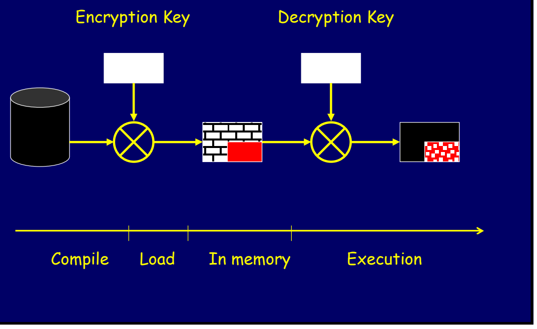
The Effectiveness of Instruction Set Randomization

Where's the FEEB?: The Effectiveness of Instruction Set Randomization. Nora Sovarel, David Evans, Nate Paul. To appear at USENIX Security, August 2005

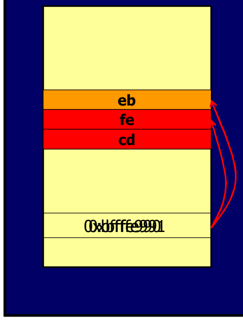
Nora Sovarel
http://www.cs.virginia.edu/nora
University of Virginia
Computer Science

2005 IEEE Symposium on Security and Privacy

Instruction Set Randomization



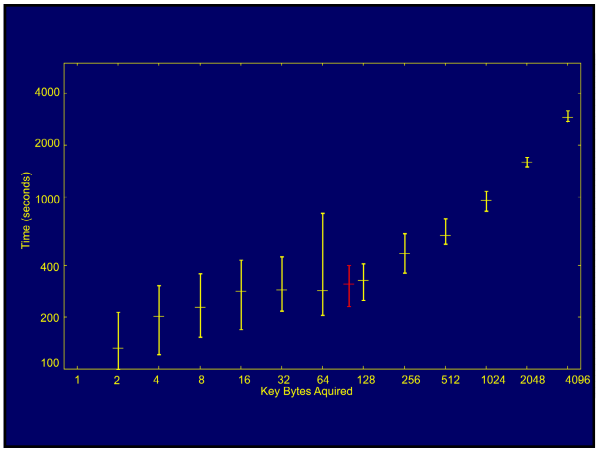
Jump Attack: jmp -2



- 2-byte instruction
- Correct: infinite loop
- Wrong:
  - Usually crashes
  - Sometimes false positive
- False positives
  - Conditional jumps
  - Used to reduce the number of attempts (average 24 per byte)

Requirements

- Multiple guess attempts on same key
  - Server forks process
  - No rerandomization
- Remotely observable behavior
- Injection at known address
- Simple encryption scheme
  - Byte-wise
  - Learn key from one plain/cipher pair



Conclusion

- It sometimes works
- Possible countermeasures
  - Rerandomize periodically
  - Stronger encryption

http://www.cs.virginia.edu/nora

***Where's the FEEB?: The Effectiveness of Instruction Set Randomization.* Nora Sovarel, David Evans, Nate Paul**. To appear at USENIX Security 2005