Lancaster University

Attributes and Dimensions of Trust in Secure Systems

11:30 - 12:00 7th November 2022

STaR-IoT, Delft, NL

Matthew Bradbury, Daniel Prince, Victoria Marcinkiewicz and Tim Watson

Presented by: **Sam Maesschalck**

Agenda

1. Problems with the use of trust in the literature
2. Our position on:
    1. Alternate general definitions
    2. Attributes used to focus general definitions
    3. Dimensions to measure these attributes along
3. Example system highlighting issues and application of these definitions

What problems exist with trust in the literature?

1. Definitions of concepts tend to be overly specific
   - Prevents reuse in different contexts

2. Trustees are typically described/assessed as trusted
   - Not realistic when considering systems holistically

3. A measurement of trust is typically along a single dimension
   - Not realistic, due to the complexity of measuring trust

Lancaster University

Problem 1: Definitions

Many definitions focus on behaviour/actions of an entity

- “willingness of a party to be vulnerable to the **actions** of another” - Mayer et al. 1995
- “Trust is the expectation of an entity with respect to certain **properties or actions** of another entity” - Lee
- “trust is a particular level of the subjective probability with which an agent assesses that another agent or group of agents will perform a particular **action**” - Gambetta
- digital trust as “a trust based either on past experience or evidence that an entity has **behaved** and/or will **behave** in accordance with the self-stated behaviour.” - Akram and Ko

Not all definitions focus on behaviour

- “I trust you because your **interests** encapsulate mine” - Hardin
- “**Risk**, or **meaningful personal investment**, is a prerequisite of trust” - Deutsch

An issue with defining trust in this way

- Problem
  Definitions of trust can be too specific and therefore not re-usable in other contexts
- Solution
  Define trust generally, then allow that general definition to be specific when needed

Definitions

Measurements

- Trustiness – "A measurement of the **attributes** under consideration by the trustor to assess the ability of the trustee to meet the trustor's trust **expectations**."
- Trustworthiness – "A measure of the **uncertainty** in the trustiness the trustor has in the trustee."

States

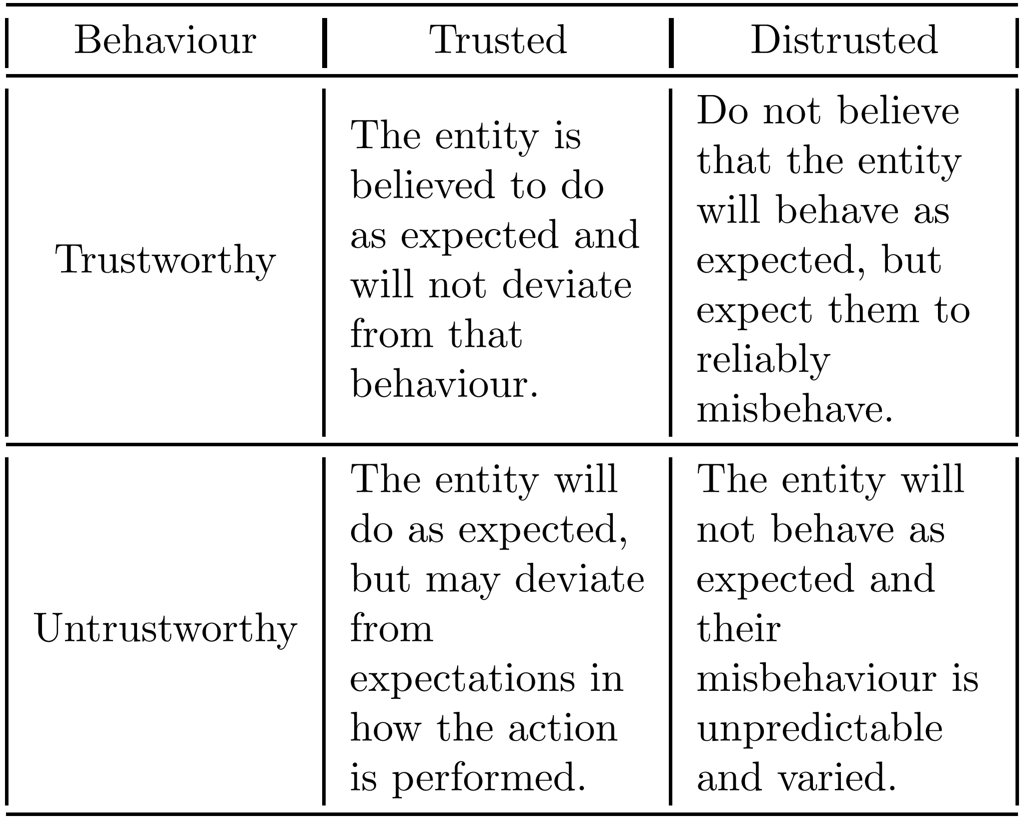
- Trusted – "An entity in a system is deemed to be trusted when the **trustiness** is sufficiently high."
- Trustworthy – "An entity in a system is deemed to be trustworthy when the **trustworthiness** is sufficiently high."

Other Definitions Reminder

- Entity – A thing in a system.
- Trustor – The entity assessing trustiness/trustworthiness, or designating another entity as trusted/trustworthy.
- Trustee – The entity that trustiness/trustworthiness is being assessed on.

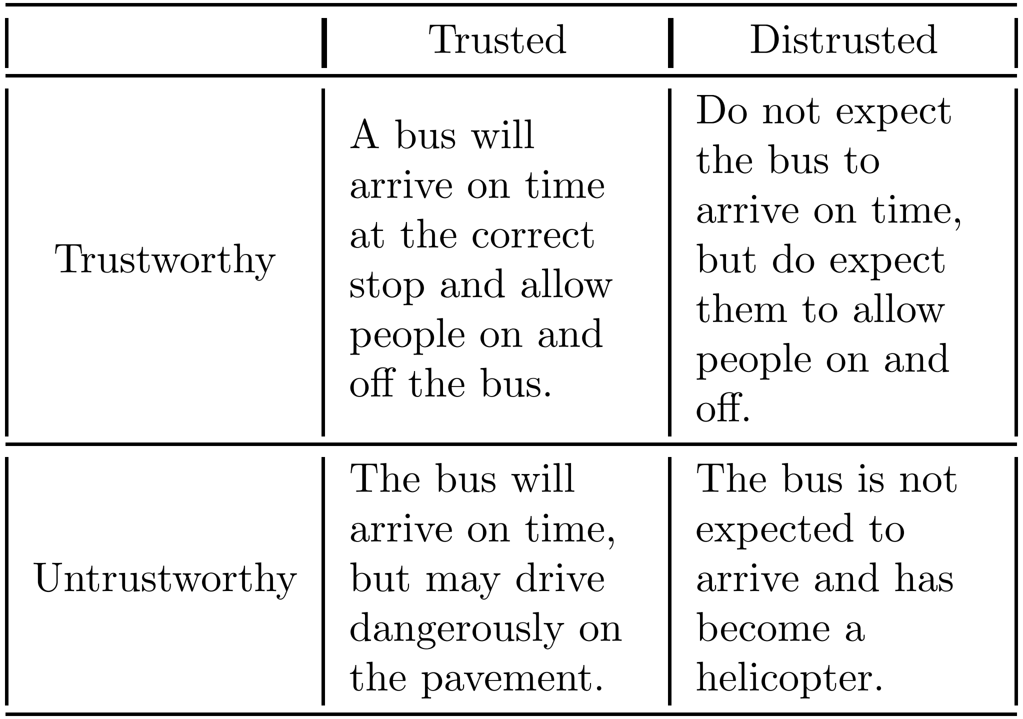
Definition Analogy

Table 1: Example of Trust and Trustworthy being assigned to an entity in a system based on their *behaviour*.



Behaviour	Trusted	Distrusted
Trustworthy	The entity is believed to do as expected and will not deviate from that behaviour.	Do not believe that the entity will behave as expected, but expect them to reliably misbehave.
Untrustworthy	The entity will do as expected, but may deviate from expectations in how the action is performed.	The entity will not behave as expected and their misbehaviour is unpredictable and varied.

Table 2: Example of Trust and Trustworthy being assigned to an example system



	Trusted	Distrusted
Trustworthy	A bus will arrive on time at the correct stop and allow people on and off the bus.	Do not expect the bus to arrive on time, but do expect them to allow people on and off.
Untrustworthy	The bus will arrive on time, but may drive dangerously on the pavement.	The bus is not expected to arrive and has become a helicopter.

Uncertainty in trust measures

- Not the first work to consider uncertainty in trust measures
  - Belief, Disbelief and Uncertainty in Beta Reputation System (Jøsang and Ismail, 2002)
- Trustworthy is often defined as being deserving of trust
- We have linked the state of “Trustworthy“ to the level of uncertainty held by the trustor
- A low level of uncertainty does not mean that a trustee is trusted

Problem 2: What is being measures/classified?

What is a trust attribute?

- An aspect for which trust is being assessed/assumed
- They are how the general trust definitions can be focused
- Not limited to the ones defined
- Jøsang et al. 2007 and Daubert et al. 2015 both presented different set of attributes

- Identity
- Behaviour
- Limitation
- Execution
- Correctness
- Data
- Environment

Attribute: Identity

- Who is the trustee?
- Potential for multiple identities

Techniques

- Low level
  - HMAC
  - Digital signatures
- Higher level
  - Web of trust
  - Digital identity systems (e.g., EU’s eIDAS)

Attribute: Behaviour / Limitation / Execution / Correctness

- Behaviour: Do **actions taken** by trustee match trustor’s expectations?
- Limitation: Do **actions not taken** by trustee match trustor’s expectations?
- Execution: Is the **software executed** by the trustee as the trustor expects?
- Correctness: Is the software executed by the trustee **implemented correctly**?

- Software and systems are complex
- Not sufficient to have limited attributes to describe them
- Example different approaches to assess:
  - Behaviour/Limitation: Observations
  - Execution: Remote attestation
  - Correctness: Verification

Attribute: Data

- Variety of sub-attributes
  - Confidentiality
  - Integrity
  - Availability
  - Accuracy
  - Provenance
  - …

- Dependency on other trust attributes
  - Need trusted identity to have provenance
- Different approaches for sub-attributes

Attribute: Environment

- Is the environment in which the trustee acts/interacts in the expected state?

- Necessary to have sensors to monitor environment
- Dependency on:
  - correct software
  - calibrated sensors
  - …

Problem 3: How are attributes being measures/classified?

Dimensions

- In what ways can the different attributes be described?
- Non-exhaustive list, potential for other dimensions of interest

- Scale
- Activity
- Scope
- Strength
- Source
- Time of Evidence

Time at which Evidence is Gathered

Assumed → Single → Sampled → Continual

- How evidence is gathered is important
  - Assumed is poor practice – assign trustee as trusted without evidence
  - Gathering evidence in a single instance will become outdated
  - Gathering sampled evidence has the potential for trustiness/trustworthiness to drop between the samples without detection
  - Continual gathering of evidence is hard and expensive

Scale

Nominal → Ordinal → Interval → Ratio

- Nominal – Unlikely to be used as there is no ordering of variables
- Ordinal – Variables with ordering (e.g., low, medium, high)
- Interval – Same as ordinal, but with fixed widths between variables
- Ratio – Same as interval, but includes the notion of true zero

Most trust scales likely to be ratio (e.g., probability, numerical measures), ordinal also likely to be common.

Proactive or Reactive

Proactive ↔ Reactive

- Trustiness/trustworthiness can be assessed proactively or reactively
- No hierarchy, each may be the preferred approached in different scenarios
- Proactive: Trustor challenges the trustee to assess trust
- Reactive: Trustor responds to actions from the trustee to assess trust

Evidence Scope and Source

Scope: None → Local → Distributed → Global

- From where has evidence come from?
  - None – Nowhere
  - Local – A single trustor
  - Distributed – Many trustors
  - Global – All entities in the system

Source: Indirect → Direct

- Evidence directly gathered is stronger than evidence provided by another trustor
- Need to consider **reputation**, do a trust assessment of the entity providing indirect evidence

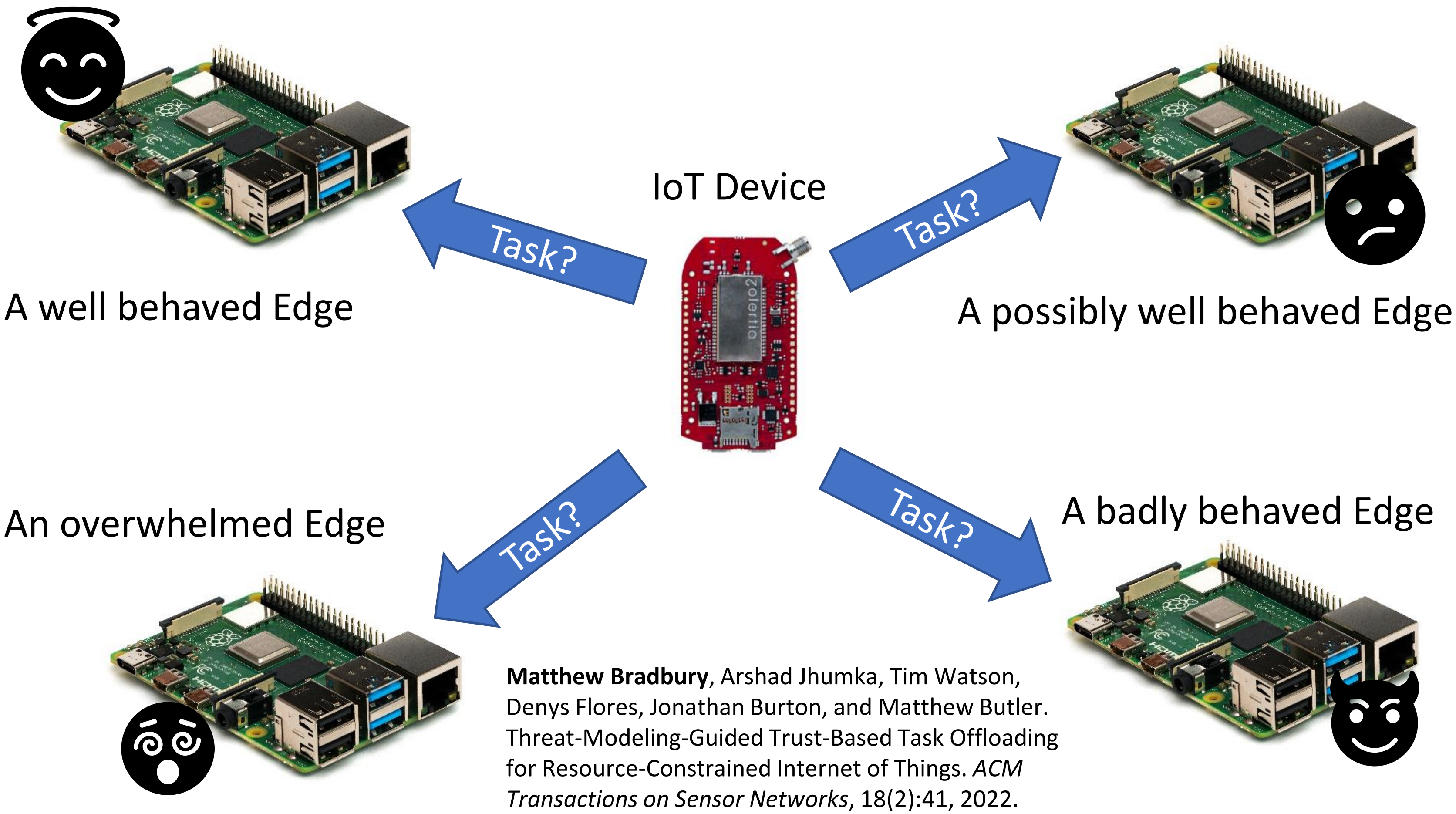
Evidence Strength

Strength: …

- Some evidence will be stronger than others
- Scale of strength will vary depending on the type of evidence
  - Not sensible to provide a unified scale

Example Classification

Example System – Task Offloading



IoT Device

Task?

Task?

Task?

Task?

A well behaved Edge

A possibly well behaved Edge

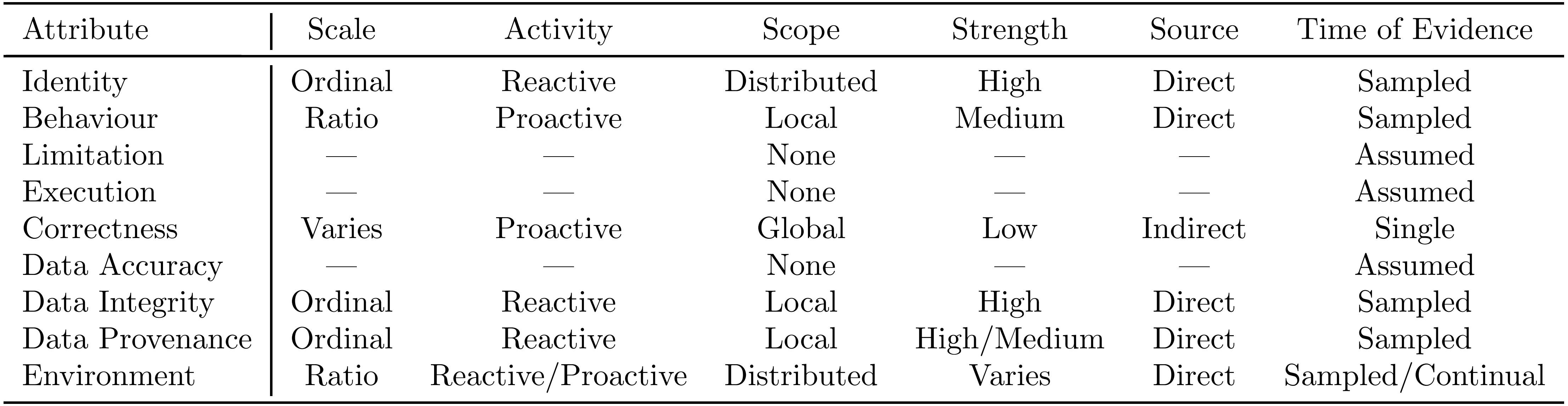
An overwhelmed Edge

A badly behaved Edge

- Resource-constrained IoT offload expensive tasks to resource-rich Edge
- How to decide who to offload to?
- Measure trustiness of accepting task and executing it correctly and timely

Matthew Bradbury, Arshad Jhumka, Tim Watson, Denys Flores, Jonathan Burton, and Matthew Butler. Threat-Modeling-Guided Trust-Based Task Offloading for Resource-Constrained Internet of Things. *ACM Transactions on Sensor Networks*, 18(2):41, 2022. doi:10.1145/3510424.

Example Classification Matrix



Attribute	Scale	Activity	Scope	Strength	Source	Time of Evidence
Identity	Ordinal	Reactive	Distributed	High	Direct	Sampled
Behaviour	Ratio	Proactive	Local	Medium	Direct	Sampled
Limitation	—	—	None	—	—	Assumed
Execution	—	—	None	—	—	Assumed
Correctness	Varies	Proactive	Global	Low	Indirect	Single
Data Accuracy	—	—	None	—	—	Assumed
Data Integrity	Ordinal	Reactive	Local	High	Direct	Sampled
Data Provenance	Ordinal	Reactive	Local	High/Medium	Direct	Sampled
Environment	Ratio	Reactive/Proactive	Distributed	Varies	Direct	Sampled/Continual

This example system focuses on assessing trustiness of one entity (IoT device) in another (Edge)

- Identity – via public key infrastructure (digital signatures)
- Behaviour – via beta reputation system record of good/bad task execution
- Correctness – Manual testing of software
- Data Integrity / Provenance – via OSCORE security layer on top of CoAP
- Environment – Wireless medium sensed by IoT operating system
- Assumed to be trusted: Limitation, Execution, Data Accuracy

Matthew Bradbury, Arshad Jhumka, and Tim Watson. Trust Trackers for Computation Offloading in Edge-Based IoT Networks. In *IEEE INFOCOM*, 1–10. Vancouver, BC, Canada, 10–13 May 2021. IEEE. doi:10.1109/INFOCOM42981.2021.9488844.

Limitations

- Evidencing trustiness/trustworthiness can be expensive
  - Especially with limited resources. What is feasible?
- Trustiness/trustworthiness will change over time
  - IoT devices need to keep up-to-date with what state to assign to a trustee
- Bootstrapping trust may require a trusted entity outside of the evaluation framework
  - E.g., Certificate authorities need to be evaluated via other means than a certificate (e.g., the organisation's behaviour and policies – have they had their private keys revealed?)
- Is trust assessment always wanted?
  - Overly constraining in some cases – e.g., preventing open source community adopting abandonware

Conclusions

- Three common issues with trust in the literature:
  1. Definitions are too specific
  2. Systems are designated as trusted based on limited evidence
  3. Measurements of trust are often along a single dimension
- Proposals in this work:
  1. Use a general definition of
     - Trustiness/Trustworthiness (measures)
     - Trusted/Trustworthy (states/labels)
  2. Use attributes to focus the general definitions
  3. Measure the trust attributes along different dimensions

Lancaster University

Thank you for attending, any questions?