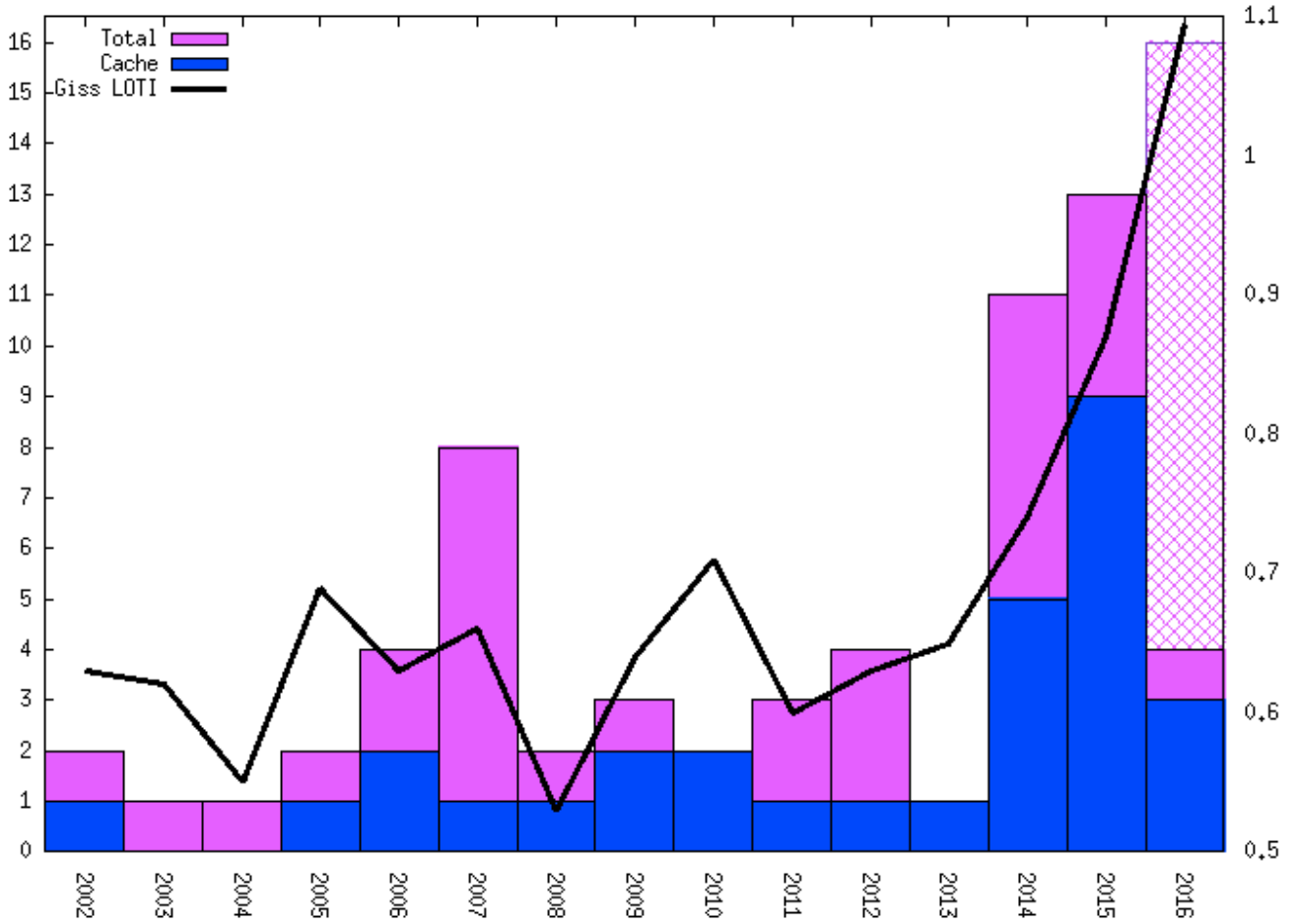
Yuval Yarom
The University of Adelaide and
Data61, CSIRO

Publications on microarchitectural side-channel attacks



Data from [GYCH16]

Publications and Global Temperature



Global Average Temperatures Vs. Number of Pirates

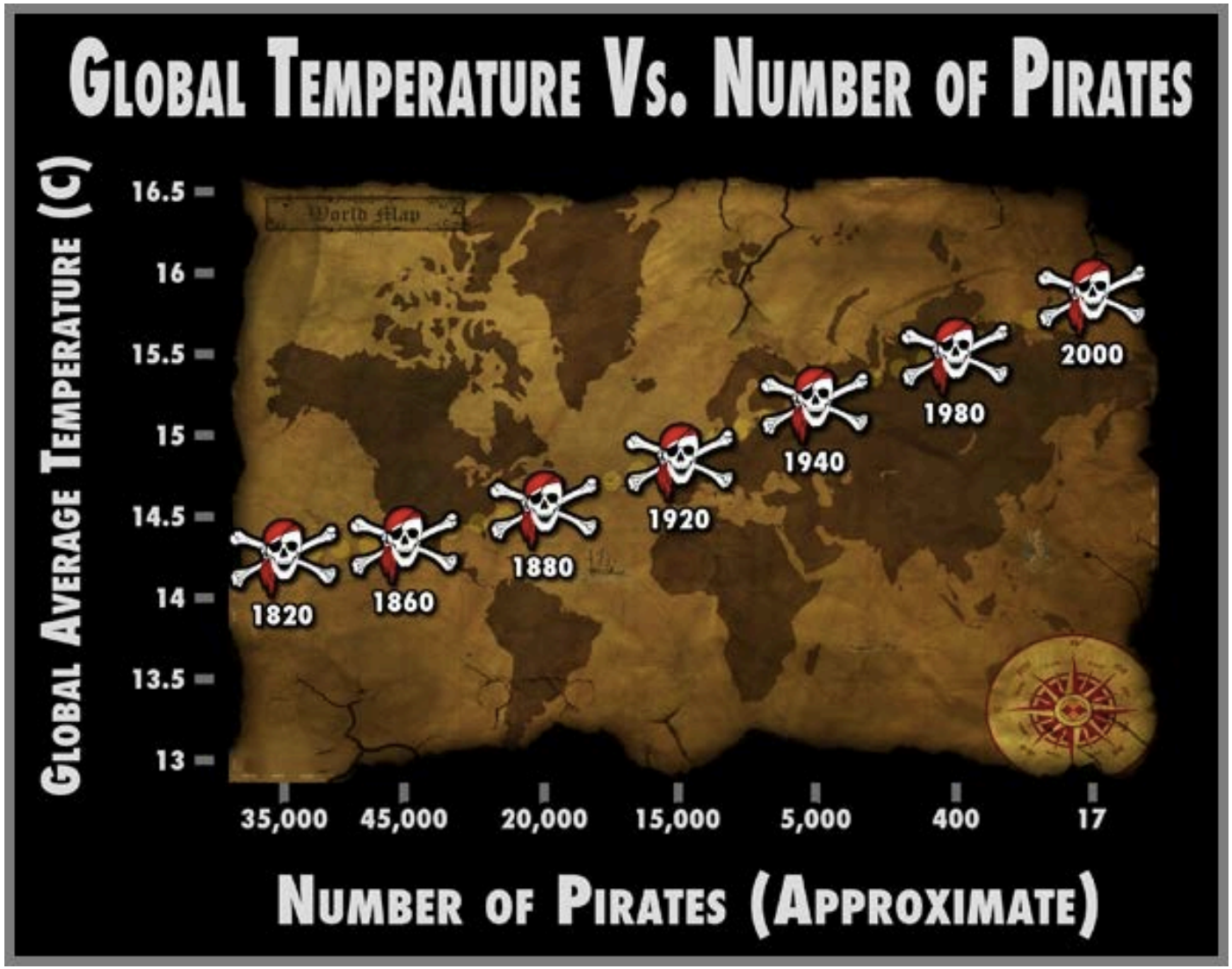
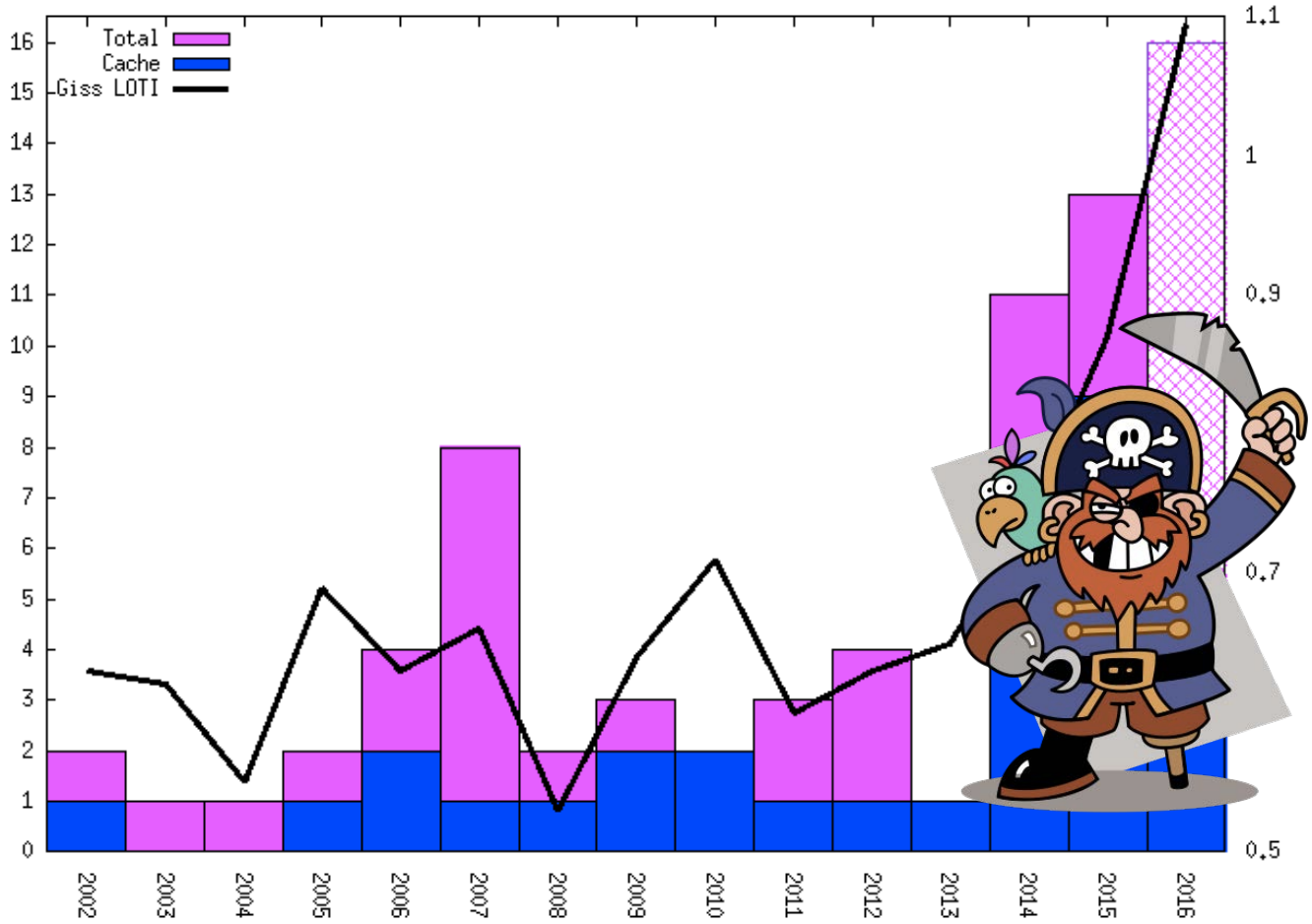


Image from: https://illuminutti.com/2014/02/04/true-fact-the-lack-of-pirates-is-causing-global-warming/

Pirates Transitioning to Cryptography

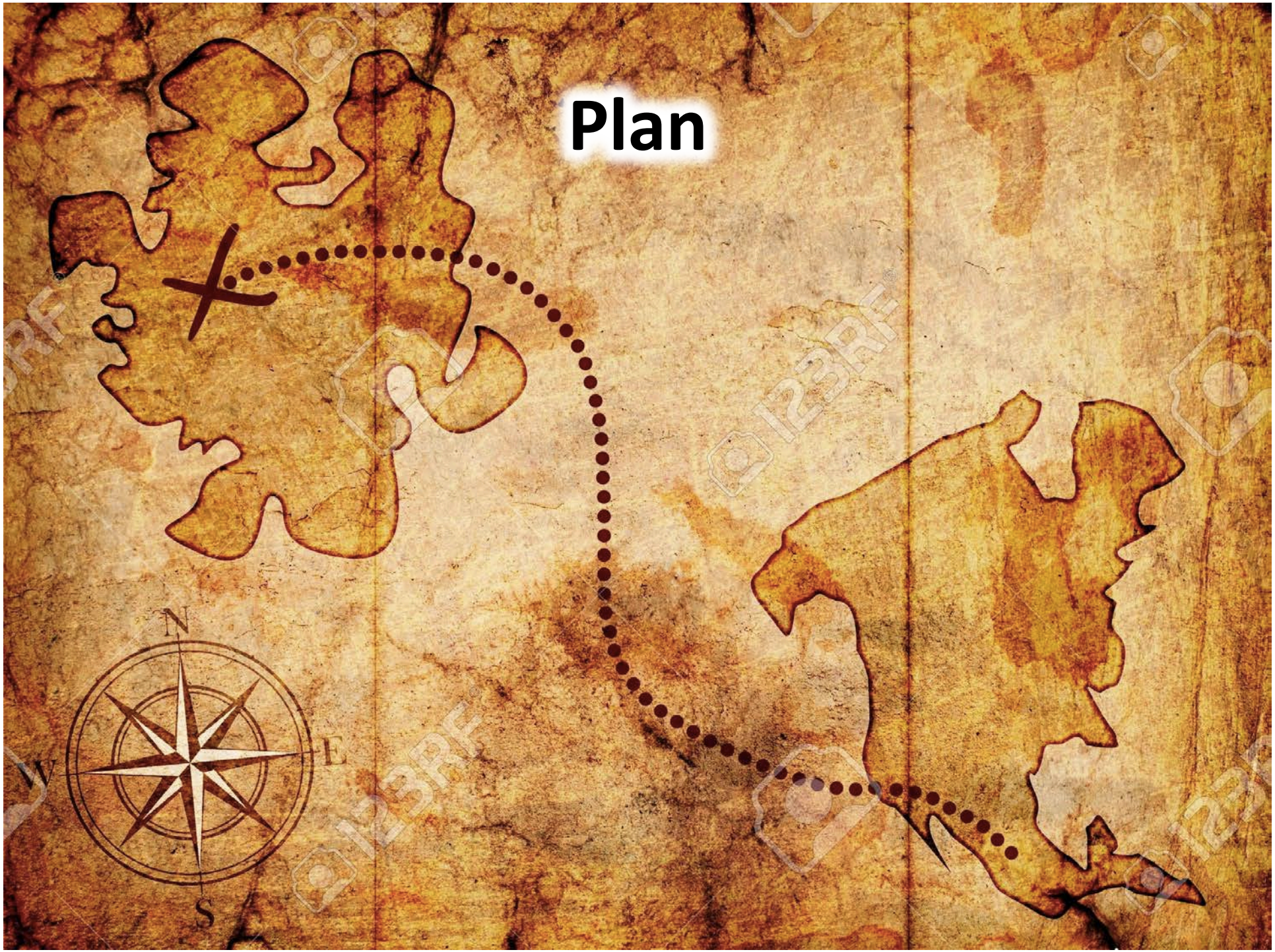


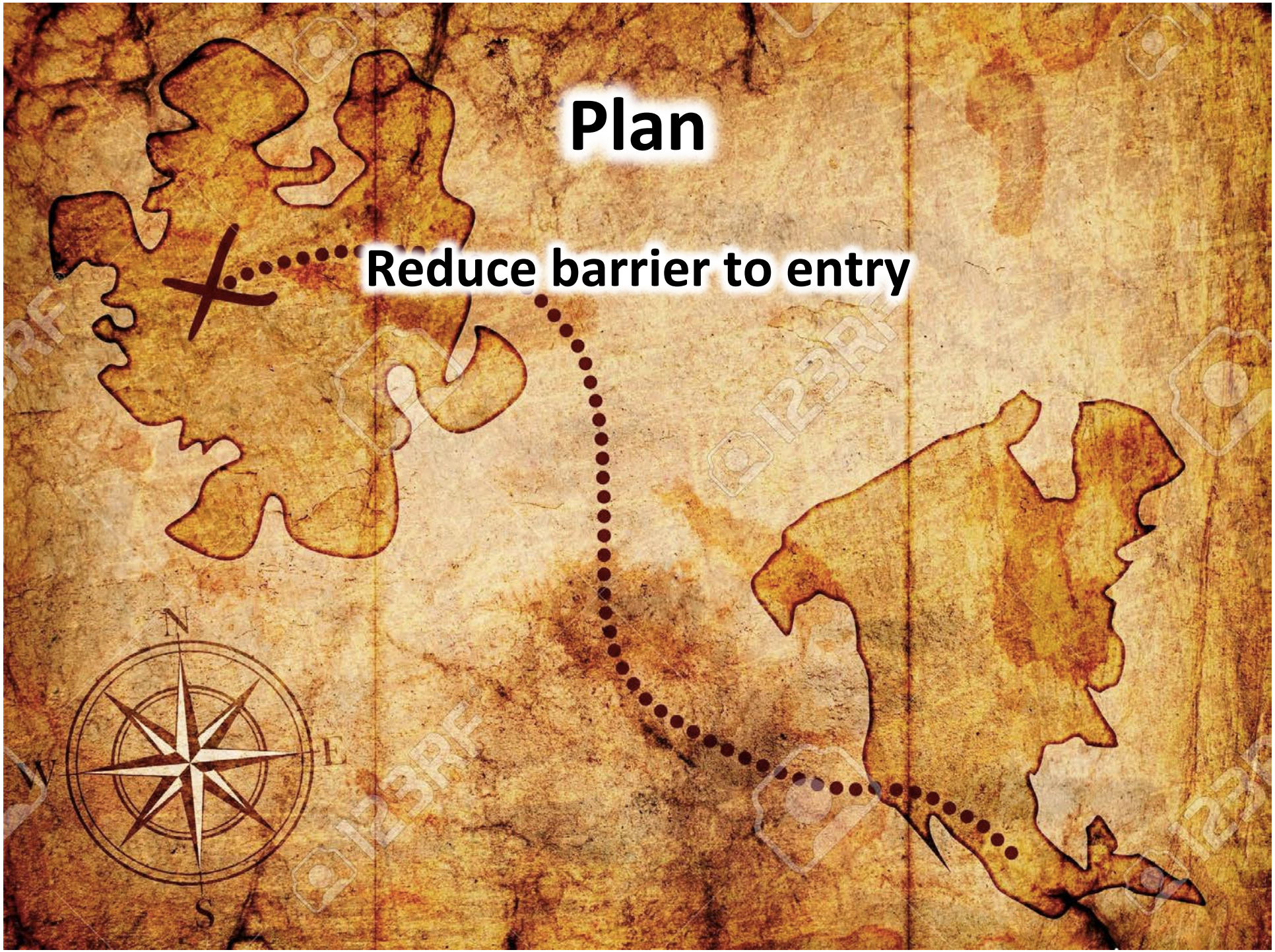
Piracy easy. Side-Channels hard.

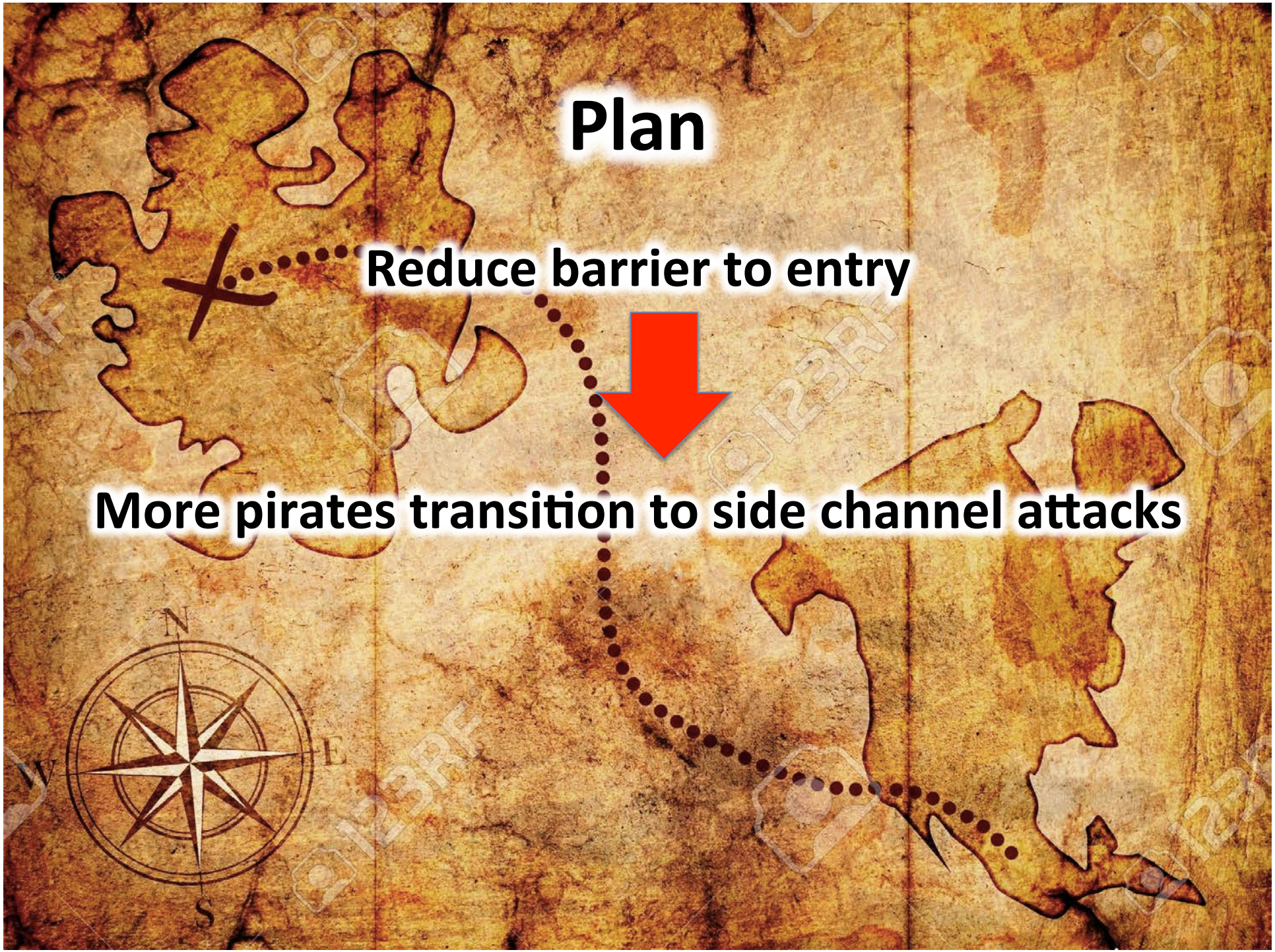
- OpenSSL

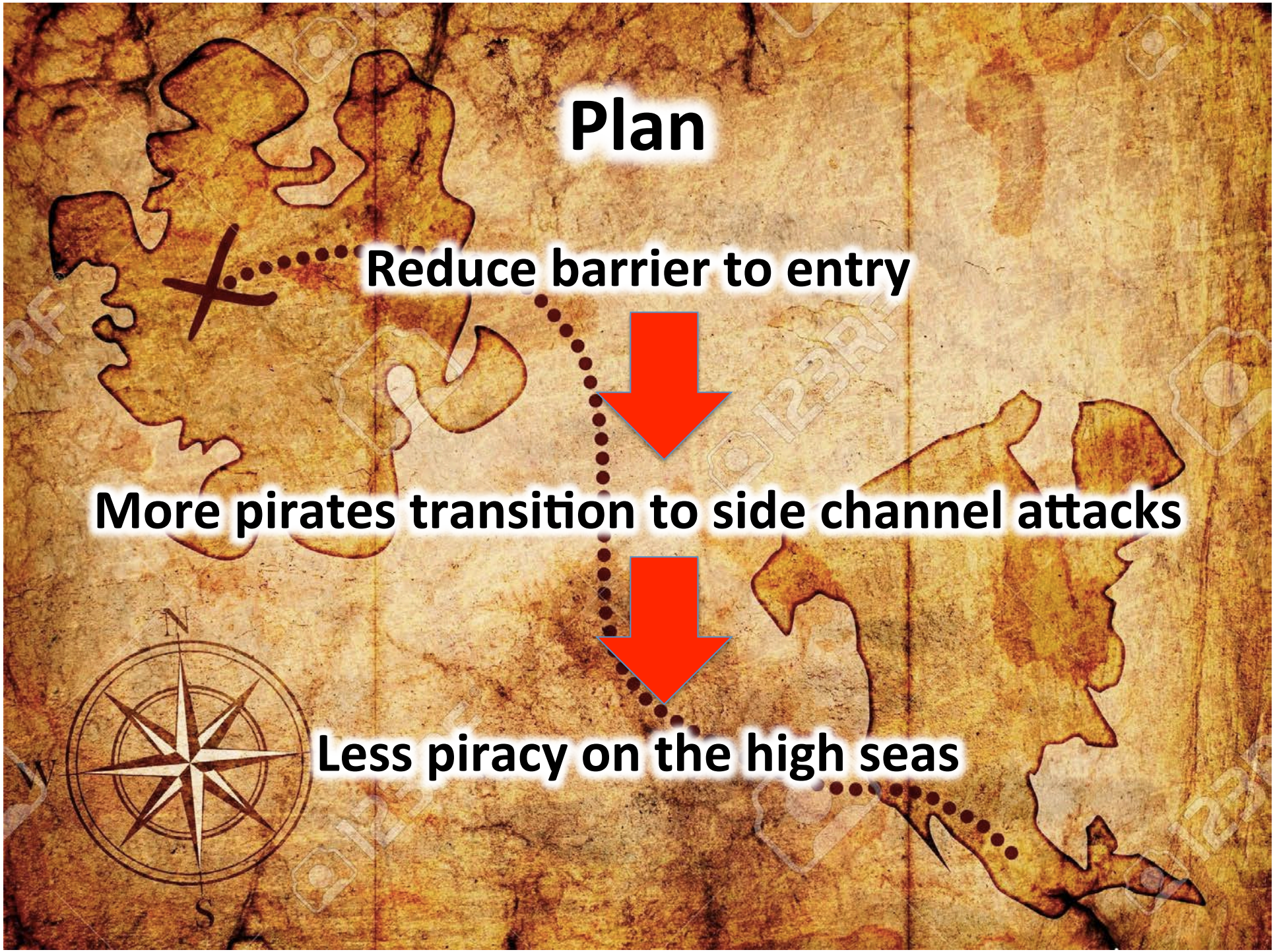
  LOW Severity. This includes issues such as those that … or hard to exploit timing (side channel) attacks.

  https://www.openssl.org/policies/secpolicy.html


Plan
N
W
E
S


Plan
Reduce barrier to entry
N
W
E
S


Plan
Reduce barrier to entry
More pirates transition to side channel attacks
N
W
E
S


Plan
Reduce barrier to entry
More pirates transition to side channel attacks
Less piracy on the high seas
N
S

Mastik

- Extremely bad acronym for
  Micro-Architectural Side-channel ToolKit
- Aims
  - Provide somewhat-robust implementations of all known SC attack techniques for every architecture
  - Provide Implementation of generic analysis techniques
  - Overcome the barrier to entry into the area
  - Shift focus to cryptanalysis

Status

- Reasonably solid implementation of four attacks
  - Prime+Probe on L1-D, L1-I and L3, Flush+Reload
- Only Intel x86-64, on Linux and Mac
  - x86-32 and limited ARM currently working in the lab
- Zero documentation, little testing
- No user feedback

Version 0.01 (code name Scurvy Dog)

http://cs.adelaide.edu.au/~yval/Mastik/