Secure Messaging and Beyond: Privacy's Relevance Today

NADIM KOBEISSI

CONSERVATOIRE NATIONAL DES ARTS ET METIERS

INSTITUT NATIONAL DE RECHERCHE EN INFORMATIQUE ET AUTOMATIQUE

About me

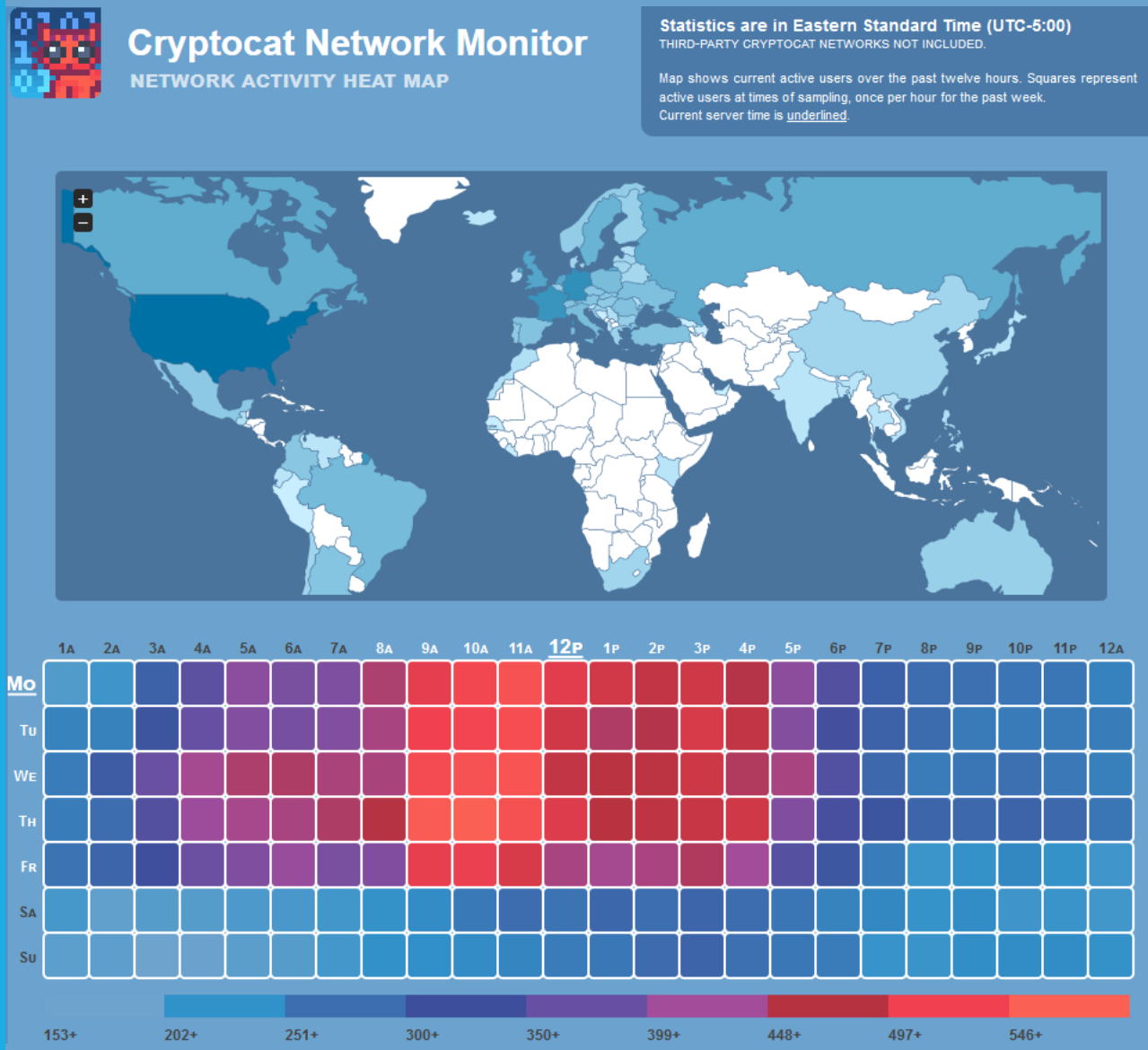
- PhD researcher at INRIA (with PROSECCO).
- Interested in verified cryptographic protocol implementation.
- Background in secure messaging, worked on a lot of open source projects.

Cryptocat:
Secure Messaging for Everyone

- Easy private messaging in the browser.
- Started in 2011, open source project. Millions of users today.
- One of the first modern *usable encryption* efforts.

Usage Statistics

Translated into 28 languages, Cryptocat is used in every continent.



Arguments Behind Cryptocat

- Encryption had to be *accessible* in order for it to make a public difference.
- Algorithms and standards aren't enough: encryption needs to be practical and has to defeat social barriers.
- Similar ideas seen today in *Signal* (for mobile devices.)

Technical Challenges

- First full-featured experimental attempt for end-to-end secure messaging *in the browser*.
- Inspiration for today's Web Cryptography API (joint work with W3C).
- Usable encryption is no longer a side-issue but a studied field.

What About Today?

- Usable, accessible encryption can be seen as "democratic access" to encryption.
- Questions remain: what about verifiable security? Debate over backdoors?
- We need to discuss legitimate economic and social incentives for cryptography.

What About Today?

- Usable, accessible encryption can be seen as "democratic access" to encryption.
- Questions remain: what about verifiable security? Debate over backdoors?
- We need to discuss legitimate economic and social incentives for cryptography.

SECTIONS

International New York Times

N.Y. / REGION

Volkswagen's Diesel Fraud Makes Critic of Secret Code a Prophet

About New York

By JIM DWYER SEPT. 22, 2015

Email
Share
Tweet
Save
More

A Columbia University law professor stood in a hotel lobby one morning and noticed a sign apologizing for an elevator that was out of order. It had dropped unexpectedly three stories a few days earlier. The professor, Eben Moglen, tried to imagine what the world would be like if elevators were not built so that people could inspect them.

Mr. Moglen was on his way to give a talk about the dangers of secret code, known as proprietary software, that controls more and more devices every day.

"Proprietary software is an unsafe building material," Mr. Moglen had said. "You can't inspect it."

RELATED COVERAGE

Volkswagen Says 11 Million Cars Worldwide Are Affected in Diesel Deception SEPT. 22, 2015

How Volkswagen Got Away With Diesel Deception OCT. 8, 2015

Volkswagen and Encryption

- Volkswagen: use software backdoor to trick *regulation* and serve *customers*.
- Encryption: use software backdoor to serve *regulation* and trick *customers.*
- Volkswagen didn't really serve customers: environment still damaged for everyone.
- Encryption backdoors don't really serve regulators: security still weakened for everyone.

Volkswagen and Encryption

- Volkswagen's emissions fraud was only possible because they had a way to ship safety-critical software that was impervious to inspection.
- A backdoor that can subvert regulation can also subvert security: same methodology.

“Democratizing encryption”

to move freely between countries while outpacing the intelligence sharing needed to stop them.

“Every time there is an attack, we discover that the perpetrators were known to the authorities,” said François Heisbourg, a counterterrorism expert and former defense official. “What this shows is that our intelligence is actually pretty good, but our ability to act on it is limited by the sheer numbers.”

The missed opportunities before and since the attacks in Paris, intelligence officials and

- “Democratizing encryption” isn’t limited to making it usable on your device or accessible in your language.
- It’s also a question of safeguarding its legitimacy against misguided policy.
- *Poor standards* encourage tolerance to opacity in society.

A Question of Poor Standards

- An immature approach to verifiability is what allows opacity in security, and what hurts policy-makers as well as private citizens.
- Moral discipline comes with *verifiability*. So does security and cryptography.
- We *already have the means* to obtain mathematical guarantees on the software operating cars, smartphones…

Towards Verifiable Security

- Lesson: Unverified software, backdoors hurt everyone and don't work in any industry. Automobiles, smartphones, weapons systems…
- Verifiable encryption is necessary for our economy, our privacy, *and* our ability to regulate and enforce the law.

Towards Verifiable Security

- *Law enforcement benefits from this.*
- Instead of mass surveillance, mass verification across industries.
- Instead of mass surveillance, targeted law enforcement.

Towards Verifiable Security

- Upcoming work: towards the *automated formal verification* of security software systems written by *regular engineers.*
  - We brought encryption to everyone – let's bring the ability to openly verify it to those who need it the most.
- Upcoming work: present legal arguments to a European judiciary audience.
  - Upcoming paper: *L'algorithme et l'ordre public*, in *Archives de Philosophie de Droit.*

Towards Verifiable Security

- My website: https://nadim.computer
- INRIA's PROSECCO: http://prosecco.gforge.inria.fr
- Cryptocat: https://crypto.cat

Thank you!