Do we need an expanded Internet threat model?

Brian Trammel, Jari Arkko, Ted Hardie, Stephen Farrell

IETF 105

Drafts

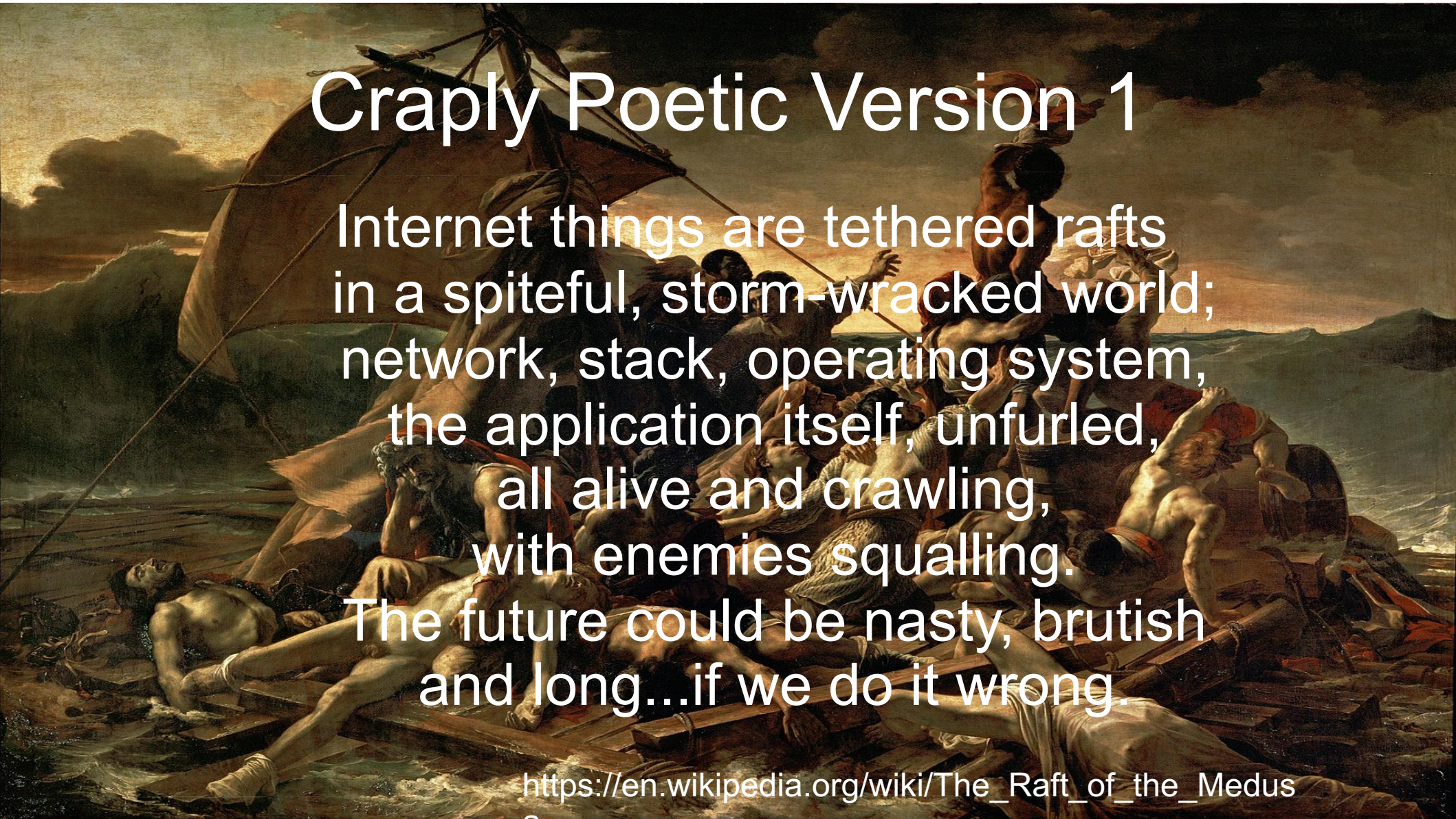
- draft-arkko-arch-internet-threat-model-01
- draft-farrell-etm-02
- Discussion at the IAB DEDR workshop
- Discussion at IETF-105 (IAB, SAAG, RTGAREA)

Question

- RFC3552 says:
  - Thing1: “ we assume that the attacker has nearly complete control of the communications channel over which the end-systems communicate”
  - Thing2: “we assume that the end-systems engaging in a protocol exchange have not themselves been compromised”
- We believe Thing1 is still **necessary** for protocol design
- But... Is Thing2 still sufficient?

So is Thing2 no longer sufficient?

- Better COMSEC motivates attackers to look elsewhere
- Government surveillance agencies focusing more on acquiring data from content providers or end-devices
- Surveillance capitalism: new risks due to some applications having an
  - increased breadth of collection of information
  - increasingly large information data bases,
  - increasingly common involvement of fewer/centralised parties
- Interests of a communicating party not aligned with your interests
- A network you thought wasn't interestingly vulnerable turns out to be attackable



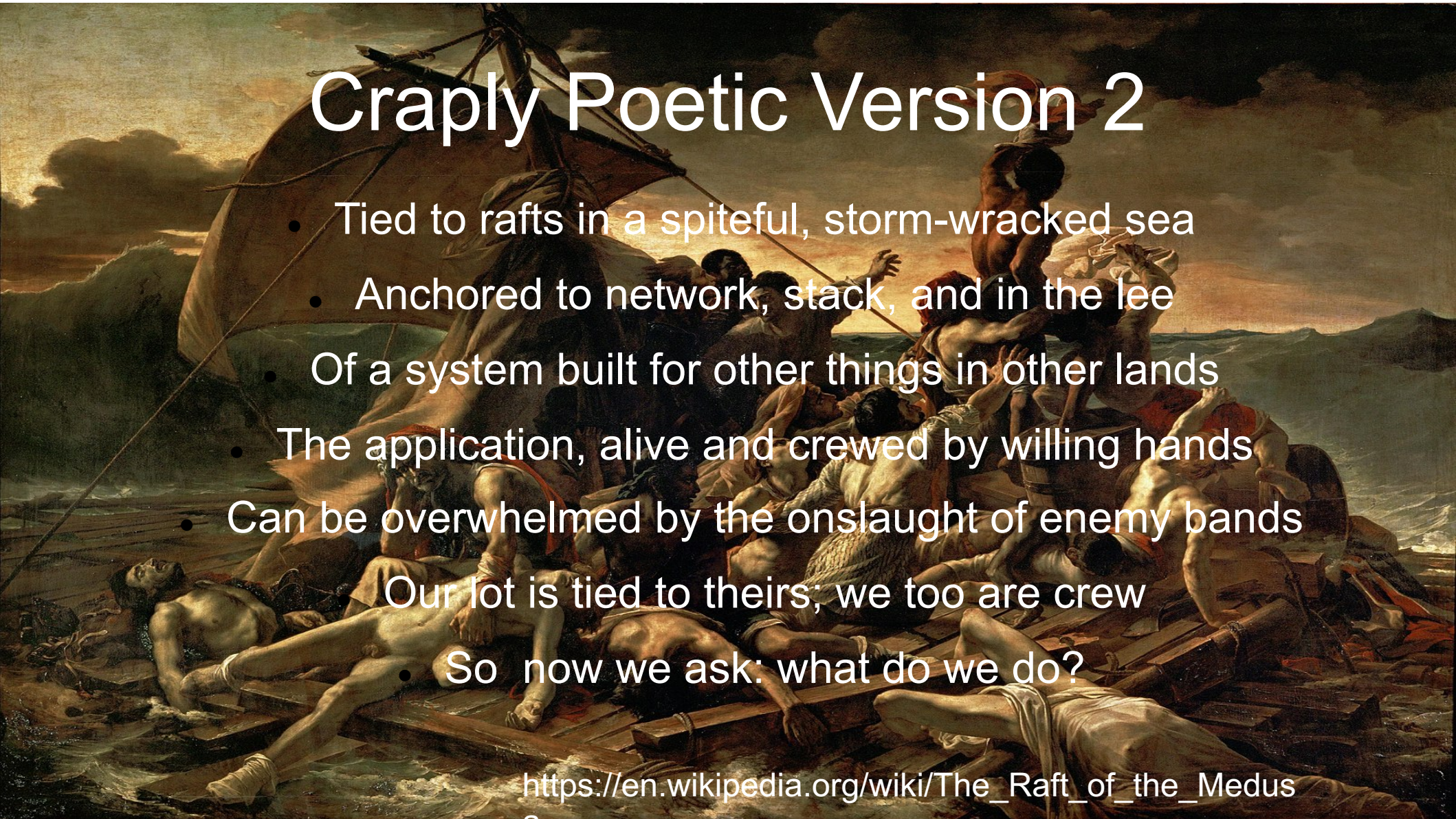
Craply Poetic Version 1

Internet things are tethered rafts
in a spiteful, storm-wracked world;
network, stack, operating system,
the application itself, unfurled,
all alive and crawling,
with enemies squalling.
The future could be nasty, brutish
and long...if we do it wrong.

https://en.wikipedia.org/wiki/The_Raft_of_the_Medus

Craply Poetic Version 2

- Tied to rafts in a spiteful, storm-wracked sea
- Anchored to network, stack, and in the lee
- Of a system built for other things in other lands
- The application, alive and crewed by willing hands
- Can be overwhelmed by the onslaught of enemy bands
- Our lot is tied to theirs; we too are crew
- So now we ask: what do we do?



https://en.wikipedia.org/wiki/The_Raft_of_the_Medus

Prose is likely a better output:-)

"We assume that the application managing a protocol exchange may itself be working for an adversary, may be on a network with other endpoints hostile to its interests, or may be in an environment hostile to its aim, either directly (e.g. via a compromised OS or OS function) or indirectly (e.g. via action of a hosting substrate for a container or VM).”

Where/what to do?

- The 4 of us have been chatting about this (not an “IAB thing”)
- We’d like guidance and feedback
- We can think of some useful end results, but plenty of this is unclear also
  - Technical means of protection might include data minimisation, avoid creating new centralised architectures, perfect forward secrecy, …
  - Design work might benefit from use- and abuse-cases
- Informational RFC or updates to RFCs? Maybe some day
- Possible to-do: make a mailing list, talk about it

Impact on operator networks

- It helps when one does not have to worry about the interest misalignment within one's own network and own devices
- But even a closed network or network owned by one party is very much vulnerable
  - Compromised nodes, CPUs, node hijacking due to various vulnerabilities, etc.
- One should assume there can be compromised nodes in all networks, and design architectures with that in mind
  - Understand implications of individual nodes (e.g., control nodes) failing in interesting ways
- The general case of Byzantine routers is hard/unsolvable