Stealing Bitcoin with Math

Ryan Castellucci
Filippo Valsorda

Ryan Castellucci

DEF CON 23 - “Cracking Cryptocurrency Brainwallets”

“The Bitcoin Brain Drain: A Short Paper on the Use and Abuse of Bitcoin Brain Wallets” - Marie Vasek, Joseph Bonneau, Ryan Castellucci, Cameron Keith, and Tyler Moore

“Speed Optimizations in Bitcoin Key Recovery Attacks” - Nicolas Courtois, Guangyan Song, and Ryan Castellucci

Filippo Valsorda

CLOUDFLARE®

HITB2014KUL - “Exploiting ECDSA Failures in the Bitcoin Blockchain”

“Private Key Recovery Combination Attacks: On Extreme Fragility of Popular Bitcoin Key Management, Wallet and Cold Storage Solutions in Presence of Poor RNG Events” - Nicolas T. Courtois, Pinar Emirdag, and Filippo Valsorda

The Washington Post

Rampage | Opinion

Ivy League economist ethnically profiled, interrogated for doing math on American Airlines flight

By Catherine Rampell May 7

Private keys

399BD8987FC57DB698311E04B2C3412C75C9F7CCB455630B544CED0608C57659

Crypto magic

Public keys

0394FDD134FA7105E0B7E2FB5FC56C332D89A8FFB0C5E8F8C2C274A29FE24E866F

Hash

Addresses

1FCKkv8bhCt6SKKS3k99TydxkTZEjiEFoJ

Receive

Addresses

`1FCKkv8bhCt6SKKS3k99TydxkTZEjiEFoJ`

Receive

Addresses ← published

`1FCKkv8bhCt6SKKS3k99TydxkTZEjiEFoJ`

Private keys

```
399BD8987FC57DB698311E04B2C3412C75C9F7CCB455630B544CED0608C57659
```

Spend

Private keys

399BD8987FC57DB698311E04B2C3412C75C9F7CCB455630B544CED0608C57659

Steal

Private keys

```
0000000000000000000000000000000000000000000000000000000000000001
```

Crypto magic

Public keys

```
0279BE667EF9DCBBAC55A06295CE870B07029BFCDB2DCE28D959F2815B16F81798
```

Hash

Addresses

```
1BgGZ9tcN4rm9KBzDn7KprQz87SZ26SAMH
```

Private keys

```
0000000000000000000000000000000000000000000000000000000000000002
```

Crypto magic

Public keys

```
02C6047F9441ED7D6D3045406E95C07CD85C778E4B8CEF3CA7ABAC09B95C709EE5
```

Hash

Addresses

```
1cMh228HTCiwS8ZsaakH8A8wze1JR5ZsP
```

Private keys

0000000000000000000000000000000000000000000000000000000000000003

Crypto magic

Public keys

02F9308A019258C31049344F85F89D5229B531C845836F99B08601F113BCE036F9

Hash

Addresses

1CUNEBjYrCn2y1SdiUMohaKUi4wpP326Lb

brainflayer

https://rya.nc/brainflayer

```
$ ./brainflayer -v -I 0000...0001 -b bloom.blf -f addr.bin -o cracked
rate: 110268.38 p/s found:   112/6815744    elapsed:   60.751 s

$ tail cracked
7ff45303774ef7a52fffd8011981034b258cb86b:c:(hex)priv/btc:
0000000000000000000000000000000000000000000000000000000002de40f
a91bc8e0cc56b5951cc54b14d4aa1f713cfee41c:c:(hex)priv/btc:
0000000000000000000000000000000000000000000000000000000003b01f1
d0a79df189fe1ad5c306cc70497b358415da579e:c:(hex)priv/btc:
0000000000000000000000000000000000000000000000000000000556e52
5baa200a8ec459e1d9e8488be9bc69e97b40fcb5:u:(hex)priv/btc:
0000000000000000000000000000000000000000000000000000000056cd81
bb45374137f6cb0630443f45bb1f208275c9e8ff:u:(hex)priv/btc:
0000000000000000000000000000000000000000000000000000000056cd82
5b32135cd104e01e5454d41ddcf8ae3f786f01bc:u:(hex)priv/btc:
0000000000000000000000000000000000000000000000000000000056cd83
9e8cf1917702c6dd9251537bcaf35582ee6eb9e1:c:(hex)priv/btc:
0000000000000000000000000000000000000000000000000000005d2100
```

149 hits

Range: 1 - 150,000,000,000

February 2016

Highest publicly broken key

~700,000,000,000,000

Highest possible private key

115,792,089,237,316,195,423,570,
985,008,687,907,852,837,564,279,
074,904,382,605,163,141,518,161,
494,336

00000000000000000000000000000000000000000000000031323334

00000000000000000000000000000000000000010000000000000000

00000010000000000000000000000000000000000000000000000000

11000000000000000000000000000000000000000000000000002002

11111111111111111111111111111111111111111111111111111111

42000000000000000000000000000000000000000000000000000000

91779177917791779177917791779177917791779177917791779177

aaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaa

cdcdcdcdcdcdcdcdcdcdcdcdcdcdcdcdcdcdcdcdcdcdcdcdcdcdcdcd

eeeeeeeeeeeeeeeeeeeeeeeeeeeeeeeeeeeeeeeeeeeeeeeeeeeeeeee

Raw addresses

```
0000000000000000000005fcfb1c0143be4d42cea9bd74ab63e175f34be17
0000000000000000000028bc56c889111335c23e6715a0aeb92e0adeb2e6
```

Block hashes

```
00000000c5fef55bc9cc3d4bd26d4f5495af1dba2c4e284a3e9915f7c4a77980
0000000000000114420273c901e448a0a51a89fe2e6964541994c7eb1a3e615b
```

Mystery blockchain data

```
31077625bc49683784096ad0855553c10e5144e0e0090889a403187924c7ba47
4624779f38a4d14755537416539 2c6963165a0449f2abb651a29b74f1c029814
```

Brainwallets

Brainwallets

Memorable string

`correct horse battery staple`

Stupidly fast hash

Private key

Crypto magic

Public key

Hash

Address

correct horse battery staple

1JwSSubhmg6iPtRjtyqhUYYH7bZg3Lfy1T

4097 Tx – 15.41512035 BTC

bitcoin is awesome

14NWDXkQwcGN1Pd9fboL8npVynD5SfyJAE

19 Tx – 501.06500863 BTC

"" (an empty string)

1HZwkjkeaoZfTSaJxDw6aKkxp45agDiEzN

273 Tx - 58.89151975 BTC

thequickbrownfoxjumpedoverthelazydog

1MjGyKiRLzq4WeuJKyFZMmkjAv7rH1TABm

147 Tx - 106.071 BTC

[–] **btcrobinhood** 137 punti 2 anni fa

The address 15gCfQVJ68vyUVdb6e3VDU4iTkTC3HtLQ2 is the brainwallet "You don't win friends with salad!" PSA, don't use names of songs as brain wallets. Mijalis, I'm happy to return your coins; please send me a safe (non-brainwallet) address under your control.

permalink **embed** **salva** **dona gold**

https://www.reddit.com/r/Bitcoin/comments/1j9p2d/

123

Brain wallet disaster (self.Bitcoin)

inviato 2 anni fa da thonbrocket

Just lost 4 BTC out of a hacked brain wallet. The pass phrase was a line from an obscure poem in *Afrikaans*. Somebody out there has a *really* comprehensive dictionary attack program running.

Fuck. I thought I had my big-boy pants on.

343 commenti **condividi** **salva** **nascondi** **dona gold** **segnala**

https://www.reddit.com/r/Bitcoin/comments/1ptuf3/

Brainflayer — latest version

735,091,890,625 addresses scanned

~$50, <24 hours on EC2 spot instances

Let’s lose some money.

DEMO: https://blockchain.info/address/1JEnL6xYG9iHPWFV4Zz1xYUq1kQTKmnJwM

Summary	
Address	1p4gsrzTc3mFAgJKYqMzhm6UsJzhgy1KX
Hash 160	08e6a0def1903561bf466c56406cd1213fdc6525
Tools	Taint Analysis - Related Tags - Unspent Outputs

Transactions		
No. Transactions	109	
Total Received	4.37823824 BTC	
Final Balance	4.30318824 BTC	

Brainwallet

Secret Exponent

›7908c31998a630b3fc52f6cd34562bb5d749006dfc1995bb2 Random

Point Conversion

Uncompressed Compressed

Private Key

5JUaEgUrg2BjahDdWg9ocYimmA7wTRfLfS7gzgQeHeq4PrCD9P9

```
/**
 * BitcoinJS-lib v0.1.3-default
 * Copyright (c) 2011 BitcoinJS Project
 *
 * This program is free software; you can redistribute it and/or modify
 * it under the terms of the MIT license.
 */

[...]

        randomBytes: function(e) {
            for (var t = []; e > 0; e--)
                t.push(Math.floor(Math.random() * 256));
            return t
        },
```

```
/**
 * BitcoinJS-lib v0.1.3-default
 * Copyright (c) 2011 BitcoinJS Project
 *
 * This program is free software; you can redistribute it and/or modify
 * it under the terms of the MIT license.
 */

[...]

        randomBytes: function(e) {
            for (var t = []; e > 0; e--)
                t.push(Math.floor(Math.random() * 256));
            return t
        },
```

```
/**
 * BitcoinJS-lib v0.1.3-default
 * Copyright (c) 2011 BitcoinJS Project
 *
 * This program is free software; you can redistribute it and/or modify
 * it under the terms of the MIT license.
 */

[...]

        randomBytes: function(e) {
            for (var t = []; e > 0; e--)
                t.push(Math.floor(Math.random() * 256));
            return t
        },
```

```
t.push(Math.floor(Math.random() * 256));
```

```
t.push(Math.floor(
```

```
() * 256));
```

Firefox RNG: seeded with milliseconds since unix epoch xor'd with two pointers

66

PSA: brainwallet.org's "random" button uses low-entropy Math.random() (self.Bitcoin)

Aa+ inviato 2 anni fa da btclittlejohn

71 commenti **condividi** **salva** **nascondi** **dona gold**

segnala

[–] **btccolo** 1 punto 2 anni fa

There was a mistake in the adress, here is the right one: 1GVP2D1kvJb9PjDRrosvmpMEoUpycR2Y4R

permalink **embed** **salva** **riferimento** **dona gold**

66

PSA: brainwallet.org's "random" button uses low-entropy Math.random() (self.Bitcoin)

Aa+ inviato 2 anni fa da btclittlejohn

71 commenti **condividi** **salva** **nascondi** **dona gold** **segnala**

[–] **btccolo** 1 punto 2 anni fa

There was a mistake in the adress, here is the right one:
1GVP2D1kvJb9PjDRrosvmpMEoUpycR2Y4R

permalink **embed** **salva** **riferimento** **dona gold**

Private key:
c75be3b8aec0ec17f9b2a28b0171b90de3a66dbfb98d28b1569911f24eb65644

Seed: 1385738483307

Transactions

Transaction

- A public statement
- Signed with the address private key
- Recorded on the blockchain

"This money I can spend,
can now be spent by this other address"

Transaction

- Source public key
- Signature by corresponding private key
- Target address(es) (hash of public keys)

Transaction

```
OP_DUP OP_HASH160
<pubKeyHash>
OP_EQUALVERIFY
OP_CHECKSIG
```

```
<sig> <pubKey>
```

Transaction

- Source public key
- Signature by corresponding private key
- Target address(es) (hash of public keys)

ECDSA

ECDSA

Elliptic Curve
Digital Signature Algorithm

Math ahead

Math ahead
Take cover

Math ahead

Math ahead
Take cover

Math ahead

Math ahead
Take cover

ECDSA signature

$$r = (k \cdot G)_x \quad (r, \frac{z + r \cdot d}{k})$$

- G is the global curve base point
- d is the private key
- k is a random number (the nonce)
- z is the hash of the signed message

ECDSA signature

$$r = (k \cdot G)_x \qquad \boxed{(r, \frac{z + r \cdot d}{k})}$$

- G is the global curve base point
- d is the private key
- k is a random number (the nonce)
- z is the hash of the signed message

If you know k

$$(r, \frac{z + r \cdot d}{k}) = (r, s)$$

$$d = \frac{s \cdot k - z}{r}$$

If you know k

$$(r, \frac{z + r \cdot d}{k}) = \boxed{(r, s)}$$

$$d = \frac{s \cdot k - z}{r}$$

If you know k

$$(r, \frac{z + r \cdot d}{k}) = (r, s)$$

$$d = \frac{\boxed{s} \cdot k - z}{\boxed{r}}$$

If you know k

$$(r, \frac{z + r \cdot d}{k}) = (r, s)$$

$$d = \frac{s \cdot k - \boxed{z}}{r}$$

If you know k

$$(r, \frac{z + r \cdot d}{k}) = (r, s)$$

$$\boxed{d} = \frac{s \cdot \boxed{k} - z}{r}$$

If you know k

$$r = (k \cdot G)_x$$

```
$ ./brainflayer -v -I 0000...0001 -b bloom_r.blf -f r.bin -o cracked
rate: 113965.05 p/s found:     3/9170845696 elapsed: 81116.841 s

$ tail cracked
79be667ef9dcbbac55a06295ce870b07029bfcdb:r:(hex)priv/btc:
0000000000000000000000000000000000000000000000000000000000000001
cabc3692f1f7ba75a8572dc5d270b35bcc006505:r:(hex)priv/btc:
000000000000000000000000000000000000000000000000000000000bc614e
6a5df9fae6ef2925cd2db1b7c404b148714994f2:r:(hex)priv/btc:
0000000000000000000000000000000000000000000000000000000080001fff
```

3 hits

Range: 1 - 9,170,845,696

July 2016

If you REUSE k and d

$$s_1 = \frac{z_1 + r \cdot d}{k}$$

$$s_2 = \frac{z_2 + r \cdot d}{k}$$

If you REUSE k and d

$$s_1 = \frac{z_1 + r \cdot \boxed{d}}{\boxed{k}}$$

$$s_2 = \frac{z_2 + r \cdot \boxed{d}}{\boxed{k}}$$

If you REUSE k and d

$$s_1 = \frac{z_1 + \boxed{r} \cdot d}{k}$$

$$s_2 = \frac{z_2 + \boxed{r} \cdot d}{k}$$

If you REUSE k and d

$$s_1 = \frac{z_1 + r \cdot d}{k} = \frac{z_1}{k} + \frac{r \cdot d}{k}$$

$$s_2 = \frac{z_2 + r \cdot d}{k} = \frac{z_2}{k} + \frac{r \cdot d}{k}$$

If you REUSE k and d

$$s_1 = \frac{z_1 + r \cdot d}{k} = \frac{z_1}{k} + \boxed{\frac{r \cdot d}{k}}$$

$$s_2 = \frac{z_2 + r \cdot d}{k} = \frac{z_2}{k} + \boxed{\frac{r \cdot d}{k}}$$

If you REUSE k and d

$$s_1 - s_2 = (\frac{z_1}{k} + \frac{r \cdot d}{k}) - (\frac{z_2}{k} + \frac{r \cdot d}{k})$$

If you REUSE k and d

$$s_1 - s_2 = \left(\frac{z_1}{k} + \cancel{\frac{r \cdot d}{k}}\right) - \left(\frac{z_2}{k} + \cancel{\frac{r \cdot d}{k}}\right)$$

If you REUSE k and d

$$s_1 - s_2 = (\frac{z_1}{k} + \cancel{\frac{r \cdot d}{k}}) - (\frac{z_2}{k} + \cancel{\frac{r \cdot d}{k}})$$

$$s_1 - s_2 = \frac{z_1}{k} - \frac{z_2}{k}$$

If you REUSE k and d

$$s_1 - s_2 = \frac{z_1 - z_2}{k}$$

If you REUSE k and d

$$s_1 - s_2 = \frac{z_1 - z_2}{k}$$

$$k = \frac{z_1 - z_2}{s_1 - s_2}$$

If you REUSE k and d

$$s_1 - s_2 = \frac{z_1 - z_2}{k}$$

$$k = \boxed{\frac{z_1 - z_2}{s_1 - s_2}}$$

If you REUSE k and d

$$k = \boxed{\frac{z_1 - z_2}{s_1 - s_2}}$$

$$d = \frac{s \cdot k - z}{r}$$

27th Chaos Communication Congress

Console Hacking 2010

PS3 Epic Fail

fail0verflow

bushing, marcan, segher, sven

Sony's ECDSA code

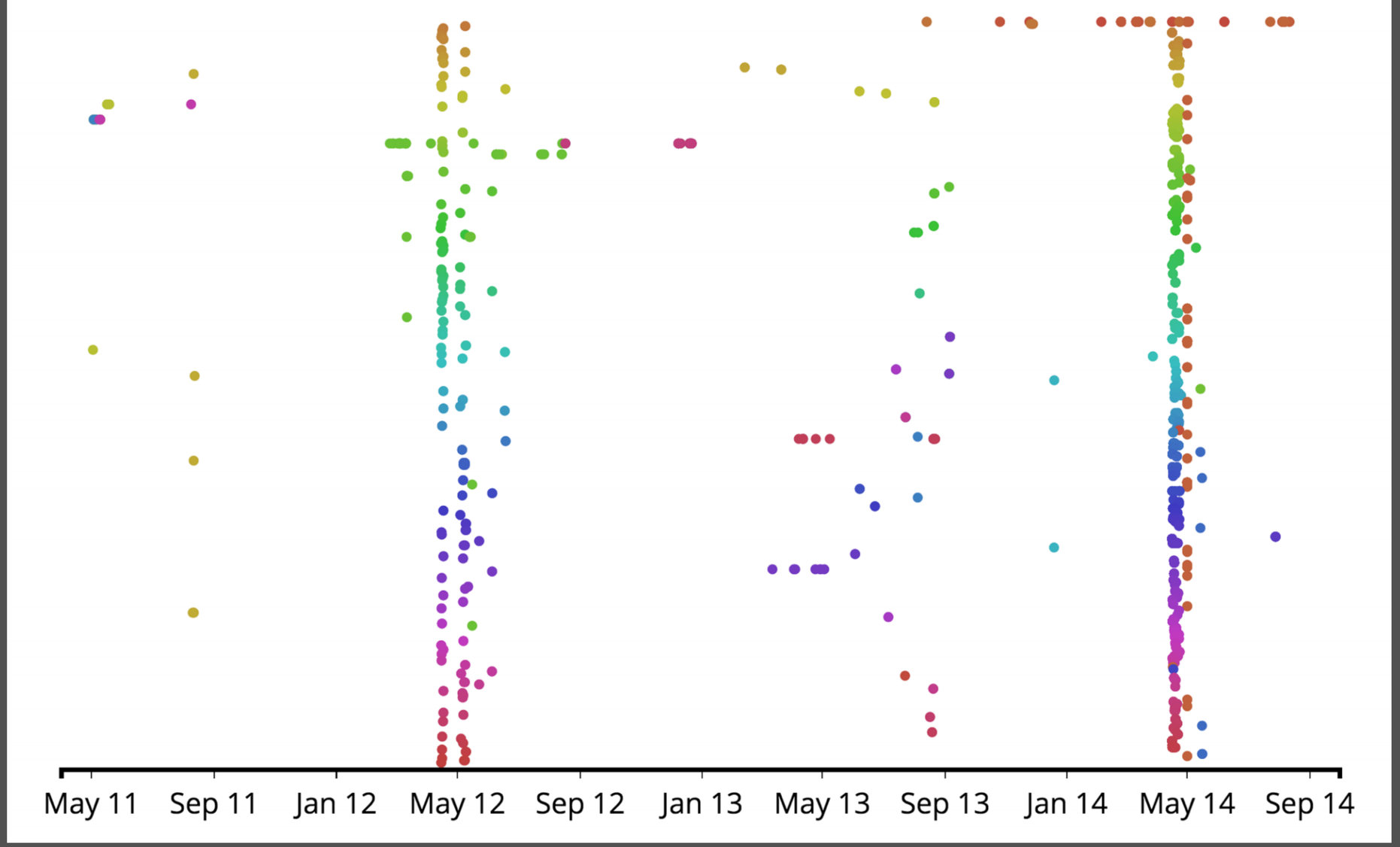
```
int getRandomNumber()
{
    return 4;  // chosen by fair dice roll.
               // guaranteed to be random.
}
```

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

Nadia Heninger[†*] Zakir Durumeric[‡*] Eric Wustrow[‡] J. Alex Halderman[‡]

[†] *University of California, San Diego*
nadiah@cs.ucsd.edu

[‡] *The University of Michigan*
{zakir, ewust, jhalderm}@umich.edu



https://speakerdeck.com/filosottile/exploiting-ecdsa-failures-in-the-bitcoin-blockchain

Author | Topic: Bad signatures leading to 55.82152538 BTC theft (so far) (Read 33421 times)

BurtW
Legendary

Online

Activity: 1218

I no longer support vanity addresses

Ignore

Bad signatures leading to 55.82152538 BTC theft (so far)

August 10, 2013, 10:53:13 PM #1

I have only seen this discussed in the newbies section so I thought I would open a thread here for a more technical discussion of this issue.

Several people have reported their BTC stolen and sent to https://blockchain.info/address/1HKywxiL4JziqXrzLKhmB6a74ma6kxbSDj

As you can see the address currently contains 55.82152538 stolen coins.

It has been noticed that the coins are all transferred in a few hours after a client improperly signs a transaction by reusing the same random number. As discussed here:

https://bitcointalk.org/index.php?topic=271486

Author Topic: Blockchain.info security [FUNDS STOLEN] (Read 15842 times)

giantdragor
Legendary

Activity: 1190

Ignore

Blockchain.info security [FUNDS STOLEN]
August 19, 2013, 03:27:16 PM #1

I used Blockchain.info online wallet for small transactions on my Windows 7 64-bit PC with strong password kept in KeePass.
Today I noticed that about 1.8 BTC was stolen from one of the addresses (which used for Anonymous Ads earnings), but funds from other addresses in this wallet were not affected.
This leads me on thoughts that **Blockchain.info or Firefox may have some weakness in random number generator** like the vulnerability was recently found in the Android.

TXID with my funds gone:
https://blockchain.info/tx/975412ecc21a0ad949deba3f47c6ac41e42fb7

https://bitcointalk.org/index.php?topic=277595

https://bitcoin.org/en/alert/2013-08-11-android

~~Let’s lose some money.~~

1NaM3Pra49oEDPGUXggUsRqbBXGG6nwyQM
14L6gBjYuEQedxPvedy5em2twMbVhrnKgB

RFC 6979

Deterministic r from z and d

If you REUSE k and d

$$k = \frac{z_1 - z_2}{s_1 - s_2}$$

$$d = \frac{s \cdot k - z}{r}$$

ECDSA pivot attack

```
TX 1: r: 5c16a3f7bafc1ef0, public key: 956fb654bcb2e061
TX 2: r: 5c16a3f7bafc1ef0, public key: 956fb654bcb2e061
```

```
TX 1: r: 5c16a3f7bafc1ef0, public key: 956fb654bcb2e061
TX 2: r: 5c16a3f7bafc1ef0, public key: 956fb654bcb2e061

TX 3: r: 5c16a3f7bafc1ef0, public key: 4b20eabe93918281
```

```
TX 1: r: 5c16a3f7bafc1ef0, public key: 956fb654bcb2e061
TX 2: r: 5c16a3f7bafc1ef0, public key: 956fb654bcb2e061

TX 3: r: 5c16a3f7bafc1ef0, public key: 4b20eabe93918281
TX 4: r: 94ce2b1e34d3fddc, public key: 4b20eabe93918281
```

```
TX 1: r: 5c16a3f7bafc1ef0, public key: 956fb654bcb2e061
TX 2: r: 5c16a3f7bafc1ef0, public key: 956fb654bcb2e061

TX 3: r: 5c16a3f7bafc1ef0, public key: 4b20eabe93918281
TX 4: r: 94ce2b1e34d3fddc, public key: 4b20eabe93918281

TX 5: r: 94ce2b1e34d3fddc, public key: 56b28d8ac3bcc4f5
```

719 additional private keys exposed

96532 nonces

Chains as long as 7 hops

Zero suffix

```
7d4e33841b80c4c087842816c92706510000000000000000000000000000000
f6c5b49263919ef195d67ee83999c963000000000000000000000000000000
23c61103d2705d892315f2c5b59a102a000000000000000000000000000000
89253c9caa14fb4de93b6db0a691df5f000000000000000000000000000000
```

Shared suffix

```
36ecfa6a21a30ec26ab43de5d7c8c3f653489c0af2b35a9827d79f4e2d9cc310
eaa8473108fc101b047bf9fd0a5c2d7753489c0af2b35a9827d79f4e2d9cc310
434c638ab45e6fa7c0ae299ede3d3e9753489c0af2b35a9827d79f4e2d9cc310
e1ce045618535145 1bf47457ead5066853489c0af2b35a9827d79f4e2d9cc310
```

Uninitialized memory?

```
0000000000000922c5000922c5000922c5000922c5000922c5000921ed200880
```

Related nonce attack

If you know k_2 - k_1

$$c = k_2 - k_1$$

$$k_1 = \frac{r_2 z_1 + r_1 s_2 c - r_1 z_2}{s_1 r_2 - s_2 r_1}$$

If you know k_2 - k_1

$$k_2 = k_1 + c$$

$$(k_2 \cdot G)_x = (k_1 \cdot G)_x + (c \cdot G)_x$$

$$r_2 = r_1 + (c \cdot G)_x$$

Double spending

Transaction malleability

Thank you! Questions?

@ryancdotorg - Ryan Castellucci

@FiloSottile - Filippo Valsorda

https://github.com/StealingBitcoinWithMath/

No innocent Bitcoins were harmed in the making of this talk
(Just to spell it out: we didn't steal anyone's Bitcoin)