How to Tell the Birds from the Primes

Martin Abadi, Andrew Birrell,
Ilya Mironov, Ted Wobber, Yinglian Xie

Microsoft Research Silicon Valley

Valentine's Day
February 14, 2012

Ron was wrong, Whit is right

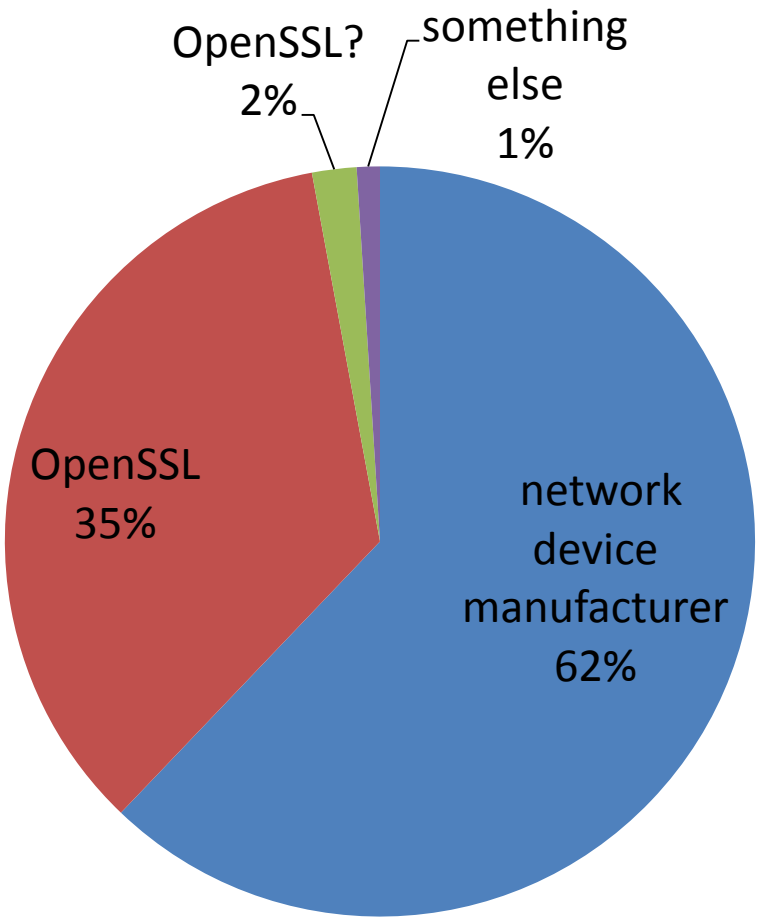
Arjen K. Lenstra[1], James P. Hughes[2],
Maxime Augier[1], Joppe W. Bos[1], Thorsten Kleinjung[1], and Christophe Wachter[1]

[1] EPFL IC LACAL, Station 14, CH-1015 Lausanne, Switzerland
[2] Self, Palo Alto, CA, USA

Ron was wrong, Whit is right, Arjen is ...?

- Snapshot of EFF Observatory from 2010
- 4.4M distinct keys
- 10K distinct factorizable RSA moduli
- Reproduced results from Lenstra et al., ePrint 2012/64

Origin?


OpenSSL?
2%
something
else
1%
OpenSSL
35%
network
device
manufacturer
62%

How OpenSSL Samples Safe Primes?

Safe primes: $q = 2p + 1 \in \mathbb{P}$, where $p \in \mathbb{P}$

1. Sieving step:

   Find "candidate" odd q, such that

   $$q \not\equiv 0,1 \bmod 3,5 \ldots, 17863$$

2. Verification step:
   a) Apply Miller-Rabin to q
   b) Apply Miller-Rabin to $(q-1)/2$

How OpenSSL Samples ~~Safe~~ Primes?

~~Safe primes: $q = 2p + 1 \in \mathbb{P}$, where $p \in \mathbb{P}$~~

1. Sieving step:

   Find "candidate" odd q, such that

   $$q \not\equiv 0,1 \bmod 3,5 \ldots, 17863$$

2. Verification step:
   a) Apply Miller-Rabin to q
   b) Apply Miller-Rabin to $(q-1)/2$

How OpenSSL Samples ~~Safe~~ Primes?

~~Safe primes: $q = 2p + 1 \in \mathbb{P}$, where $p \in \mathbb{P}$~~

1. Sieving step:

   Find "candidate" odd q, such that

   $$q \not\equiv 0,1 \bmod 3,5 \ldots, 17863$$

2. Verification step:

   a) Apply Miller-Rabin to q

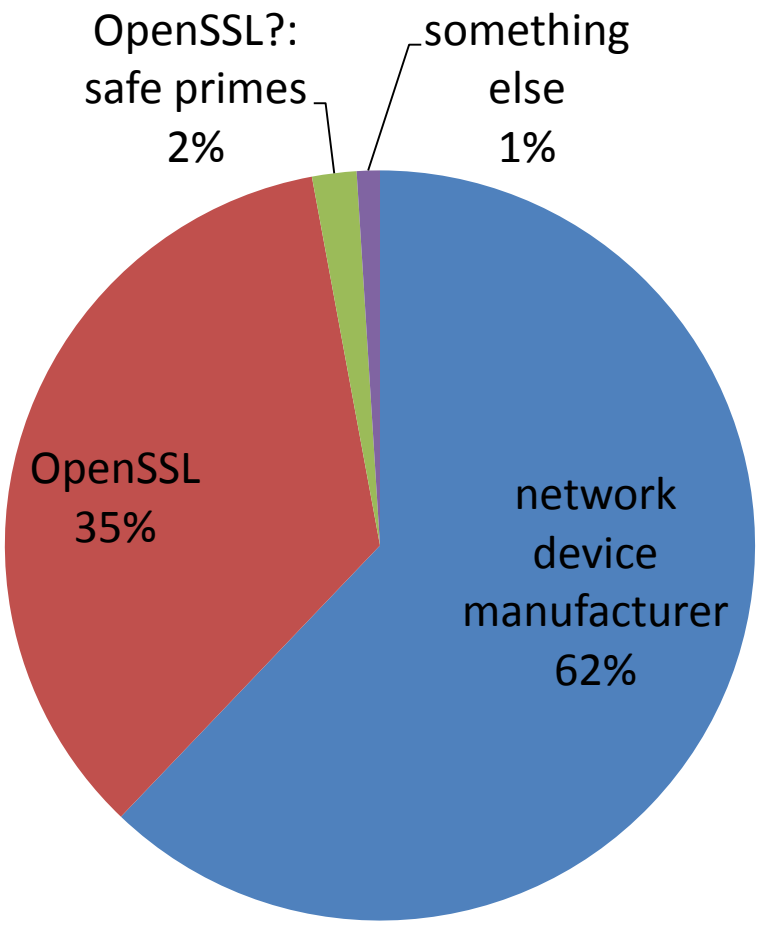
   ~~b) Apply Miller-Rabin to $(q - 1)/2$~~

OpenSSL can only output a prime q, such that $q - 1 \nmid 3,5, \ldots, 17683$

1:15 primes have this property

Not a vulnerability, but a fingerprint

Origin


OpenSSL?:
safe primes
2%
something
else
1%
OpenSSL
35%
network
device
manufacturer
62%