Elliptic Curve Cryptography in Practice

Joppe W. Bos, J. Alex Halderman,
Nadia Heninger, Jonathan Moore,
Michael Naehrig, and Eric Wustrow

A Brief History of Elliptic Curve Cryptography

1985-1987 Miller & Koblitz: elliptic curves can be used for public-key cryptography

2000 Certicom: standards for ECC

2006 NIST: standard for ECDSA

2006 RFC 4492: ECC in TLS

2009 RFC 5656: ECC in SSH

2009 Nakamoto: Bitcoin

Research Program

1. Acquire keys.
2. Profit?

Acquiring keys

1. Port-scan the entire Internet.

2. Download bitcoin blockchain.

The Good News

People are actually using ECC!

- $\approx$ 10% of SSH (1.2 million hosts)
- $\approx$ 7% of TLS (2.2 million hosts)
- All of bitcoin. (15 million public keys)

TLS curves

Curves (one vote per host that had a successful handshake):

```
2144467 (98.3%) secp256r1
2099848 (96.3%) null
1751780 (80.3%) secp384r1
 379638 (17.4%) secp521r1
  55000 (2.5%) sect233r1
  24860 (1.1%) sect163k1
  24233 (1.1%) secp224r1
  23355 (1.1%) secp192r1
      ...
  22847 (1.0%) sect193r1
  22846 (1.0%) sect193r2
      4 (0.0%) brainpoolP256r1
      4 (0.0%) brainpoolP384r1
      4 (0.0%) brainpoolP512r1
```

SSH curves

```
1674663  ecdh-sha2-nistp256
1672521  ecdh-sha2-nistp521
1672486  ecdh-sha2-nistp384
117  ecdh-sha2-h/SsxnLCtRBh7I9ATyeB3A==
117  ecdh-sha2-qcFQaMAMGhTziMTOz+Tuzw==
116  ecdh-sha2-VqBg4QRPjxx1EXZdVOGdWQ==
116  ecdh-sha2-5pPrSUQtIaTjUSt5VZNBjg==
116  ecdh-sha2-9UzNcgwTlEnSCECZa7V1mw==
```

Bitcoin curves

```
secp256k1
```

The Less Good News

Efficiency > security

Most TLS, SSH hosts support NIST curves in increasing order of security.

`nistp256,nistp384,nistp521`

Our SSH scan client supported only ECC cipher suites.

- 500,000 hosts sent us a DSA public key.
- 30,000 hosts sent us an RSA public key.
- 8,000 hosts sent us an *empty* public key.

The Bad News

Repeated public keys

- 400,000 (30%) of SSH hosts serve non-unique ECDSA keys.
- 200,000 (4%) of TLS ECDHE values non-unique.

Cloud Hosting Issues

July 2013, Digital Ocean
Avoid duplicate SSH host keys

> *"The SSH host keys for some Ubuntu-based systems could have been duplicated by DigitalOcean's snapshot and creation process."*

5614 hosts served the public key contained in Digital Ocean's SSH setup guide.

Repeated ECDSA Signature Nonces

158 bitcoin addresses repeated signature nonces.

Address `1HKywxiL4JziqXrzLKhmB6a74ma6kxbSDj` has stolen 59 **BTC** $\approx$ 3.6 **million rupees** from these addresses.

3 of these repeats due to Android Java RNG vulnerability.

Elliptic Curve Cryptography in Practice

Joppe W. Bos and J. Alex Halderman and Nadia Heninger and Jonathan Moore and Michael Naehrig and Eric Wustrow

http://eprint.iacr.org/2013/734