surething

Project Overview

Miguel.Pardal@tecnico.ulisboa.pt

inesc-id.pt

Systems @ inesc id lisboa 20 YEARS

DEFINING TECHNOLOGY

The **D**istributed, **P**arallel and **Secure** **S**ystems Group of INESC-ID

Miguel L. Pardal

- *PhD* (2014)
  - Scalable and Secure RFID data discovery
- *Researcher* at INESC-ID
  - Distributed Systems Group
    - Cybersecurity
- *Guest Scientist* at TUM (2018)
- *Assistant Professor* at Técnico Lisboa
  - Tenure (2019)

Project facts

- Proposal submitted April 2017
- Funded by the Portuguese national funding agency for science, research and technology (FCT)
  - Reference No. PTDC/CCI-COM/31440/2017
- Project officially started October 2018
  - Duration: 3 years
  - Total budget is € 238K
- Web site:
  - http://surething-project.eu

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

Team

- Current
  - Rui Claro (PhD Candidate)
  - João Tiago (MSc Candidate)
  - João Costa (MSc Candidate)



- Soon
  - 2 Post-Docs

Outline

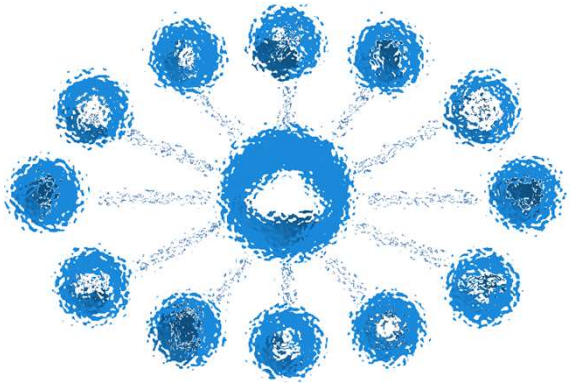
- Research Context
  - Our idea
  - Project goal
- Work Packages
- Use Cases
- Expected Contributions

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

Security challenges

- The current Internet already has some serious, unresolved security issues
  - Adding physical world connections brings even more concerns
  - **Attacks** and their consequences to **people** and **goods**



Our Idea

- Turn the heterogeneity of the IoT
  – complex systems, with large attack surfaces –
  into a security advantage

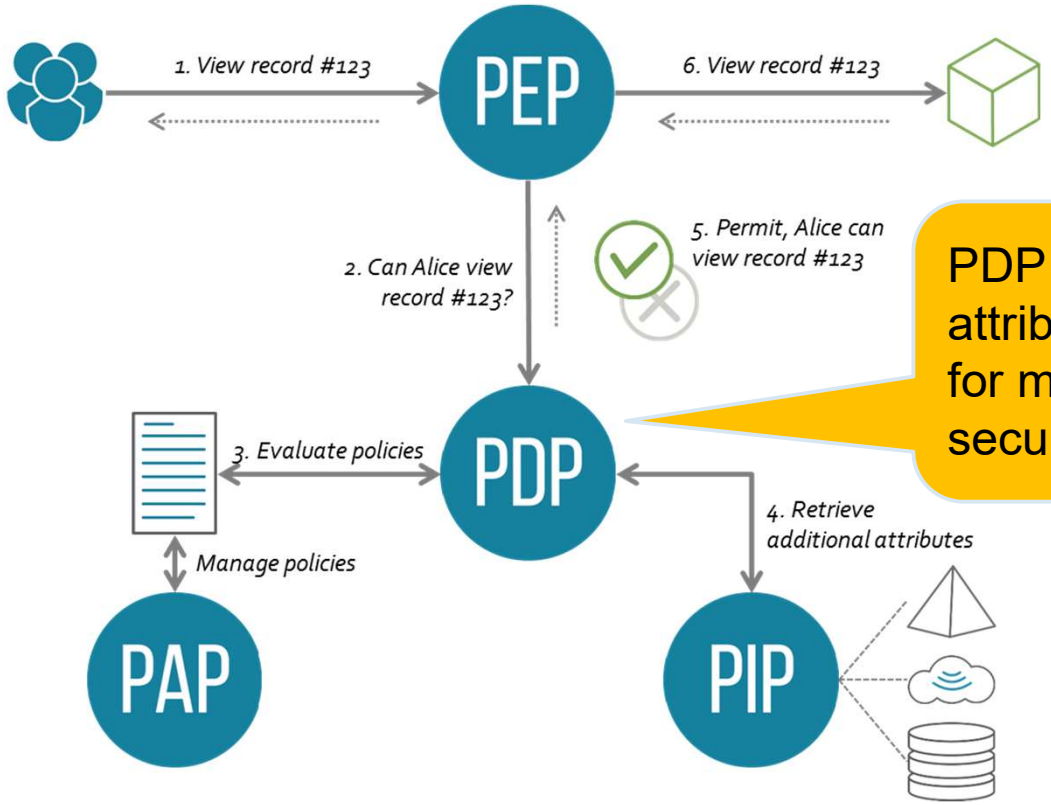
Ecosystem Access Control	Device Memory	Device Physical Interfaces
Device Web Interface	Device Firmware	Device Network Services
Administrative Interface	Local Data Storage	Cloud Web Interface
Ecosystem Communication	Vendor Backend APIs	Third-party Backend APIs
Update Mechanism	Mobile Application	Vendor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

Externalized security

- Unify the security management across applications
  - Business rules applied consistently and can change dynamically
- Externalized security encompasses:
  - User management
  - Authentication
  - Authorization
  - Logging and auditing

- Policy Points architecture [RFC 2753]
  - P**A**P – Administration, P**E**P – Enforcement, P**D**P - Decision

Example of authorization flow



PDP requires trusted attributes **e.g. location** for making good security decisions!

By **Axiomatics** - Axiomatics, CC BY 3.0, https://commons.wikimedia.org/w/index.php?curid=48397652

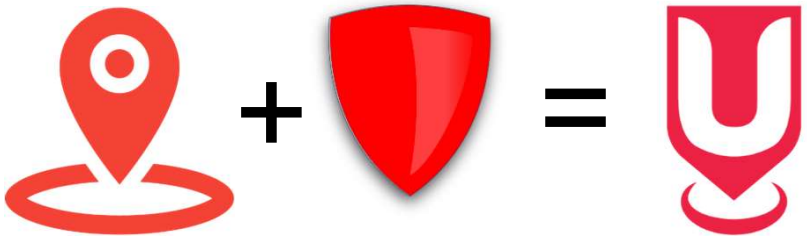
Location attribute

- Location Based Services (LBS) provide geographic or topological context
  - To mobile applications
  - To IoT services
- Usually the location is detected by the device and then trusted by the applications

Location proof

- In some cases, 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
- Device location can be a certified attribute
  - And be used for making security policy decisions

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



Location use example

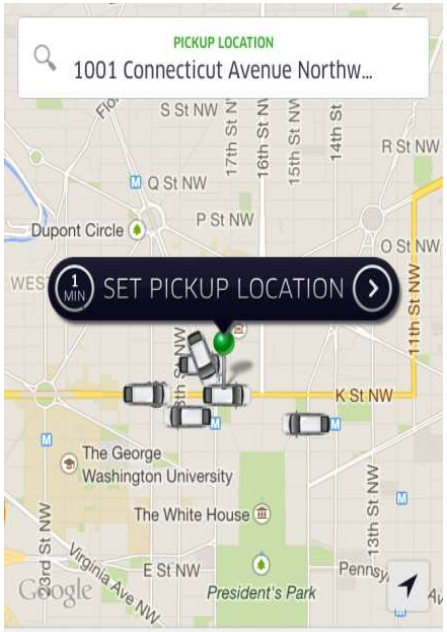
- Car navigation
  - Insert destination
  - Detect geographic location
  - Retrieve map for coordinates
  - Display map, plot path

- Committed resources belong to the user
  - It is in user's self-interest to trust the location data of its device

Location proof use example

- Hail a cab
  - Insert destination
  - Detect geographic location
  - Insert pickup location

- Committed resources belong to the cab
  - An attacker may spoof user locations



Challenge-Response to prove presence

- *Peggy* (Prover)
- *Victor* (Verifier)
- *William* (Witness)

- "Hey, *Peggy*, if you are really at location X, right now, as you claim, then…
  - tell Victor what are the signal strengths from all nearby devices!
  - tell Victor the level of ambient noise for the past 3 seconds!
  - ask William to testify he is seeing you, and tell Victor
  - tell Victor …

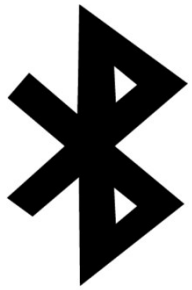
Location certificate

- The location certificate contains:
  - Claim
  - Evidence
  - Testimonies
  - Digital signature by Prover

Location evidence collection goes beyond GPS…

GPS

Wi-Fi



Bluetooth

Ambient Sensing

Etc…

IEEE 802.15 WPAN UWB

Location certificate details

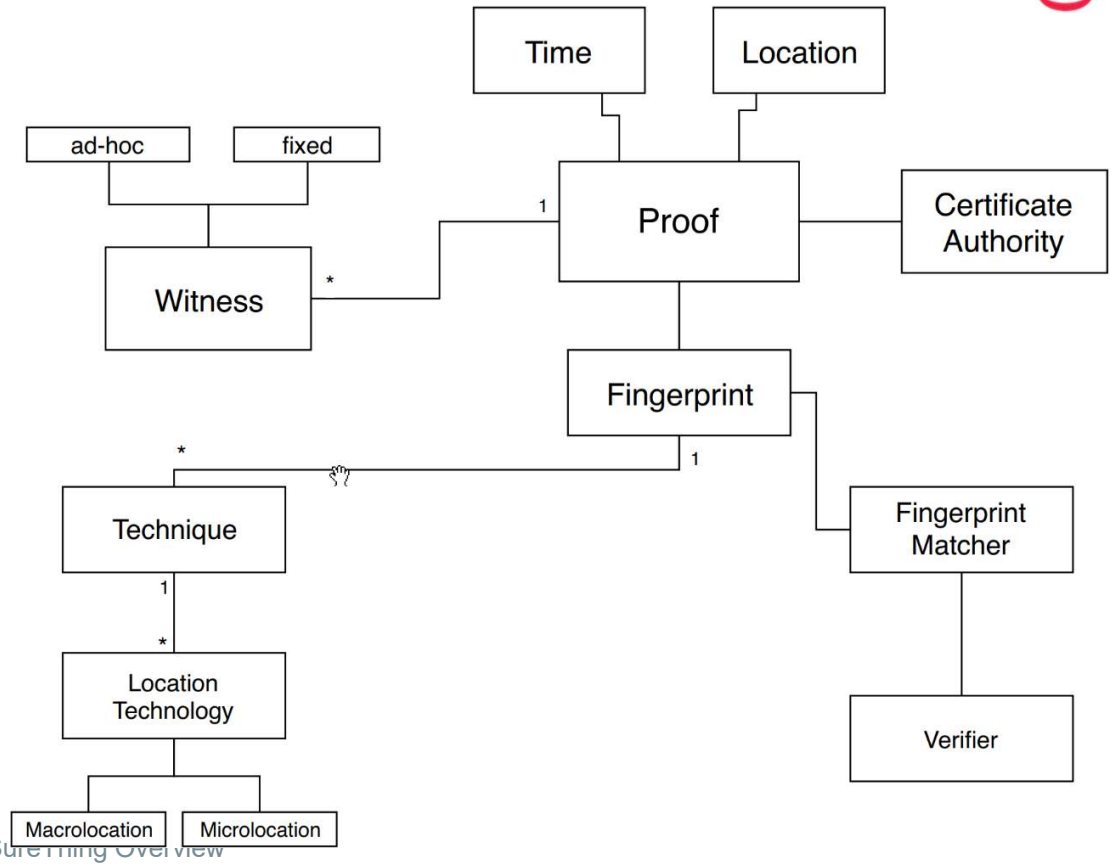
- Location claim is made by the Prover
  - *“I am at location X at time T”*
- Evidence was collected at time and place
  - Using diverse techniques
- Testimonies are made by other devices
  - *“I saw the Prover at location X and time T”*
  - Witness signs the testimony
- Digital signature asserts identity of Prover

Project goal

- Provide a flexible framework to support creating and validating location of devices using diverse challenge-response 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

Conceptual model



Witness

- Something that can testify and say what it saw
  - Ad-hoc (circumstantial) witness
  - Trusted witness

Beacon

- When location does not have enough “uniqueness”
  - Or does not change with desired time granularity
- Solution: Transmit unique data sequences
  - Generated from secret seed e.g. TOTP
  - Ask prover to capture the signal
- Alternative: transmit random data
  - Ask prover and witness to capture the signal

- Verifier can check if the transmission was correctly received
  - Assume the device was at location in the specified time-window

Use Cases

- This project is validating its contributions with 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.)

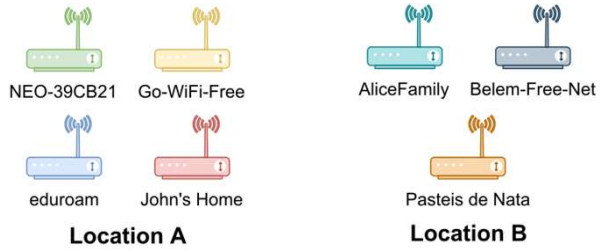
- WP4: Smart Tourism Use Case
  - Working prototype for city trek
- WP5: Distributed Proof Ledgers
  - To be developed
- WP6: Smart Taxes Use Case
  - Working prototype for vehicle inspection

What have we done so far

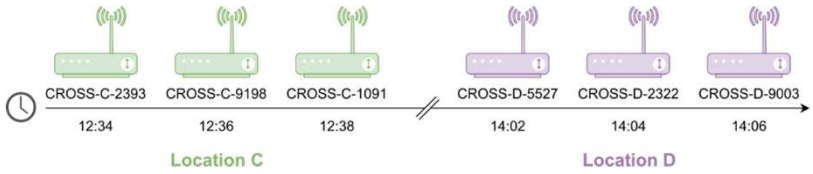
- CROSS – Smart Tourism Application – City trekking
- STOP – Smart Taxes – Vehicle inspections
- Other works in IDS for IoT (not presented)

CROSS location proofs for smart tourism

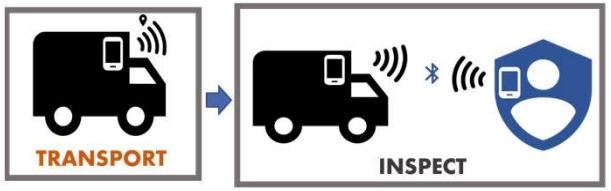
- Rewarding tourists for their visits to city locations
- Location proofs using Wi-Fi Scavenging
  - Scan existing, 3rd party Wi-Fi networks



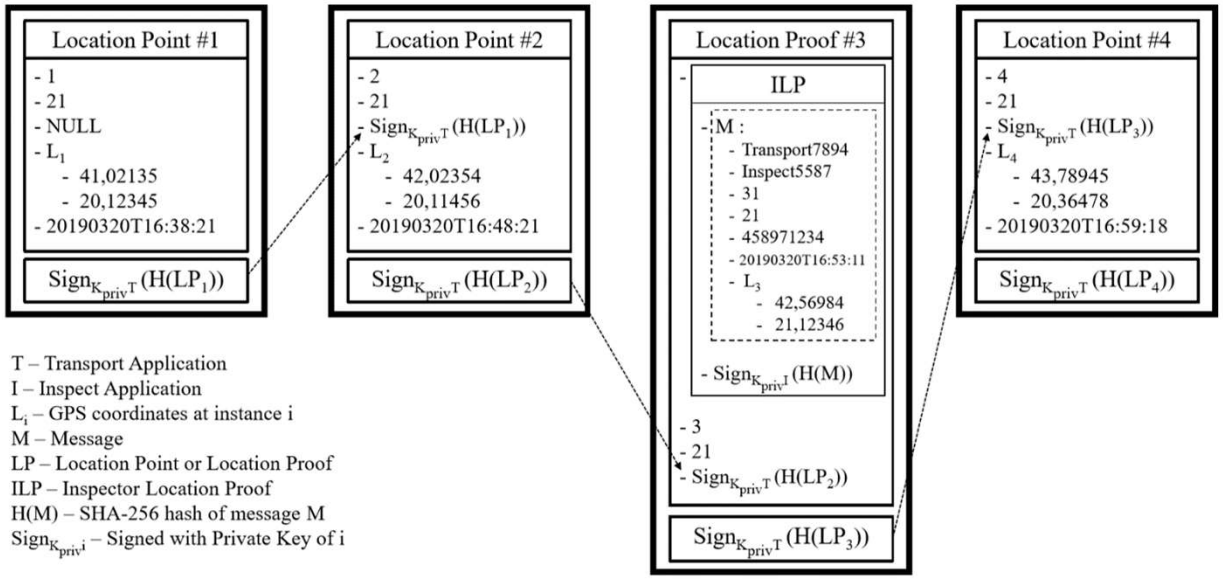
- Stronger proofs with Wi-Fi AP TOTP
  - (Time-based One-Time Password)



STOP Secure Transport lOcation Proofs



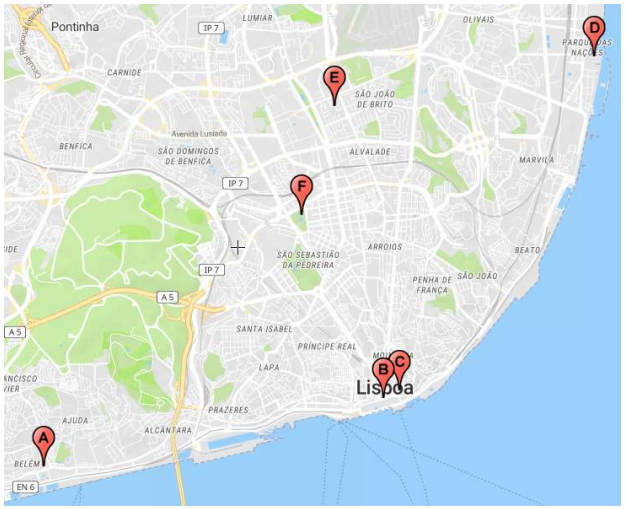
- **Vehicle** and **Inspector** apps
- Central ledger
- Location chain: events and witnesses



What are we doing now

- Wi-Fi scavenging for proofs
- Composite proofs in smart spaces
- Privacy protections
- (Framework libraries)

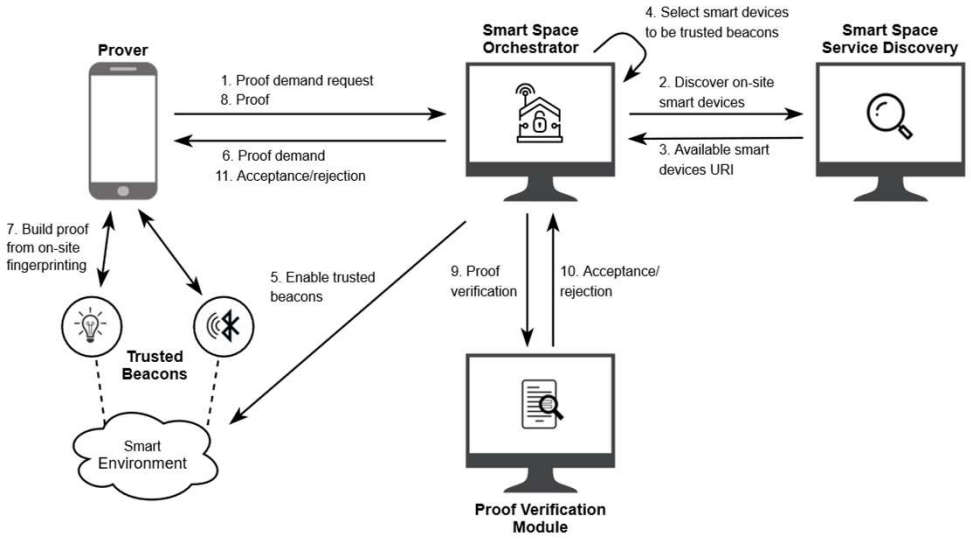
Wi-Fi scavenging



- Compiled Wi-Fi traces
  - Various points of interest in the city of Lisbon
  - Compiled traces into a dataset
- Extend the scavenging method of CROSS (Smart Tourism)
  - To provide time-bound location proofs
- Use the diversity of Wi-Fi networks observed in the dataset
  - **Stable networks** (trigger) to determine **location**
  - **Volatile networks** (hotspots) to determine **time** window

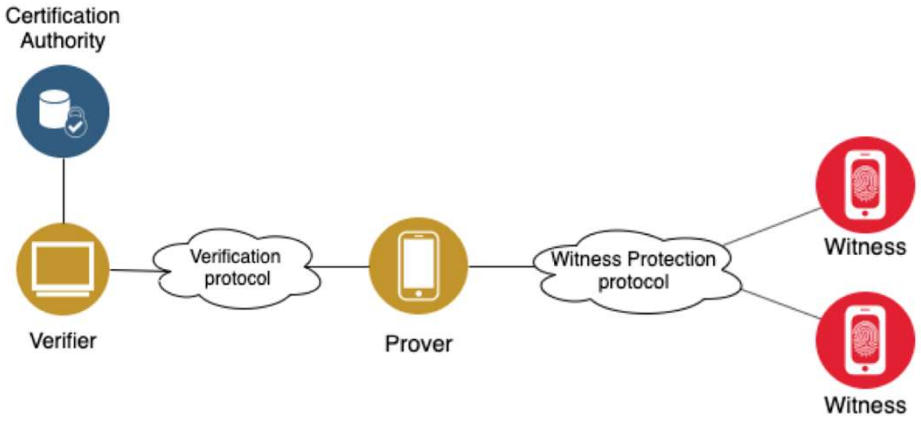
Composite proofs in smart spaces

- Leverage instrumented smart devices as trusted beacons
  - Use a smart space management framework to discover, configure and control them
- Use case: hospital cleaning verification (robots or humans)



Privacy protections

- **Witness Protection protocol**
  - Differential privacy
  - Geo-Indistinguishability
    - Location clustering



Why a framework?

- Interoperability
  - Proof formats and interpreters
- Extensibility
  - Allow novel techniques to be integrated as they appear
- Diversity
  - Combine different techniques to provide stronger proofs
- Flexibility
  - Choice of faster proofs vs more elaborate and reliable proofs
  - Single or multiple techniques
  - Beacons and/or witnesses

Expected Contributions

- Novel research needed to provide trusted attributes for effective IoT security policy enforcement
  - SureThing: location you can **trust** and **verify**
- Framework will make state-of-the-art techniques available
  - Extensible to incorporate new techniques as they are available
- Validated in useful applications
  - Produce proofs suited to the **use case** requirements


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.

Visit us in Lisbon

TÉCNICO LISBOA

Use case suggestions

- Propose innovative use cases for location proofs
  - What is the business context for the use case ?
  - What is the business process being improved ?
  - Who are the people/stakeholders involved ?
  - What will be the benefits of using location proofs?
  - What are the risks of using location proofs ?

- https://tinyurl.com/surething-use-case