Namecoin

Andreas Loibl

Chair for Network Architectures and Services

Department for Computer Science
Technische Universität München

July 11, 2014
1 Motivation

2 Alternative naming systems
   - DNSSEC
   - Tor hidden services
   - Petname systems

3 Namecoin

4 Problems

5 Statistics

6 Conclusion
Recent DNS irregularities in the news:
Recent DNS irregularities in the news:

**Widespread Twitter outages in Turkey after PM threatens ban**

Twitter users in Turkey reported widespread outages on Friday, hours after Prime Minister Tayyip Erdogan threatened to shut down access to the social media platform as he battles a damaging corruption scandal.

Some users trying to open the Twitter.com website were taken to a statement apparently from Turkey's telecommunications regulator (TIB). The statement cited four court orders as the basis for blocking the site, where some users in recent weeks have posted voice recordings and documents purportedly showing evidence of corruption among Erdogan's inner circle.
Recent DNS irregularities in the news:

Israeli, US terror victims could ‘own’ Iran’s Internet

A decision by an American court would allow for the Islamic Republic to be kicked off the web altogether

BY DAVID SHAMAH | June 25, 2014, 3:45 pm | Updated: June 25, 2014, 9:35 pm

A United States court on Tuesday effectively awarded a group of American and Israeli victims of Iranian terror the rights to the .ir domain, the suffix used to identify Iranian websites, along with all of Iran’s IP addresses.

As a result, said the group’s attorney, Nitsana Darshan-Leitner of the Shurat Hadin Law Center, Iran could find itself kicked off the Internet by ICANN, a Los Angeles-based organization that manages the web.

The United State District Court decided that the .ir domain name, along with Iran’s IP addresses — without which Iranian websites cannot be included in the World Wide Web — were assets that could be seized to satisfy judgments against the Islamic state of more than a billion
Recent DNS irregularities in the news:

**Millions of dynamic DNS users suffer after Microsoft seizes No-IP domains**

Legitimate users caught in legal fire designed to take down botnets.

by Dan Goodin - July 1 2014, 1:42am CEST

Microsoft enforced a federal court order making the company the domain IP resolver for the No-IP domains. Microsoft said the objective of the seizure was to identify and reroute traffic associated with two malware families that abused No-IP services. Almost immediately, end users, some of which were actively involved in Internet security, castigated the move as heavy handed, since there was no evidence No-IP officially sanctioned or actively facilitated the malware campaign, which went by the names Bladabindi (aka NJrat) and Jenxcus (aka NJw0rm).

"By becoming the DNS authority for those free dynamic DNS domains, Microsoft is now effectively in a position of complete control and is now able to dictate their configuration," Claudio Guarnieri, co-founder of Radically Open Security, wrote in an e-mail to Ars Technica. "Microsoft fundamentally swept away No-IP, which has seen parts of its own DNS infrastructure legally taken away."
Motivation

Current DNS structure is centralized, so server operators can:

- monitor users
- censor information
- redirect domains
- seize domains
Motivation

Current DNS structure is centralized, so server operators can:

- monitor users
- censor information
- redirect domains
- seize domains

Andreas Loibl: Namecoin
1 Motivation

2 Alternative naming systems
   - DNSSEC
   - Tor hidden services
   - Petname systems

3 Namecoin

4 Problems

5 Statistics

6 Conclusion
Desirable properties for a naming system:

- secure (globally unique)
- human meaningful
- decentralized
Zooko’s triangle

Desirable properties for a naming system:

- secure (globally unique)
- human meaningful
- decentralized

Zooko’s triangle: any naming system can fulfill at most two of those properties
Domain Name System Security Extensions (DNSSEC)

- Digitally signed records for DNS lookup using public-key cryptography
Zooko’s triangle

Domain Name System Security Extensions (DNSSEC)

- Digitally signed records for DNS lookup using public-key cryptography
- Authentication via a chain of trust, starting from the DNS root zone
Zooko’s triangle

Domain Name System Security Extensions (DNSSEC)

- Digitally signed records for DNS lookup using public-key cryptography
- Authentication via a chain of trust, starting from the DNS root zone

- example.com. IN A 93.184.216.119
- example.com. IN RRSIG A 8 2 86400 201407... mivJbnH8...
- example.com. IN DNSKEY 256 3 8 AwEAActyzh2Mv4Aywxmdz3...
- example.com. IN DS 31589 8 1 3490A6806D47F17A34C2...
Zooko’s triangle

Domain Name System Security Extensions (DNSSEC)

- Digitally signed records for DNS lookup using public-key cryptography
- Authentication via a chain of trust, starting from the DNS root zone

- example.com. IN A 93.184.216.119
- example.com. IN RRSIG A 8 2 86400 201407... mivJbnH8...
- example.com. IN DNSKEY 256 3 8 AwEAActyzh2Mv4Aywxmdz3...
- example.com. IN DS 31589 8 1 3490A6806D47F17A34C2...

- Hierarchical with powerful root
Zooko’s triangle

Tor hidden services (.onion)

- Tor: open-source anonymous communication service

- Allows services (e.g. webserver) without revealing IP or identity
- Reachable via pseudo-top-level domain .onion
- Hashed representation of the public key used by the hidden service, e.g. http://3g2upl4pq6kufc4m.onion/

Not human meaningful
Zooko’s triangle

Tor hidden services (.onion)

- Tor: open-source anonymous communication service
- Allows services (e.g. webserver) without revealing IP or identity
Tor hidden services (.onion)

- Tor: open-source anonymous communication service
- Allows services (e.g. webserver) without revealing IP or identity
- Reachable via pseudo-top-level domain .onion
Zooko’s triangle

Tor hidden services (.onion)

- Tor: open-source anonymous communication service
- Allows services (e.g. webserver) without revealing IP or identity
- Reachable via pseudo-top-level domain .onion
- Hashed representation of the public key used by the hidden service, e.g. http://3g2upl4pq6kufc4m.onion/
Zooko’s triangle

Tor hidden services (.onion)

- Tor: open-source anonymous communication service
- Allows services (e.g. webserver) without revealing IP or identity
- Reachable via pseudo-top-level domain .onion
- Hashed representation of the public key used by the hidden service, e.g. http://3g2upl4pq6kufc4m.onion/
- Not human meaningful
Petname systems

- Memorable names achieved by mapping petnames to identifiers

Human-meaningful
Decentralized
Secure
Zooko’s triangle

Petname systems

- Memorable names achieved by mapping petnames to identifiers
- Simple example: `/etc/hosts`
  
  `93.184.216.119 example.com`
Petname systems

- Memorable names achieved by mapping petnames to identifiers
- Simple example: `/etc/hosts`
  
  93.184.216.119 example.com

- Only local, not unique for other users
Namecoin fulfills all three properties of Zooko’s triangle:

- human meaningful: .bit domains
Namecoin fulfills all three properties of Zooko’s triangle:

- human meaningful: .bit domains
- decentralized: P2P, controlled by majority
Namecoin fulfills all three properties of Zooko’s triangle:

- human meaningful: .bit domains
- decentralized: P2P, controlled by majority
- secure: based on Bitcoin

Namecoin is based on Bitcoin and uses the distributed blockchain as a proof-of-work to establish consensus of domain name ownership.
Namecoin: Coins

Cryptocurrency:

- form of money using cryptography to control its creation and transactions
Cryptocurrency:

- form of money using cryptography to control its creation and transactions
- decentralized P2P consensus network instead of central authority
Cryptocurrency:

- form of money using cryptography to control its creation and transactions
- decentralized P2P consensus network instead of central authority
- coins as reward for actively participating and contributing to the network (“mining”)
Namecoin: Coins

Cryptocurrency:

- form of money using cryptography to control its creation and transactions
- decentralized P2P consensus network instead of central authority
- coins as reward for actively participating and contributing to the network (“mining”)
- coins assigned to addresses
Namecoin: Coins

Cryptocurrency:

- form of money using cryptography to control its creation and transactions
- decentralized P2P consensus network instead of central authority
- coins as reward for actively participating and contributing to the network (“mining”)
- coins assigned to addresses
- users store their addresses in a wallet
Creating a Namecoin address:

- create a public/private keypair, e.g.:
  - Privkey: AD9483226E4... (256 bit)
  - Pubkey: 04B90977D32... (512 bit)

- hash the public key to derive a Namecoin address:
  - ripemd160(sha256(04B90977D32...))
  - (usually Base58-encoded into a string, e.g. N123K7cjhEKJxZyapzYKCRx8e7PAJ9VqZg)
Namecoin: Transactions

- moves coins between one or more inputs and outputs
- each input is a transaction and address supplying coins
- each output is an address + amount of coins going there
- signed using the private key of the input address(es)

<table>
<thead>
<tr>
<th>Transaction</th>
<th>Fee</th>
<th></th>
</tr>
</thead>
<tbody>
<tr>
<td>fbb22...</td>
<td>0.005 NMC</td>
<td></td>
</tr>
<tr>
<td>NAqg4vyW...</td>
<td>9.86 NMC</td>
<td>NCmBVeGM... 9.84 NMC</td>
</tr>
<tr>
<td></td>
<td></td>
<td>NAVzJeEw... 0.015 NMC</td>
</tr>
<tr>
<td>8ee39...</td>
<td>0.005 NMC</td>
<td></td>
</tr>
<tr>
<td>NCmBVeGM...</td>
<td>9.84 NMC</td>
<td>N64UoNVz... 9.82 NMC</td>
</tr>
<tr>
<td></td>
<td></td>
<td>N7qyymUX... 0.015 NMC</td>
</tr>
</tbody>
</table>
Namecoin: Blockchain

**Block Structure**
- **Header**
  - Version (4 bytes)
  - Previous Block Hash (32 bytes)
  - Transactions Merkle Root (32 bytes)
  - Epoch Timestamp (4 bytes)
  - Bits / Difficulty Target (4 bytes)
  - Nonce (4 bytes)
- **Body**
  - Transaction 1
  - Transaction 2
  - ... 
  - Transaction x

**Transaction Structure**
- **Input**
  - Previous Transaction Hash
  - Sender’s Public Key
  - Sender’s Signature w/ Private Key Index
- **Output**
  - Value / Amount
  - Recipient’s Public Key

- **Block Chain**
  - Block 1 (Genesis)
  - Block 2
  - ... 
  - Block m
  - Block m+1
  - Block m+2
  - Block m+3

- **Discarded Branch**
- **Main Block Chain**
Namecoin has additional RPC commands to record and transfer arbitrary names (keys) and attach data (values) to those keys in the blockchain via special transactions:

- `name_new` (pre-register a name)
- `name_firstupdate` (register a pre-registered name)
- `name_update` (update value of a registered name)

Names stored in the blockchain ⇒ secure and decentralized names can be arbitrarily chosen ⇒ human-meaningful ⇒ Zooko’s triangle fulfilled ⇒ secure, decentralized naming system is possible
Namecoin’s namespace “d/” can be used to register domain names for the virtual TLD “.bit”, e.g. to register the domain example.bit:
Namecoin’s namespace “d/” can be used to register domain names for the virtual TLD “.bit”, e.g. to register the domain example.bit:

**Step 1: secretly pre-order the name**

name_new sends a transaction with a hashed version of the domain name, salted with a random value, to prevent others from stealing the domain while the transaction is broadcasted

```
$ namecoind name_new d/example
[
    "7004db3cfda8c09945e00b5a793...", 
    "abf1c2b6a64c1575"
]
```
Step 2: wait for 12 confirmations

`name_firstupdate` will only be accepted after at least 12 confirmations of the corresponding `name_new` (between 2 hours and 2 days, depending on the network activity).
Step 2: wait for 12 confirmations

`name_firstupdate` will only be accepted after at least 12 confirmations of the corresponding `name_new` (between 2 hours and 2 days, depending on the network activity).

Step 3: publicly register the name

```
$ namecoind name_firstupdate d/example \
> abf1c2b6a64c1575 7004db3cfda8c09945e00b5a793... \
> '{"ip":"127.0.0.1"}'
8b21511aa033ff4f5e219f548df...
```

Now `example.bit` would point to `127.0.0.1`
Namecoin: Resolving a domain

.bit virtual TLD not sanctioned by the ICANN ⇒ NXDOMAIN

$ namecoind name_show d/example
{
    "name" : "d/example",
    "value" : "{"ip":"127.0.0.1"}",
    "txid" : "8b21511aa033ff4f5e219f548df...",
    "address" : "My9KLVRidgX7s8vNZW6zfBvB1gBtg85",
    "expires_in" : 32806
}

- NMControl: daemon acting as a local DNS server, requires namecoind running in the background
- FreeSpeechMe: Firefox browser extension, requires NMControl running in the background
registering a new .bit domain for one year - 0.025 NMC:
0.01 NMC network fee (⇒ destroyed)
0.015 NMC transaction fees (⇒ miners)
current exchange rate of $ 1.81 per NMC ⇒ $ 0.045 / year
Outline

1 Motivation

2 Alternative naming systems
   - DNSSEC
   - Tor hidden services
   - Petname systems

3 Namecoin

4 Problems

5 Statistics

6 Conclusion
Problems

- domain squatting: cheap and anonymous registration, no authority to handle disputes and enforce domain transfers ⇒ most popular, trademarked or copyrighted .bit domains are registered
Problems

- domain squatting: cheap and anonymous registration, no authority to handle disputes and enforce domain transfers ⇒ most popular, trademarked or copyrighted .bit domains are registered

- mobile support: devices not suitable for running a full Namecoin node and keeping a local copy of the whole, ever growing blockchain in sync with the Namecoin network (size of blockchain 1.90 GB currently)
Problems

- bugs: severe bug in the name verification code that allowed everyone to take an already registered name and update it with a new value, even though this name did not belong to them (October 2013)
Problems

- bugs: severe bug in the name verification code that allowed everyone to take an already registered name and update it with a new value, even though this name did not belong to them (October 2013)
- weaknesses of cryptocoins, e.g. 51% attack: Attacker controlling more than 50% of the whole Namecoin network’s mining power can modify an existing block and change the (recent) blockchain history, e.g. to steal a domain registration
Outline

1 Motivation

2 Alternative naming systems
   - DNSSEC
   - Tor hidden services
   - Petname systems

3 Namecoin

4 Problems

5 Statistics

6 Conclusion
Statistics

- > 9.1 million Namecoins in existence (of 21 million)
- block count > 185,000 blocks
- blockchain size: 1.90 GB
- 57 transactions / hour, confirmation time: 8.19 minutes
- network hashrate: 74 Phash/s (fastest ASIC: 15 Thash/s)
- 122,772 non-expired names registered in the “d/” namespace (100%)
  (TLDs .com: 113,639,892 / .de: 15.743.799)
- 108,114 of those are valid .bit domain names (88%)
- 6,790 of those can be resolved to a website (5.5%)
- 429 of those are unique (0.3%)
Namecoin is currently the only operational decentralized DNS system which has gained (some) acceptance among the community.

However, scalability, efficiency, and price stability are long-term concerns.

Andreas Loibl: Namecoin
Conclusion

- Namecoin is currently the only operational decentralized DNS system which has gained (some) acceptance among the community
- However unlikely to be adopted by a significant number of internet users at this time (usability)
Conclusion

- Namecoin is currently the only operational decentralized DNS system which has gained (some) acceptance among the community.
- However unlikely to be adopted by a significant number of internet users at this time (usability).