Cyber Security Research Centre

Lancaster University

Academic Centre of Excellence In Cyber Security Research

in association with National Cyber Security Centre

Automating Threat Modelling

21st April 2022

Matthew Bradbury

Lecturer in Cyber Security

Introduction

Lecturer in Cyber Security at Lancaster University

Research focus:

- Cyber Security and Privacy
- Computing devices with limited resources (e.g., IoT)
- Context Privacy – How the actions a system takes reveals important information to an adversary

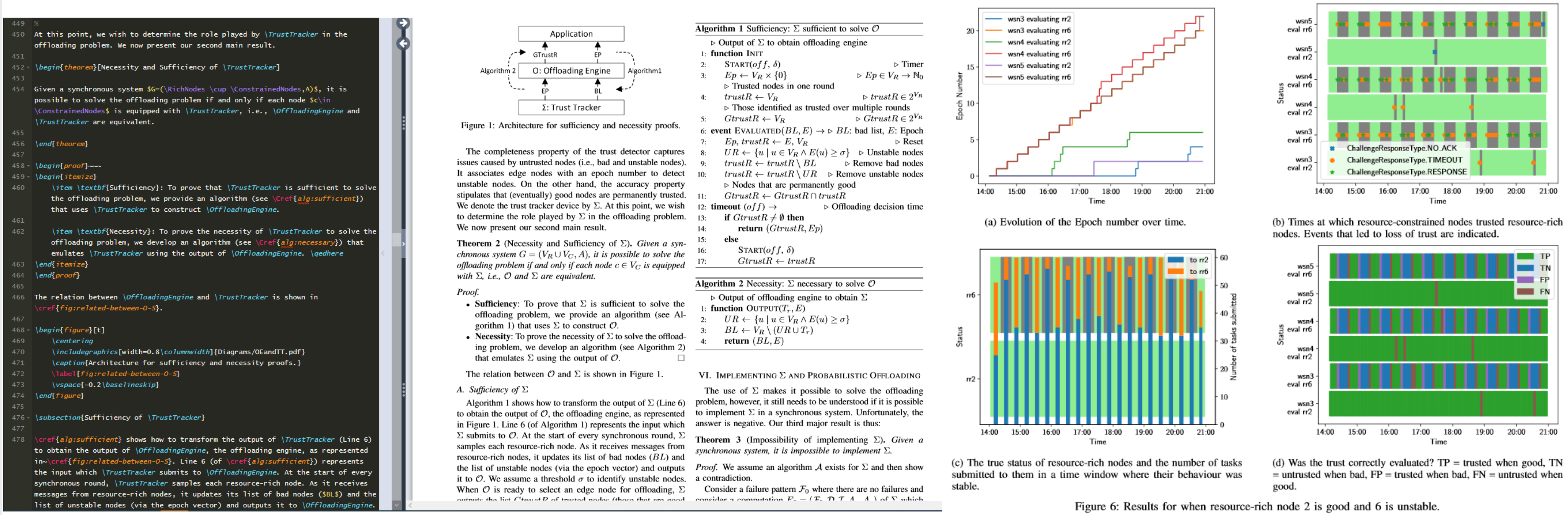
What is Academic Research?

Expectation: Write Code

```c
float calculate_trust_value(edge_resource_t* edge, edge_capability_t* capability)
{
    // Get the stereotype that may inform the trust value
    edge_stereotype_t* s = NULL;
    public_key_item_t* item = keystore_find_addr(&edge->ep.ipaddr);
    if (item != NULL)
    {
        s = edge_stereotype_find(&item->cert.tags);
    }

    float trust = 0;
    float w_total = 0;
    float w, e;

    beta_dist_t temp;

    w = find_trust_weight(capability->name, TRUST_METRIC_TASK_SUBMISSION);
    beta_dist_combine(&edge->tm.task_submission, s ? &s->edge_tm.task_submission : NULL, &temp);
    e = beta_dist_expected(&temp);
    trust += w * e;
    w_total += w;

    w = find_trust_weight(capability->name, TRUST_METRIC_TASK_RESULT);
    beta_dist_combine(&edge->tm.task_result, s ? &s->edge_tm.task_result : NULL, &temp);
    e = beta_dist_expected(&temp);
    trust += w * e;
    w_total += w;

    w = find_trust_weight(capability->name, TRUST_METRIC_RESULT_QUALITY);
    e = beta_dist_expected(&capability->tm.result_quality);
    trust += w * e;
    w_total += w;
```

```python
class Simulator:
    def __init__(self, seed: int, agents: List[Agent], escls, duration: float, utility_targets: UtilityTargets, log_level: int):
        # Initialise the PRNG and record the seed
        self.seed = seed
        self.rng = random.Random(self.seed)

        self.agents = agents
        for agent in self.agents:
            agent.set_sim(self)

        self.es = escls(self)

        self.duration = duration
        self.utility_targets = utility_targets

        self.current_time = 0
        self.queue = []

        self.metrics = Metrics()

        self.log_level = log_level

    def add_event(self, event):
        heapq.heappush(self.queue, event)

    def run(self, max_start_delay: float):
        # Add start event
        for agent in self.agents:
            self.add_event(AgentInit(self.rng.uniform(0, max_start_delay), agent))

        while self.queue:
            item = heapq.heappop(self.queue)

            assert item.event_time >= self.current_time

            # Has the simulation finished?
            if item.event_time > self.duration:
                break

            self.current_time = item.event_time

            item.action(self)
```

Reality: Developing new theory



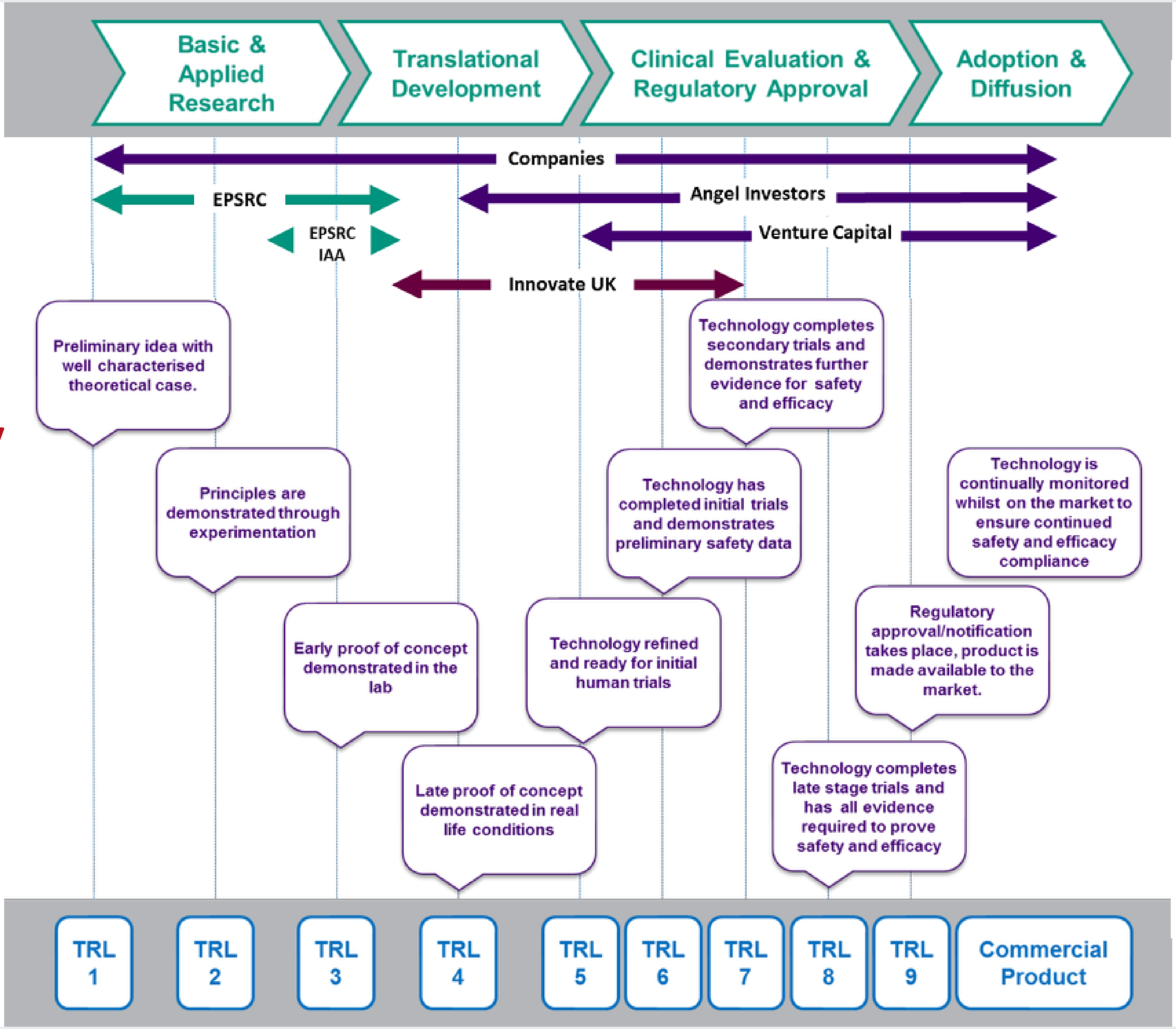
Reality: Experimentation, Outreach, …

Academic Research

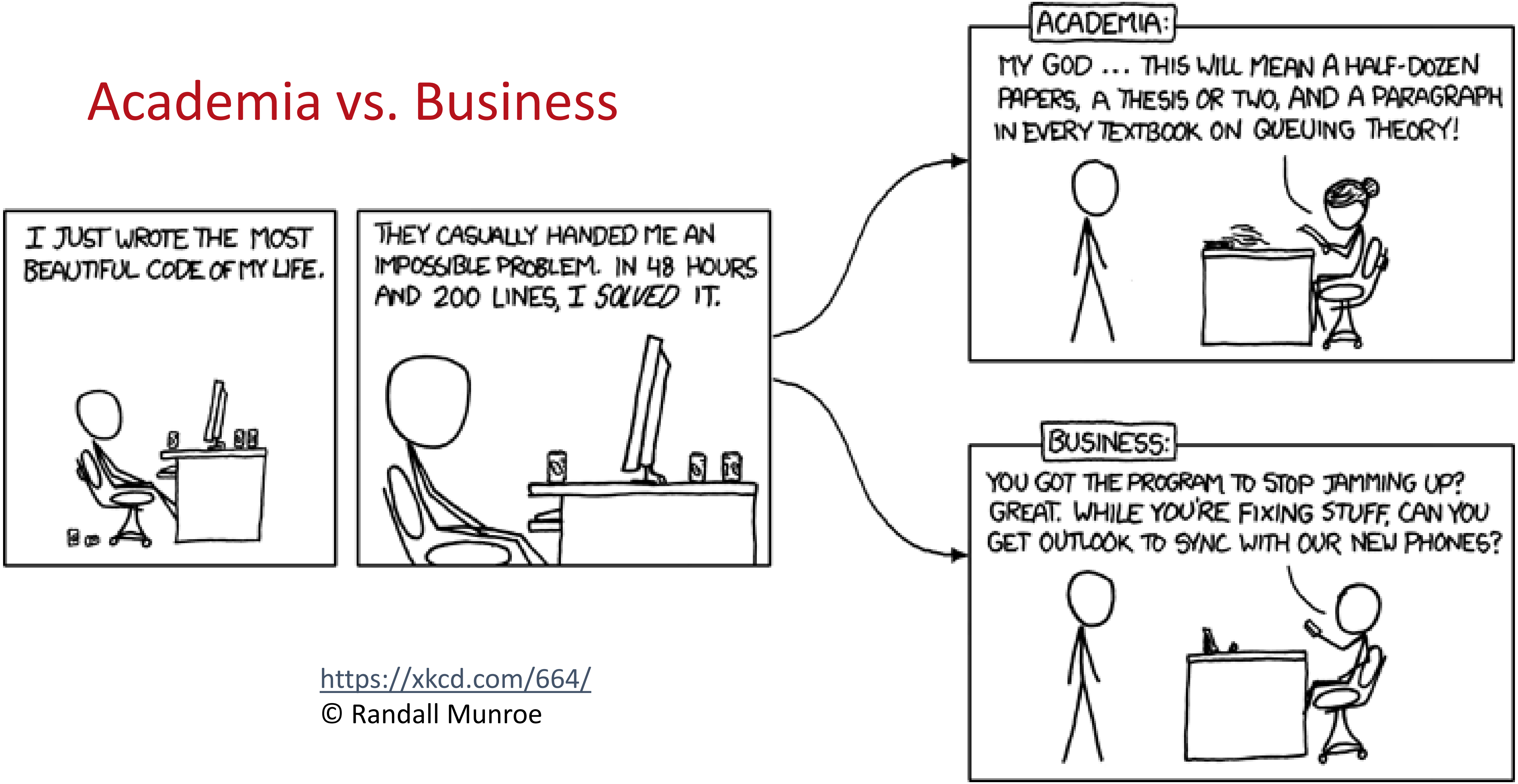
Identify and address **novel** problems

- Novel – a **new** problem, a **new** and **better** solution
- We tend not to focus on engineering activities
- Our work may incorporate building a system, but also:
  - Quantification of security / privacy / performance
  - Formal modelling to prove security / privacy of a system
  - Experimentation and analysis on a system

Technology Readiness Levels



Academia vs. Business



https://xkcd.com/664/

Engaging with Academia

Lancaster University

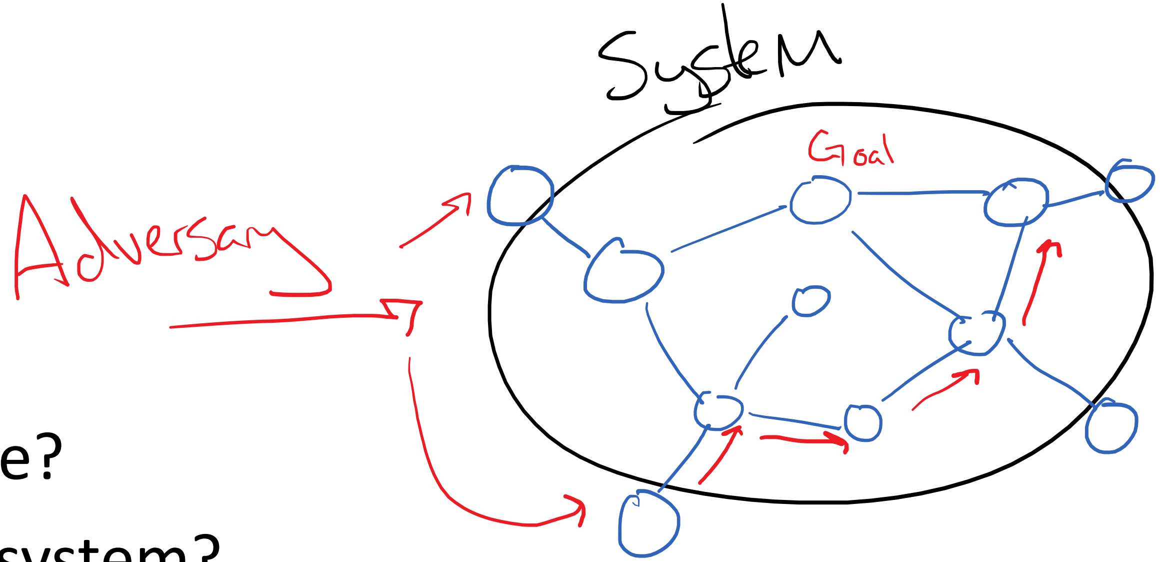
- Student Projects (Both UG and PG)
- Summer internships
- Knowledge Transfer Partnerships & Other Innovate UK Funded Initiatives
- Consultancy
- Contract / Collaborative Research
- CASE Studentship Sponsorship
- PhD students
- & More

Automating Threat Modelling

What is Threat Modelling

You have a system:

- How can an adversary attack it?
- What goals might the adversary have?
- What path does it take through the system?
- How does it compromise different components of your system?



Threat Modelling tends to be Manual

Lancaster University

Define the system

Do you know all components in your system?

↓

What is your adversary, what are their capabilities, TTPs, …

↓

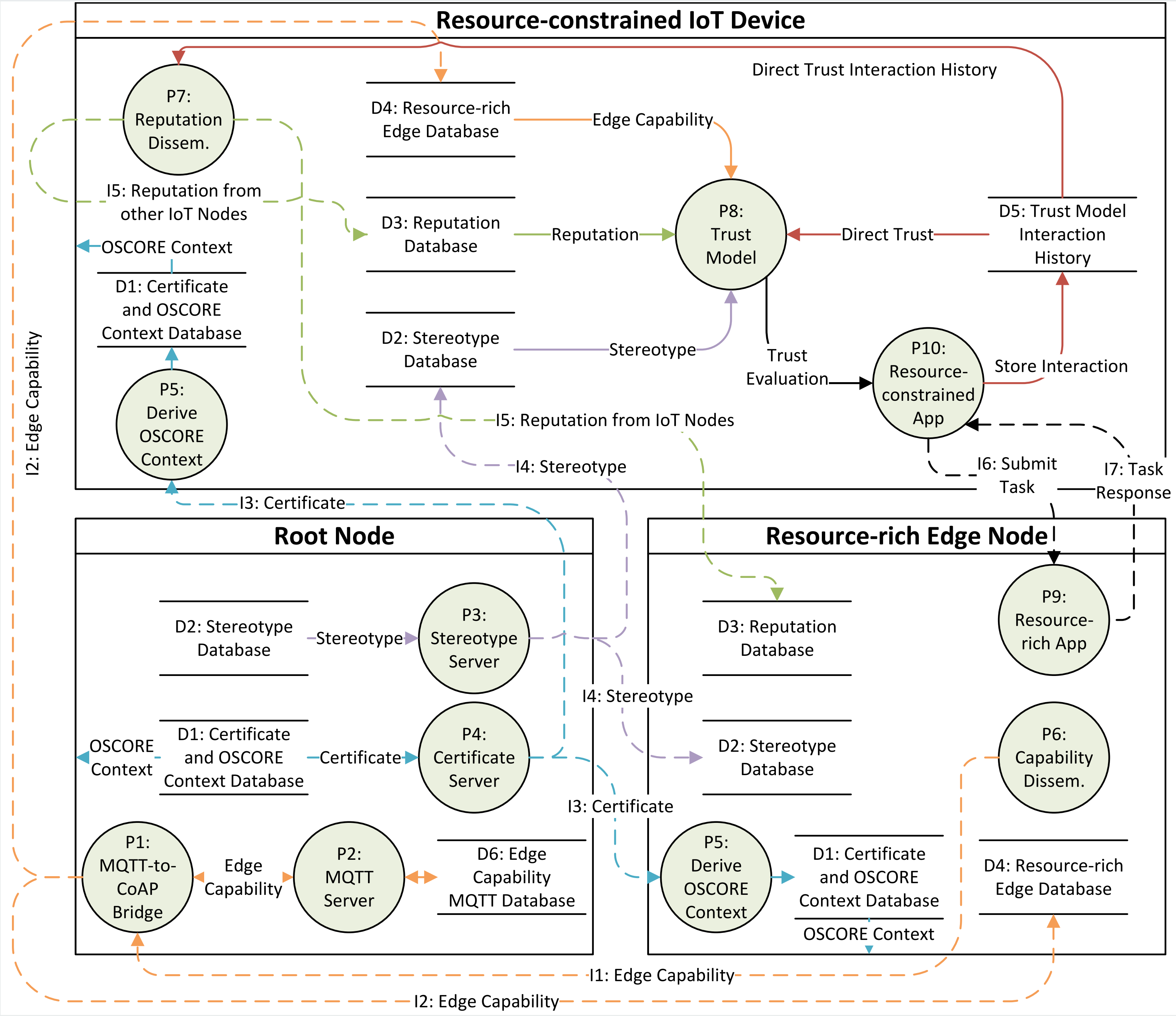
Identify how each component can be attacked

How do you know the component can be attacked in this way?

↓

What path does the adversary take through the system to reach its goal?

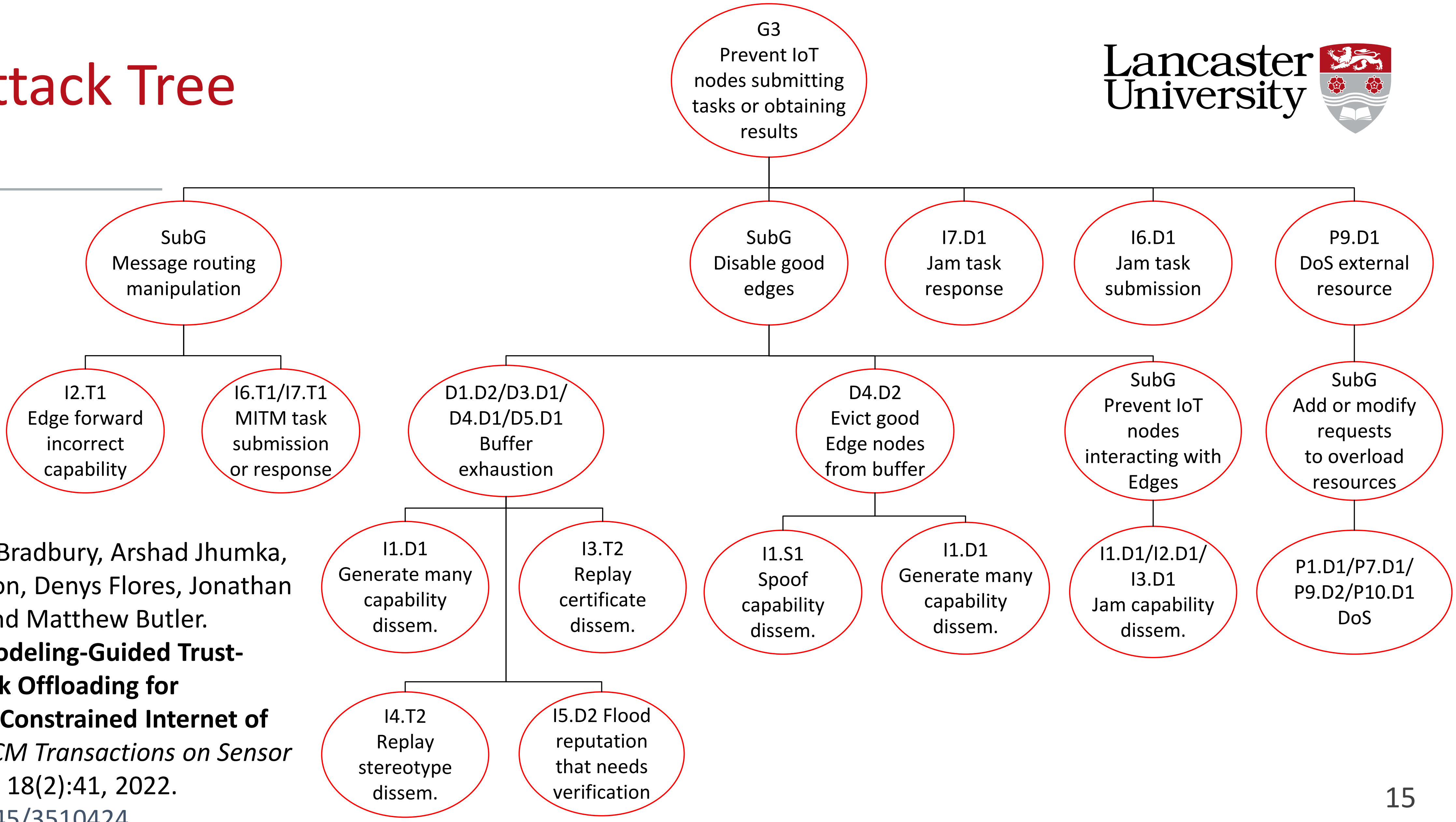
How do you know what an adversary is capable of after a compromise?



Data Flow Diagram

- Resource-constrained IoT devices offloading tasks to resource-rich Edge nodes
- What data is used to assess a measure of *behavioural trust* in an Edge node performing a task?

Attack Tree



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.

Existing Automatic Tools

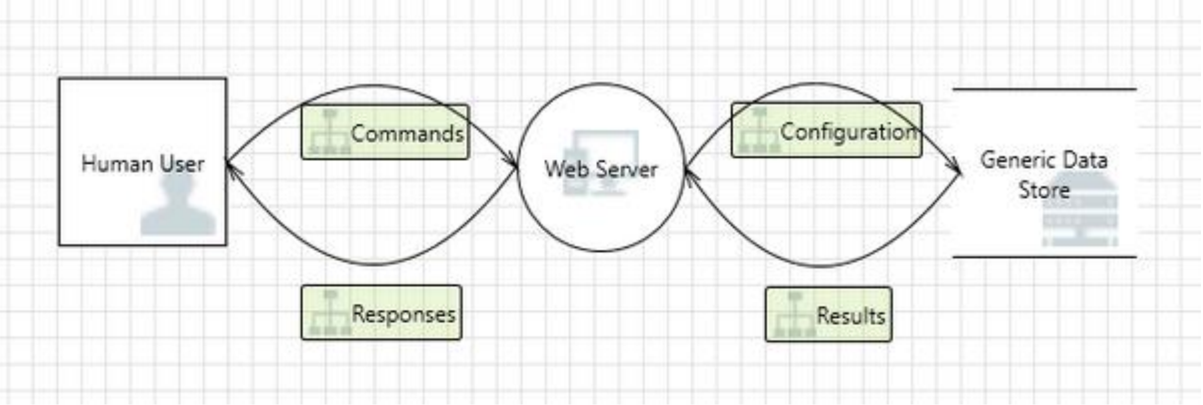
- Automatic threat modelling tools exist!
- Typically aim to solve the problem of:
  "Identify how each component can be attacked"

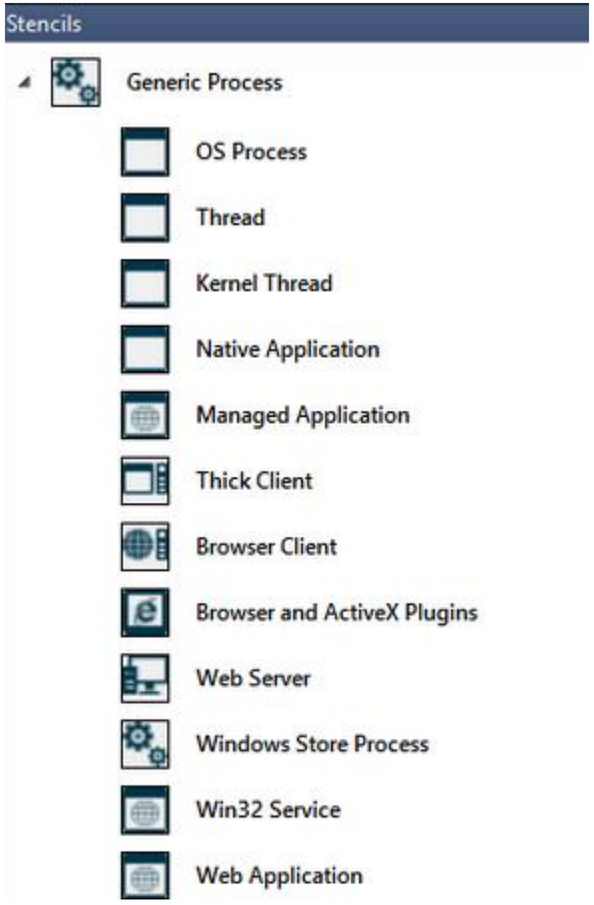
```
"SID": "INP02",
"target": [
  "Process"
],
"description": "Overflow Buffers",
"details": "Buffer Overflow attacks target improper or missing bounds checking on buffer
    operations, typically triggered by input injected by an adversary. As a consequence, an
    adversary is able to write past the boundaries of allocated buffer regions in memory,
    causing a program crash or potentially redirection of execution as per the adversaries'
    choice.",
"Likelihood Of Attack": "High",
"severity": "Very High",
```

https://github.com/izar/pytm/blob/master/pytm/threatlib/threats.json

Existing Automatic Tools

- Typically these tools have pre-defined components
- You can define that these components interact
- The tool then produces threats against individual components





https://docs.microsoft.com/en-us/azure/security/develop/threat-modeling-tool-getting-started

The Problem

- How do we answer:
  “What path does the adversary take through the system to reach its goal?”
- Challenging to do realistically with tools targeting high-level and low-level abstractions

- Do these tools tell us useful information?
- Do they just tell us about known attack vectors instead of discovering new ones?

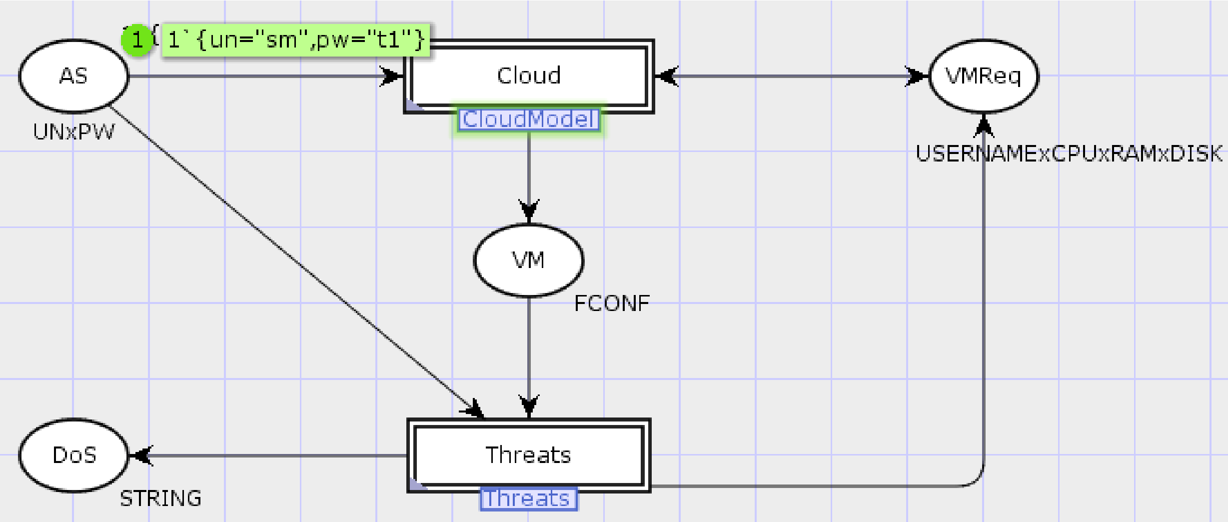
Scope for Academic Research

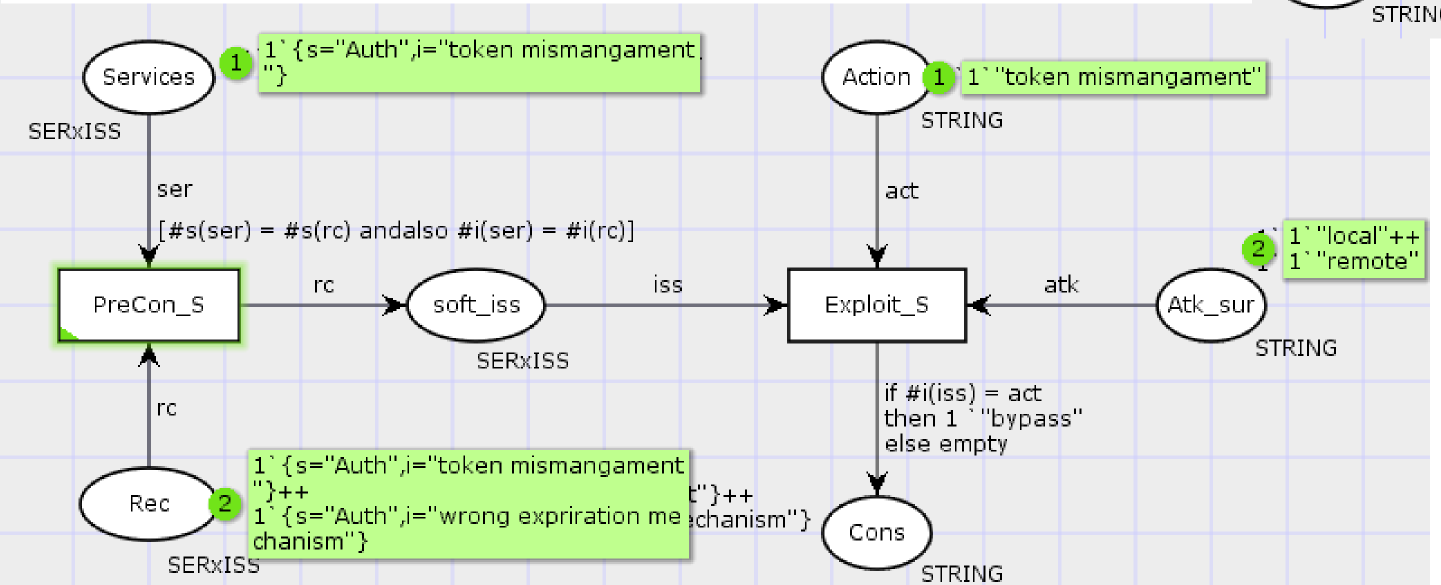
- Research questions:
  - How do we describe a system at the appropriate level?
  - How do we model adversary capability escalation?
  - Can we describe past attacks?
  - Can we speculate on future possible attacks?

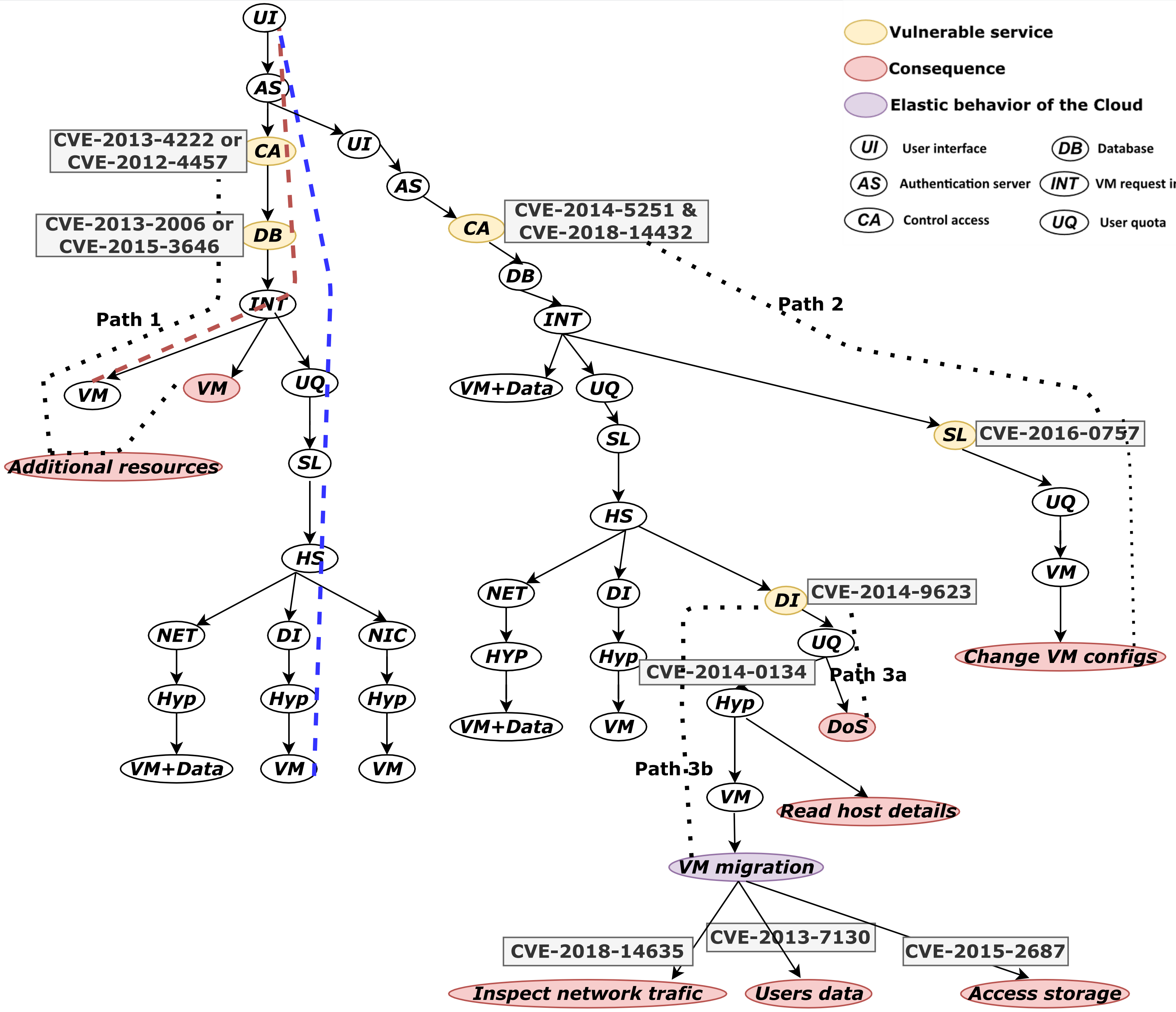
- Make the model arbitrary – suitable for general systems

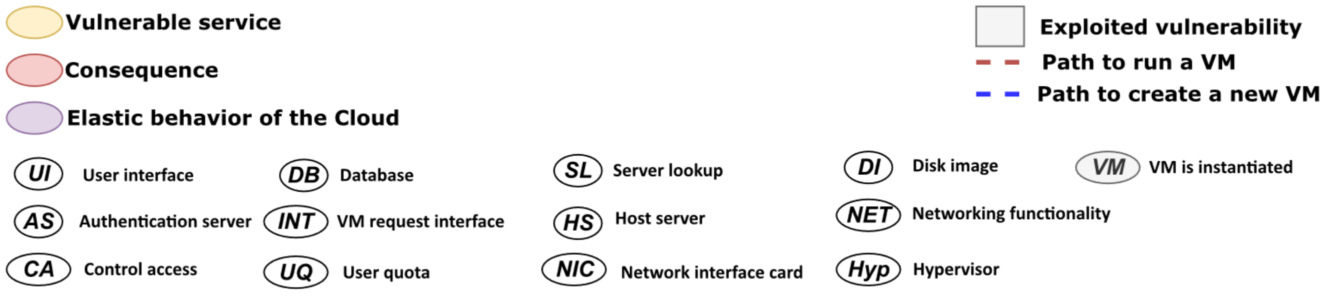
Some preliminary work

Model the system and adversary using Petri nets









- Analyse previous attacks
- Speculate on potential avenues for attack

More to be done

- Research questions:
  - How do we describe a system at the appropriate level? ✓
  - How do we model adversary capability escalation? Not yet
  - Can we describe past attacks? ✓ (partially)
  - Can we speculate on future possible attacks? ✓ (partially)

- The cost of creating these models is high - can we automate this process?
- How can cyber physical systems be considered?

References

- https://www.oreilly.com/library/view/threat-modeling/9781492056546/ch04.html
- https://github.com/threatspec/threatspec
- https://docs.microsoft.com/en-us/azure/security/develop/threat-modeling-tool-threats
- https://github.com/izar/pytm
- https://owasp.org/www-project-threat-dragon/

Thank you for watching!

Dr. Matthew Bradbury

Matthew Bradbury is a Lecturer conducting research into security, context privacy and trust assessment in resource-constrained and distributed systems.

Get in contact via:
https://lancaster.ac.uk/cybersecurity

https://mbradbury.github.io
m.s.bradbury@lancaster.ac.uk