State-of-the-art FLOSS tooling for DPA

Ilya Kizhvatov
Digital Security group

Radboud Universiteit

Joint work with Cees-Bart Breunesse (Riscure)

Why

- unlike SW hacking scene, lack of state-of-the-art free open-source tooling in SCA community

What

2007: OpenSCA. Not maintained. MATLAB

2012: ChipWhisperer. HW+SW, SCA+FI. Python

2016: Daredevil. 1- and 2-order CPA. C++

2016: Jlsca. CPA, LRA… and more! Julia

Julia

- high-level dynamic language
- high performance through use of LLVM just-in-time compiler
- https://github.com/stevengj/julia-mit#why-julia

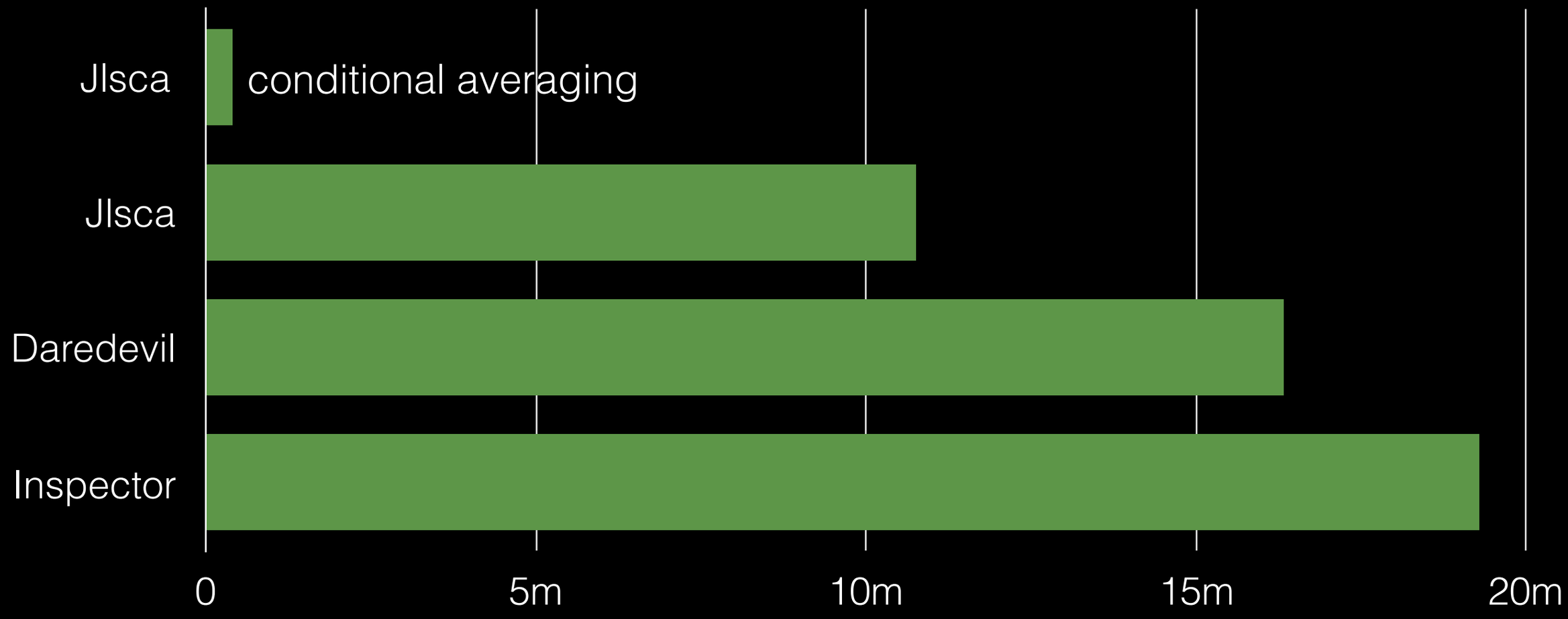
Jlsca

- https://github.com/Riscure/Jlsca, GPLv3
- started from an effort to implement efficient and state-of-the-art techniques from eprint:2013/794, first in Python (https://github.com/ikizhvatov/pysca)
- re-worked and significantly extended by Cees-Bart Breunesse in Julia

- Julia package, simple install
- usage: script / REPL / notebook

Radboud Universiteit

Performance

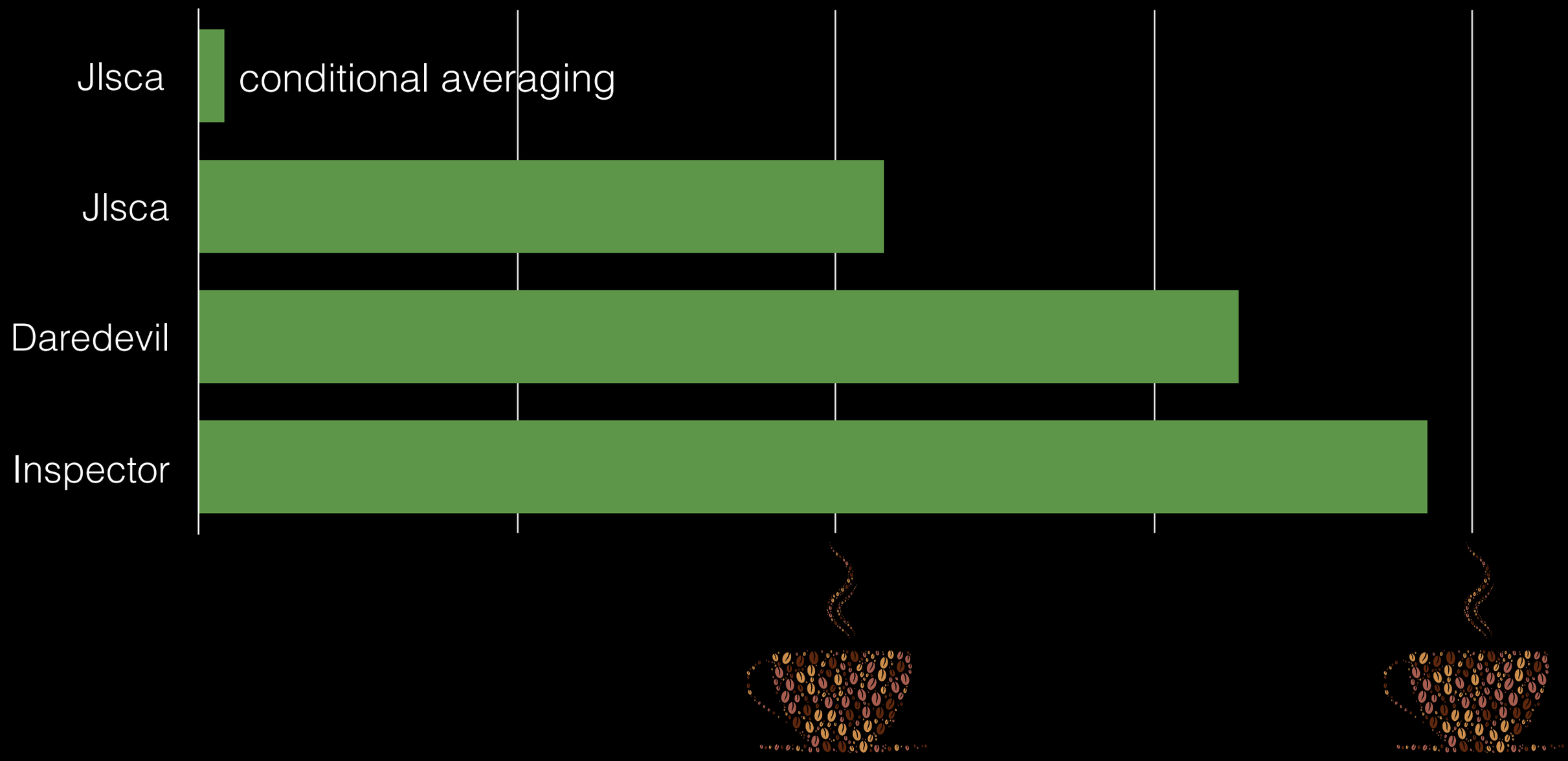


Attack: all-bits abs-sum CPA on AES-128
Dataset: 100K traces of 512 float32 samples (200 MB)
Platform: a modest dual-core laptop

https://github.com/ikizhvatov/dpa-tools-benchmarking

Radboud Universiteit

Performance



https://github.com/ikizhvatov/dpa-tools-benchmarking

Scaling

	Laptop	Workstation	Ratio
Jlsca	10m45s	3m57s	**2.7**
Daredevil	16m40s	6m32s	**2.5**
Inspector	19m17s	9m33s	**2.0**

Laptop: dual-core i5 2.6 GHz, 4 GB DDR3, HDD
Workstation: quad-core i7 3.4 GHz, 64 GB DDR4, HDD

https://github.com/ikizhvatov/dpa-tools-benchmarking

README.md

Jlsca tutorials

Examples on how to use Jlsca, the side channel analysis toolkit written in Julia.

Prerequisites

- Julia, https://julialang.org
- IJulia, https://github.com/JuliaLang/IJulia.jl
- Jlsca package, https://github.com/Riscure/Jlsca
- Pycall and PyPlot packages, install in julia via Pkg.add()

It all works alike on Linux, Mac, and Windows.

Examples RHme2

- piece of SCAke - correlation power analysis attack on unprotected AES-128
- still not SCAry - linear regression analysis attack on AES-128 with a misalignment countermeasure
- eSCAlate - correlation power analysis attack on on AES-128 with a misalignment countermeasure

Tarballs with power traces available at https://drive.google.com/drive/folders/0B2slHLSL3nXaTFBWMUxHSkNmSTg

https://github.com/ikizhvatov/jlsca-tutorials