Discussion: Remote Timing Attacks are Practical

600.624
2/11/05
Outline

• Why are timing attacks important?

• Clarifications
  • Zero-One Gap / Neighborhood Size etc.

• Problems

• Questions

• Extensions

• Contribution

• Discussion
How fast can we factor?

- Seny: RSAP. How do you go after crypto?
- RSA Challenge
  - RSA-576
    - 576 bits (174 digits)
    - Factored in 2 years (2001-2003) used “Lattice Sieving”
- http://www.rsasecurity.com/rsalabs/
How fast can we factor? (2)

- Number Field Sieves
- “Fast Algorithms”
- Complexity:

\[ O\left(e^{c \left(\log n\right)^{1/3} \left(\log \log n\right)^{2/3}}\right) \]
Dangers of Timing Attacks

• Probably not going to crack RSA (or El Gamal) any time soon

• Dangers: Poor passwords (keys, entropy), timing attacks
Clarifications
What is the Zero-One Gap?

Zero-One Gap = $| \Delta_1 - \Delta_0 |$
Zero-One Gap

![Graph showing time difference in CPU cycles against bits guessed of factor q for different keys. The graph has a horizontal line at 0, with Key 1, Key 2, and Key 3 represented by different lines. The x-axis represents the bits guessed of factor q, ranging from 0 to 250, and the y-axis represents the time difference in CPU cycles, ranging from -1.5e+07 to 1.5e+07.](image)
What is the “neighborhood size”? 

• Need to get better estimates at number of reductions (more on that later...)

\[ T_g = \sum_{1=0}^{n} \text{DecryptTime}(g + i) \]

\[ T_{ghi} = \sum_{1=0}^{n} \text{DecryptTime}(ghi + i) \]

\[ \Delta = |T_g - T_{ghi}| \]

• Why increment \( i \)? (Multiplication??)
Neighborhood
Neighborhood

increasing neigh. = larger zero-one gap
1 ms?

- State that 1 ms of Zero-One Gap is sufficient for attack.
- Where did this number come from?
Can we really tolerate 1 ms network variance?
Problems
Great Paper! (?)

- Were the mathematics adequately explained?
- Did they provide empirical evidence that this attack is feasible?
“remote timing attacks are **PRACTICAL**

- **Setup:**
  - 3 Hop Network
  - Load on the server

- **Experiments:**
  - broke 2.5/3 keys
  - sample size (?!?)

- What does this mean for failure rate?
Questions

• What about the first bits?
Questions (2)

• Would using OAEP prevent the attack?
  • Quick Answer: no.

• What about RSA Signatures?
  • hashing?
Questions (3)

- Why include the VM Model?
  - Some people liked it...
- What is the failure rate?
  - Come back to this...
Questions (4)

• How are they averaging their timing samples?
  • What does this imply about distribution?
  • What does this mean about their error rate?
Defenses ("Hacks")

- Queueing Algorithms
- Add a delay on decryption failure
- Application layer Firewall
- What about RSA batching?
Better Defenses (?)

• Blinding

  • “Are we wrong to rely on blinding considering it isn’t provably secure?”

• Quantizing
Extensions

• What is the smallest neighborhood/sample size parameters such that the attack will work?
Extensions (2)

• Are there $p/q$ or $e/d$ pairs for which Multiplication and Reductions offset? (See key 3.) If so, what percent of the key space is vulnerable? (HARD??)
Contribution

- We all accepted this paper... discuss why.
Discussion

• Anything you would like to bring up?