RSAConference2016

San Francisco | February 29 – March 4 | Moscone Center

Connect to Protect

SESSION ID: IDY-R02

Doing Something Smart with All the Smart Things

Andrés Molina-Markham

Visiting Scholar
Dartmouth College

Kevin Bowers

Manager
RSA Labs

#RSAC

Smart cars, homes, buildings, cities

LOCATION OF STOP
250 FEET

ASSIGNED PATROL SQUARE

TOP CRIME RISKS

1 AGGRAVATED ASSAULT
2 GUN CRIME
3 BURGLARY
4 LARCENY
5 SIMPLE ASSAULT

Digital environments

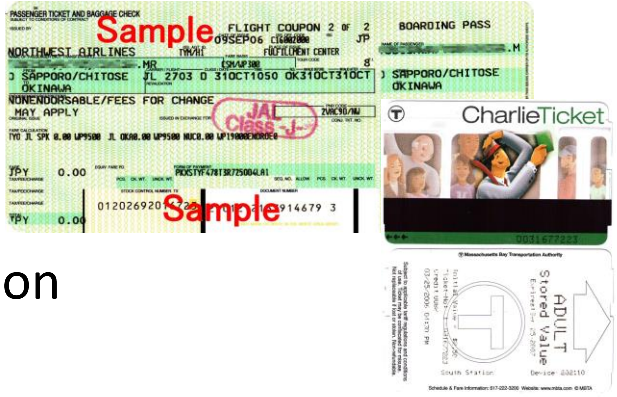
Digital environments for access management

- This talk explores how to leverage digital environments for access management
- Smart objects can provide:
  - Context
  - Feedback
  - Enforcement

Access Management and Authentication

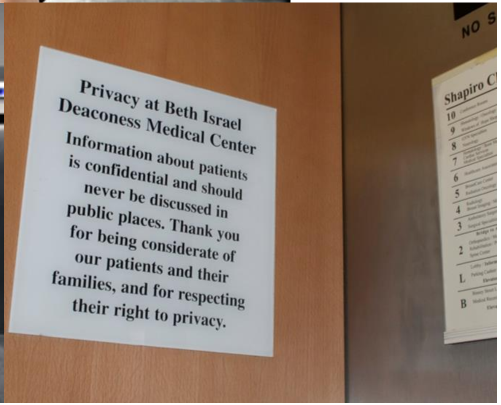
- Authentication
  - Validating that the claimed identity is accurate

- Access Management
  - Given an authenticated identity, determining what resources can be accessed
  - Sometimes does not require authentication



Issues with access management

- Access is often “all or nothing”
  - Rarely contextual
  - Users are trusted to do the right thing
- Contextual AM would be difficult to configure
- Usability is often as important as security



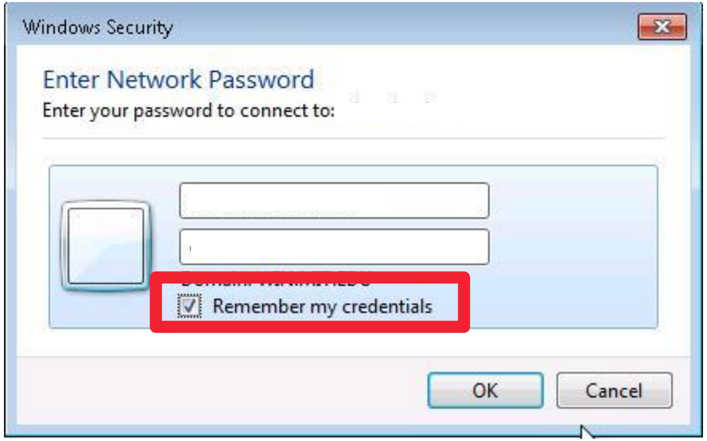
Privacy at Beth Israel Deaconess Medical Center

Information about patients is confidential and should never be discussed in public places. Thank you for being considerate of our patients and their families, and for respecting their right to privacy.

NO S
Shapiro C

To remember or not

- Access control and authentication are typically all-or-nothing (there is no room for shades of gray)
- Strong authentication is rarely user-friendly
- This leads to two options
  - Remember my credentials
  - Re-enter my credentials
- Poor usability often results in less security



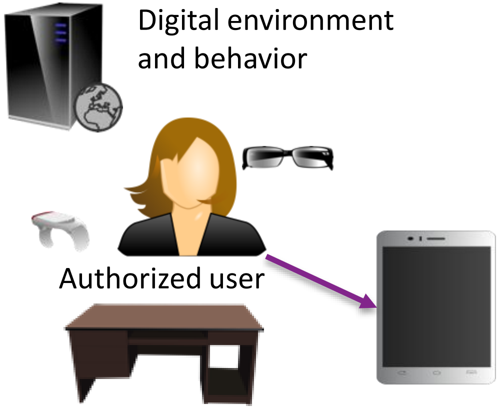
Windows Security

Enter Network Password

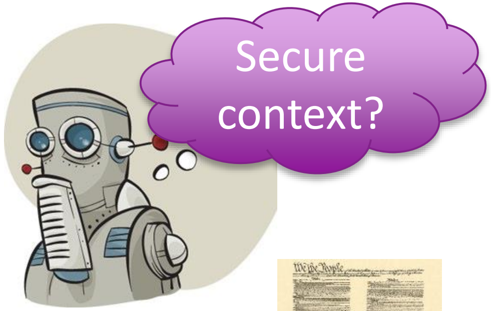
Enter your password to connect to:

☑ Remember my credentials

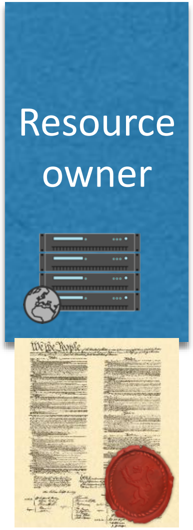
Key ideas



Utilize smart objects in an individual's environment to provide context and enforcement in access management decisions



The conditional access response may contain cryptographic material requiring the involvement of specific smart objects



Security Challenge

- Context and behavior should not guarantee access: prior research has proposed alternate authentication-like methods (behavioral biometrics, context-based risk assessment)
- Access management flexibility should be hard to exploit

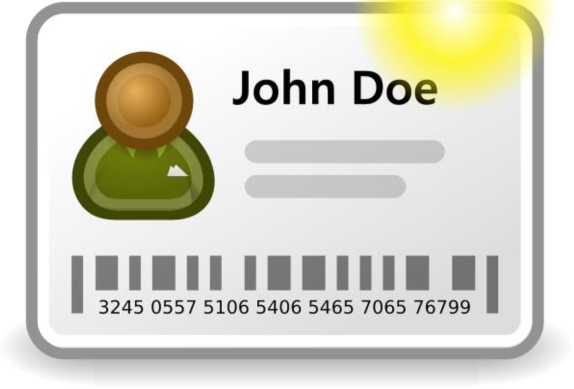
Usability Challenge

- Granular context-aware decisions should require minimal configuration by the user
- Recommendations should adjust to new user behavior
- Solution should accommodate complex scenarios and trust relationships

vs

Use cases

- Access to corporate resources



- Use of in-home systems (i.e. TV programming)

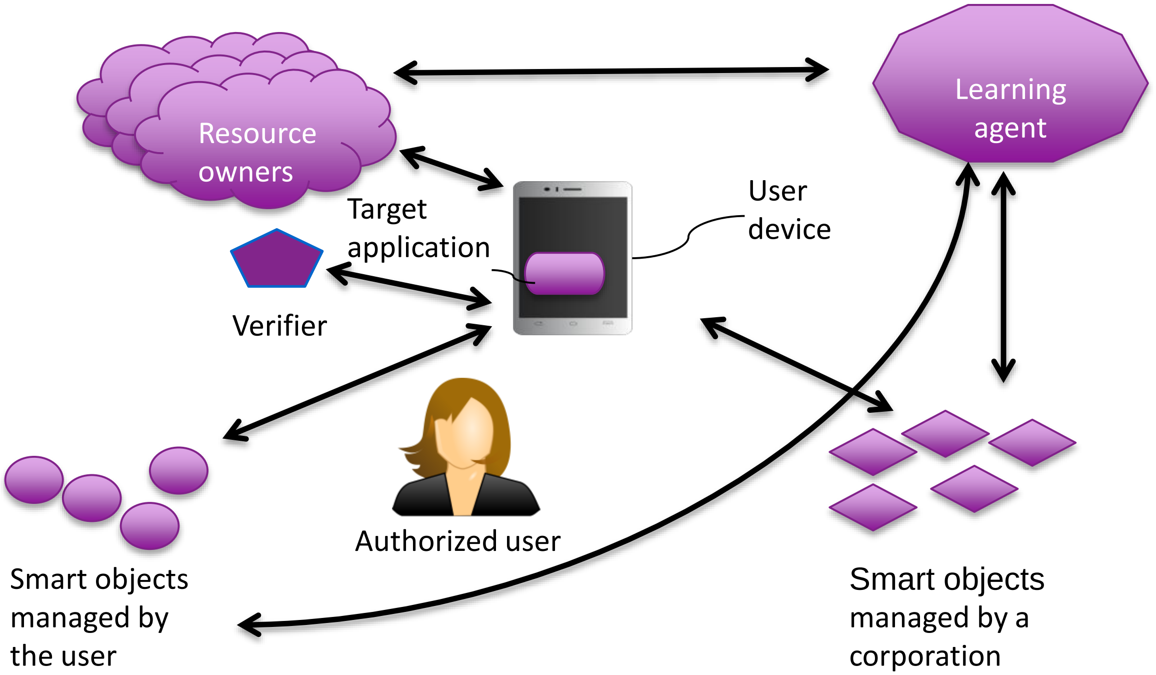
- AM in partially-trusted environments (i.e. subscription service in a hotel room)

A guardian angel

- If we are going to create more granular controls that we expect to change frequently (multiple times per day), we do not want a person to have to manage that
- We need an agent, acting on a user's behalf, adjusting access management and permissions for them
  - A guardian angel, following them wherever they go and protecting them from threats

Active Environments

Active environments



“What is around you”:

Active Environment *unlocks* a device or application when the authorized user---with the device---is near a set of active smart objects (SOs)

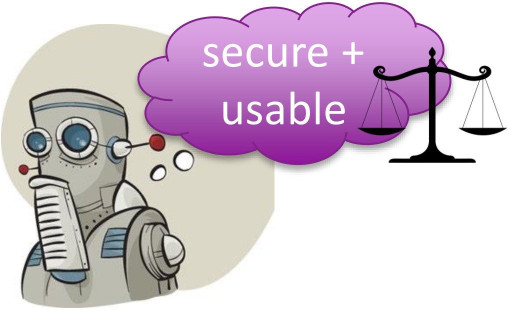
- Smart objects only activate when their activation is consistent with access control policies
- The agent that activates SOs learns an activation strategy that **optimizes** security and usability
- The agent does not learn the access keys

Key benefits:

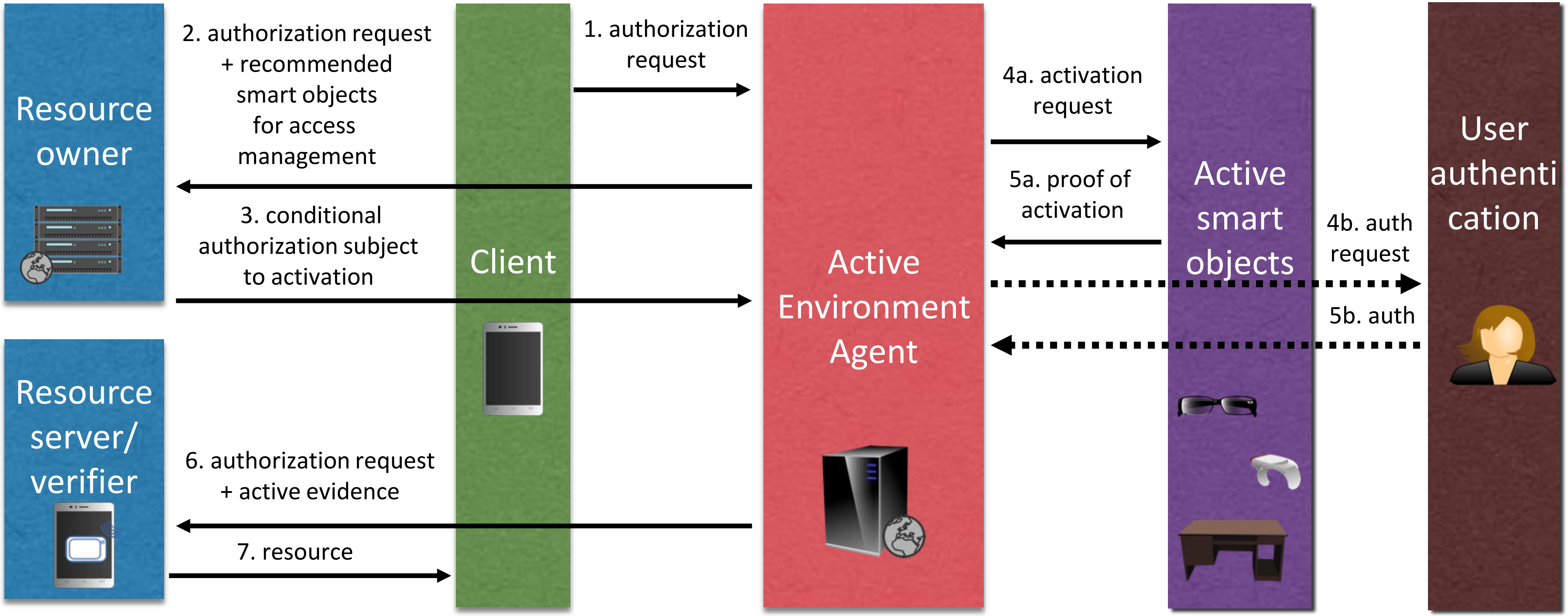
Enforcement & Flexibility

AE’s main components

- **Intelligence:**
  - **Reinforcement Learning**
    Intelligent agent that knows where and when the user will use her device



- **Security:**
  - **Distributed access control framework**
    - Resource owners and smart objects
  - **Multiparty enforcing protocol**
    - Resource owners, smart objects, target device, and verifier



Resource owner

2. authorization request + recommended smart objects for access management

Client

1. authorization request

Active Environment Agent

4a. activation request

5a. proof of activation

Active smart objects

4b. auth request

5b. auth

User authentication

3. conditional authorization subject to activation

Resource server/ verifier

6. authorization request + active evidence

7. resource

Balancing security and usability

Agent's goal: The agent wants to find an optimal strategy that maximizes the expected utility given by

$$U(s) = R(s, a, s') + \gamma \sum_{s'} T(s, a, s') U(s')$$

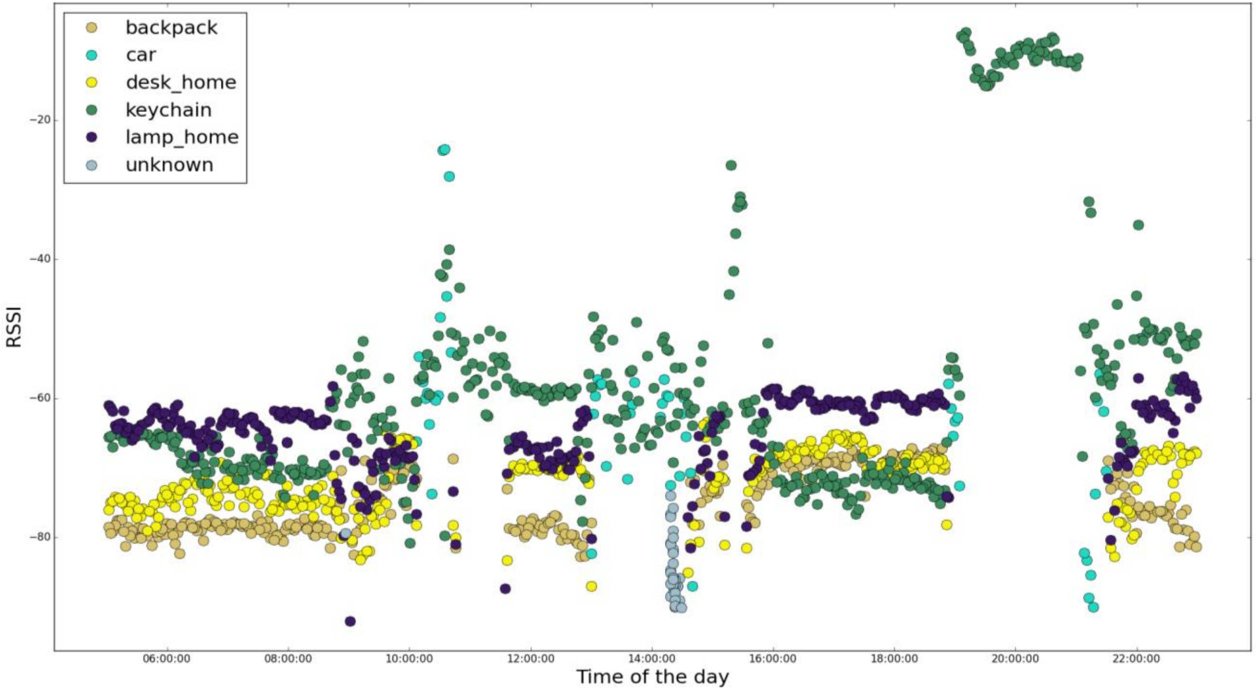
The expected sum of rewards depends on

- The rewards (usability vs security)
- The (state, action) pairs:
  ({context, app usage, smart objects} , a set of objects to *activate*)

Rewards

- Positive rewards when:
  - the legitimate user finds her smartphone unlocked and wants to use it
  - the smartphone remains locked when it is not used
  - the smartphone is used with a high implicit authentication score
- Negative rewards when:
  - the legitimate user finds her smartphone locked and wants to use it
  - the smartphone remains unnecessarily unlocked
  - the smartphone is used with a low implicit authentication score

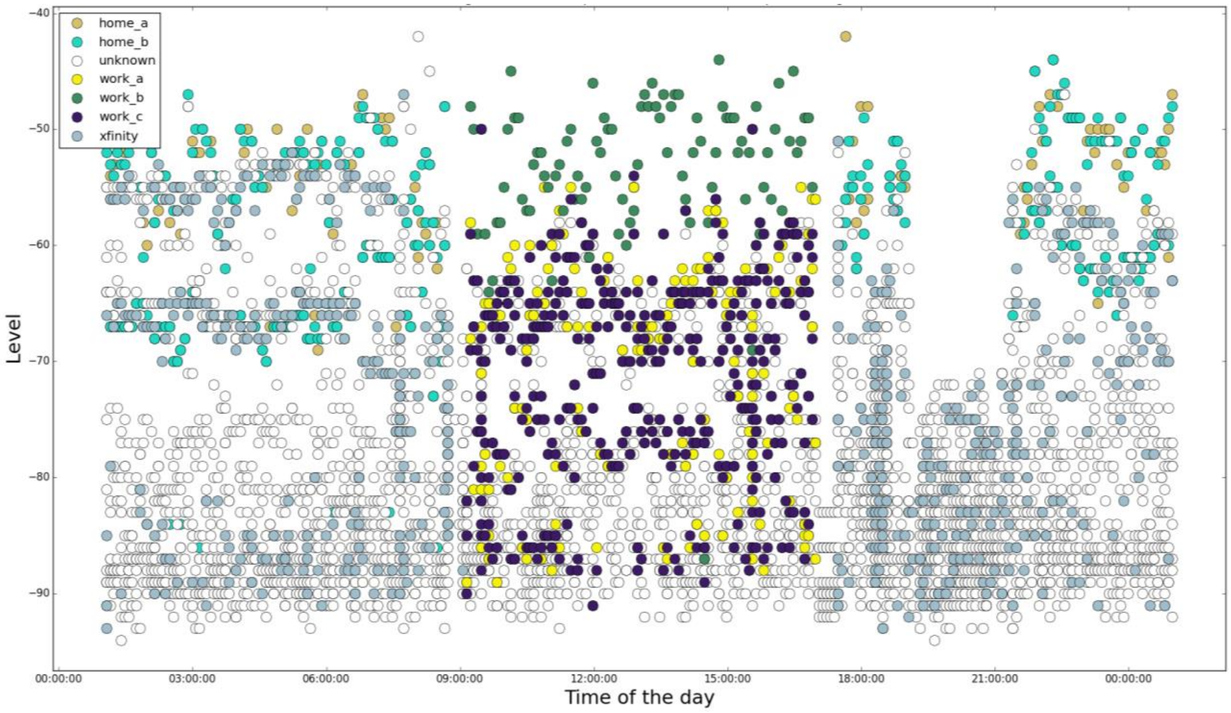
Smart objects:
Able to *activate* according to a policy



IoT smart devices:

- Wearables
- Appliances
- Personal computers
- Mobile devices

Not-so-smart objects:
Activation could be implicit



- Wi-Fi APs
- Lamps
- Devices with actuators

Why not a centralized solution?

- The guardian angel does not necessarily have the keys to access the resources

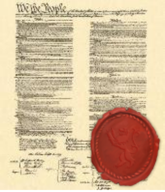
Open please?

- This allows for coexistence of multiple stakeholders
  - Multiple owners of devices and resources

- Some transactions may not necessarily need to disclose the identity of the authorized user

Distributed access control

- Distributed access control framework
  - Policies and queries in a **logic-based language** (e.g., DKAL)



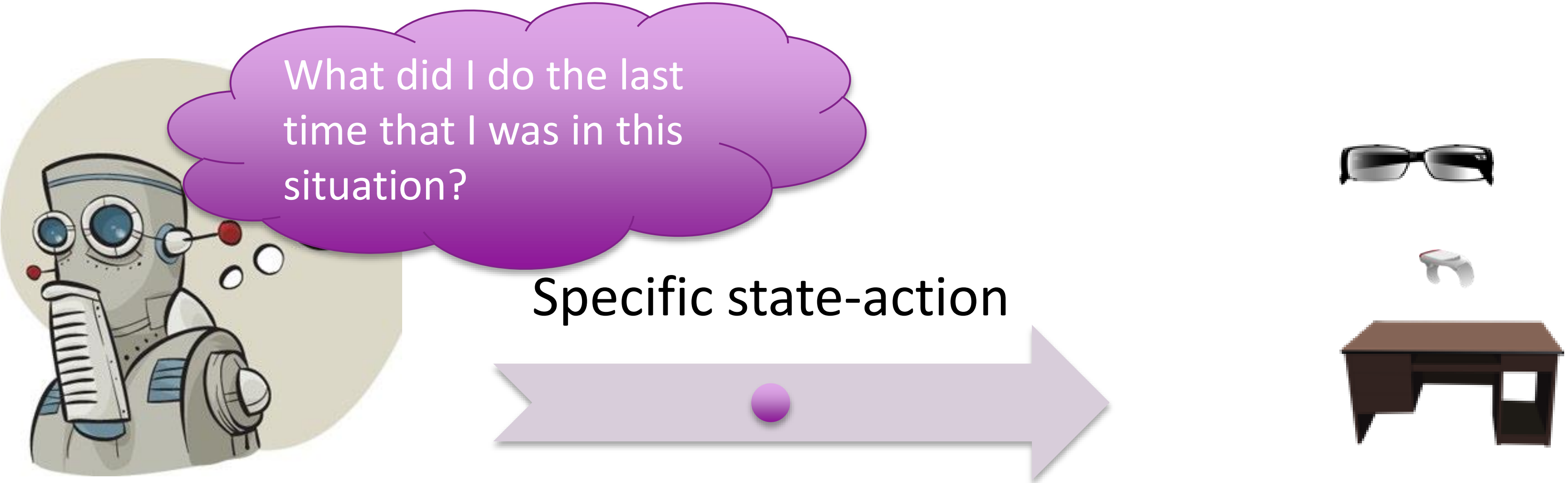
- Crypto enforcement
  - For example, derived from a **cryptographic solution** such as Shamir's secret sharing

- Each approach places different trust in clients and smart objects

Intelligence:
How could the agent be implemented?

Q-learning

A learning algorithm that determines the best action based on values associated to state-action pairs



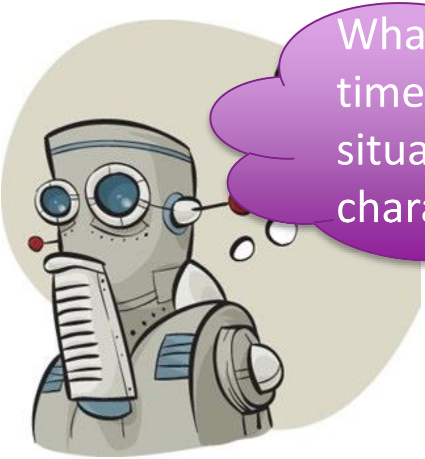
What did I do the last time that I was in this situation?

Specific state-action

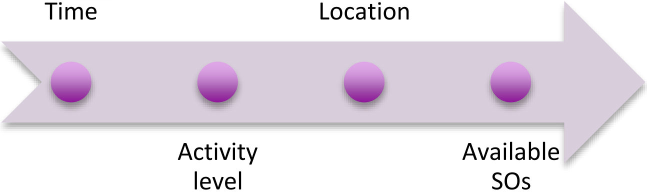
Action: Activate

Approximate Q-learning

A learning algorithm that determines the best action based on values associated to features of states and actions rather than specific states themselves



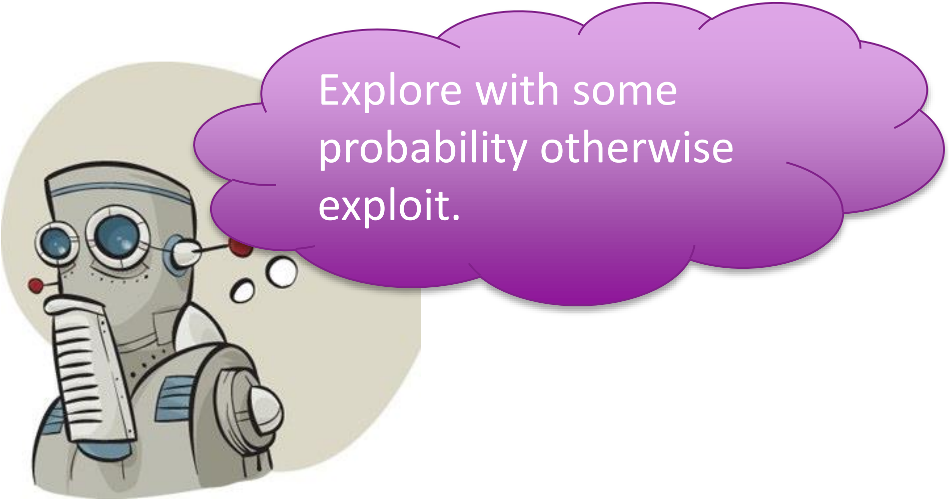
What did I do the last time that I was in a situation with similar characteristics?



Action: Activate

Exploration and exploitation

An agent can be configured with parameters that weigh how much exploration vs exploitation is done each time



Explore with some probability otherwise exploit.

- Some actions will not be as good but the agent will learn useful info
- Initially, the agent can mostly explore in order to learn quickly
- Eventually, the agent can mostly exploit what it has learned

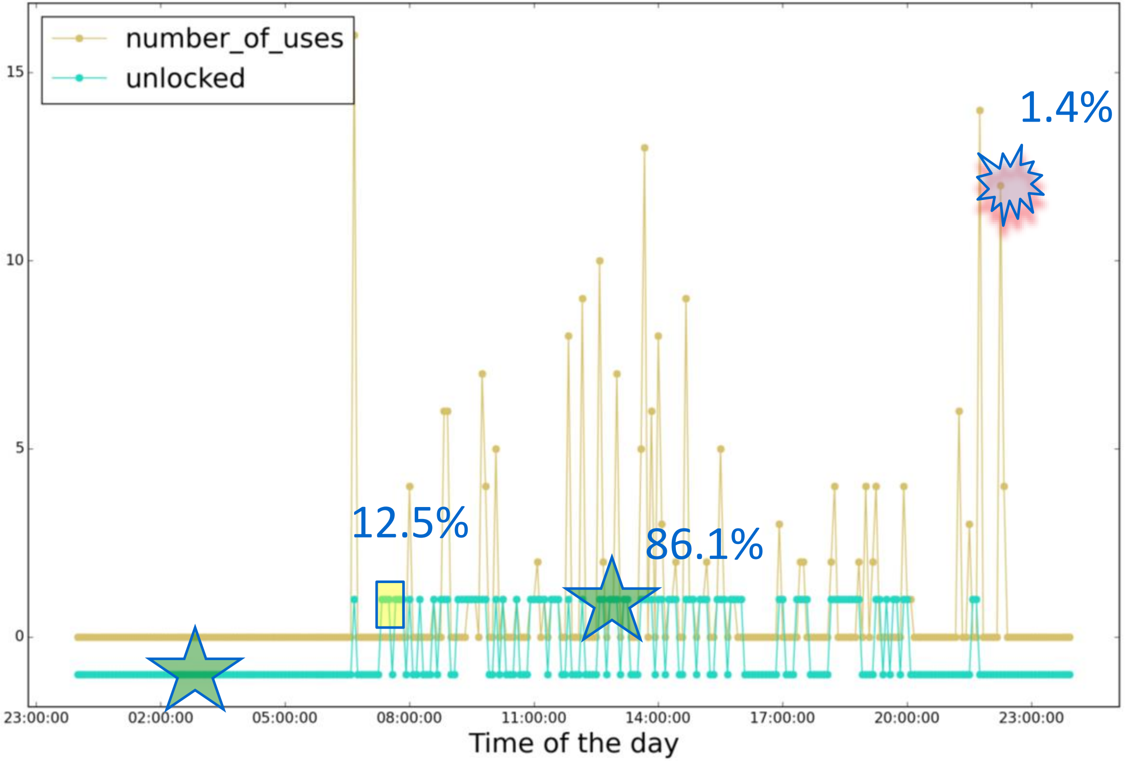
How quickly can the agent learn?

- How many days will it take for the agent to provide utility?
  - How many days would the agent need to mostly explore?

- It depends on:
  - How well the agent's actions fit the user's expectations?

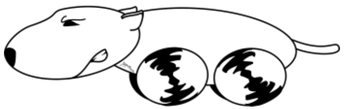
  (While maximizing security)

Usage/unlocking overlap after 5 days



Observations

- The agent learns under which conditions to unlock
  - The agent learns which actions unlock
  - The learning process can be fast



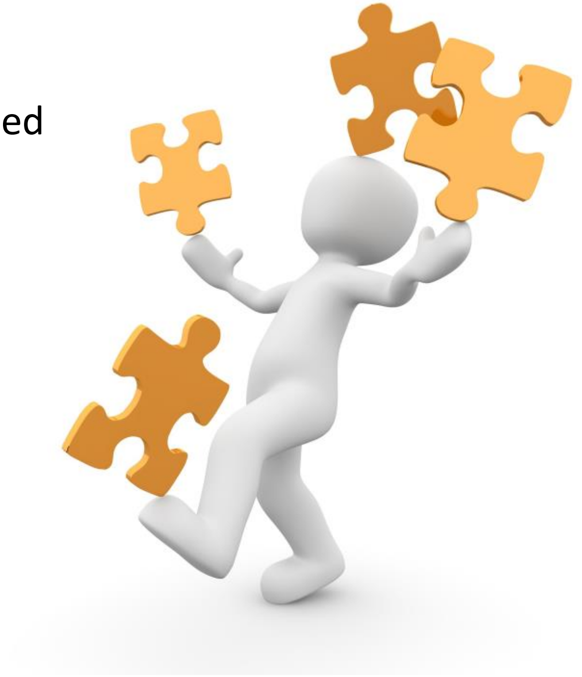
- The approach is flexible:
  - allows for configuration:<secure---usable>
  - allows for the leveraging of various kinds of SOs
  - enforcement is decoupled: the agent suggests when to unlock but the resource owner and SOs can deny access

- It is possible to implement the approach without storing large amounts of data

Apply

Access management in your organization?

- Rethink access management decisions
  - Is AM contextual? Flexible? Easy to use and configure?
- “Things” provide useful data for AM. They can also be leveraged for enforcing safe contexts (e.g., possession or proximity of/to trusted devices). Devices can be configured to be “active” according to specific policies.
- Do you have a plan for AM that is not perimeter-driven but rather user-centric?
- Leverage “things” to implement enforcing mechanisms off-premises:
  - personally owned devices (BYOD)
  - remote access



Questions?

Andrés Molina-Markham, Ph.D.
Visiting Scholar
Dartmouth College
andres.d.molina-markham@dartmouth.edu

Kevin Bowers
Manager
RSA Labs
kevin.bowers@rsa.com