Owner: Thyla van der Merwe

About this workshop…

- Cryptography is hard, writing robust cryptographic code might be harder!
- Open sourcing this code comes with a unique set of challenges:
  - How is a wide array of users going to interact with this code? Large organisations? Small organisations? Individual users?
  - What use cases do they have?
  - Will they use it correctly?
  - What does maintenance look like? Where does the burden lie?
  - Vulnerabilities, patching and propagation of fixes?

About this workshop…

- Cryptography is hard, writing robust cryptographic code might be harder!
- Open sourcing this code comes with a unique set of challenges:
  - How is a wide array of users going to interact with this code? Large organisations? Small organisations? Individual users?
  - What use cases do they have?
  - Will they use it correctly?
  - What does maintenance look like? Where does the burden lie?
  - Vulnerabilities, patching and propagation of fixes?

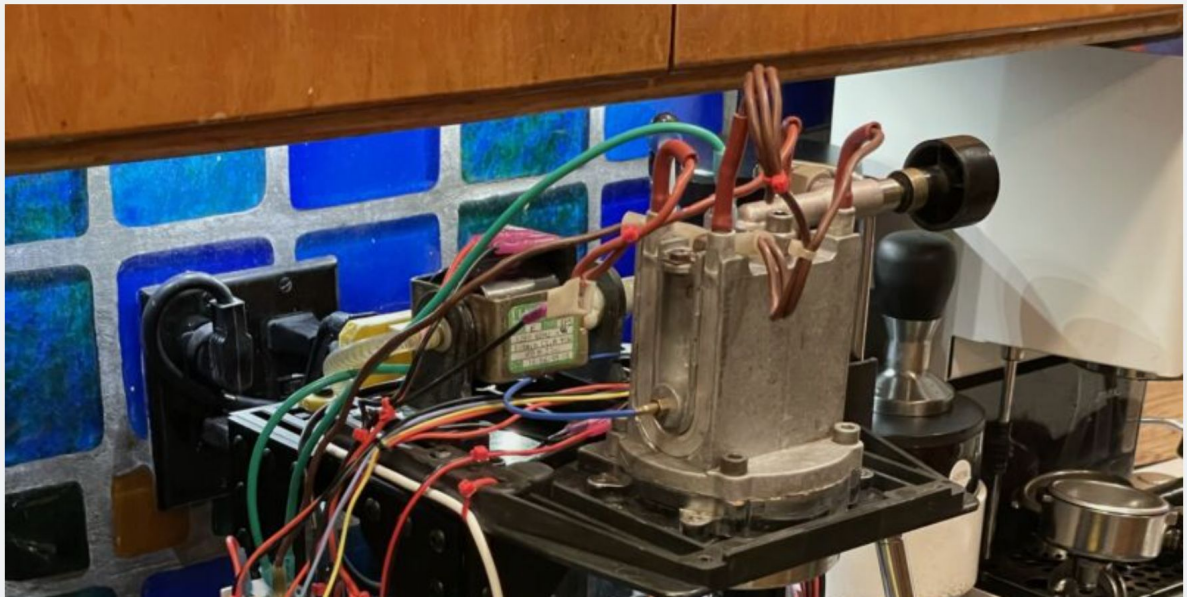
Usability | Applicability | Security

HOMEBREW FOR REAL —

Open source espresso machine is one delicious rabbit hole inside another

The path to epic coffee winds past Arduinos, breadboards, and firmware flashing.

KEVIN PURDY - 3/29/2023, 2:41 AM



cryptography

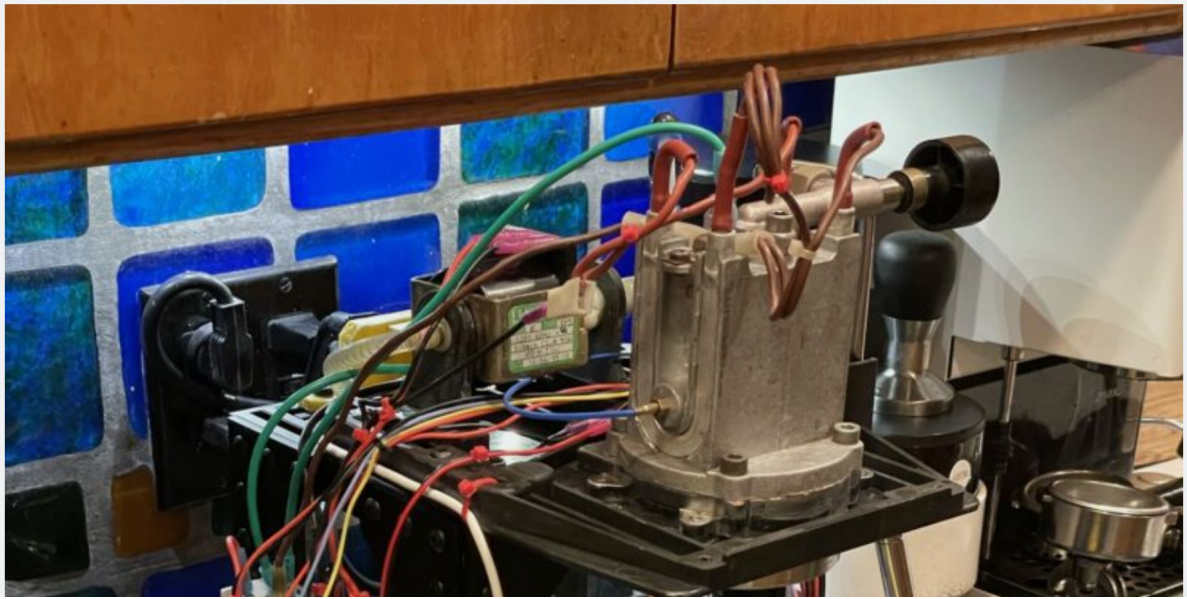
HOMEBREW FOR REAL —

Open source ~~espresso machine~~ is one ~~delicious~~ rabbit hole inside another

deliciously complicated

The path to epic coffee winds past Arduinos, breadboards, and firmware flashing.

KEVIN PURDY - 3/29/2023, 2:41 AM



About this workshop…

- Cryptography is hard, writing robust cryptographic code might be harder!
- Open sourcing this code comes with a unique set of challenges:
  - How is a wide array of users going to interact with this code? Large organisations? Small organisations? Individual users?
  - What use cases do they have?
  - Will they use it correctly?

How can we make open source cryptographic code better everyone?

Program

09:50 - 10:00	Opening remarks (now!)
10:00 - 10:30	Using Open Source Crypto – Interactive Session
10:30 - 11:00	Making it Memory Safe – J.C. Jones (recorded)
11:00 - 11:15	**Break**
11:15 - 11:45	Tink Mechanics – Moreno Ambrosin
11:45 - 12:15	Low-level Impl. of Finite Field Operations - Shigeo Mitsunari
12:15 - 14:00	**Lunch**

Program

14:00 - 14:30	Implementing Oblivious HTTP in Firefox – Dana Keeler
14:30 - 15:30	Live Hacking – Thai Duong
15:30 - 16:00	Lightning Talks (5 mins, no slides)
16:00 - 16:10	**Close**

Thank you!

J.C. Jones

Cindy Lin

Liza Tretiakova

Fernando Lobato Meeser

Moreno Ambrosin