namecoin

I Won Awards for Hacking Botball Controllers; Now I’m Protecting the Anonymity of At-Risk Internet Users

(Or: How Botball Prepared Me for a Career in Security/Privacy Research)

Jeremy Rand
Lead Application Engineer, The Namecoin Project
(Alumni, Norman Advanced Robotics / Team SNARC)

A little bit about me…

- Alumni of Norman Advanced Robotics (Class of 2011).
- Mentored Alcott Middle School 2011-2015.
- Presented at GCER on hacking the XBC, CBC, Link, AR.Drone, and Create (2008-2015).
- Interested in the intersection of technology and human rights. Joined Namecoin developer team in 2013.

A little bit about Namecoin…

- Core activity: website addresses on a blockchain.
  - If you’re curious about Namecoin’s core (blockchain-related) activities, check out my GCER papers from 2017 and 2022.
- Lots of side projects, not just blockchain work.
  - We are effectively a privacy/security research group.

Namecoin’s Scope Expanded Over Time

- We needed Tool X to do blockchain work, so we made one – everyone else benefits.
- While doing blockchain work, we gained some rare expertise, allowing us to make Tool Y – everyone else benefits.
- This talk will cover 3 side projects.

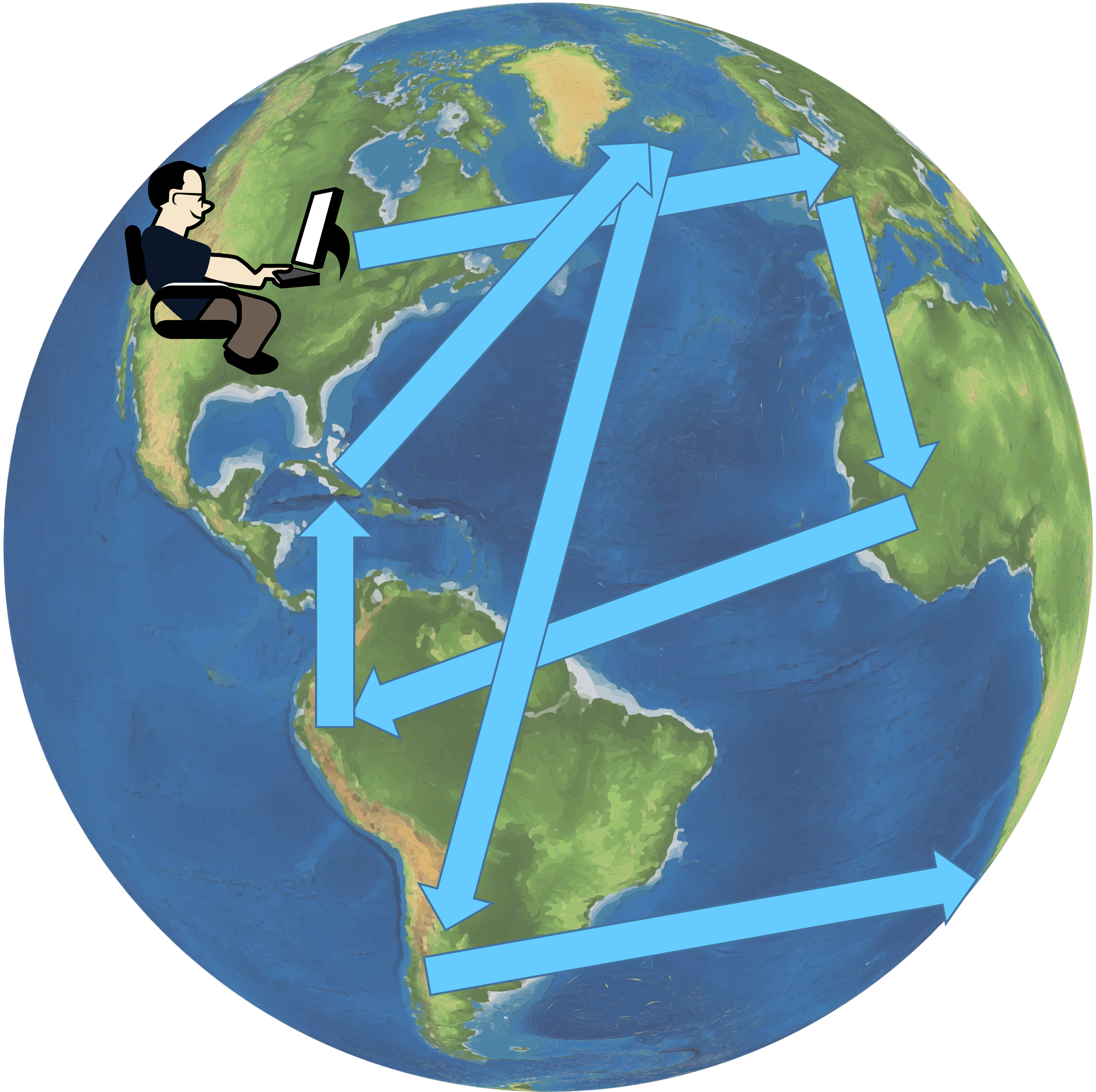
HTTPS

- The secure version of HTTP.
- Implemented using *asymmetric encryption*.
- Main point: to send encrypted data to a website, you need to know its *public key* (a large, publicly available number).

How do you know the correct public key for a given website?

- Corporations called “Certificate Authorities (CA’s).”
  - CA’s issue “certificates” saying which website has which public key.
- Yes, the CA’s could be lying.
  - That’s a big security liability in HTTPS.
- I’ll come back to this.

Tor: Anonymity for the Internet



Websites hosted anonymously using Tor: “onion services”

- http://odmmeotgcfx65l5hn6ejkaruvai222vs7o7tmtllszqk5xbysola.onion/
- Also uses asymmetric encryption.
  - The randomness in the address is actually a built-in public key! No need for certificate authorities.
- HTTP, not HTTPS.

Why no HTTPS?

- In theory, onion services are already encrypted, so HTTPS isn’t needed.
- In reality, HTTPS would yield an improvement.
  - But then you’d need to use certificate authorities.

HTTPS for Onion Services

- Onion services have a public key in their URL.
- Could we jerry-rig web browsers to reuse that public key for HTTPS purposes instead of asking a certificate authority?
- I had already done some similar witchcraft for Namecoin: make browsers look up public keys on the blockchain.
- Doing this for onion services seemed easy enough.

But there’s a problem!

- Onion service keys and HTTPS keys are in different formats.
  - You can’t interchange them.
  - But you *can* make an onion service key *sign* an HTTPS public key.
- If you have the resulting signature, you can verify that the onion service owner authorized the HTTPS key that was signed.

Namecoin Side Project #1: Encaya (Hack for Onion HTTPS)

- Encaya is a compatibility shim I made for onion services and HTTPS.
  - When web browsers validate HTTPS certificates, they pass the website address and a serial number (chosen by the CA) to the operating system.
  - Operating system checks with the CA, and returns whether a given public key is owned by the website.

What’s the hack?

- Encaya hides the onion service signature inside the serial number!
  - Web browser passes the “serial number” to Encaya.
  - Encaya extracts the disguised onion service signature, checks if it’s valid.
  - Encaya pretends to be a CA, returns the HTTPS public key that was signed.
- Voila! HTTPS for onion services, without certificate authorities.
- I gave a talk about this at the 38C3 hacker conference in December 2024.

How do you make an application use Tor?

- Tor exposes a *proxy* (default 127.0.0.1 port 9050).
  - Configure your application (web browser, chat client, etc.) to use that proxy.
  - Everything *should* be anonymized.
- Except… what if there’s a bug in your application?
  - What if a few of the networking code paths ignore your proxy setting?
  - Your anonymity is gone!

Namecoin Side Project #2: SocksTrace: Proxy Leak Auditor

- This is called a “proxy leak vulnerability”.
- Proxy leaks have always been hard to audit for.
- So my colleague Robert Mindo made SocksTrace.
  - SocksTrace can automatically audit any Linux application for proxy leaks.
  - It can block the leaks firewall-style, or log details for a bug report, or even redirect the connections to go over Tor.
- Presented at the 37C3 hacker conference in December 2023.

How else can you get deanonymized?

- Imagine you’re in a chat, under a pseudonym.
  - You mention casually “it started snowing here yesterday.”
  - Uh oh. That reveals a lot about your location.
- Not theoretical: a whistleblower was arrested in 2012 due to this kind of mistake.

Large Language Models (LLM’s)

- Sabri and Ross have already talked about LLM’s (e.g. ChatGPT).
- LLM’s are pretty good at reasoning about the topic of a conversation.
- *Local* LLM’s (unlike ChatGPT) can be run on your own machine (not the cloud).
  - So you’re not giving all your data to a corporation.

Namecoin Side Project #3: Occlumask: Avoid Doxing Yourself

- My colleague Alice Margatroid is working on Occlumask.
  - Occlumask scans what you type with a local LLM…
  - And warns you if you’re about to say something that might dox you.
    - The weather, your school or employer, your disabilities, etc.
- You’re the first conference to hear about Occlumask in a presentation!
  - Project is very new, hoping to do a full talk at a hacker conference in 2025.

What does this have to do with Botball?

- We’re at a STEM education conference, after all.
- Here are some common skills between Botball and Namecoin.

Testing the Limits of your Parts

- Show of hands: have you ever had to test the functionality limits of a Botball part?
  - Maximum speed of a motor?
  - Min/Max distance of a rangefinder?
  - Etc.?
- I had to do that in Namecoin this year!

Testing the Limits of your Parts (In Encaya)

- You know how we’re hiding a signature inside a serial number?
  - …what’s the length limit on that serial number?
  - Industry is transitioning toward quantum-resistant signature schemes like CRYSTALS-Dilithium.
  - …which have much bigger signatures.
- Important to know whether this will break things for us.

Working Under Stress and a Time Limit

- Show of hands: have you needed to fix a bot or a program with less than an hour before the next DE round?
- How well did it go?
- This happens in security research fairly often.

Working Under Stress and a Time Limit (at Namecoin)

- I got contacted by a vulnerability response team a few years ago.
  - Bitcoin had just patched a critical vulnerability.
  - They wanted to make sure Namecoin got a chance to patch it.
  - We had a few days before the Bitcoin public disclosure.
  - Also the Namecoin code in question was in use by Tor.
- My colleague Yanmaani and I had to carefully audit whether the vulnerable code was triggerable from Tor.
  - (Luckily, it was not triggerable.)

Cross-Pollination of Ideas

- Show of hands: have you gotten a cool idea from seeing another team’s bot, and found a new use for that concept?
- I came up with the “hide a signature in the serial number” trick for Tor usage…
  - But I realized later that it could also save space on the Namecoin blockchain.
  - So I’m going to repurpose it for that.

Fundraising/Grantwriting

- You’ve probably had to fundraise for your team’s registration or travel expenses.
- Namecoin resembles a nonprofit, we’re mostly funded by donations and grants.
  - In Botball, I got pretty good at explaining why Botball was cool in ways that other people could relate to.
  - I do the same thing when writing grants for Namecoin.

Mentoring

- I mentored Botball for four years.
  - I encouraged students to learn for fun, build up unique expertise, and not just follow instructions.
- At Namecoin, I’ve mentored two new developers.
  - I reused my Botball mentoring style for Namecoin.
  - It worked great: both developers have carved out their niche very well, and are still with us today.
  - SocksTrace started out as an internship project (Namecoin was under Tor’s umbrella); Robert was the only Tor intern that year (of 4) who finished his project successfully.

Handing Off Project Ideas

- Some of you have probably had trouble deciding what robotics projects to work on, because you have too many ideas.
- That was me in Botball, and in Namecoin!
  - You can solve it by handing off projects to teammates who aren’t as busy or a better-suited skill set.
  - SocksTrace and Occlumask originated as ideas in my head – I handed them off to Robert and Alice because I didn’t have the time or skill set to do them justice.

Extracurricular Projects

- Show of hands: has your Botball team worked on projects that aren’t focused on the competition?
  - Norman Advanced partnered with University of Oklahoma on a bot for climatology research a few years ago.
- That’s a big part of Namecoin.
  - Encaya, SocksTrace, and Occlumask all have little to do with putting website addresses on a blockchain.
  - But it’s a good reason why we’re successful.

Also See My Earlier Papers!

- My GCER papers from 2017 and 2022 have more examples, if you’re curious.

Takeaways

- The Botball skill set has a deceptively strong resemblance to the skill set of security/privacy research.
- I’m pleased that GCER takes some time to showcase this in talks.
- If you think this is cool, make sure you tell other people (e.g. your school board) so that they know how important Botball’s educational benefits are.

Why you might want to join Namecoin

- You get to make the world a better place (help make privacy a universal human right!).
- Doing open-source software development while you’re a student is great for your resume or college applications.
- You can create new knowledge (original research!), not just blindly follow instructions like in many internships.

Do you know, or want to learn, any of these?

- Go
- Python
- C++
- Qt GUI’s
- PyQt GUI’s
- Usability testing

- Documentation
- Packaging (any OS)
- Android apps
- DNS
- TLS

- Bitcoin
- Anonymity
- Sandboxing
- Basic applied cryptography
- Writing unit / integration tests

jeremy@namecoin.org
jeremyrand@danwin1210.de
https://www.namecoin.org