# Mining Your Ps and Qs: Detection of Widespread Weak Keys in Network Devices

**Nadia Heninger**
Zakir Durumeric  Eric Wustrow  Alex Halderman

Usenix Security August 8-10 2012.

`factorable.net`

# Research plan

1. Get public keys.
2. Look for stuff that might go wrong with public keys. (Repeated keys, RSA common factors, etc.)
3. Find that stuff went wrong with public keys.
4. Figure out why stuff went wrong with public keys.

# Linux: A tale of two RNGs

| `/dev/random` | `/dev/urandom` |
| --- | --- |
| "high-quality" randomness | pseudorandomness |
| blocks if insufficient entropy available | never blocks |

> *As a general rule, `/dev/urandom` should be used for everything except long-lived GPG/SSL/SSH keys.*—`man random`

# Linux: A tale of two RNGs

`/dev/random`

"high-quality" randomness

blocks if insufficient entropy available

`/dev/urandom`

pseudorandomness

never blocks

*As a general rule, `/dev/urandom` should be used for everything except long-lived GPG/SSL/SSH keys.*—`man random`

```
 /* Well use /dev/urandom by default, since
/dev/random is too much hassle.  If system developers
aren't keeping seeds between boots nor getting any
entropy from somewhere it's their own fault.  */
#define DROPBEAR_RANDOM_DEV "/dev/urandom"
```

## Entropy sources

Time of boot

Keyboard/mouse

Disk access timing

(Interrupt timing)

## Entropy sources

Time of boot

Keyboard/mouse

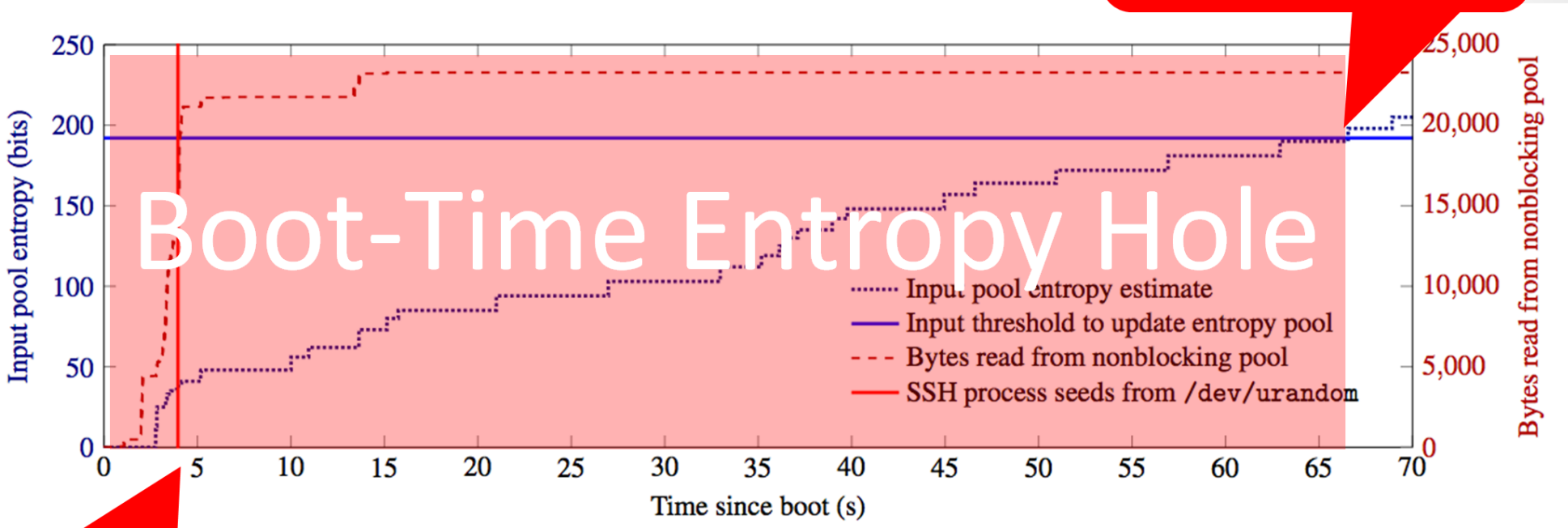
Disk access timing

(Interrupt timing)

# Ubuntu Server 10.04 Test System

## (Typical boot)

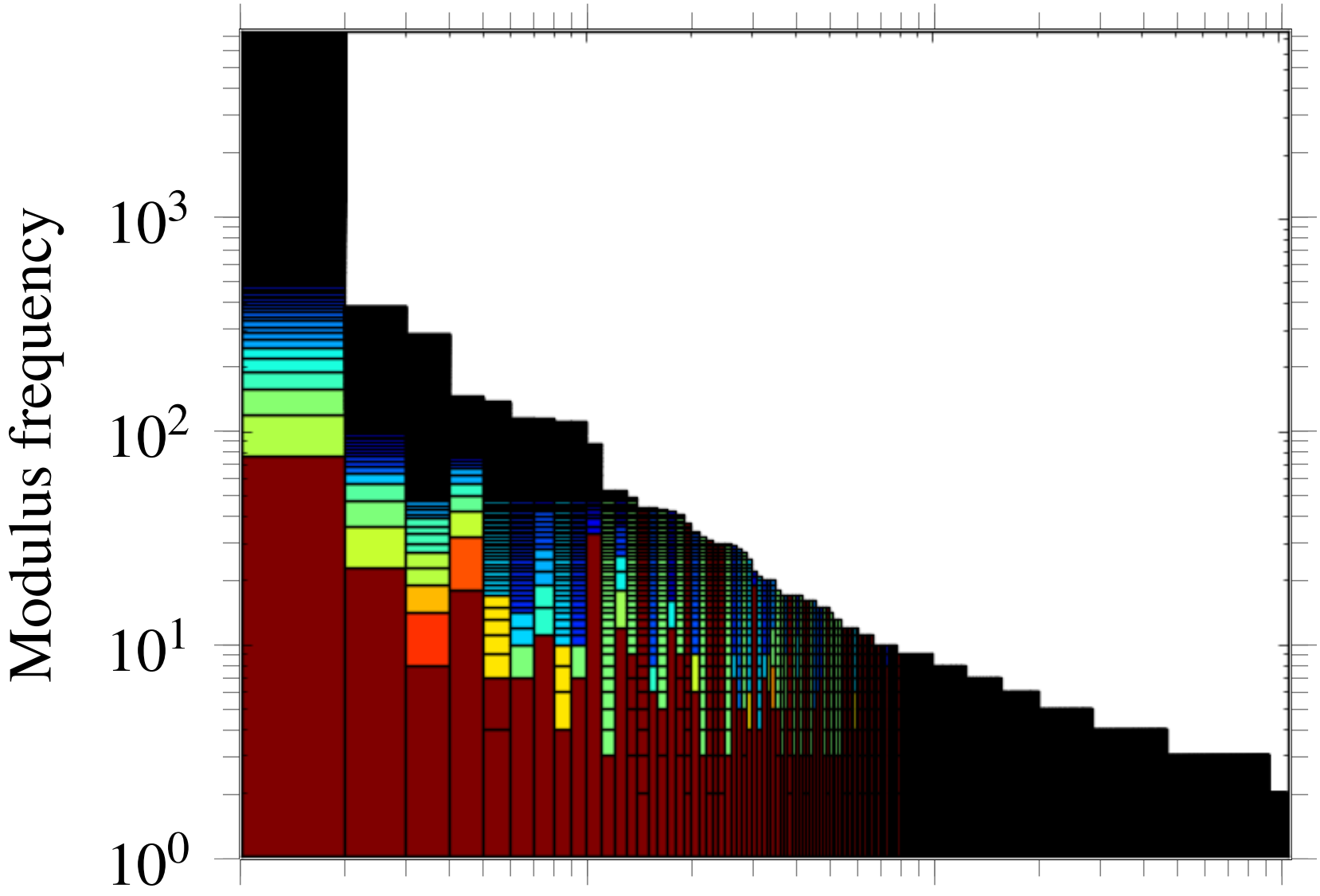
First Input entropy mixed into /dev/urandom



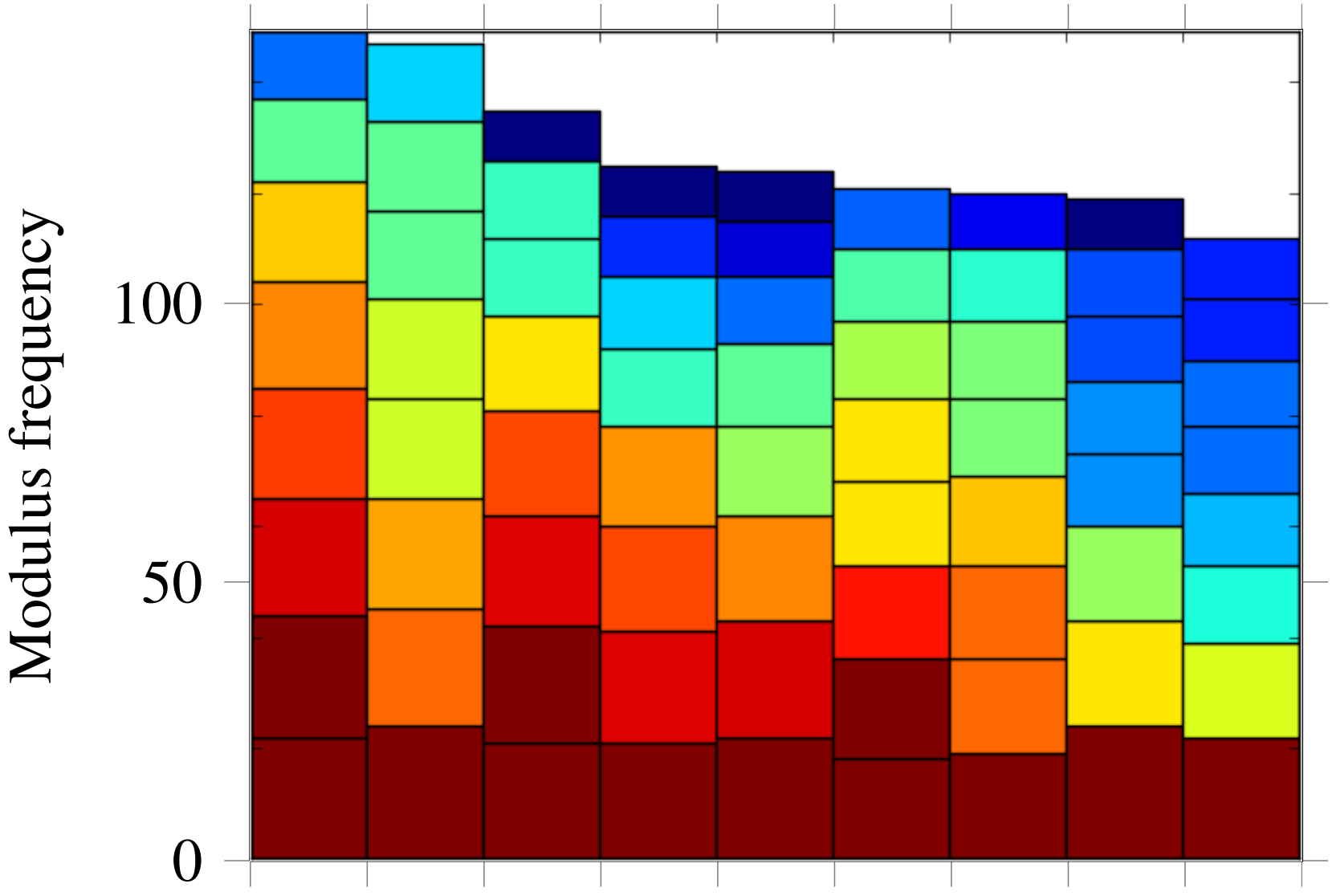

OpenSSH seeds from /dev/urandom

Dev /dev/urandom may be predictable for a period after boot.

# Primes generated by Juniper network security devices



# Primes generated by IBM remote access cards



# DSA

- Reuse signature randomness $\rightarrow$ private key revealed.

# DSA

- Reuse signature randomness $\rightarrow$ private key revealed.
- SSH handshake includes signature on key exchange.

# DSA

- Reuse signature randomness $\rightarrow$ private key revealed.
- SSH handshake includes signature on key exchange.
- We collected 9,114,925 signatures of which 4,365 used repeated randomness.

# DSA

- Reuse signature randomness $\rightarrow$ private key revealed.
- SSH handshake includes signature on key exchange.
- We collected 9,114,925 signatures of which 4,365 used repeated randomness.
- Computed private keys for 105,728 (1.6%) of SSH DSA hosts.

# Responsible disclosure

- Contacted 57 vendors.
- 11 had security contact information that we could find.
- 22 vendors actually responded to us.

- Changes to linux kernel.
- Also tried to contact some end users...

# Mining Your Ps and Qs: Detection of Widespread Weak Keys in Network Devices

**Nadia Heninger**
Zakir Durumeric  Eric Wustrow  Alex Halderman

Usenix Security August 8-10 2012.

`factorable.net`