Talla
Alexander Færøy
1. What is Talla?

2. A very quick introduction to the Erlang programming language.

3. The architecture of Talla.

4. A walk over a tiny bit of the source code.
What is Talla?

• An attempt to build a well-designed implementation of a Tor relay daemon in Erlang.

• An attempt for me to understand the inner workings of the Tor network better.

• A typical “evenings-only open source project” :-)

• I believe it will add diversity to the network over time.
My crystal ball indicates that one day there will be a Tor relay implemented in Erlang. Makes sense.
• The official Tor in C.
• PurpleOnion in C#.
• GoTor in Google’s Go language.
• Galois Inc’s Haskell implementation.
• Orchid, tor-research-framework, and OnionCoffee in Java.
• node-Tor in JavaScript.
• Oppy, pycepa, and TorPylle in Python.
• Complete list on https://trac.torproject.org/projects/tor/wiki/doc/ListOfTorImplementations
Carefulness

- Running experimental Tor implementations on the “production network” would be irresponsible.

- Test networks.

- Directory Authorities?

- Chutney :-)

- See email thread on tor-dev:
Why Erlang?

- Functional programming language designed by Ericsson in Sweden.
- Focus on concurrency via message passing.
- Extremely powerful when it comes to working with network protocols.
- Running on the BEAM virtual machine.
Performance?
An introduction to Erlang
The architecture of Talla
Applications and Libraries

- Talla
  - Core
  - Onion Routing
  - Directory

- Onion
  - RSA

- enacl

- Ed25519 (ref 10)

- Luke (New Hope)
enacl

• Written by Jesper Louis Andersen who is here at BornHack as well.

• Used for its /dev/urandom interface.

• Used for x25519 Diffie-Hellman.

• Source code: https://github.com/jlouis/enacl
Ed25519

• Used for ed25519 signatures to the directory services.

• Multiple implementations of Ed25519 :-(

• Major thanks to Yawning Angel from Tor.

• Source code: https://lab.baconsvin.org/talla/ed25519_ref10
Luke

- Experimental Erlang NIF of the New Hope Post-Quantum cryptographic system.

- Supports “normal” New Hope and Tor New Hope (Tor Proposal #270 by Isis Lovecruft and Peter Schwabe).

- Source code: https://lab.baconsvin.org/ahf/luke
Onion

• Shared utilities needed for working with the Tor network.

• Small C function for generating an RSA key pair.

• Well-tested code.

• Automated test execution.

• The most stable part of Talla right now :-) 

• Source code: https://lab.baconsvin.org/talla/onion
Talla

• Core application is for centralised services to the system.

• One application for Onion Routing.

• One application is for Directory service (announcement only as of 2016).
Internals of Talla
Peer
Community

Hackers and people who want to follow the development of Talla should feel free to join #talla on irc.baconsvin.org or 6nbtgccn5nbcohdn3.onion with TLS on port 6697.

Same IRC network as BornHack.
Source Code

The source code and issue tracker can be found at the Baconsvin Gitlab instance at https://lab.baconsvin.org/talla
Resources

- Tor specifications: gitweb.torproject.org/torspec.git - we are focused on tor-spec.txt and dir-spec.txt as of 2016.

- Ferd Hebert’s Learn You Some Erlang for Great Good: learnyousomeerlang.com and erlang-in-anger.com
Questions?
Thanks to Linus, Yawning, the hackers of Celo and Baconsvin.
Chutney and Talla demo.