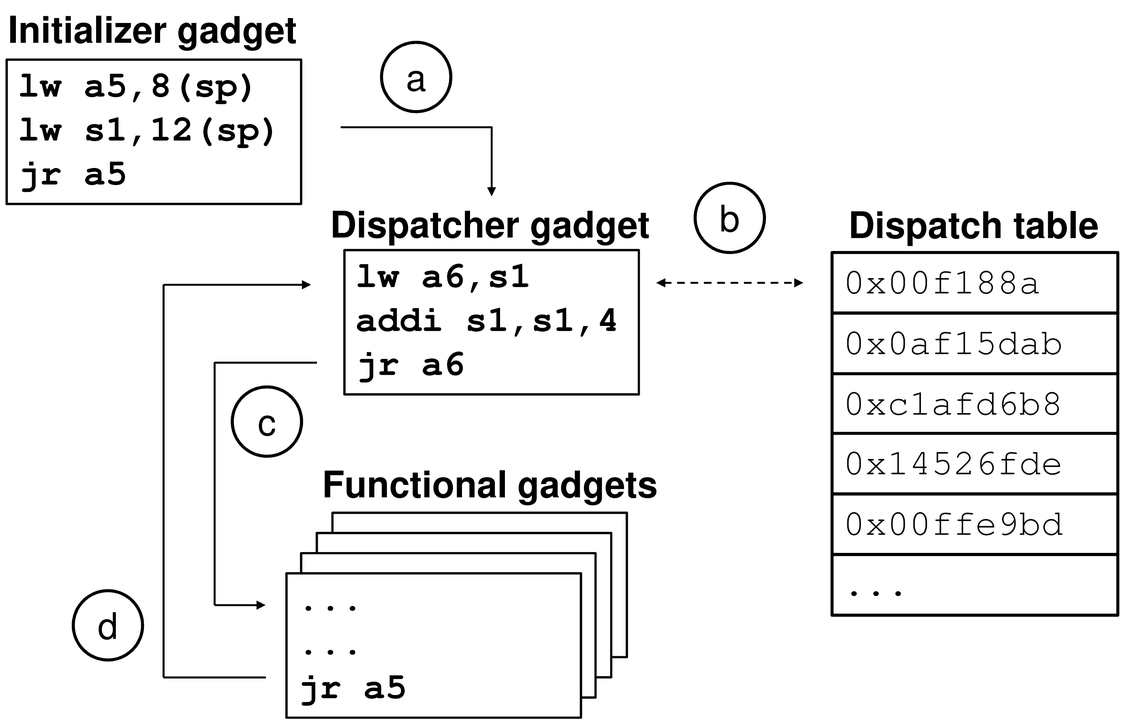
ARM vs RISC-V: Code Reuse Attacks Exploitable Surface

Code Reuse Attacks (CRAs)

- **Definition**: CRAs manipulate control flow within an application by using existing code components rather than injecting new code.
- **Mechanism:** Utilize short instruction sequences called “gadgets” stitched together to perform malicious operations.



Example CRA: structure of a jump-oriented programming attack

Surface on ARM and RISC-V

- **RISC-V** ISA is very similar in 32-bit and 64-bit, with similar instructions supported and identical general purpose registers.
- **ARM** ISAs are completely different between ARM32 and ARM64. Both instructions and registers differ significantly between the two architectures.

Example Autonomous Dispatcher Gadgets

- ADGs are special dispatcher gadgets that link back to themselves. The standard C library on all architectures contains at least one ADG, with a similar structure:

```
c.lw a5,0(s0)
c.addi s0,4
c.jalr a5
bltu s0,s1,-6
```

RV32IMAC

```
c.ld a5,0(s0)
c.addi s0,4
c.jalr a5
bltu s0,s1,-6
```

RV64G

```
ldr r3,[r5],#4
blx r3
cmp r4,r6
add.w r4 r4,#1
bne #0xf0ccc
```

ARM32

```
ldr x0,[x21,x19,lsl #3]
blr x0
cmp x19,x20
add x19,x19,#1
b.ne #0x130c88
```

ARM64

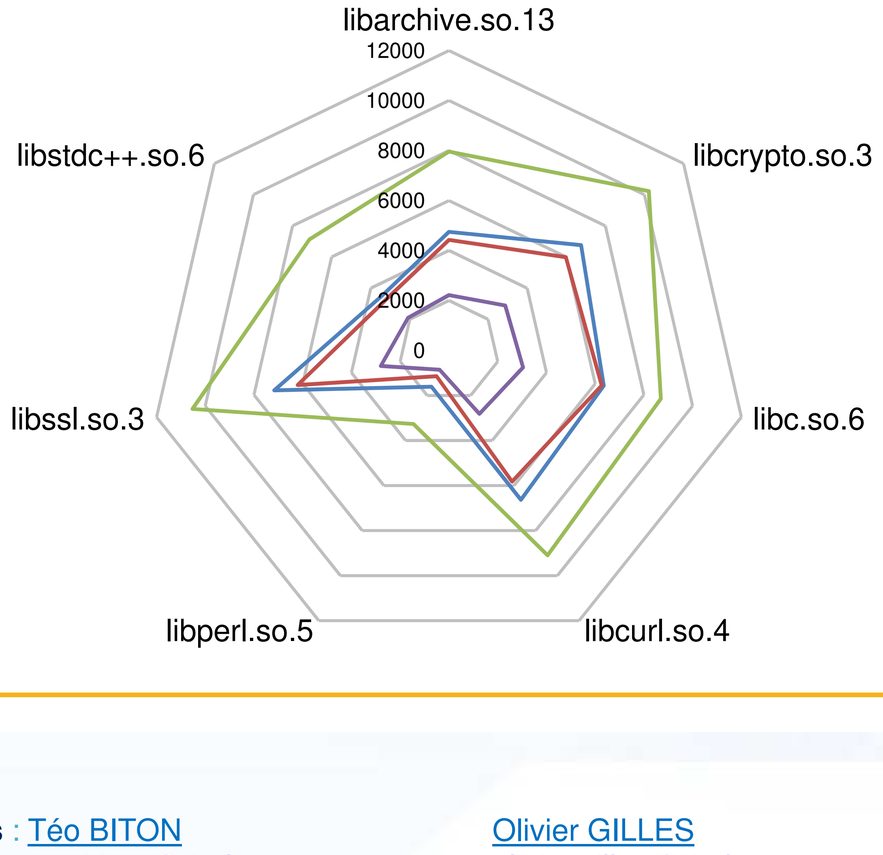
Conclusion

- Study of applicative libraries compiled for ARM and RISC-V
- ARM32 has a higher number of return-oriented programming gadgets, while RISC-V has a higher number of jump-oriented programming gadgets
- Security-related libraries such as libssl and libcrypto have a higher number of gadgets compared to other libraries

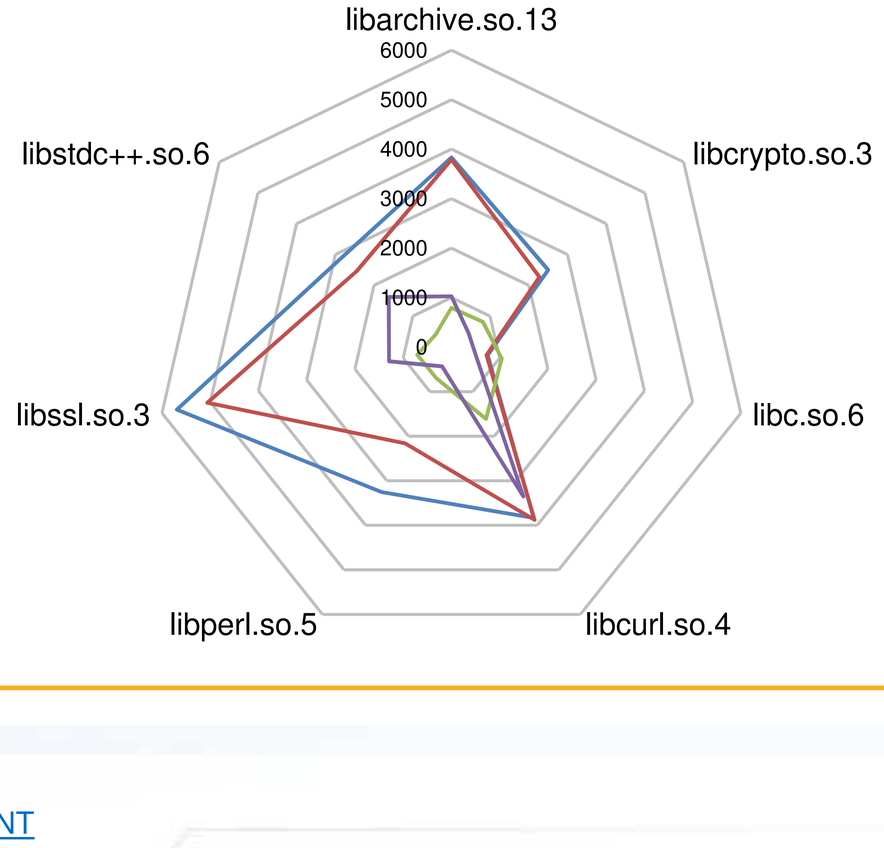
Perspectives

- Investigate gadget exploitability across all architectures
- Derive innovative hardware-based countermeasures from the signatures of gadgets

Number of return-oriented programming gadgets per section size in megabytes



Number of jump-oriented programming gadgets per section size in megabytes



Contacts : Téo BITON
teo.biton@thalesgroup.com
Olivier GILLES
olivier.gilles@thalesgroup.com
Sébastien PILLEMENT
sebastien.pillement@univ-nantes.fr