

CS 6V81-002: Quiz 19 Solutions

April 9, 2008

- Existing ISR implementations... (circle all that apply)
 - customize the instruction-fetch logic in the hardware or virtual machine**
 - customize the compiler back-end to emit encrypted machine code
 - customize the program-loader to encrypt the code segment**
 - customize the memory subsystem to encrypt/decrypt bytes written/read to/from memory at runtime

Existing ISR implementations customize the program-loader to encrypt the code segment in memory, and customize instruction-fetch logic to decrypt each instruction as it is fetched. Note that this doesn't work for self-modifying code, so future implementations might have to add something along the lines of answer (d).

- One advantage of the jump-attack as compared to the return-attack is... (circle one)
 - the jump-attack reveals two key bytes at a time instead of just one
 - the jump-attack payload fits into a smaller buffer size
 - the jump-attack can be parallelized for faster convergence
 - the return-attack corrupts the stack pointer**

The problem with the return-attack is that it corrupts the stack pointer even on success. Thus, the attacker must hope that some observably different behavior can be used to identify a successful guess before the process crashes. The jump-attack is more robust but slower because it requires guessing two bytes at a time instead of just one.

- For attack payloads larger than 1K, the authors recommend... (circle all that apply)
 - using a “nop-sled” to decrease the false positive rate
 - using probabilistic propagation to evade intrusion detectors
 - including a virtual machine in the payload**
 - including the key-cracking algorithm in the payload**

For larger payloads the authors encode a tiny virtual machine into the malicious code. The virtual machine executes the key-cracking algorithm from the compromised machine in order to propagate the virus.

- The jump-attack took about how long on average to crack a 100-byte key on a modified RISE server? (circle one)
 - 18 hours
 - 4 hours
 - 6 minutes**
 - 40 seconds

5. Would the attack described in the previous paper succeed without modification on an ISR-protected system? Why or why not?

Yes, the attack would work without modification. ISR only protects against code-injection attacks, but the previous paper described a jump-to-libc attack that used no code-injection.