From Hacking Botball Controllers to Having My Code in the Number One Privacy Web Browser

(Or: What a 2011 Botball Alumni Is Doing in 2022)

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).
- Founder+Leader of Team SNARC (Competed in KIPR Aerial and KIPR Open 2011-2015).
- Mentored Alcott and Whittier Middle Schools 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 2013 part-time; 2018 full-time.

Show of hands…

- When I mention online privacy…
  - Who here thinks of encryption?


WHAT IF I TOLD YOU
ENCRYPTION MISSES THE POINT
imgflip.com

Wait, what?

- Encryption gives you privacy for *content*.
  - i.e. the actual text of your communication.
- It doesn’t give you any privacy for *metadata*.
  - Who sent the message?
  - Who received the message?
  - What software was used to send and receive the message?
  - From what location was a message sent or received?
  - Were two different messages sent by the same person, even if we don’t know who they are?

Content vs Metadata

- Content
  - Processed via natural language parsing (what Google Translate does).
  - Very expensive for adversaries to analyze.
  - Very unreliable to analyze.
  - Protecting it is easy via encryption.
- Metadata
  - Processed via statistics and graph theory.
  - Very cheap for adversaries to analyze.
  - Relatively reliable to analyze.
  - Protecting it is nontrivial; encryption doesn’t help.

What the NSA says…

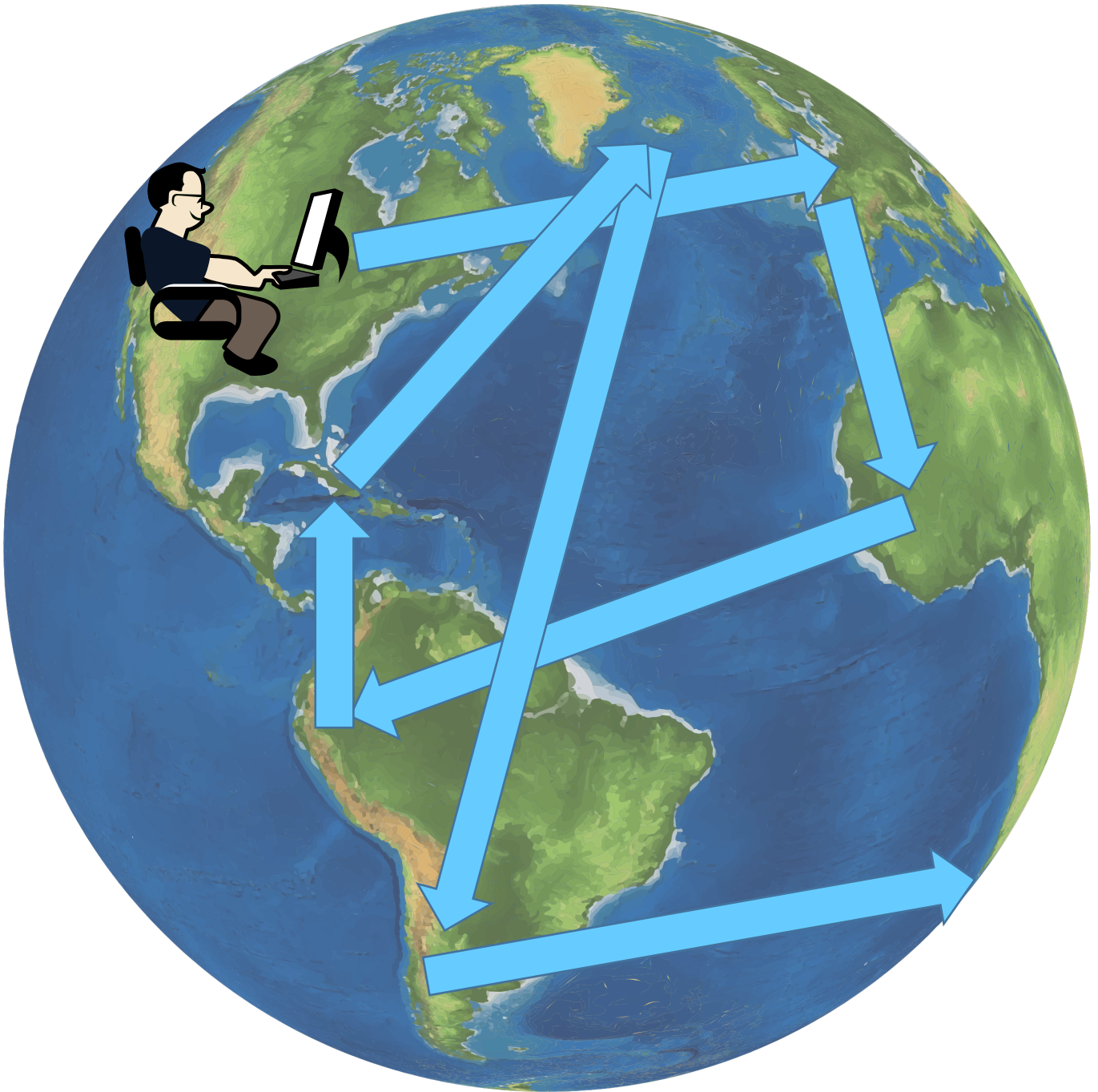
- “Metadata absolutely tells you everything about somebody’s life. If you have enough metadata, you don’t really need content.”

– Stewart Baker
NSA General Counsel

- “We kill people based on metadata.”

– Michael Hayden
NSA Director

How Tor protects metadata



Tor has a usability problem

- A website address that’s hosted with Tor looks like this:
  - https://odmmeotgcfx65l5hn6ejkaruvai222vs7o7tmtllszqk5xbysola.onion
- Past attempted workarounds:
  - Use a centralized list of Tor addresses?
    - Whoever runs the list can redirect you to a phishing site.
  - Use a local bookmarks list of Tor addresses?
    - Unhelpful if a friend tells you to go to a Tor website you’ve never been before.

Namecoin: human-meaningful Tor addresses

- Namecoin is very much like Bitcoin.
- But while Bitcoin transactions move money around…
  - Namecoin transactions register and update website addresses.
  - Namecoin website addresses end in .bit
- Namecoin addresses are difficult to impersonate, for the same reasons that bitcoins are difficult to steal.
- Namecoin addresses can point to Tor addresses.
  - Use a nice “https://kipr.bit/” address for your Tor site!

Namecoin + Tor Collaboration

- In 2018, I started working with the Tor team on integrating Namecoin into Tor.
  - Their standards are very high.
  - After ~1.5 years, we succeeded. Namecoin was shipped in the Nightly Linux version of Tor Browser in December 2019.
- Highly recommend my talk from 36C3 (largest hacker conference in Europe) for details.

How is this similar to Botball?

- It’s actually very similar.

Recap of my GCER 2017 talk

- Hacking Botball controllers is excellent practice for reverse-engineering.
- Double Elimination strategy is excellent practice for questioning security assumptions.
- The KISS Principle is excellent practice for reducing attack surface.
- International GCER paper collaboration is excellent practice for international software projects like Namecoin.
- See my GCER 2017 talk for more on these.

Parts list limits

- Show of hands…
  - Have you been unable to build your first choice of robot design, because it needed too many parts?
  - Have you been disqualified from a DE round for violating the parts list?
  - Have you gotten an opponent disqualified from a DE round for violating the parts list?
- It can be fun to operate in an environment with no parts limits.
  - Video time! (0:09)

“Parts list limits” in Namecoin

- Orders from Tor: the download size increase from adding Namecoin had to be under 3 MB.
  - Uh oh, my first prototype was 40 MB.
- Experience dealing with Botball parts list constraints was the main reason I didn’t just ragequit when realizing how far over the limit we were.
  - In Botball, you can tweak the design repeatedly until you’re within the parts limits. Same thing here.

Show of hands…

- Have you ever redesigned a bot to fit within the parts list requirements, and found that the result actually worked better?
- A Bitcoin library that I used for the Tor integration had a major security vulnerability disclosed in June 2022.
  - The vulnerable code was in files that I had stripped out of Tor Browser to comply with the size limit.
  - So Namecoin in Tor Browser was made more secure by that size limit.

Documentation

- Most of Namecoin’s funding is from NLnet Foundation (via grants from the EU and Dutch governments).
- NLnet doesn’t like excessive paperwork.
  - But they do need to know what we’re up to.
- So… they ask us to publicly blog about our progress.
  - Our users see what we’re working on, and so do our funders.
- Pretty much the same skill set as Botball documentation and GCER papers.

Technical Presentations

- I routinely give technical talks at conferences like C3 (largest hacker conference in Europe) about what we're working on.
  - This was easy for me because I had practice presenting at GCER.
- There aren't many places where middle+high school students write high-quality technical documentation and present talks and papers.
  - Botball/GCER stands out here.

Open-Source Development

- Many Botballers release open-source code at GCER.
- KIPR often releases open-source code so that Botballers can customize the controllers.
  - Sometimes Botballers even contribute code improvements back to KIPR.
- Many Botballers use Git, etc.
  - My first experience using Git (and SVN/CVS) was in Botball.

All Legitimate Security Software Is Open-Source

- If your security is dependent on attackers not knowing how your security works, you don’t have real security.
- Thus, all Namecoin and Tor code is open-source.
- Botball was great practice for this.
  - Not many middle+high school students use open-source workflows – Botball stands out here too.

Collaboration and Competition Are Compatible

- Botball is a **friendly** competition.
- Teams often swap ideas.
  - Or code.
  - Or spare parts.
  - Or co-author GCER papers.
- Norman Advanced has donated their Timeout Card to their DE final match opponent.

Namecoin has Competitors

- Our two main competitors are Monero and Handshake.
- We approach this like Botballers do.
  - I routinely swap ideas with Monero and Handshake developers.
  - My 36C3 talk on Tor Browser integration was on a stage run by the Monero team.
  - The Handshake team actually donated a $1M USD-equivalent airdrop to us.
- Our goal here is to make the Internet more secure, not to beat competitors.

Takeaways

- Botball helps students acquire a skill set that goes far beyond robotics.
- Many of these skills are fairly unique to Botball.
- STEM education research/analysis should maybe pay more attention to this aspect.
- Perhaps KIPR should market this aspect more?
- I’m successful working on Namecoin because I did Botball. Without question.

Why you might want to join Namecoin

- Open-source software development experience looks great on a resume or college application.
- Making the world a better place for human rights (e.g. privacy) is good too.
- The blockchain technology used in Bitcoin and Namecoin has a lot of industry attention these days.

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)
- Browser extensions
- Android apps
- DNS
- TLS
- Bitcoin
- Anonymity
- Sandboxing
- Basic applied cryptography
- Unit / integration testing
- Static analysis

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