Namecoin and DNS Security

Jeremy Rand
Lead Application Engineer, The Namecoin Project
https://www.namecoin.org/

jeremyrand@airmail.cc
OpenPGP: 5174 0B7C 732D 572A 3140 4010 6605 55E1 F8F7 BF85

Presented at Internet Governance Forum 2018

“Internet of Trust”?

- In the DNS, we need to trust a lot of third parties.
  - Registrars
  - TLD Registries
  - Recursive Resolvers
  - Authoritative Nameservers
  - The ICANN Root
- They usually behave correctly.
- But if they make a mistake (or are malicious), security issues (e.g. censorship or hijacking) can result.
- “Trusted Third Parties Are Security Holes.”
  – Nick Szabo
  Computer scientist, creator of Bit Gold (Bitcoin precursor)

Why are trusted third parties so concerning?

- Humans behave nondeterministically.
- Any system run by humans will behave nondeterministically.

- Even if a system has ground rules that are supposed to be inviolable, ground rules that are enforced by humans will be inconsistently enforced.

- Human behavior in the distant future is even more nondeterministic.

- (H/t to Greg Maxwell's philosophical writings on this topic.)

Namecoin: Like the DNS, but with more determinism

- Namecoin is an experiment to find out:
- Is it possible to build something vaguely similar to the DNS, but with as little involvement by humans as possible?
  - Thereby create a DNS-like system that behaves more deterministically than the DNS.
- The hope: such a system will remove as many trusted third parties as possible, and thereby eliminate some security holes.
- Namecoin uses the .bit TLD.

Under the hood…

- Namecoin is the Bitcoin codebase, with small modifications added (everything is free / libre / open-source).
- “Coins” in Namecoin can represent domain names, instead of fungible currency units.
- Censoring or hijacking a Namecoin domain name is roughly equivalent to freezing or stealing bitcoins.
  - Very difficult unless the attacker has your cryptographic private key.

Namecoin Use Case: Buying and Selling Names

- In DNS, buying or selling a name usually involves some counterparty risk or relying on an escrow agent (who becomes a trusted third party).
- In Namecoin, the buyer and seller can jointly construct a transaction that atomically pays the seller and transfers the name to the buyer.
- This eliminates counterparty risk without requiring an escrow agent's services.

- (Implementation by Phelix.)

Namecoin Use Case: Non-Interactive Buy/Sell Offers

- You can also create non-interactive buy or sell offers.

- Alice creates sell offer: "Willing to sell example.bit for 100 NMC."
- Alice signs sell offer with private key, proving that she owns example.bit and is willing to transfer it in exchange for 100 NMC.
- Alice posts the signed sell offer on a forum or pastebin.

- (Design by Ryan Castellucci)

Namecoin Use Case: Non-Interactive Buy/Sell Offers (2)

- Bob sees the offer and wants to buy example.bit.
- Bob completes the offer by signing it with a private key that owns 100 NMC; the offer is now a valid Namecoin transaction.
- Bob can now broadcast the completed transaction to the Namecoin network without contacting Alice.

- (Design by Ryan Castellucci)

Namecoin Use Case: Non-Interactive Buy/Sell Offers (3)

- Alice gets paid 100 NMC; Bob receives example.bit.
- The transaction is atomic; no counterparty risk and no escrow agent needed.
- This works for both buy offers and sell offers.

- The Namecoin protocol supports this use case; user-friendly tools hopefully coming soon.

- (Design by Ryan Castellucci)

Namecoin Use Case: TLS (HTTPS) Public Key Infrastructure

- The Certificate Authority system (relied on by HTTPS) is problematic (even with Certificate Transparency).
  - Way too many nondeterministic humans involved; trusted third parties are security holes.
- DNSSEC/DANE could improve the situation, by listing TLS certificates in the DNS.
  - But there are political issues: some people are nervous about the possibility of abuse of power (or accidental security breaches) by the DNS root, the TLD operators, or registrars.
- Namecoin could provide the advantages of DNSSEC/DANE without the political problems and without trading one trusted third party for another.

Namecoin Use Case: DNS-Like Functionality for Dark Web Sites

- “Dark Web”, noun: the set of web sites that require software besides a standard web browser in order to view them.
- Dark web systems can offer some useful advantages over regular web sites:
  - Tor improves privacy and anonymity.
  - ZeroNet improves resilience to web hosting server downtime.
  - cjdns improves resilience to ISP downtime.
- Namecoin is a natural fit for these types of systems that want to have DNS-like functionality while reducing reliance on trusted third parties.

Namecoin Use Case: Multisig

- A name is usually owned by a single private key, but it can also be owned by M-of-N private keys.
- This can be a useful protection against a single compromised key.
- A board of directors could each have a private key, and updating the name might require a supermajority of the board.

- The Namecoin protocol supports this use case; user-friendly tools hopefully coming soon.

Namecoin Multisig Use Case: Two-Factor Authentication

- Namecoin can allow very flexible name update policies to be built, depending on the security and UX needs of a name owner.
- For example, Alice is the owner of a Namecoin name, and her HTTPS certificate is listed in Namecoin. She wants to limit her risk of stolen private keys while not introducing too much counterparty risk, so she constructs the following policy:

- Alice contracts Trent to run a two-factor-authentication service.
- Alice can update her name with arbitrary data (including changing the HTTPS certificate) if Trent signs her update. (Trent promises to only do this after verifying via 2FA.)

- (Design based on GreenAddress in Bitcoin.)

Namecoin Multisig Use Case: Two-Factor Authentication (2)

- Trent pre-signs a specific transaction to revoke Alice's primary HTTPS certificate and gives the transaction to Alice. Alice can then revoke the HTTPS certificate later by signing the transaction herself even if Trent is offline or maliciously refuses to sign at that time.
- Trent pre-signs a specific transaction to transfer the name to Alice's sole control, which is only valid X days in the future. Trent gives this transaction to Alice. Alice can then recover the name after X days even if Trent goes out of business or loses his private key.

- (Design based on GreenAddress in Bitcoin.)

Namecoin Multisig Use Case: Two-Factor Authentication (3)

- Trent cannot transfer or update Alice's name without Alice's signature.
- Alice can verify that the pre-signed transactions are authentic and that she is protected from Trent, before she applies this policy to her name.

- These policies are specified in a scripting language and are enforced to the same level as standard signatures are.

- (Design based on GreenAddress in Bitcoin.)

Namecoin Multisig Use Case: Two-Factor Authentication (4)

- Namecoin doesn't mean registrars go away: "registrars" in Namecoin might look like Trent.
- But Namecoin **does** mean that "registrars" have much less ability to harm their customers than in DNS. (Either accidental or malicious harm.)
- This might lead to decreased security budgets being necessary for registrars.

- (Design based on GreenAddress in Bitcoin.)

Thanks for inviting me!

- Hopefully I've covered a (very brief) overview of some of Namecoin's security-related features.
- Happy to take questions in the Q&A.

- https://www.namecoin.org/
- My email: jeremyrand@airmail.cc
- My OpenPGP:
  5174 0B7C 732D 572A 3140 4010 6605 55E1 F8F7 BF85

Supplementary Slides

Tradeoffs: Malware

- Namecoin transactions are irreversible.
- As a result, if a name is transferred to a new owner, the old owner can't get it back without the new owner's signature.

- This means that Namecoin names are somewhat more vulnerable to hostile takeover by malware.
- Human error by the name owner could also be a problem.

Tradeoffs: Malware (2)

- Some workarounds to this include keeping private keys on an air-gapped machine, and/or assigning multisig or 2FA policies to names.

- This isn't necessarily all bad: I've heard security experts comment that one of the best public benefits of Bitcoin becoming popular is that people are finally taking endpoint security seriously.
- As Bitcoin becomes more mature, I think it is likely that endpoint security will improve substantially.

Tradeoffs: Trademark Infringement

- Namecoin doesn't have a nondeterministic human to determine which name registrations are valid.
- This is why it has security benefits and is more resistant to political issues.

- However, that also means that if someone registers a name that infringes on a trademark, there's no way to disable that name registration.
- This is inherent to the definition of trademark infringement: determining whether infringement occurred requires a human, and Namecoin is designed to not be run by humans.

Tradeoffs: Trademark Infringement (2)

- A workaround would be for users to opt into a list of known trademark-infringing names, which get blocked somewhere between the Namecoin client and the user's web browser.
- For example, the Namecoin-to-DNS bridge that the user has installed might support this as an option.
- Existing infrastructure for this already exists: PhishTank is an example.

Tradeoffs: Trademark Infringement (3)

- Caveat: A user who *wants* to view a name that infringes on a trademark could intentionally disable the blocking.
- Since the purpose of trademark law is to avoid consumer confusion, this isn't really a problem – a user who does this probably knows what they're doing.

- Caveat: Someone could buy an infringing name solely to sell it to the trademark owner (squatting).
- Since registering names costs money, it is difficult for a single person to squat on a very large number of names (similarly to how DNS names costing money reduces squatting).

Tradeoffs: Privacy

- Since the full set of Namecoin transactions is public, anyone can look at the transactions.
- Transaction graph analysis makes it fairly easy to figure out if two transactions were done by the same person.
- This also affects Bitcoin.

- So if you register two Namecoin names, it's probably a public record that both names were registered by the same person.
- And if you bought your namecoins from someone else, they can probably see what names you register.

Tradeoffs: Privacy (2)

- Workaround: we have a plan for mitigating this problem by utilizing anonymous currencies like Monero and Zcash.
  - See my talk from 34C3 last year for details on this design.
- But this design is not yet implemented. For now, Namecoin's privacy is very poor compared to the DNS.

Tradeoffs

- None of the workarounds I described for malware, trademarks, and privacy are as straightforward as the countermeasures taken by DNS.
- Finding more elegant fixes is an open research problem.

- We do not claim that Namecoin is strictly more secure than the DNS.
  - For some users, Namecoin may be more secure than the DNS.
  - For other users, the DNS will be more secure.
  - Use the best tool for the job!