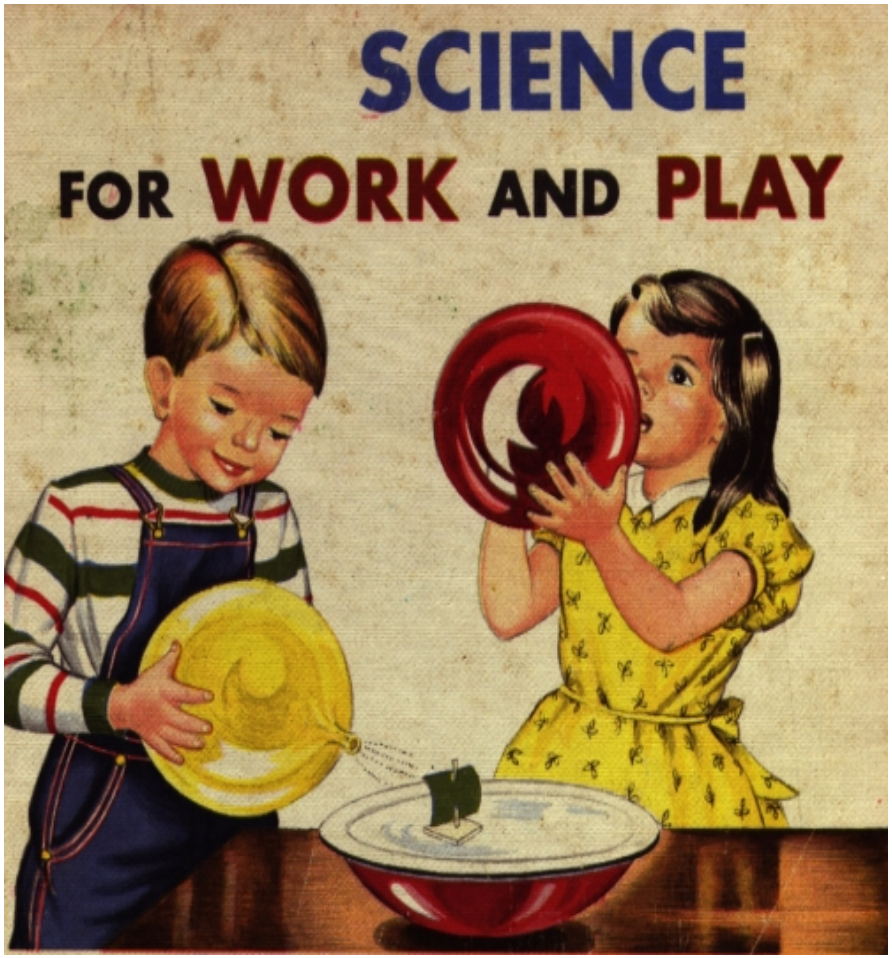
APNIC Research & Development



BRITONS

Ahem

Internet Citizens

Cryptech Needs You!


This Guy?

He found something

Where's the Trust?

- Everybody is listening in. All the time.
- What we have found out, is that there is remarkably little reason to trust any of the deployed hardware crypto solutions we're being told to use.
- We are no longer free to assume agencies like NIST are actually performing the kind of role we need them to perform, in regards to basic cryptography.
  - Algorithms have been 'played with'
  - Design choices are now potentially compromised
- If we want a trustable internet, we have to make our own.
  - The building blocks we can buy, are made of sand.

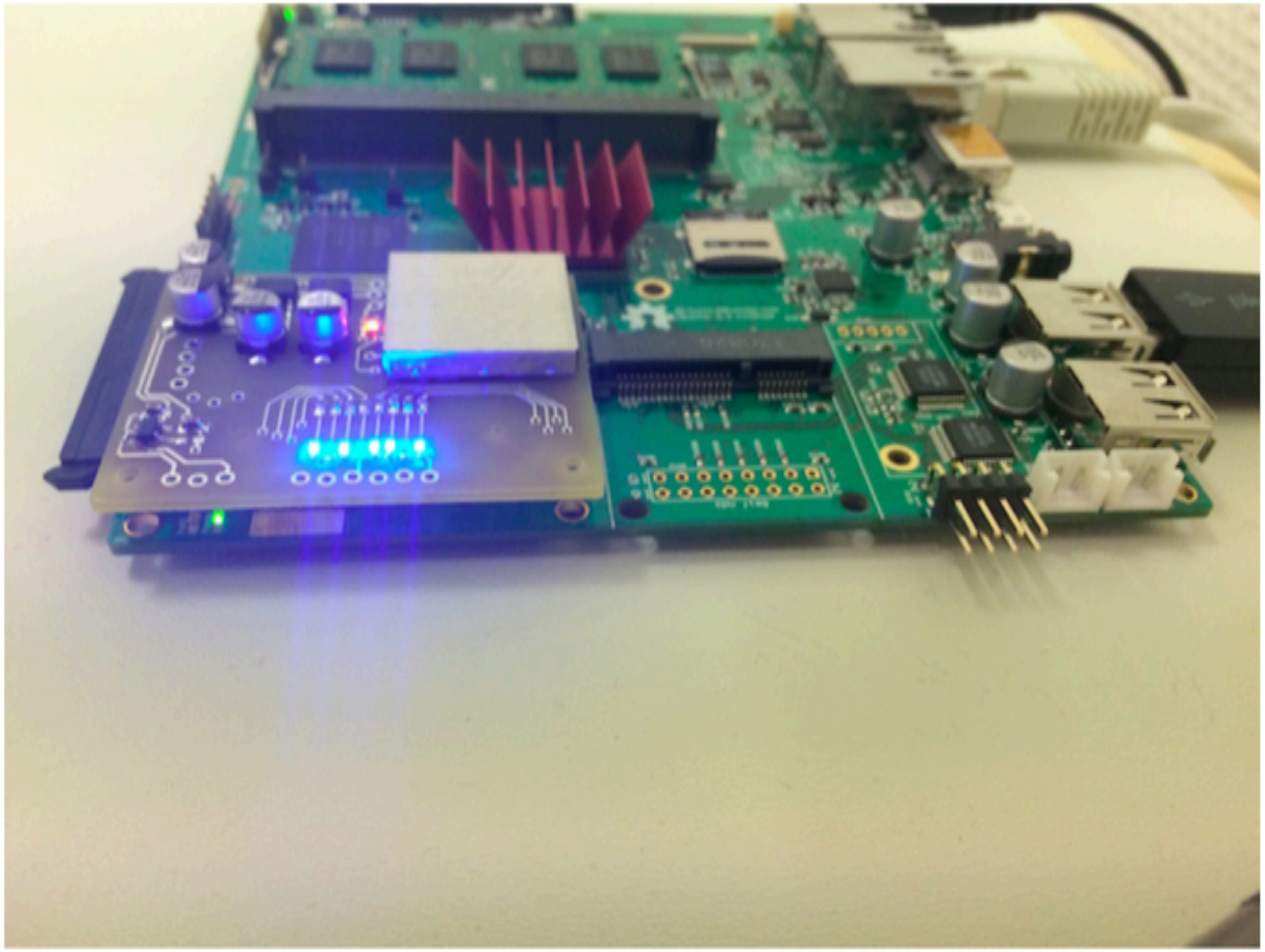
We've been here before..

- End of WWII: Britain has a huge stockpile of captured 'Enigma' encryption machines.
  - Gives them to British Colonies, Palestine
    - So they can decode what they're saying

Cryptech

- For the real info see http://cryptech.is/
  - (yes, the certificate is stale)
- Independently designed, audited FPGA for a complete Hardware Security Module (HSM)
  - Verilog/VHDL in public view.
  - Don't trust it? Check it yourself (if you know how)
- Test units now built using 'novena' board
- Strong sources of randomness have been designed and tested
  - Also now functions as GPIO (Raspberry PI!) or USB attached /dev/urandom seed
- Potting, Tamperproof, Hardening
  - Work-In-Progress
- But **Funding** is critically low…

Blue LEDS. It must be cool!



So what can I do?

- Help secure funding.
  - http://cryptech.is/funding
  - Model is to keep single donations p.a. below $100k to ensure no capture by a single funding source. ISOC can act as a clearing house
  - Individual donations welcome
- Get the word out
  - Talk to people about cryptech, the issues. Do Lightnings like this
- Think about contributing mindshare
  - Review documents. Port code. Test.

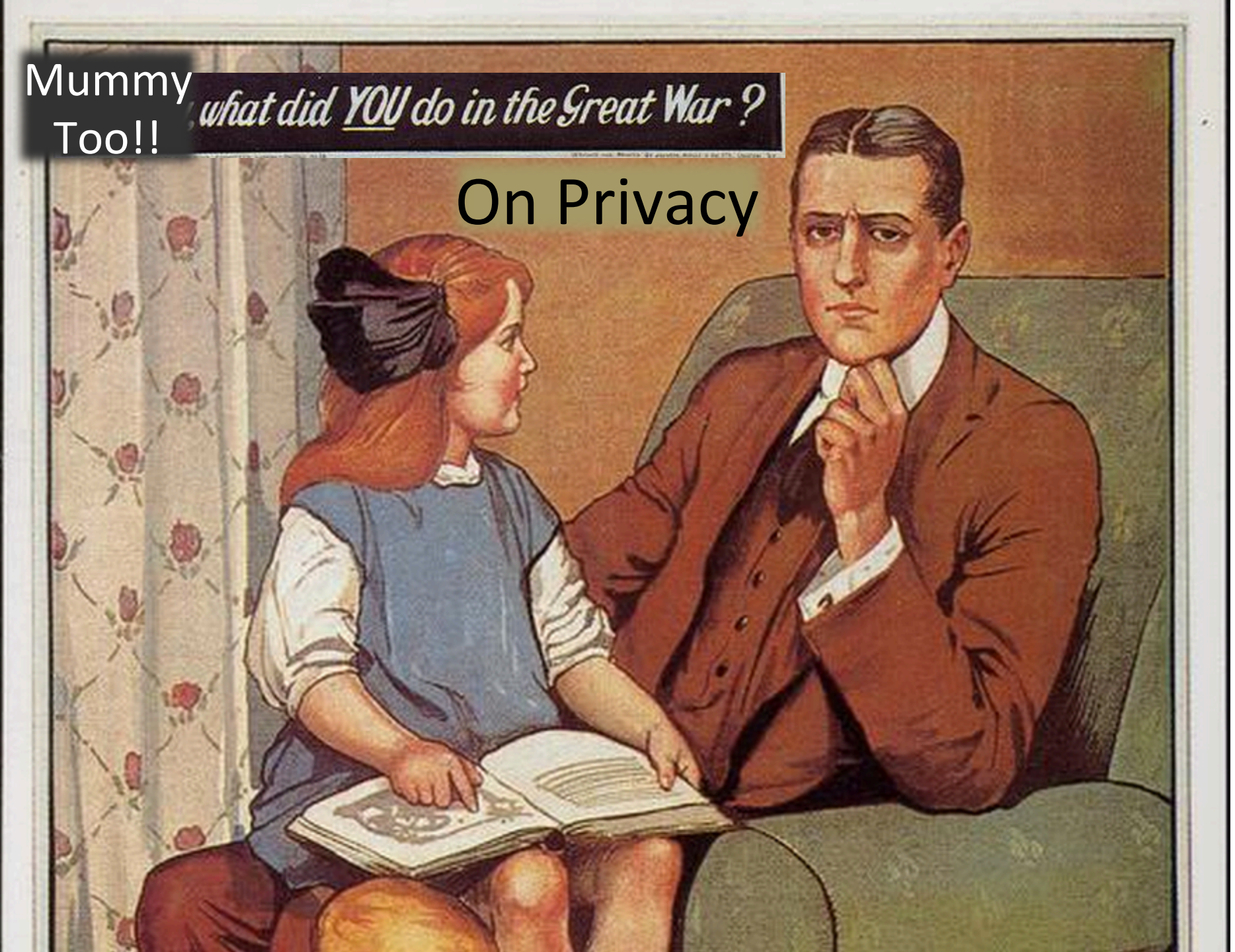
YAY!!!

- Thanks to Comcast, Internet Society, Google, IANA, PIR, SUNET, SURFNET, Afilias, **RIPE NCC** among others

- Detailed presentation available at
  http://archive.psg.com/141216.verisign-cryptech.pdf


Daddy, what did YOU do in the Great War ?

On Privacy


Mummy Too!!
what did YOU do in the Great War ?
On Privacy