Call for Action: The Internet threat model needs a change

RIOT Summit – Sept. 2019

Jari Arkko – Senior Expert at Ericsson

A member of Internet Architecture Board

[opinions expressed here are my own, but credits to Farrell/Hardie/Trammell]

Outline

- Personal background
- Internet security developments
- Motivation for re-consideration
- Examples
- What can we do?
- Implications for IOT systems

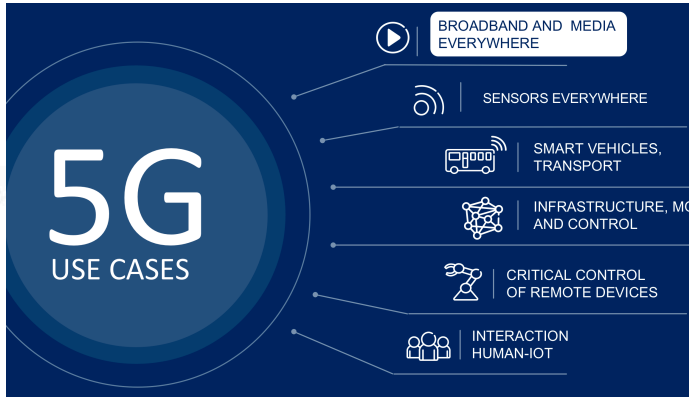

IOT
IPv6
5G
QUIC
Internet
Security
Home-networking

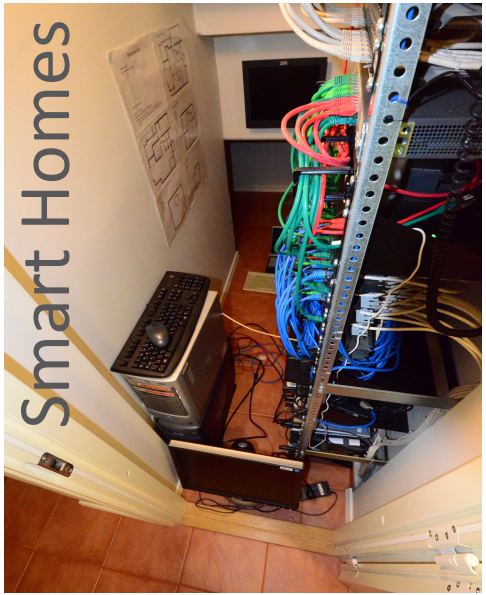
House Arkko Laundry

Laundry is dry

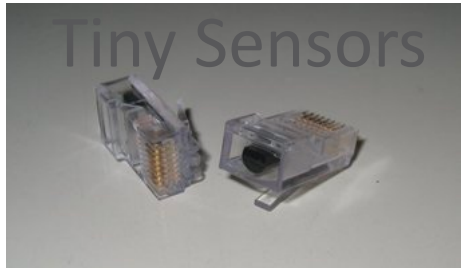
Tykkää · Kommentoi · Jaa · Eilen 6:00 via House

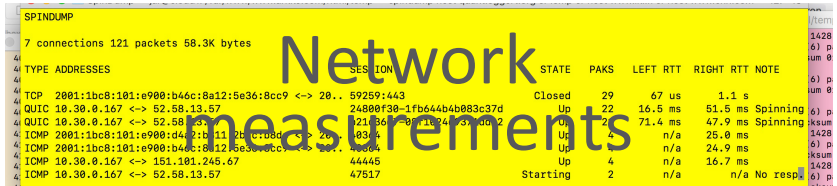
UIs



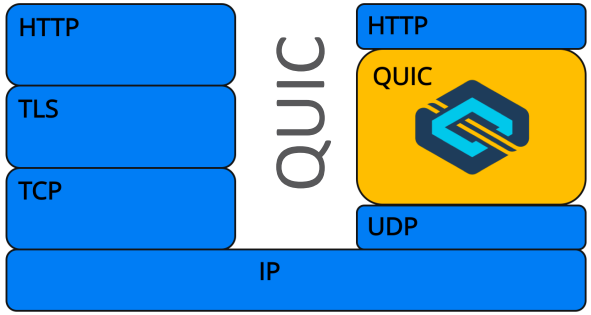


IOT
IPv6
5G
QUIC
Internet
Security
Home-networking





Network measurements



Recent Internet Developments

Evolution pace

- Internet tech evolves generally slowly, but the second half of the 2010s has brought fast pace
  - Due to new needs & market/large players
  - Snowden revelations
- The changes will make further changes easier (e.g., update applications vs. kernels)

Changes

- Security, web protocols, transport, …

Implications

- Improved communications security
- Availability of information changes radically
- New entities with access to different information sources may be created
- Potential further evolution in congestion control, naming, …

Increased Use of Encryption

Reasons

- Security issues
- Snowden revelations
- Technology and infrastructure enablers
  - More efficient protocols, implementations + Let's Encrypt
- Business incentives

Results

- Much more use of encryption
  - Particularly on web traffic (HTTPS & TLS)
  - Also on server-to-server email
- New technology adoption
- Significant increase in encrypted communications: 20% -> 80%

The 2nd Wave of Encryption

The encryption trend does not end!

- ”Encrypted” has stood for content encryption
- Much of the control and setup information is still in the clear, but you could protect more:
  - Transport headers
  - TLS setup
  - DNS queries
- There are protocols or efforts underway to protect all of the above: via QUIC, eSNI, and DOH

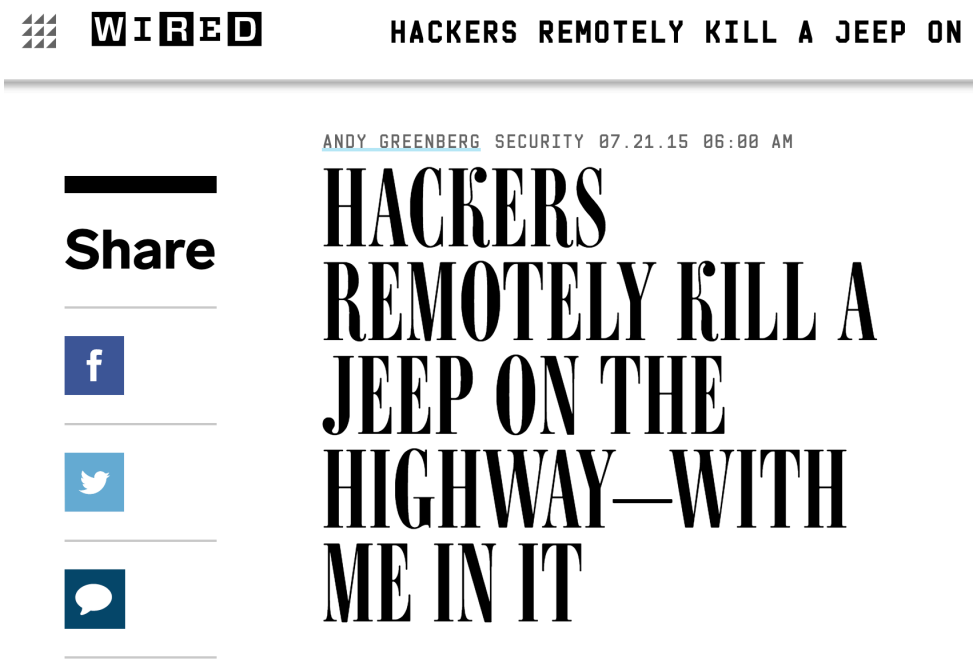
Implications

- It will be harder/impossible to determine what traffic goes through a network
- Technologies such as DPI will be less useful
- Measurements, debugging will be harder
  - QUIC allows some (RTT) measurements through explicitly measurement bit

IOT Security

Problems

- Hijacked IOT systems
- Privacy issues and data leaks
- Concerns about attacks on safety critical systems
- IOT devices attacking other systems (e.g. 2016 Dyn case)
- Manufacturers controlling devices against owner interests



Root Causes for These Failings

Technical

- Configuration and initial pairing are hard for many devices, no UI
- Technical implementation is difficult on small devices
- “This is a trusted, closed network”
- Involvement of helpful but not always reliable parties

Other

- Economics driving
  - Short development cycles
  - Minimal maintenance
- Lifecycles of consumer goods
- Externalities not taken into account

Basic Steps for Improved IOT Security

Technical

- Software update capability
- Key management and pairing process to setup authorized parties for interaction
- No default passwords
- All connections need to be secure
- System security analysis

Process

- Sufficient expertise, testing, and evaluation
- Systems need to be maintained and software regularly updated
- The availability of components from the ecosystem with reasonably security

Basic Steps for Improved IOT Security

Your role is key – and you can do it!

Question

If we encrypt all connections, are we done?

This is work done jointly with S. Farrell, T. Hardie & B. Trammell

Question

If we encrypt all connections, are we done?

No

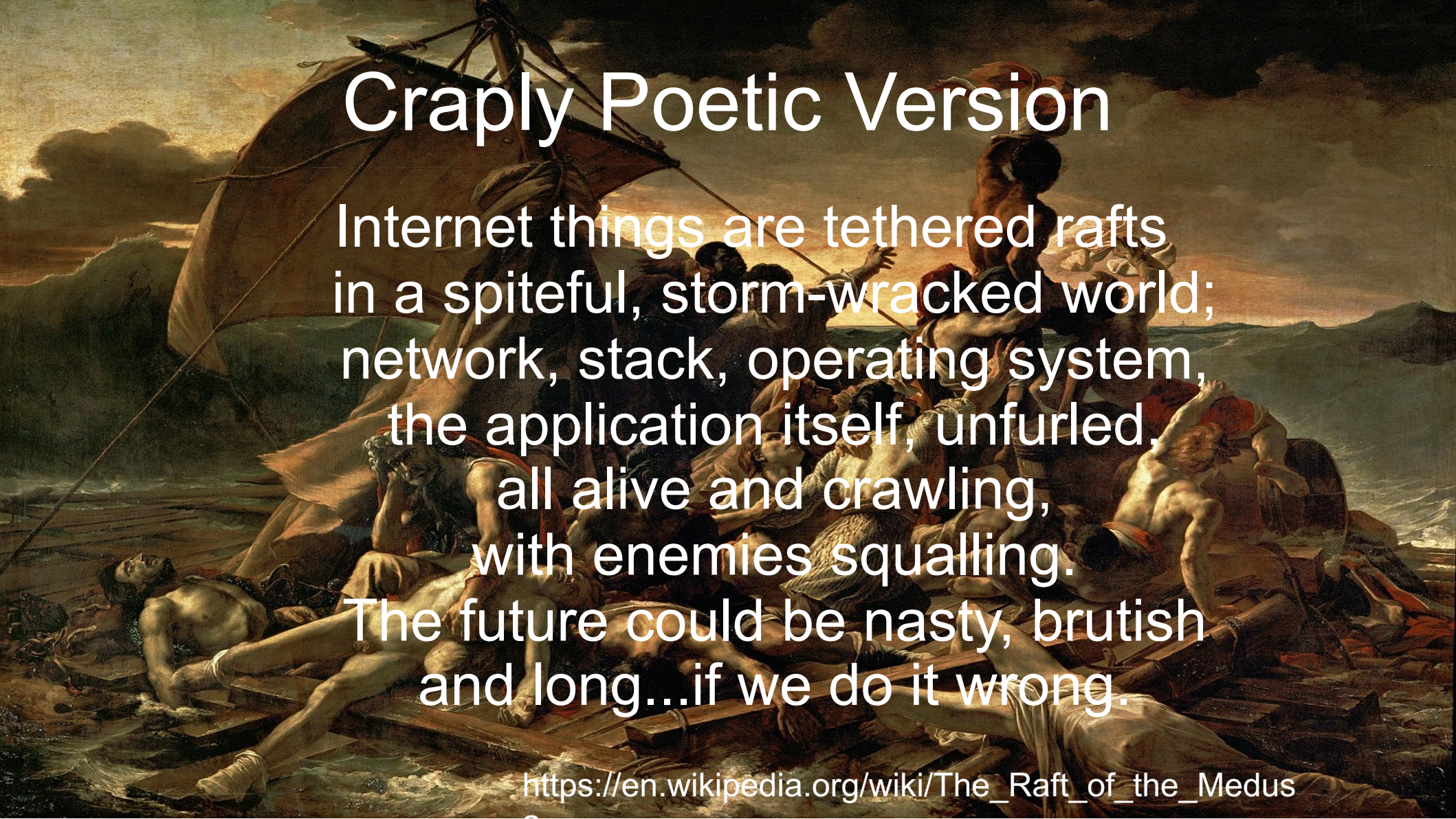
- Communications security is only a small part of the overall security setup
- We cannot always trust the parties we communicate with

Traditional Protocol Security Design

- 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... Thing2 does not match current reality

Why Thing2 is 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

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

Prose is likely a better output:-)

"We assume that the application managing a protocol exchange may have parts working for an adversary, be itself compromised, may be on a network with other endpoints hostile to its interests, or may be in an environment hostile to its aim.”

Examples

Tracking and browsers

- Many web pages collect information their users via various tracking techniques and cookies
- Is your browser working for you, or for someone else?

  Browsers differ in how much they block various tracking attempts

Centralized DNS

- Some browsers are considering replacing DNS protocol with HTTPS to (e.g.) 1.1.1.1
- Prevents filtering and capture by ISPs and MITMs
- But at the same time, puts DNS query information (today in 10^7 different places) to one entity
- Good tradeoff?

What can we do?

- At the moment, this is at the level of raising awareness
- We can think of some useful actions, 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
- IETF RFCs relating to what one should consider in protocol design may become updated at some point

Potential Guidelines

1. Consider first principles when protecting information
2. Perform end-to-end protection via other parties
3. Minimize information passed to others
4. Minimize the passing of control functions to others
5. Avoid centralized resources

New threat model and IOT

Threats

- System security analysis needed
- Are there weaknesses that lead to having compromised devices or compromised IOT gateways?
- How much should you trust the cloud components of your IOT system?
  - Is an IOT application working for you, or supplying data for others?

Remedies

- Ensure that systems can be configured to work with desired gw, app & data storage parts
- Community & distributed solutions
- Stay in control of what software sources are used for updates
- Transport layer security may not be enough – consider protecting data and actuator commands e2e and use data-object security

Additional Pointers

Mailing list

- https://www.ietf.org/mailman/listinfo/model-t

IETF drafts

- draft-arkko-arch-internet-threat-model-01
- draft-farrell-etm-02

Summary

- Encryption alone cannot provide overall good security and privacy
- There are significant threats around compromised nodes, parties whose interest do not align with the users' interests, and centralized data collection
- IOT systems are particularly prone to these issues
- Stay in control of you connect to (devices, cloud applications) and where you store data
- Secure your data, not only connections!
- The IOT technology ecosystem – including RIOT – needs to provide the tools needed for this


ERICSSON