Control Flow Enforcement Technology (CET)

Information Security Inc.

Contents

- About CET
- Why CET
- Three decades of runtime attacks
- Recent attacks
- Runtime attacks
- Defenses against code reuse
- Control-Flow Integrity (CFI)
- Hardware CFI
- Intel CET details
- Conclusions
- References

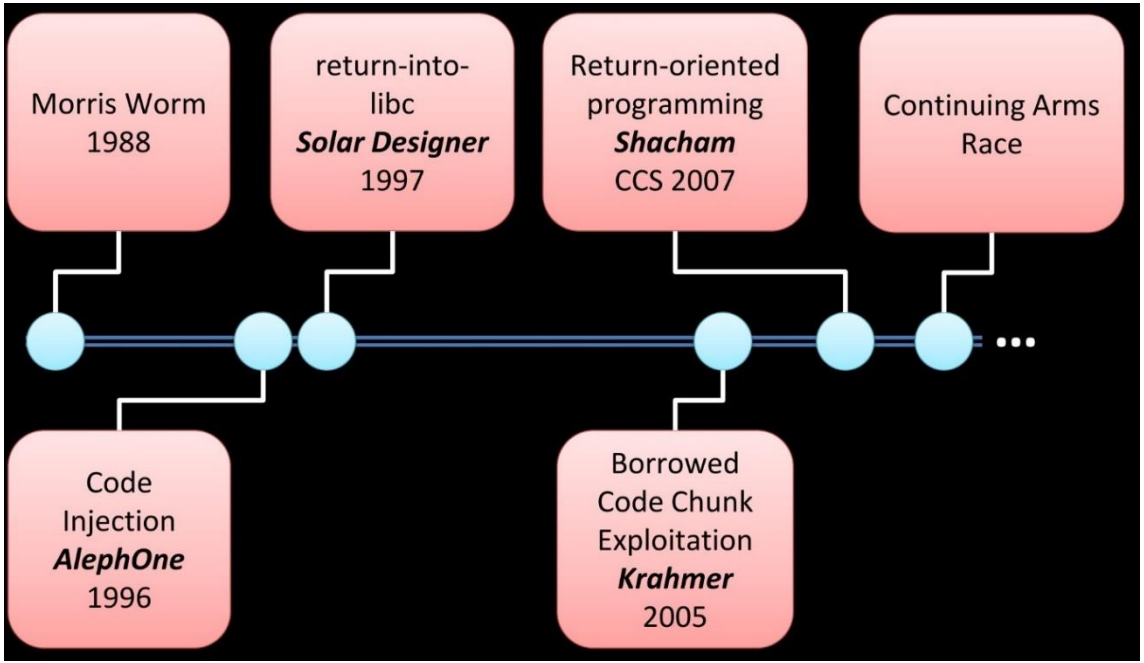
About CET

- Intel anti-ROP technology
- Builds on previous work on Control Flow Integrity (CFI) done by Microsoft and a paper by IAD proposing hardware-enforced CFI

Why CET

- Because: One of the latest anti-hacking chip enhancement
- Return-oriented Programming (ROP), and similarly call/jmp-oriented programming (COP/JOP), have been the prevalent attack methodology for stealth exploit writers targeting vulnerabilities in programs.
- Control-flow Enforcement Technology (CET) is here to defend against ROP/JOP style control-flow subversion attacks.

Three decades of runtime attacks



Recent attacks

Attacks on Tor Browser [2013]

FBI Admits It Controlled Tor Servers Behind Mass Malware Attack.

Stagefright [Drake, BlackHat 2015]

These issues in Stagefright code critically expose 95% of Android devices, an estimated 950 million devices

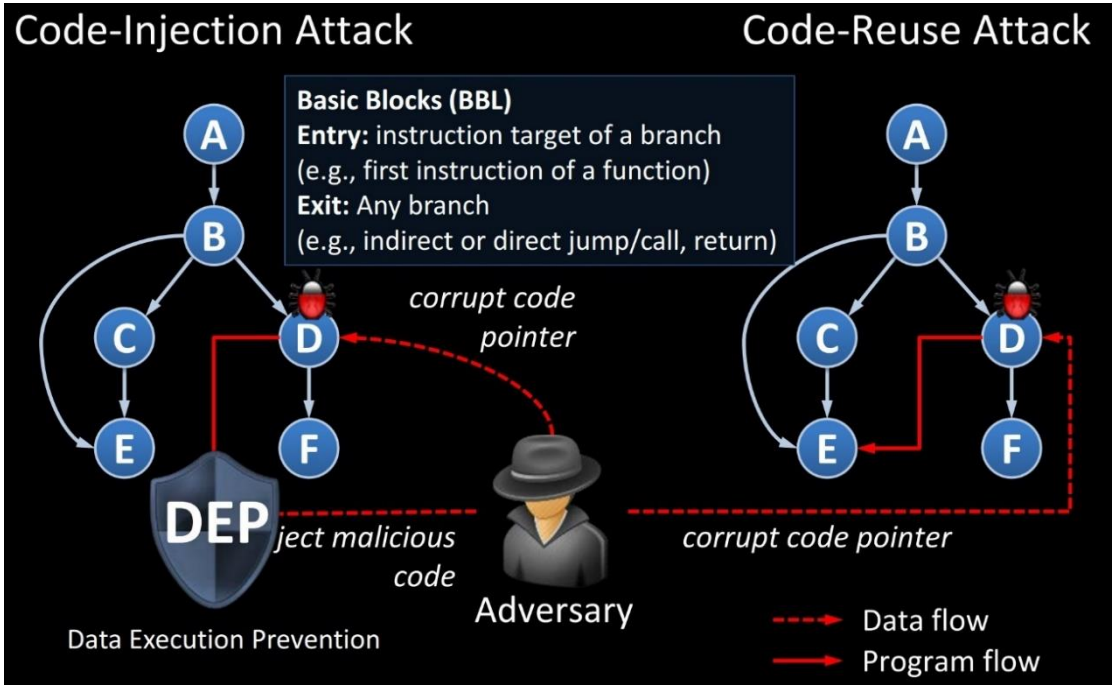
Cisco Router Exploit [2016]

Million CISCO ASA Firewalls potentially vulnerable to attacks

The Million Dollar Dissident [2016]

Government targeted human rights defender with a chain of zero-day exploits to infect his iPhone with spyware.

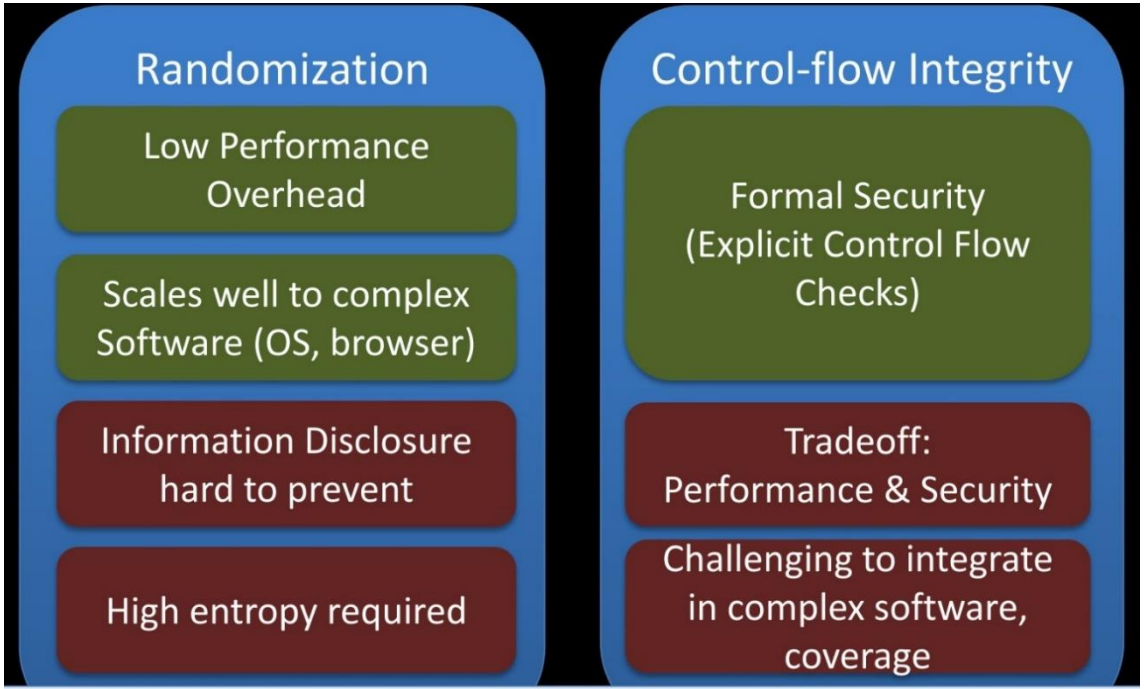
Runtime attacks



Defenses against code reuse

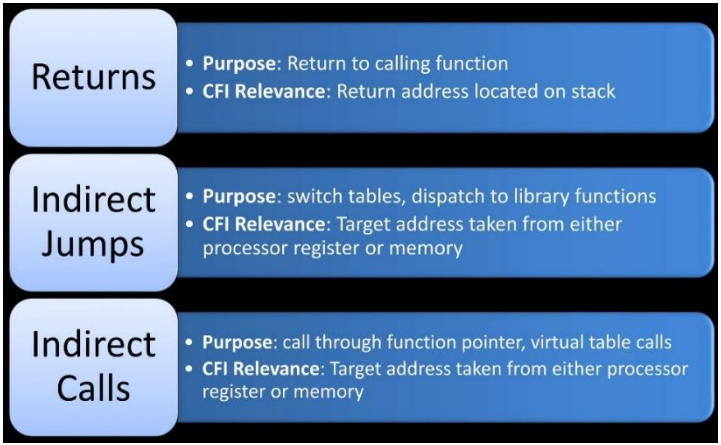
- Code Randomization
- Control-Flow Integrity (CFI)

Defenses against code reuse



Control-Flow Integrity (CFI)

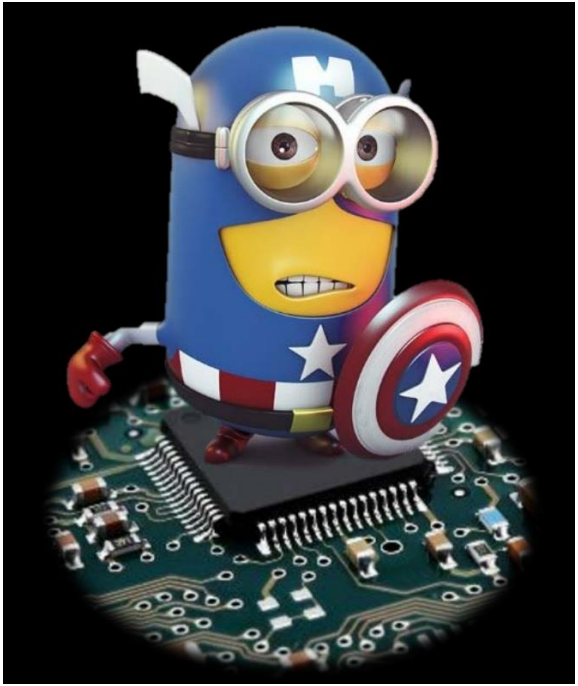
- Prevents control-flow hijacking attacks
- CFI restricts indirect branch(jmp, call, ret) source and destination
- Often coupled
- With a shadow stack
- Control flow graph maps all function calls



Control-Flow Integrity (CFI)

- A pure software solution CFI has problems and could be exploited
  http://ieeexplore.ieee.org/document/6956588/

Hardware CFI



Hardware CFI

- Method to define the intended control flow (CFG) to HW
- Method to protect dynamic control flows – a protected shadow stack
- For any call, a copy of the return address is stored into both the regular stack and the shadow area.

Intel CET details

- Shadow stack detects return-address manipulation
- Shadow stack protected, cannot be accessed by the attacker
- New register ssp for the shadow stack
- Conventional move instructions cannot used in shadow stack
- New instructions to operate on shadow stack
- New instruction for indirect call/jump targets: branched
- Could be combined with fine-grained compiler-based CFI (LLVM CFI)

Conclusions

- This is a natural evolution of exploit mitigation techniques and really the future of trusted computing.
- CET combined with boot chain trust, application white listing and existing/new anti-exploitation techniques can assure the developing trusted systems for which even more classes of threat can be eliminated.

References

- Microsoft CFI
  https://www.microsoft.com/en-us/research/publication/control-flow-integrity/?from=http%3A%2F%2Fresearch.microsoft.com%2Fpubs%2F64250%2Fccs05.pdf
- IAD paper
  https://github.com/iadgov/Control-Flow-Integrity
- Intel
  https://software.intel.com/en-us/blogs/2016/06/09/intel-release-new-technology-specifications-protect-rop-attacks