Project Overview

Miguel.Pardal@tecnico.ulisboa.pt

FCT
Fundação para a Ciência e a Tecnologia
MINISTÉRIO DA CIÊNCIA, TECNOLOGIA E ENSINO SUPERIOR

Outline

- Research Context
- Goal
- Work Packages
  - Use Cases
- Expected Contributions

Research Context

- The **scale** and geographic dispersion of the Internet of Things (IoT) will surpass the size of the current day Internet
  - By, at least, **3 orders of magnitude**
- The IoT will be the largest and most widely distributed system ever, with a multitude of connected sensors and actuators
- The current Internet already has some serious, unresolved security issues
  - Adding physical world connections brings even more concerns about **attacks** and their consequences to **people** and **goods**

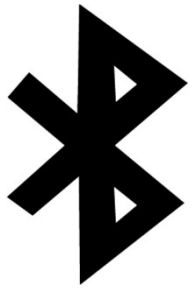
Location

- Location Based Services (LBS) provide geographic or topological context to mobile applications
  - To Internet of Things applications
- Usually the location is detected by the device and then trusted by the applications
- It is in application's self-interest to trust the location data
  - Example: Car Navigation
    - Detect geographic location,
    - Retrieve map for coordinates,
    - Display map

Location Estimation Techniques

GPS

Wi-Fi



Bluetooth

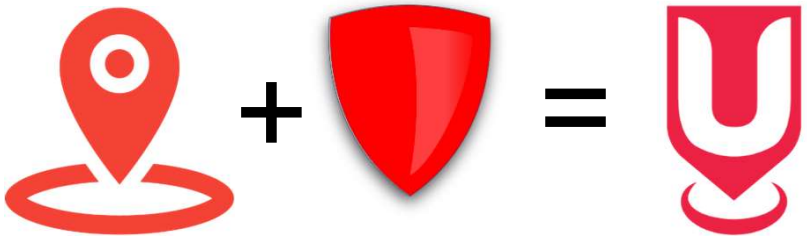
…

Location Proofs

- There are instances where we want to be **sure** the **thing** is there
  - Is the thing really at the claimed location?
  - The location of the device must be proved!

- This way, the device location can be a certified attribute
  - That can be used for making security policy decisions

- Analogy: as **identity** needs **authentication**, **location** needs to be **proven**
  - Challenge-response



Goal

- The project **goal** is to provide a flexible **framework** to support creating and validating location of devices using **diverse** techniques

- Create and validate location proofs
  - Devices can certify their location or ask for location certificates from other devices
- Proofs can be used to make security decisions
  - E.g. trustworthy attributes for policy decision in ABAC solution
- For Internet of Things applications:
  - Mobile devices (human interaction)
  - Limited devices
  - Smart Spaces

Example

- **Smart Doorbell**
  - Set of sensors used for controlling access to a home
  - Before accepting commands – *open door!*
    or responding with data – *sensitive!*
    - Can obtain proof of its location or
      can request proof of location to other devices

Location certificates

- The location certificates issued using the SureThing framework contain:
  - location data, obtained and verified using one or more techniques
  - locality-sensitive network measurements, using WiFi and Bluetooth fingerprinting, and ambience sensing

Idea

- Turn the heterogeneity of the IoT – complex systems, with large attack surface – into a security advantage
  - Observe unique features of each location and capture its specific traits
  - Compare against pattern or witness

Ecosystem Access Control	Device Memory	Device Physical Interfaces
Device Web Interface	Device Firmware	Device Network Services
Administrative Interface	Local Data Storage	Cloud Web Interface
Ecosystem Communication	Vendor Backend APIs	Third-party Backend APIs
Update Mechanism	Mobile Application	Vendor Backend APIs
Network Traffic		

Challenge-Response for verifying presence at location

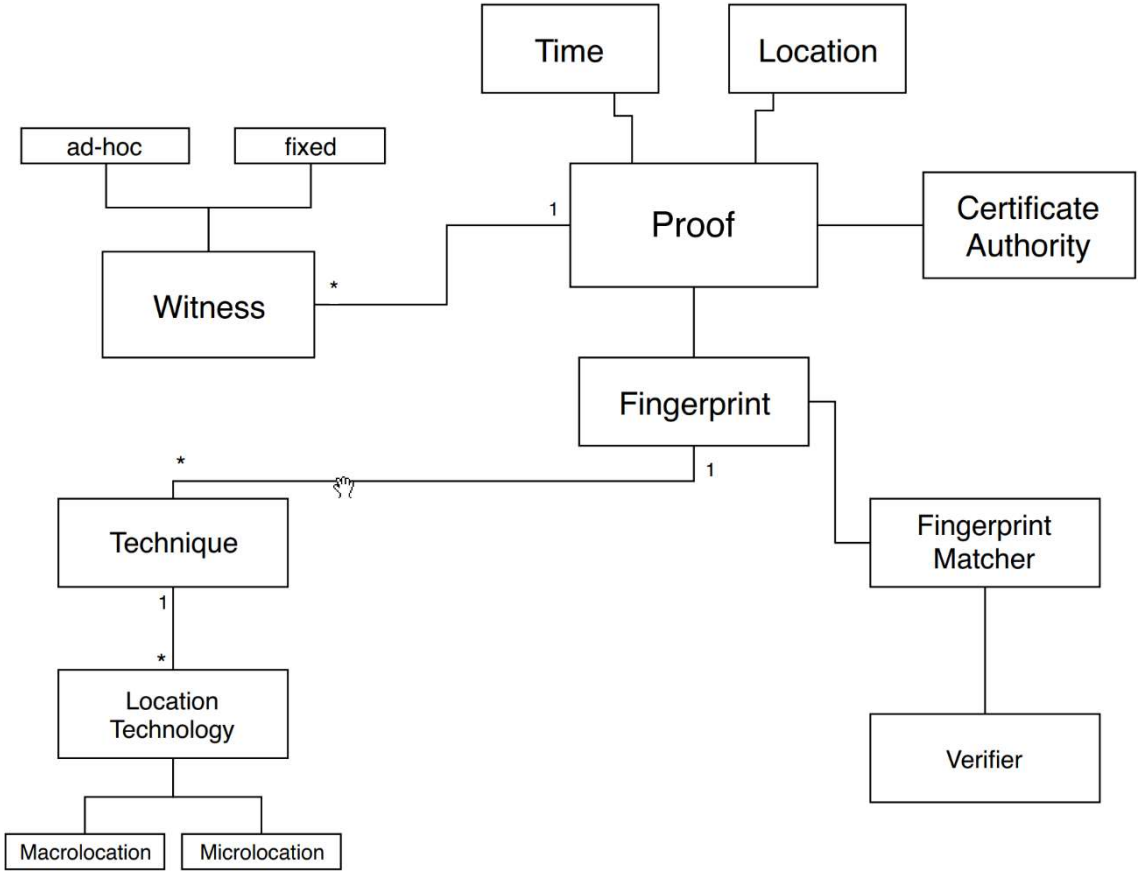
- If devices could talk, it would be something like:

- "Hey, X, if you are really at location Y as you claim, then…
  - tell me signal strengths from all nearby devices!
  - tell me the level of ambient noise for the past 3 seconds!
  - tell me …

Why do we need a framework?

- Extensibility
  - Allow for the novel techniques developed in this project or by the research community to be integrated as they appear
- Diversity
  - Allow the combination of different techniques to provide stronger proofs
- Flexibility - developers can choose between:
  - Faster location proofs vs more elaborate and reliable proofs
  - Single or multiple techniques
  - Witnesses from deployed infrastructure or found at the moment (ad-hoc)

Conceptual model



Witnesses and beacons

- Beyond the uniqueness of locations, the security model of SureThing is reinforced with **witness** models
  - Someone can say what they saw
  - Ad-hoc (circumstantial) witness
- **Beacons**
  - Add more information to allow more unique fingerprints
  - Transmit sequences generated from secret seed
    - Usually time-bound
  - Ask of prover (and witnesses) to capture the signal
  - The verified can then check if the transmission was correctly received
  - And make the assumption that the device was there

Use Cases

- This project will validate its contributions using two use cases:
- **Smart Tourism**
  - Key economic sector in Portugal
  - Build an application providing tourists with awards for each visit to a predefined set of locations, making use of reliable fast location proofs
  - Use existing infrastructure
- **Smart Taxes / Inspections**
  - Use dedicated infrastructure and agents
  - Intended to be collusion-resistant
  - Stronger proofs: combine the locations proofs with digital notaries
    - with time-stamping
    - long-term archival

Work Packages (WP)

- WP1: API Interfaces and Data Schemas
  - To be completed
- WP2: Witness models
  - Working prototypes for ad-hoc and trusted witnesses
  - Missing: integration with identity providers
- WP3: Location Proof Techniques
  - Wi-Fi, Bluetooth
  - To explore: Cellular, GPS, ambient sensing

Work Packages (cont.)

- WP4: Smart Tourism Use Case
  - Working prototype for city trek
- WP5: Distributed Proof Ledgers
  - To be developed
- WP6: Smart Taxes Use Case
  - Working prototype for vehicle inspection

Support WPs

- WP7: Impact and Outreach
- WP8: Project Management

Expected Contributions

- Novel research is needed to enable secure location proofs for the IoT

- Location you can **trust** and **verify**
  - The widespread use of SureThing location proofs will significantly improve the security decisions of policies for the IoT.
  - This will lead to more secure and trustable services in the near future

Summary

- We expect location proofs to be used in the Internet of Things as much as digital certificates are part of every web site that we visit today
- Open framework will make state-of-the-art techniques available and will be extensible to incorporate new techniques as they become available
- Tested in useful applications
  - Provide value
  - Comply with security practices in place today
  - Produce proofs suited to the use case requirements

What's next?

- Let's hear from the team!

- **Use case talks**
  - Rui Claro
  - Henrique Santos


- **Work-in-progress talks**
  - João Tiago
  - João Costa



surething
inesc id
lisboa
20
YEARS
DEFINING TECHNOLOGY
Thank you!
This work is supported by national funds through Fundação para a Ciência e a Tecnologia (FCT) with project reference PTDC/CCI-COM/31440/2017.