WASP Workshop on Attacks and Software Protection

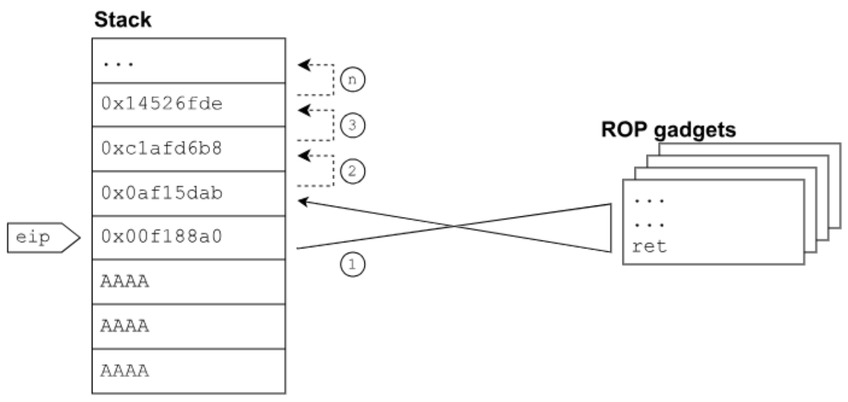
ESORICS

THALES

SEC-V

ADG-JOP: JOP attacks made easy

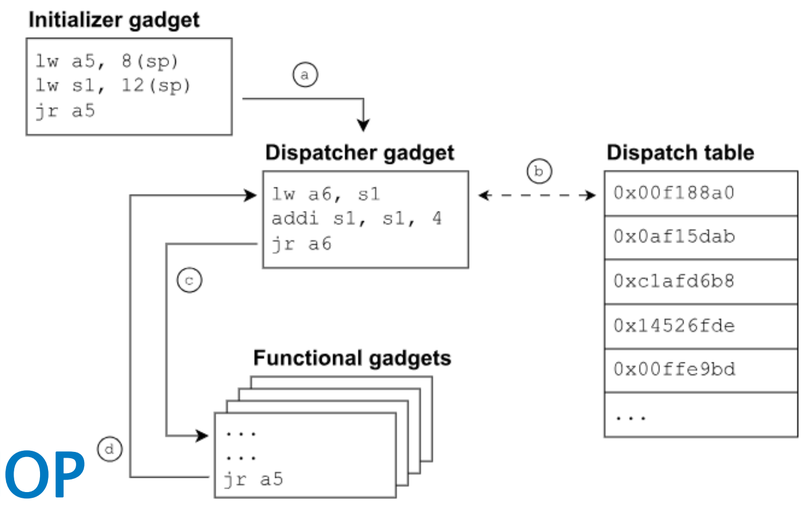
Return Oriented Programming



ROP

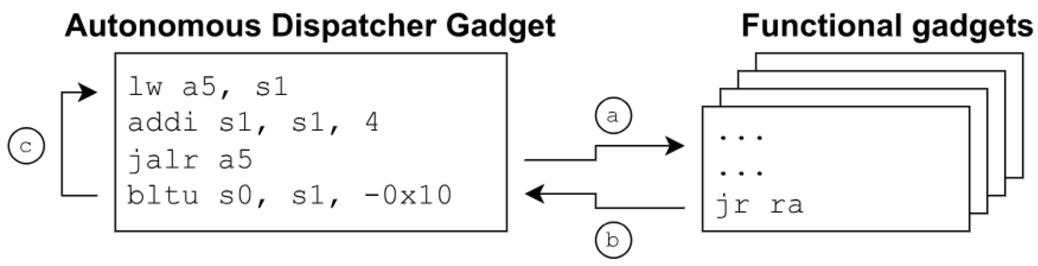
- Strong impact on stack: **easy to detect**
- Weak conditions for gadgets: **easy to setup**

Jump Oriented Programming



JOP

- No impact on stack: **hard to detect**
- Strong conditions for gadgets : **hard to setup**



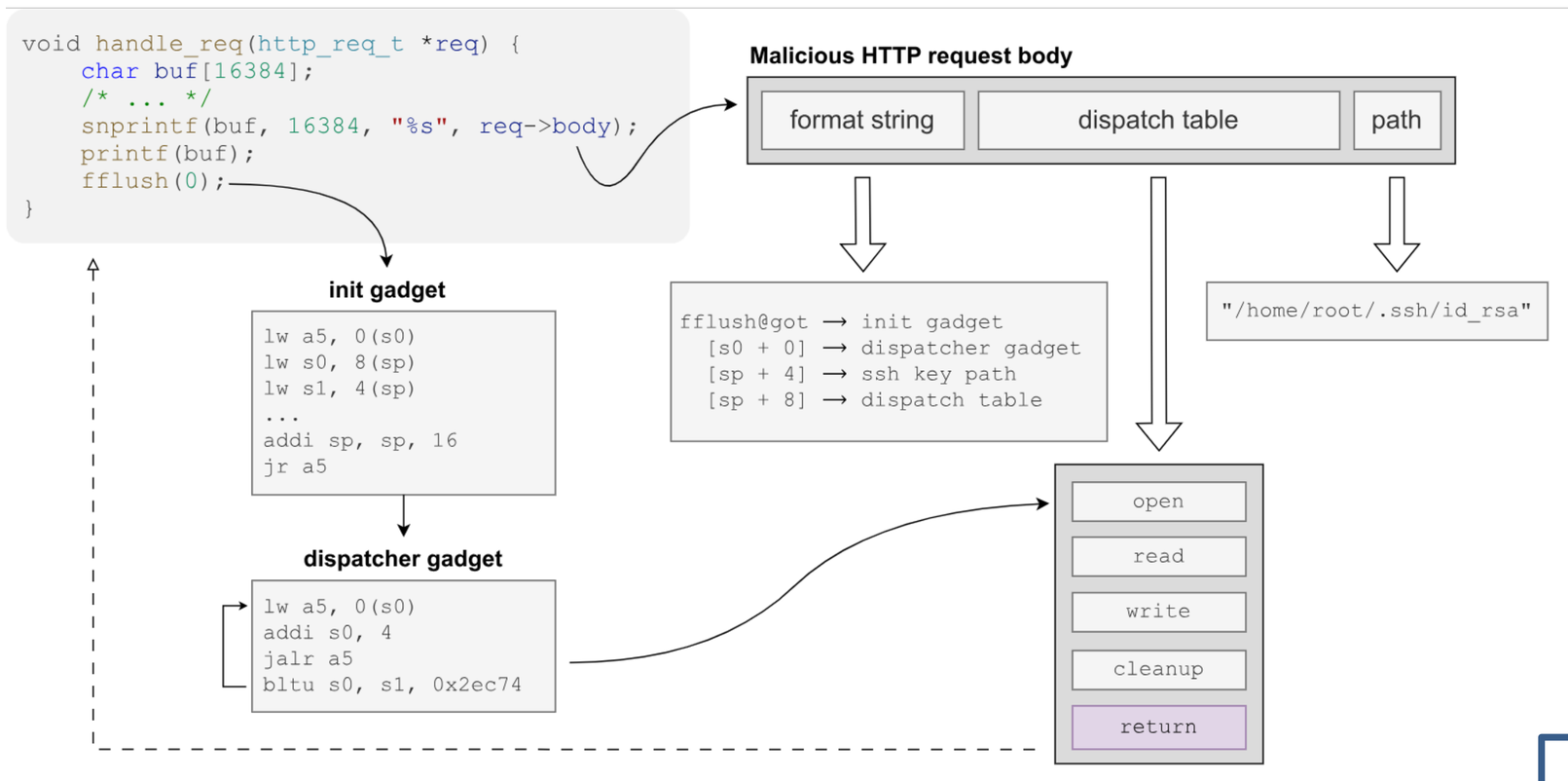
Easy as ROP

ADG-JOP

Sneaky as JOP

- No impact on stack: **hard to detect**
- Weak conditions for gadgets: **easy to setup**

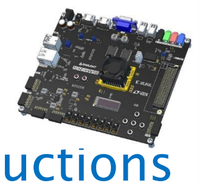
ADG-JOP Proof of concept: Stealthy attack on realistic RISC-V application



Mongoose: a realistic target

- Embedded web server
- Present on many IoT devices
- A memory vuln. was added

Tested on RISC-V CVA6



- 32-bits architecture
- Exploits compressed instructions

Portable attack

- All gadgets come from libc
- Tooled gadget chain design

Effects

1. The attacker send a malicious HTTP request
2. The attack opens/reads a secret key
3. Writes said secret into the attacker socket
4. Cleanups the application registers
5. The application resumes with nominal behavior

Our tool: *Gadget Inspector*

- Detects Init & Dispatch gadgets
- Detects functional gadgets
- RISCV 32/64, OS agnostic

Ongoing work

- Semi-auto chain assembling
- Usage for CRA exposure assessment

Acknowledgements This work is partly supported by the French research agency (ANR) under the grant ANR-21-CE-39-0017.

Contacts : Loïc BUCKWELL, Olivier GILLES (olivier.gilles@thalesgroup.com)

THALES