V-DIFT: Vector-Based Dynamic Information Flow Tracking
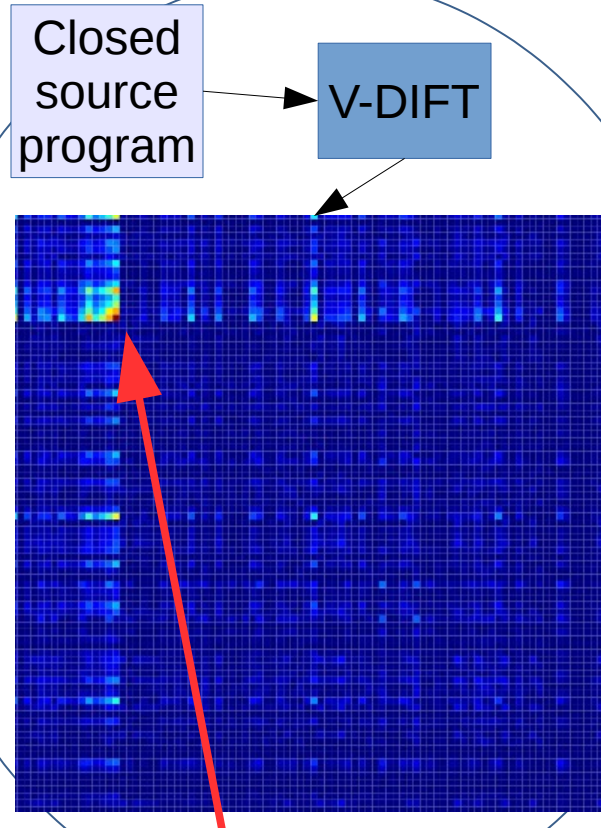

Challenge:

- Track data in a program for reverse engineering purposes

Closed source program → V-DIFT

Scientific Impact:

- Tracking how information flows is fundamental to information security
- Previous approaches ignore indirect flows (if statements, for loops, arrays, *etc.*) or offer no general way to handle them in real programs

Solution:

- Overcome the challenge of indirect flows via vector-based tracking
- Working on IDA Pro and radare2 plug-ins

Potential cryptographic key located in memory!

Broader Impact:

- Collaborating with the Citizen Lab to inform general audiences about reverse engineering results
- See https://netalert.me