Flaw in RSA Implementation

Lois Fozzard

February 28, 2012

RSA

- Remember RSA?

RSA

- Remember RSA?
  - pick two primes, product n

RSA

- Remember RSA?
  - pick two primes, product n
  - public key
    - n and e, relatively prime to $\phi(n)$

RSA

- Remember RSA?
  - pick two primes, product n
  - public key
    - n and e, relatively prime to $\phi(n)$
  - private key
    - n and d, $e^{-1} mod \phi(n)$

RSA

- Remember RSA?
  - pick two primes, product n
  - public key
    - n and e, relatively prime to $\phi(n)$
  - private key
    - n and d, $e^{-1} mod \phi(n)$
- hard to factor n

Finding the Flaw

- Team of mathematicians and cryptographers discovered a flaw

Finding the Flaw

- Team of mathematicians and cryptographers discovered a flaw
    - 7,000,000 keys examined

Finding the Flaw

- Team of mathematicians and cryptographers discovered a flaw
  - 7,000,000 keys examined
  - 27,000 have common factor

Finding the Flaw

- Team of mathematicians and cryptographers discovered a flaw
  - 7,000,000 keys examined
  - 27,000 have common factor
  - 1 in 500 keys insecure

Finding the Flaw

- RSA said the problem is the implementation

Finding the Flaw

- RSA said the problem is the implementation
    - algorithm still secure

Finding the Flaw

- RSA said the problem is the implementation
  - algorithm still secure
- Implementations "randomly" generate primes

Finding the Flaw

- RSA said the problem is the implementation
    - algorithm still secure
- Implementations "randomly" generate primes
    - can computers be truly random?

Finding the Flaw

- RSA said the problem is the implementation
  - algorithm still secure
- Implementations "randomly" generate primes
  - can computers be truly random?
- Researchers did not determine exact problem
  - however, it was in multiple implementations

Why Should We Care?

Part 1

Why Should We Care?

Part 1

- 99.8% of keys unaffected

Why Should We Care?

Part 1

- 99.8% of keys unaffected
- Have hackers also discovered this weakness?

Why Should We Care?

Part 2

Why Should We Care?

Part 2

- RSA

Why Should We Care?

Part 2

- RSA
- Confidentiality

Why Should We Care?

Part 2

- RSA
- Confidentiality
    - Eve could discover Bob’s private key

Why Should We Care?

Part 2

- RSA
- Confidentiality
  - Eve could discover Bob's private key
- Authentication

Why Should We Care?

Part 2

- RSA
- Confidentiality
  - Eve could discover Bob's private key
- Authentication
  - Alice encrypts a symmetric key

Why Should We Care?
Part 2

- RSA
- Confidentiality
  - Eve could discover Bob's private key
- Authentication
  - Alice encrypts a symmetric key
  - Eve interecpts and decrypts it

Why Should We Care?

Part 2

- RSA
- Confidentiality
  - Eve could discover Bob's private key
- Authentication
  - Alice encrypts a symmetric key
  - Eve interecpts and decrypts it
  - Alice thinks Eve is Bob

Super Awesome Amazing Spectacular References Slide

- http://www.nytimes.com/2012/02/15/technology/researchers-find-flaw-in-an-online-encryption-method.html?_r=2
- http://news.cnet.com/8301-1009_3-57377744-83/researchers-find-flaw-in-key-generation-with-popular-cryptography/
- http://spectrum.ieee.org/tech-talk/telecom/security/update-rsa-responds-to-flaw-finding

The End

(You may clap now)