Security Information Exposure for Trust Modelling & Measurement

Ayoub Messous (Fujitsu research of Europe)

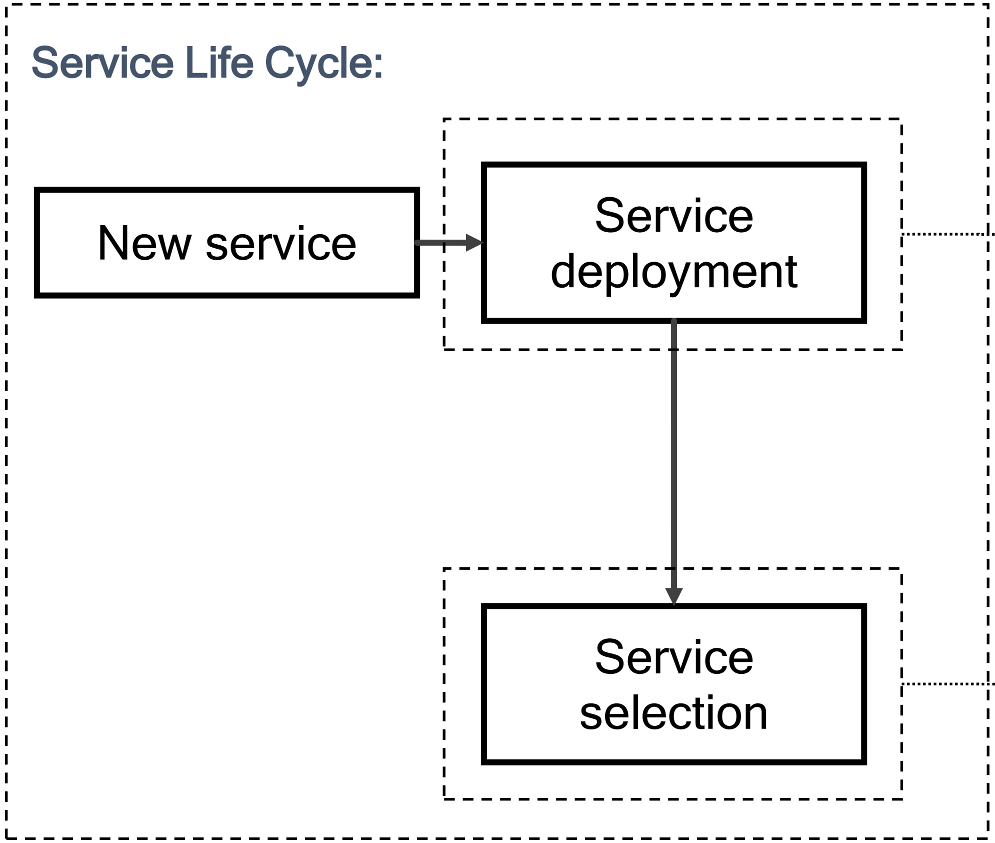
ayoub.messous@fujitsu.com

IETF 118 Meeting in Prague

Side meeting:

Exposure of Network and Compute information to Support Edge Computing

Problem Space: Service Lifecycle and Information Exposure



Action to take	Information needed	Who needs it	IETF WGs
• Service placement	• Compute • Communication • + Trust	• Service provider	• ALTO

Action to take	Information needed	Who needs it	IETF WGs
• Service selection • Path selection	• Compute • Communication • + Trust	• Network provider	• CATS
		• Application (client or proxy)	• ALTO

Towards Trust-Centric Networking

- Networks and IT infrastructure need to be enhanced to include **trust considerations**

- What is trust in networking?
  - There is not a single framework/definition
  - Is Trust an additional cyber security objective?
  - Relationship between trust and Quality of Service / Quality of Experience?
  - Subjective nature of trust makes it challenging to define a framework for **Modelling & Measuring Trust**?

Trust Considerations

- Trust is the result of an evaluation performed by the **Trustor** upon the **Trustee**, for a specific **context**
  - After the evaluation, the trustor can decide to perform a set of actions with the trustee.

- **Trust is a property that enables a set of actions between subjects**
  - The relationship to cybersecurity and IT is that trust must be a precondition that enables certain communication operations (actions) to take place among subjects

Trust Model Components

Subjects:

Network end device, router, trust administrator, or any other network appliance

Subjects have properties that can be related to cybersecurity or performance

Actions:

Authorised by trust functions

Most common action in networking is forwarding packets

Other examples: register a node into a network

Objects

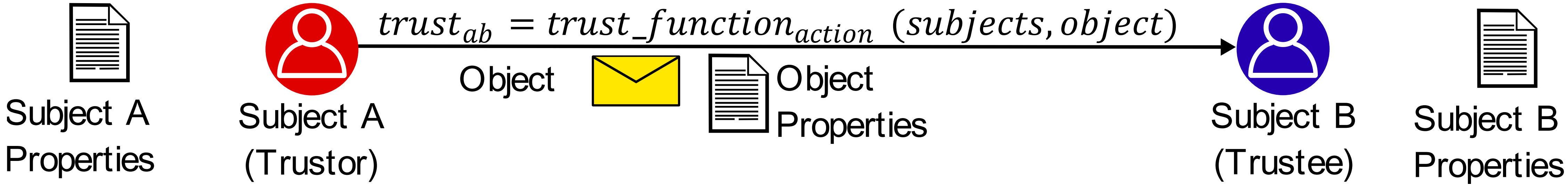
Entities used by the actions

Could have different levels of granularity, example:

- “TCP traffic with port 80 as destination”

Trust Model

- Model based in trust function
  - Trust functions take as inputs a group of subjects and objects (with their properties) and evaluate function to obtain a trust measurement.
- Trust functions are mapped to a specific action

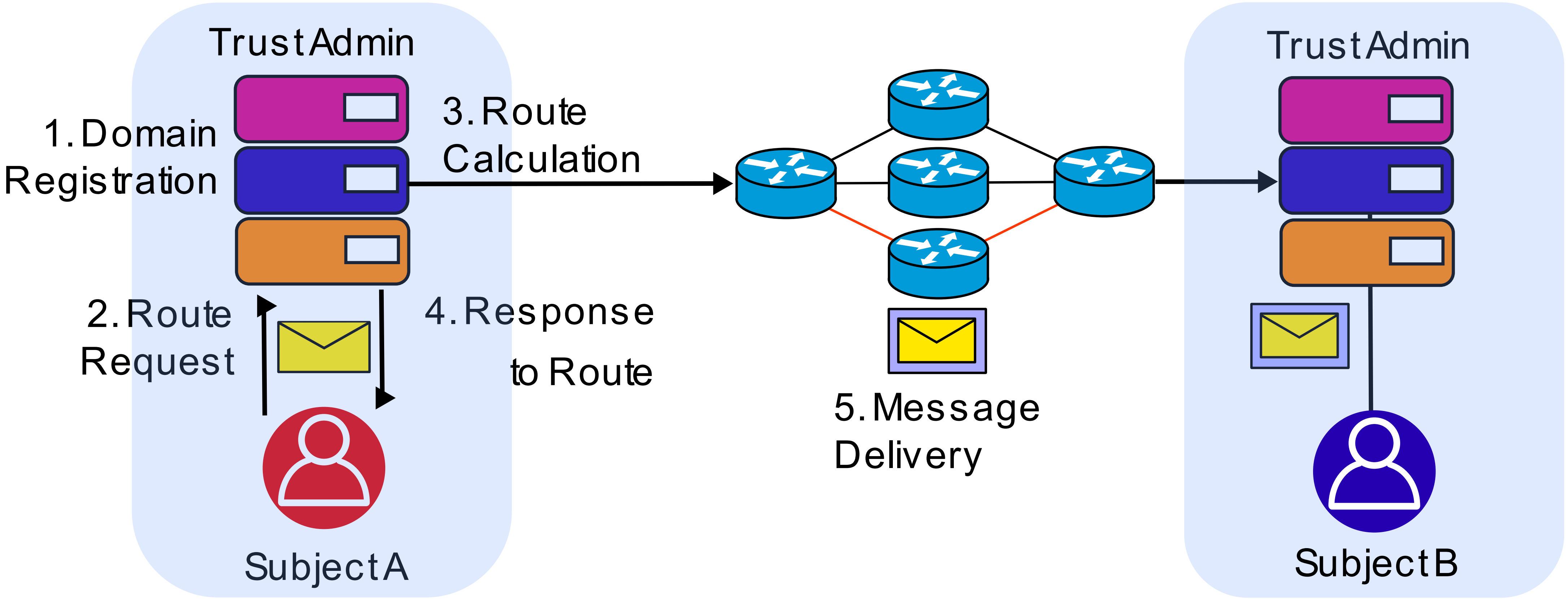


$$trust_{ab} = trust\_function_{action}\ (subjects, object)$$

Use Case: Trust Enhanced Networking

- **Subjects**:
  - Subject A (Domain A)
  - Subject B (Domain B)
- **Actions**:
  - Send message

- **Object**:
  - Confidential message
  - Should only be forwarded/store in certain routers



Trust & Compute Information Exposure for Edge Computing

- Allow EC applications to **discover** and **access** the available edge resources and services in a network.
- Enforcing Trust at the Edge by:
  - Facilitate the selection of the optimal edge site for each application component based on
  - Use **trust level** and **Compute attributes** to select the right resources.
  - Leverage **geographically-trusted routes** and **anchor points** to ensure secure and compliant transfers and computation of data.
  - Reduce the dependency on centralized cloud services (improved scalability and performance).
- Compute information exposure is a key enabler for realizing the full potential of TEN in an edge computing environment.

Discussion and Future Work

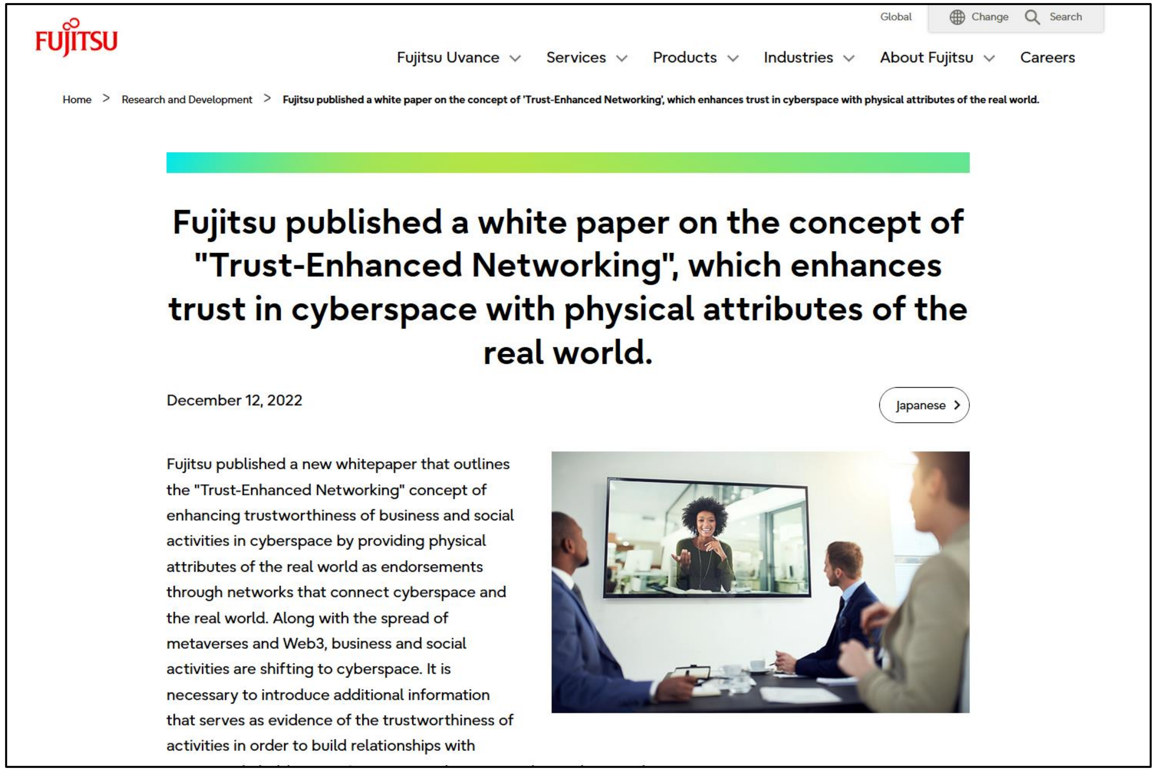
Relationship to Compute metrics

- Consider compute information in the evaluation of Trust levels
- What Trust measurements should be included as part of information exposure

Thank you

Previous Activities

- We published a 1st white paper introducing our "Trust-Enhanced Networking“ concept in **Dec 2022**



Home > Research and Development > Fujitsu published a white paper on the concept of 'Trust-Enhanced Networking', which enhances trust in cyberspace with physical attributes of the real world.

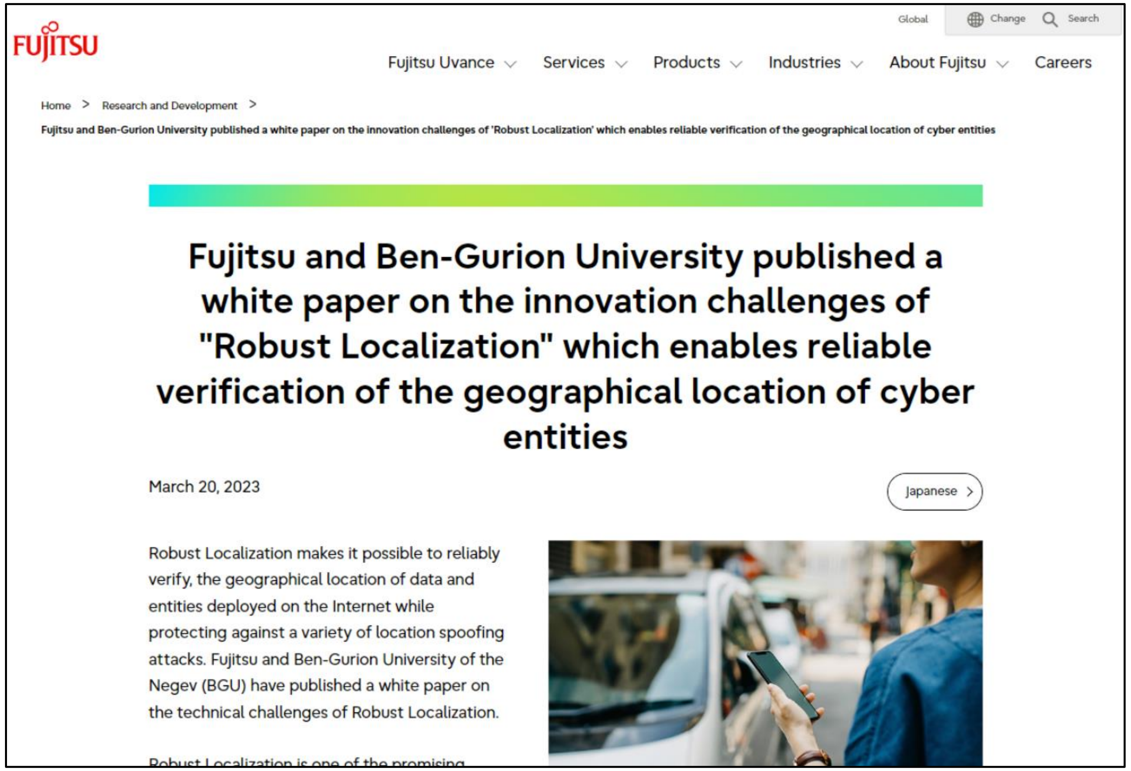
Fujitsu published a white paper on the concept of "Trust-Enhanced Networking", which enhances trust in cyberspace with physical attributes of the real world.

December 12, 2022

Fujitsu published a new whitepaper that outlines the "Trust-Enhanced Networking" concept of enhancing trustworthiness of business and social activities in cyberspace by providing physical attributes of the real world as endorsements through networks that connect cyberspace and the real world. Along with the spread of metaverses and Web3, business and social activities are shifting to cyberspace. It is necessary to introduce additional information that serves as evidence of the trustworthiness of activities in order to build relationships with

https://www.fujitsu.com/global/about/research/article/202212-trust-enhanced-networking.html

- We published a 2nd white paper focusing on “Robust Localization” as part of "Trust-Enhanced Networking“ concept in **Mar 2023**



Home > Research and Development >

Fujitsu and Ben-Gurion University published a white paper on the innovation challenges of 'Robust Localization' which enables reliable verification of the geographical location of cyber entities

Fujitsu and Ben-Gurion University published a white paper on the innovation challenges of "Robust Localization" which enables reliable verification of the geographical location of cyber entities

March 20, 2023

Robust Localization makes it possible to reliably verify, the geographical location of data and entities deployed on the Internet while protecting against a variety of location spoofing attacks. Fujitsu and Ben-Gurion University of the Negev (BGU) have published a white paper on the technical challenges of Robust Localization.

Robust Localization is one of the promising

https://www.fujitsu.com/global/about/research/article/202303-robust-localization.html