

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
- There was also discussion about this at the IAB DEDR workshop
- Discussion at IETF105 (IAB/IESG, RTGWG, SAAG)

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?

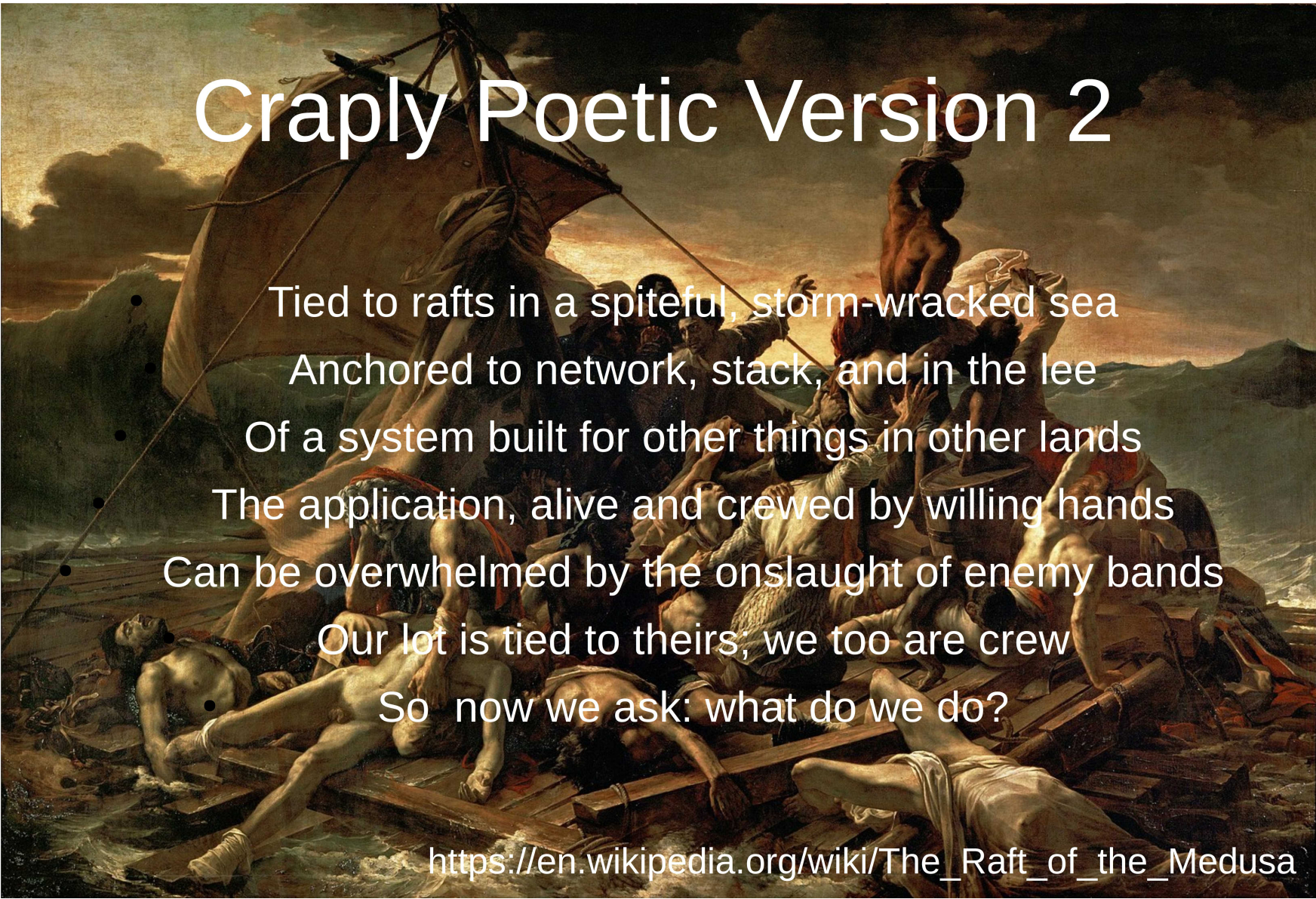
- Better COMSEC motivates attackers to look elsewhere
- Government surveillance agencies focusing more on acquiring data from content providers or end-devices
- Surveillance capitalism: new risks due to some applications having an
 - increased breadth of collection of information
 - increasingly large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

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_Medusa

Craply Poetic Version 2

The background of the slide is a reproduction of the painting 'The Raft of the Medusa' by Théodore Géricault. It depicts a group of survivors on a makeshift raft of planks and debris in a stormy sea. The scene is chaotic, with people in various states of distress, some reaching for help, others appearing exhausted or dead. The sky is dark and stormy, with a bright light source on the horizon. The overall tone is one of tragedy and desperation.

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_Medusa

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
 - It's not an "IAB thing" (but we are currently on the IAB:-)
- We'd like guidance and feedback
- We can think of some useful end-results, but plenty here is unclear:
 - Technical means of protection might include data minimisation, avoid creating new centralised architectures
 - Design process mechanisms might include analysis of abuse-cases as well as use-cases
- It's very unclear if an IETF consensus RFC (whether info or BCP) is a good target or whether an informational RFC (ISE or IAB) might be more practical
- An IETF consensus document would be "better" but we might not be ready for that yet, and we won't know 'till we have a better idea of how a (useful) expanded threat model might look
- Possible to-do: make a mailing list, talk about it