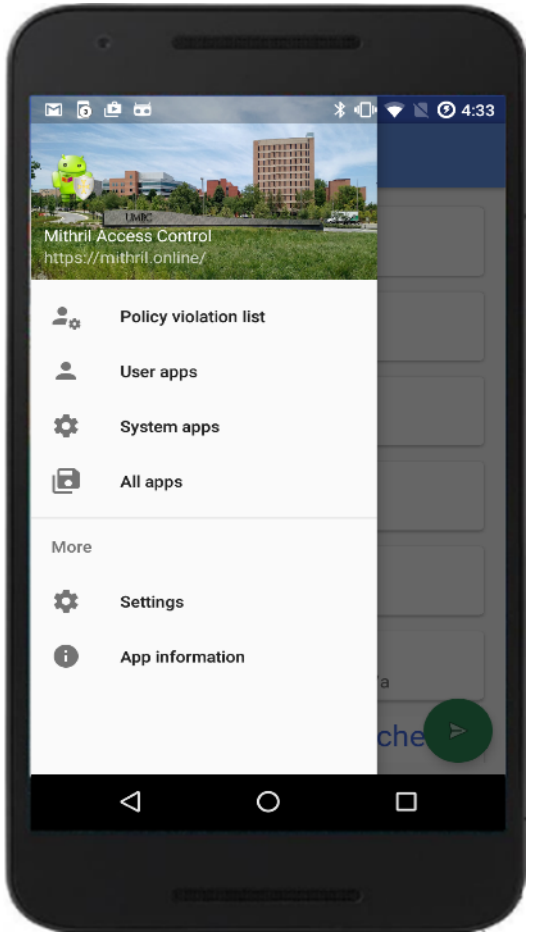
UMBC
AN HONORS UNIVERSITY IN MARYLAND

Capturing policies for fine grained access control on mobile devices

PRAJIT KUMAR DAS, ANUPAM JOSHI, TIM FININ

Motivation

We present MITHRIL, a framework for capturing user access control policies that are fine-grained, context-sensitive and are represented using Semantic Web technologies and thereby manages access control decisions for user data on mobile devices.



Android image source courtesy: Aha-Soft

Related Work

- Policy Engineering: Requires substantial technical knowledge, understanding of access control issues *(Feltus'08)*
- Most people are 'Privacy Pragmatists' *(Kumaraguru'05)*
- Convergence of Enterprise usage and personal usage due to BYOD adoption *(Kodeswaran, Chakraborty et. al.'13)*
- Users unsure of policy *(Benisch, Sadeh'11)*
- Privacy profiles used for user preferences *(Liu et. al.'14)*

Image courtesy: Android App Market

6 December 2013 Last updated at 06:42 ET

Data haul by Android Flashlight app 'deceives' millions

The "brightest flashlight" app was downloaded to millions of Android devices

Tens of millions of Android users have been "deceived" by a developer who covertly gathered personal data, the US Federal Trade Commission (FTC) said.

Relat

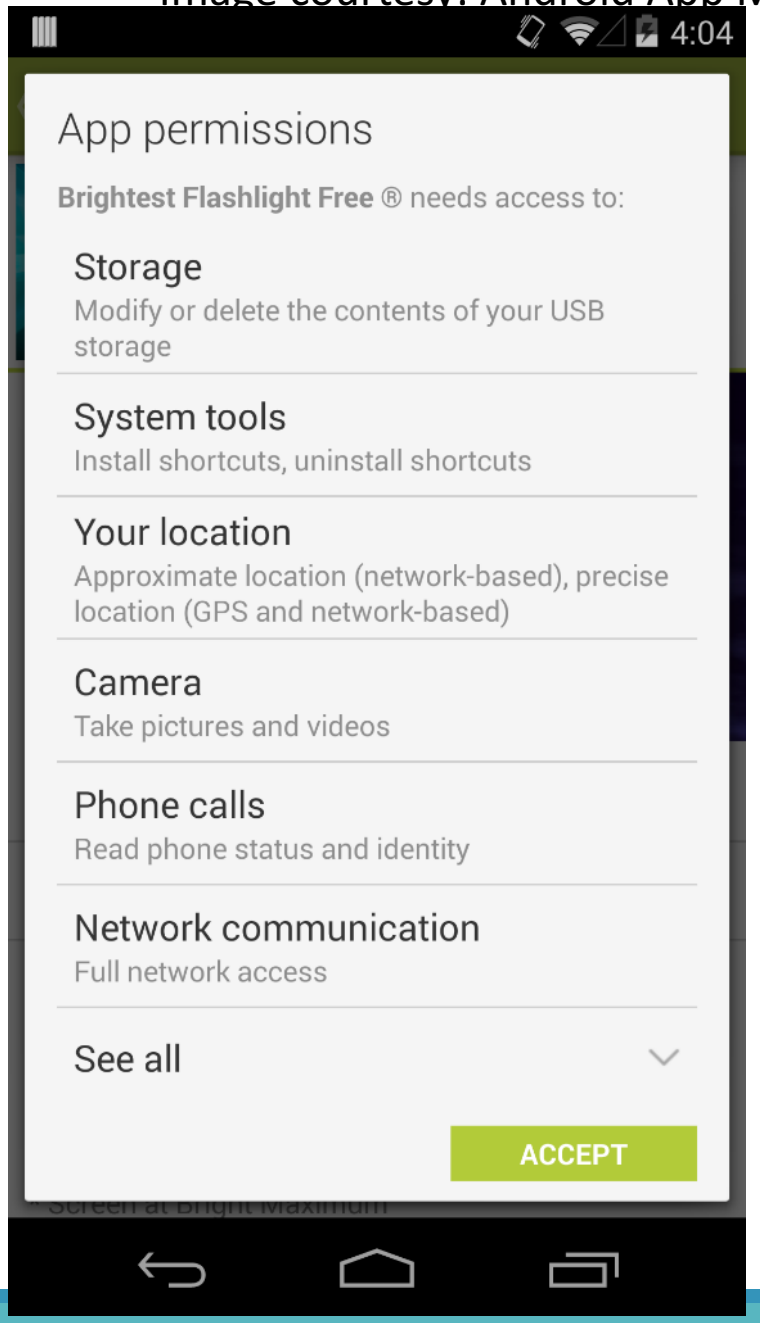
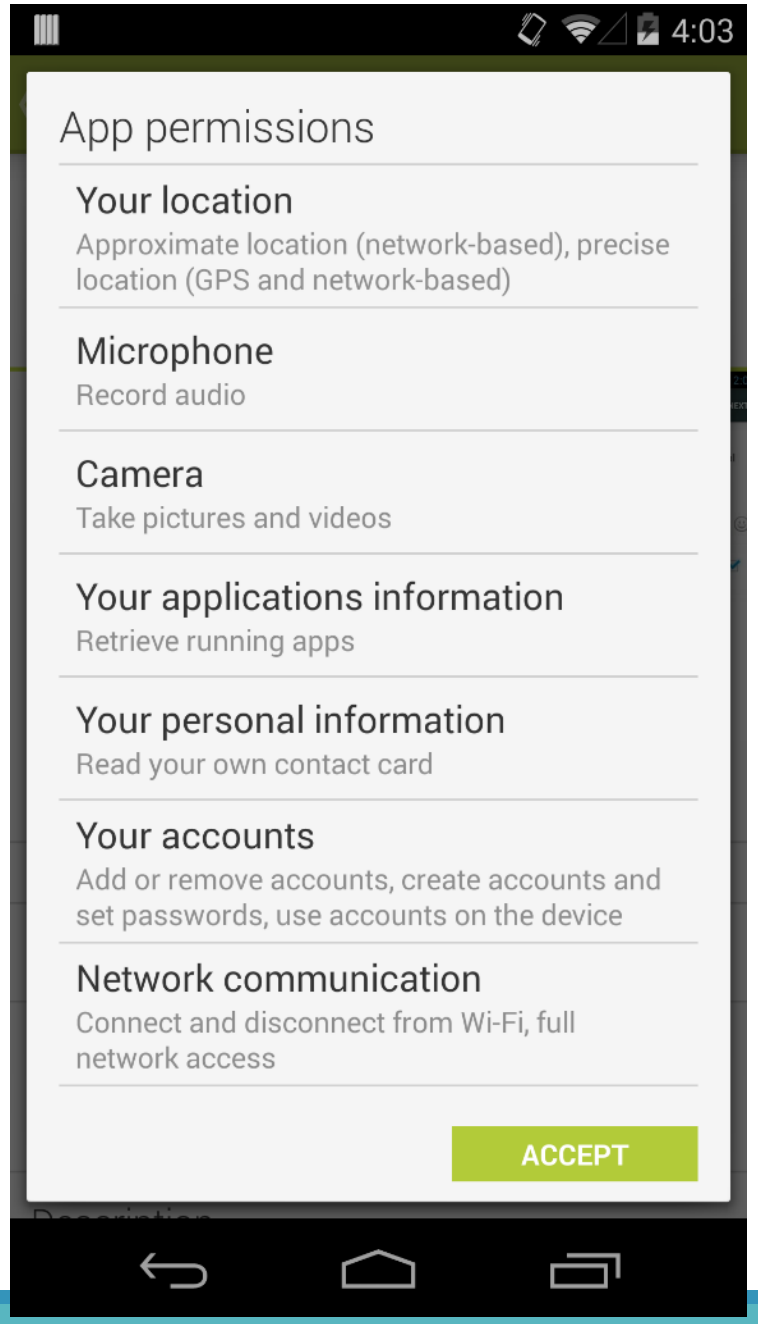


Image courtesy: Android App Market



WhatsApp user chats on Android liable to theft due to file system flaw

Android version of app stores user database on SD card with poorly secured encryption keys, says Dutch security researcher

Alex Hern

Follow @alexhern Follow @guardiantech

theguardian.com, Wednesday 12 March 2014 11.13 EDT

Jump to comments (100)

Global messaging service WhatsApp Photograph: Alex Milan Tracy/Demotix/Corbis

A newly discovered security flaw in the Android version of WhatsApp allows another application to upload a user's entire database of chats to a third-party server, without their consent.

Image courtesy: Android App Market

Apple faces privacy breach charges with its secret user tracking file

By Monami Thakur
on April 21 2011 6:38 AM

f 0 0 in 0 g+ more

Researchers at a technology conference in San Francisco on Wednesday have accused Apple of breaching the privacy line of consumers by storing user's location and other details in a secret file. Reuters.

Researchers at a technology conference in San Francisco on Wednesday have accused Apple of breaching the privacy line of consumers by storing user's location and other details in a secret file.

The file called consolidated.db. stores latitude-longitude coordinates along with a timestamp.

SECURITY

How many mobile apps collect data on users? Oh ... nearly all of them

Free or paid, Android or iOS, your apps are spying on YOU – report

By Neil McAllister, 21 Feb 2014 Follow 519 followers

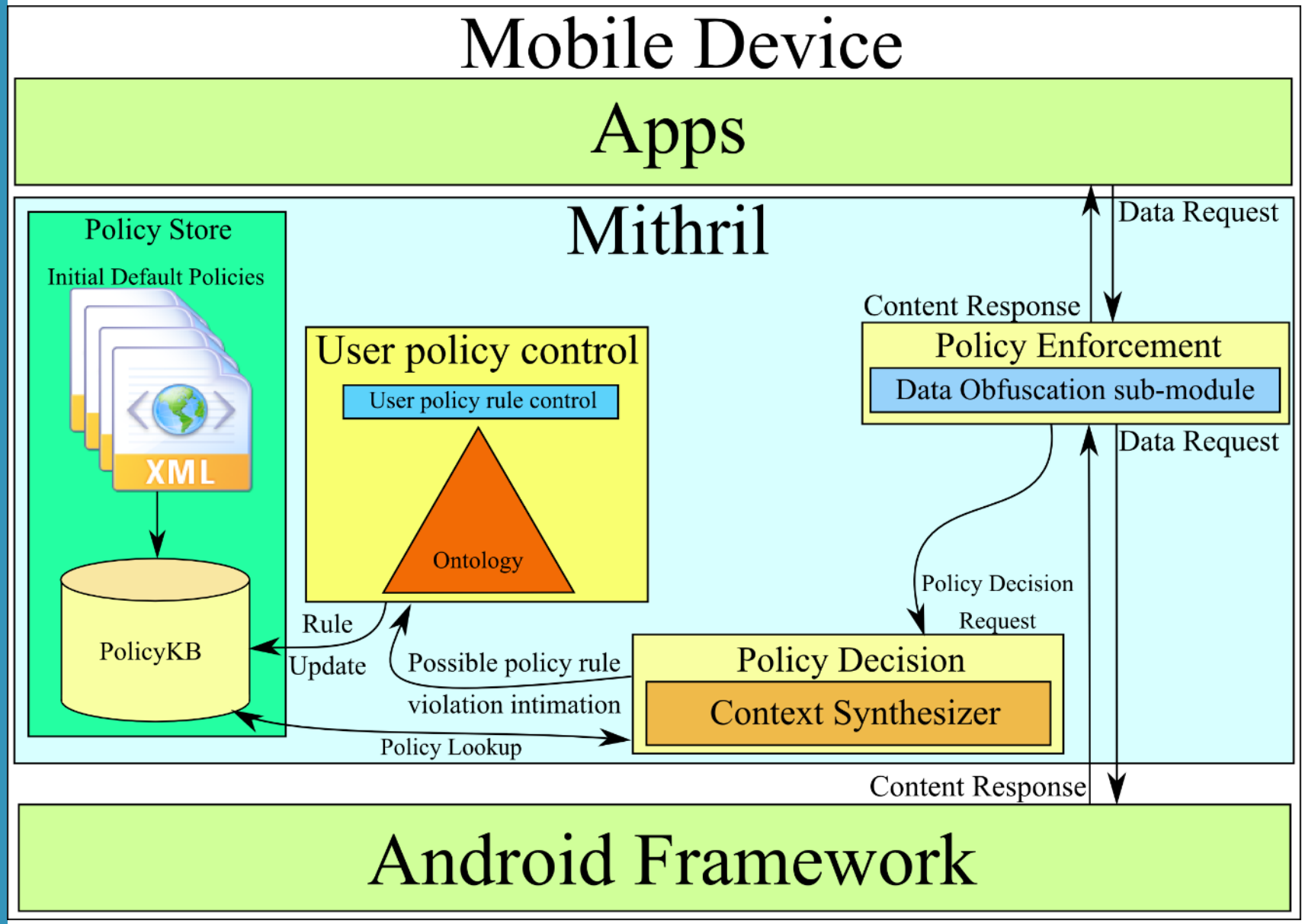
Contributions

MITHRIL has three key contributions

- Policy representation
  - Expressing policy rules: extensible & expressive semantic model
  - RDF/OWL allows easy reuse/integration with concepts from DBpedia, Linked Data, schema.org,etc.
- User-preferred & specific policy capture
- Policy enforcement

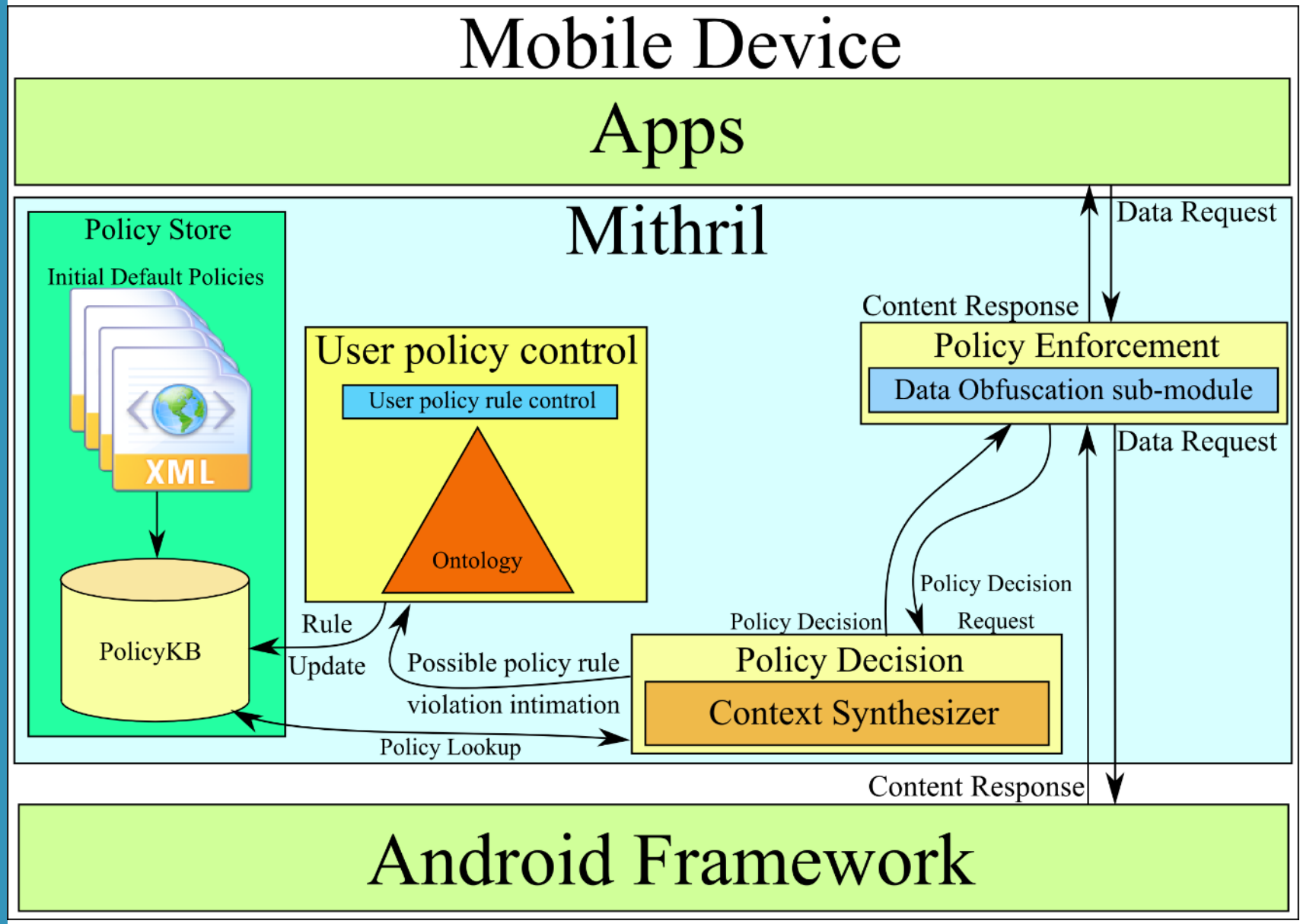
System overview

Observer mode



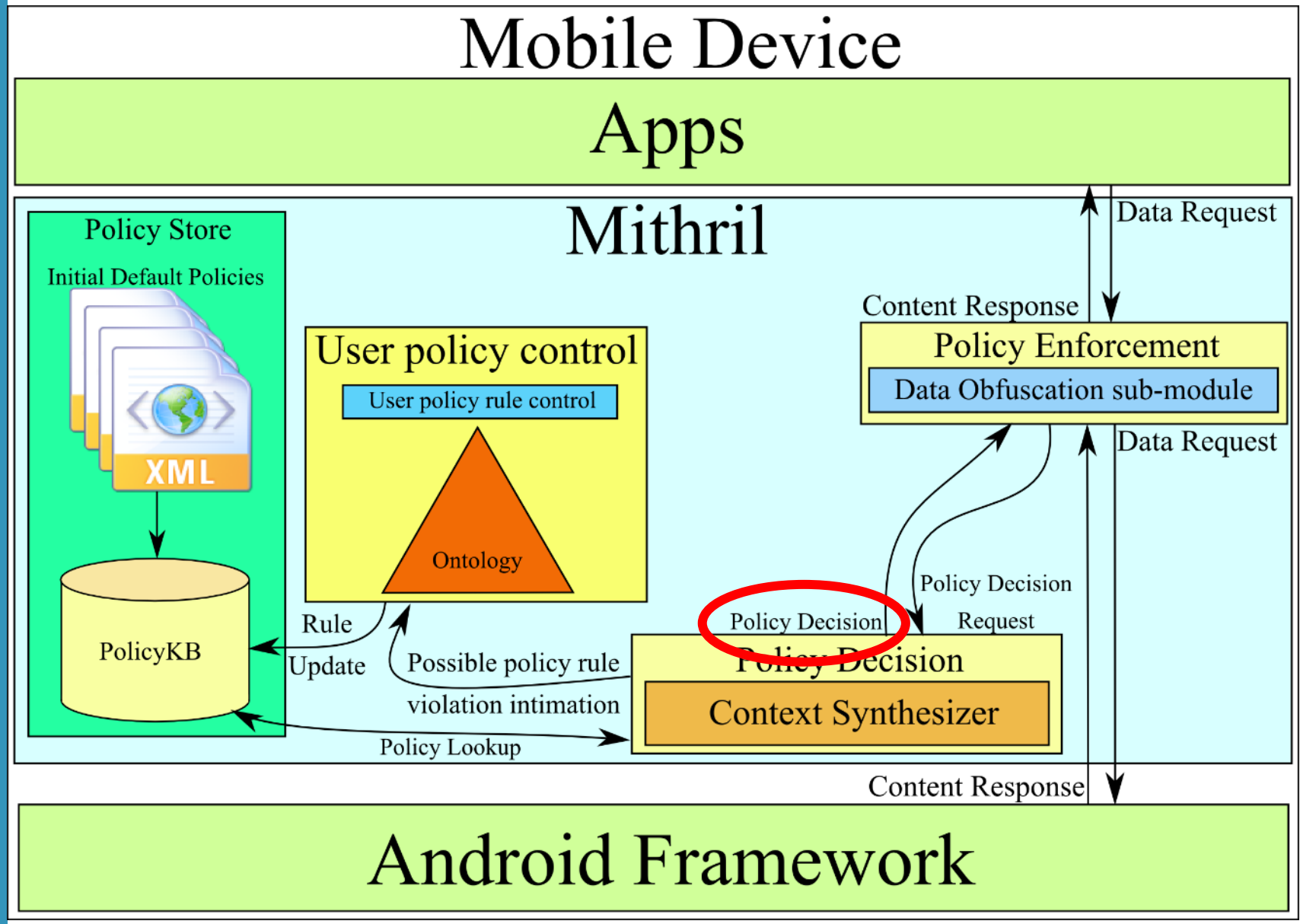
System overview

Enforcer mode



System overview

Enforcer mode



Rule representation

- Semantic Web Rule Language
- antecedent => consequent
- Attribute-Based Access Control model
- Context pieces as attributes

Rule representation

A1: RequesterInfo = Facebook &
A2: UserActivity = Work &
A3: UserLocation = Office &
A4: UserTime = Working hours on Week day &
A5: ProtectedResource = Location
->
C1: Prohibit

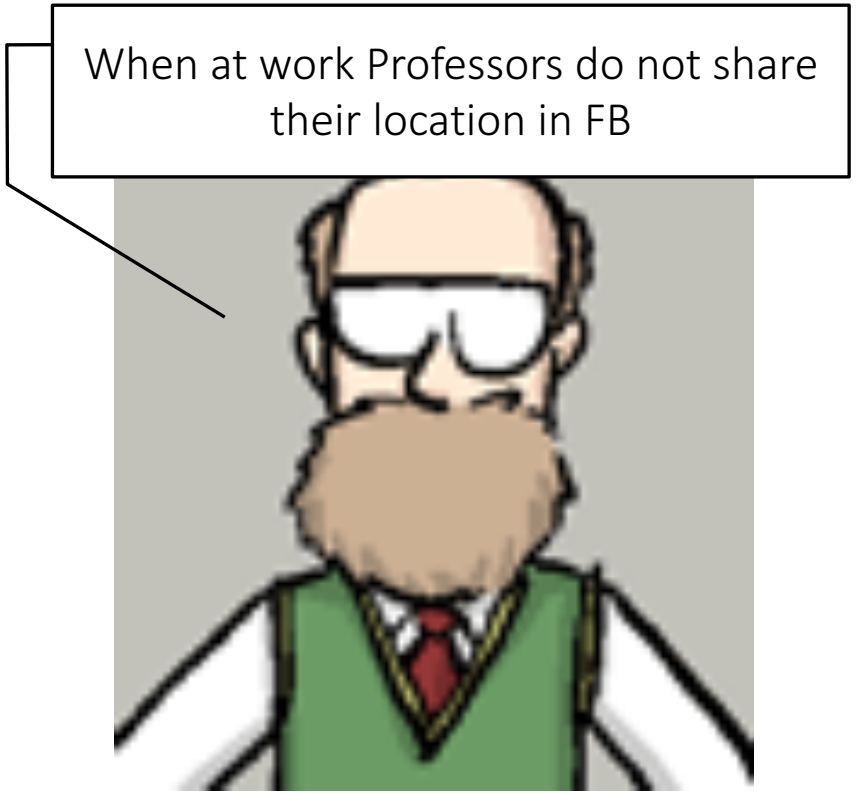
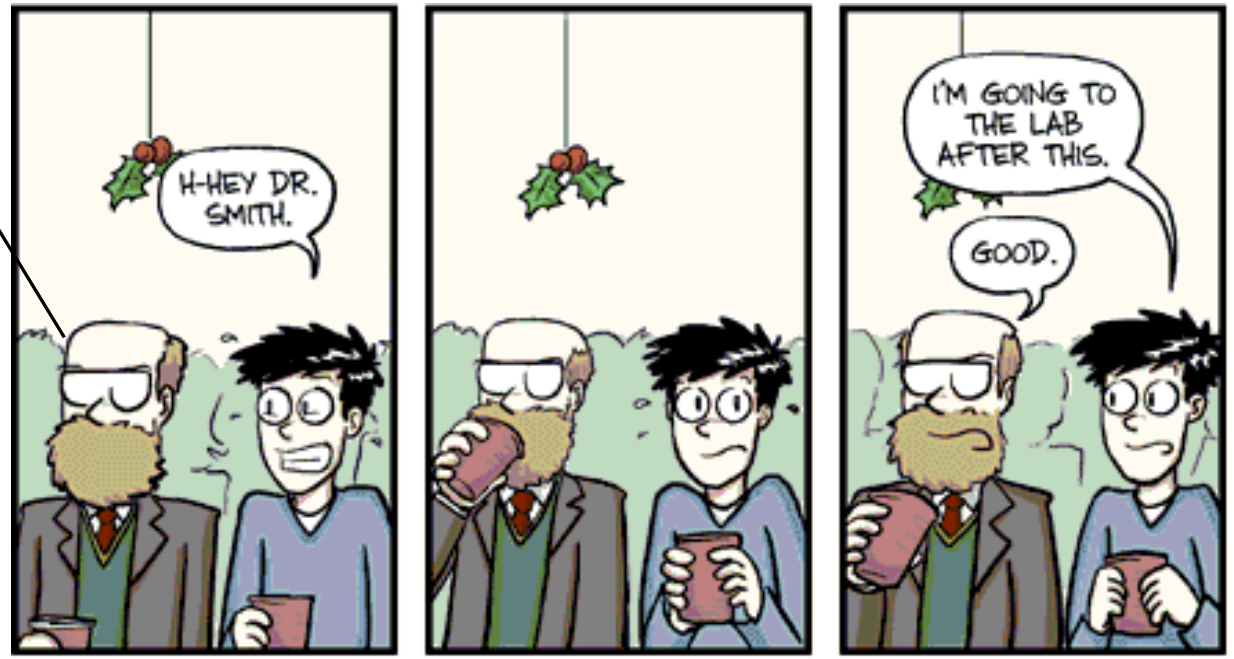


Image courtesy: www.phdcomics.com

Rule learning

This is Prof. Smith. He likes to check in to FB during lunch.

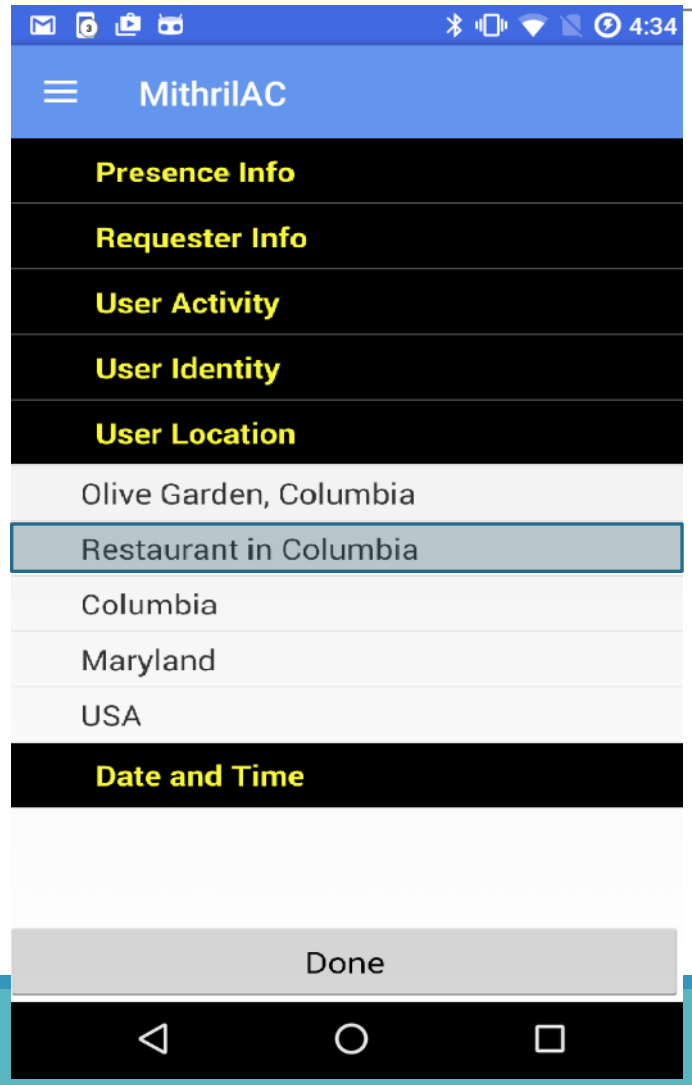
<u>During lunch</u> Professor Smith shares location

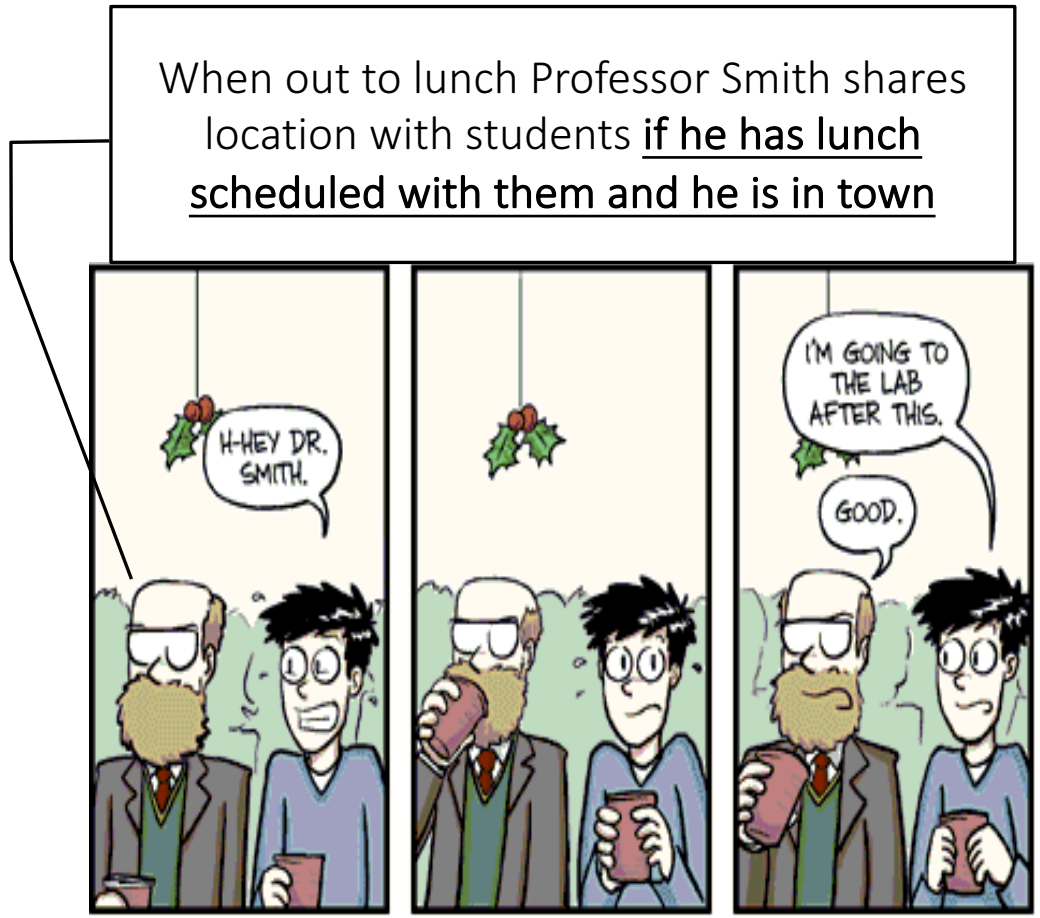


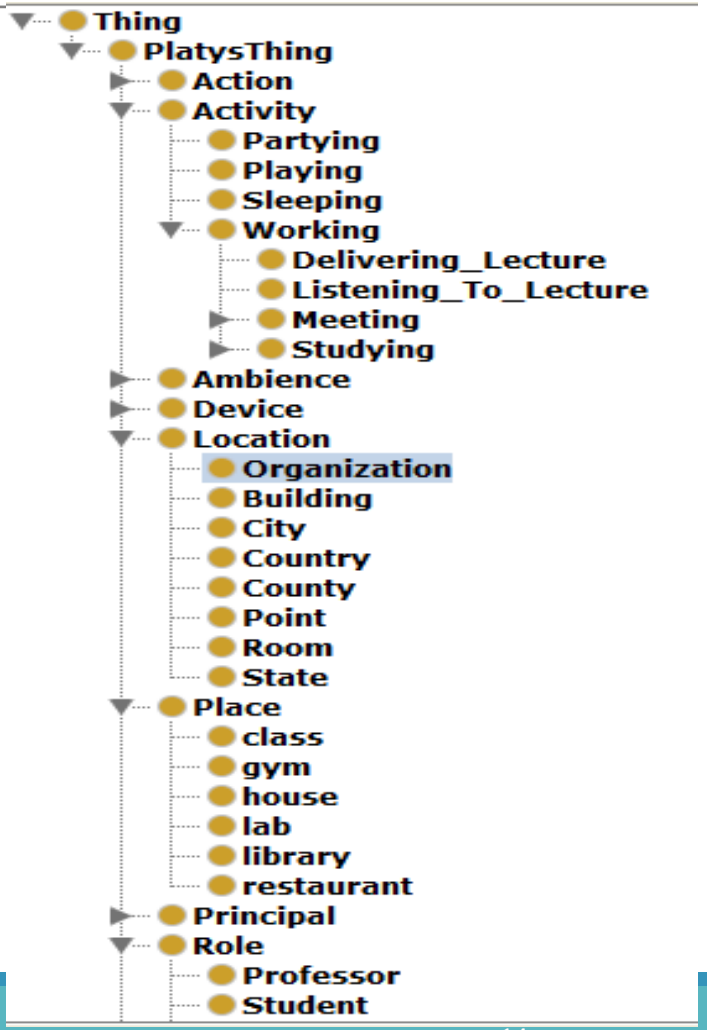
Generic Rule: Professors do not share their location on FB

Image courtesy: www.phdcomics.com

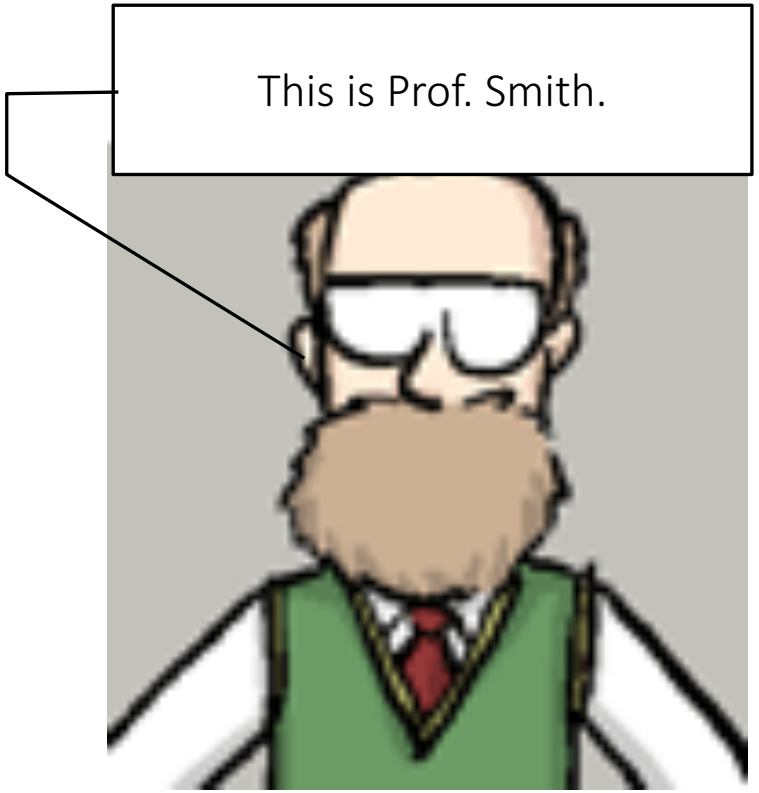
Rule Learning – User Feedback Capture







Violation Metric



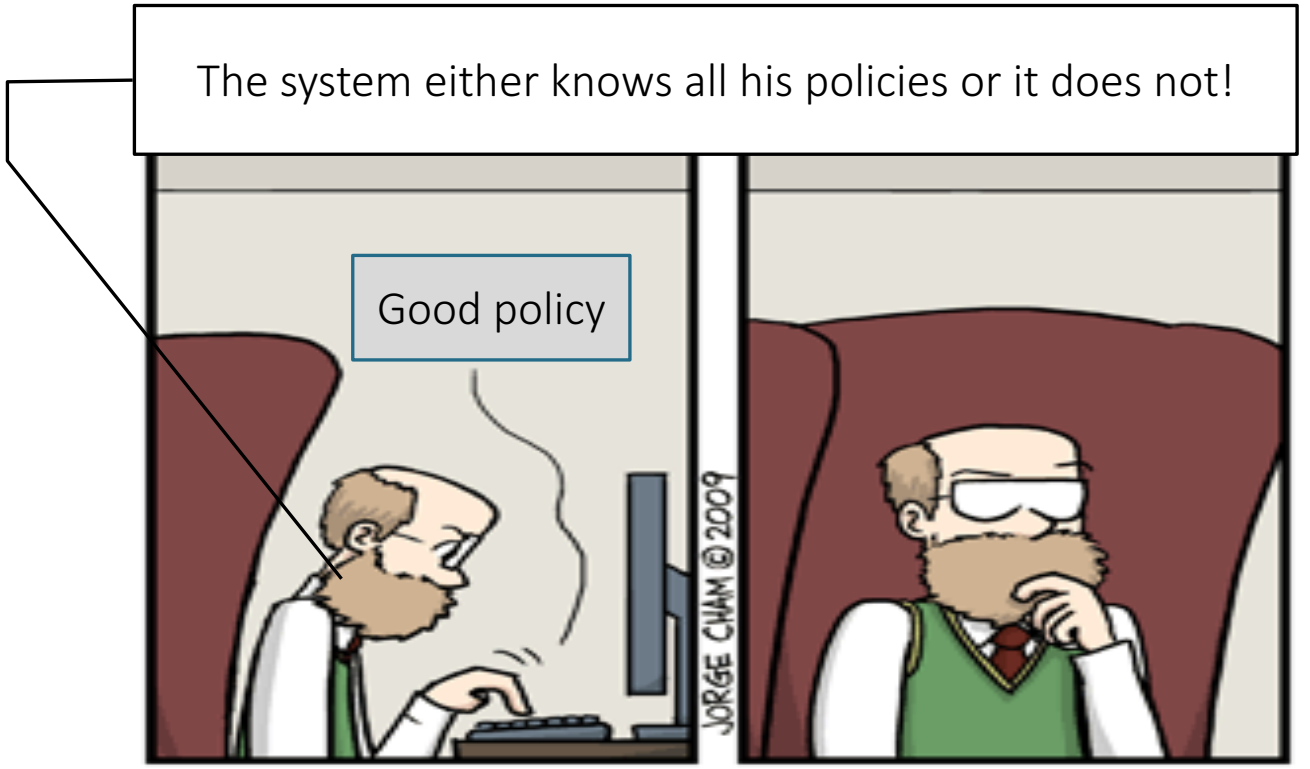
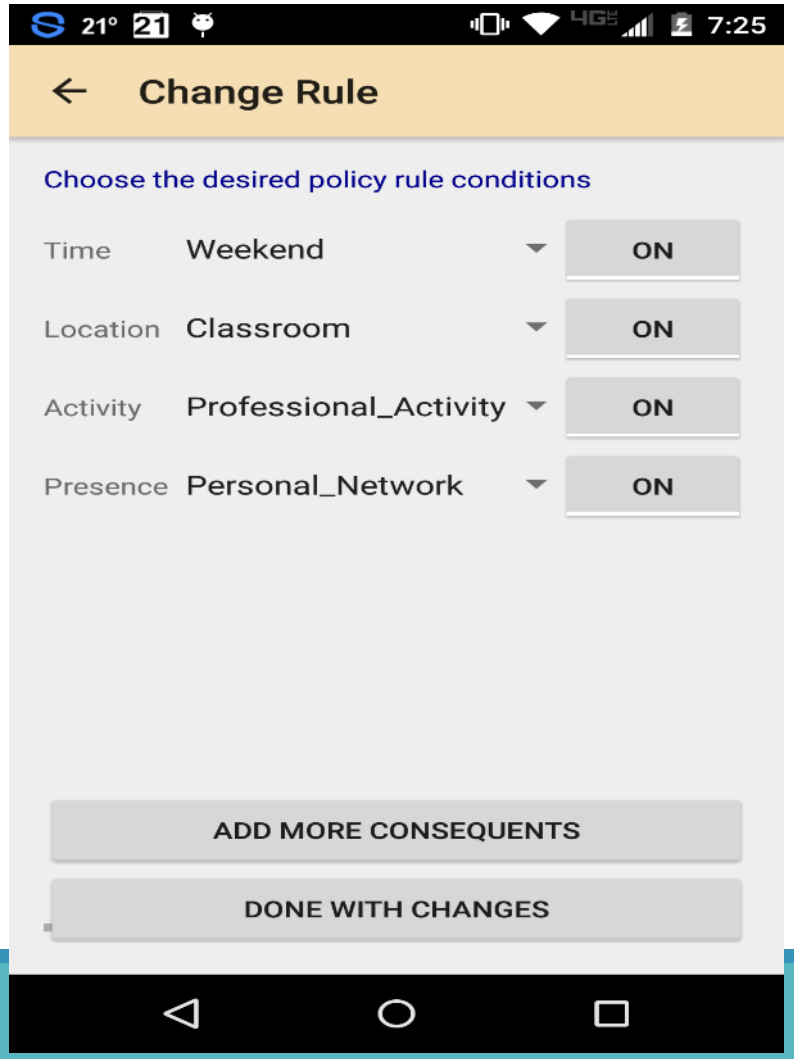


Image courtesy: www.phdcomics.com

Violation Metric



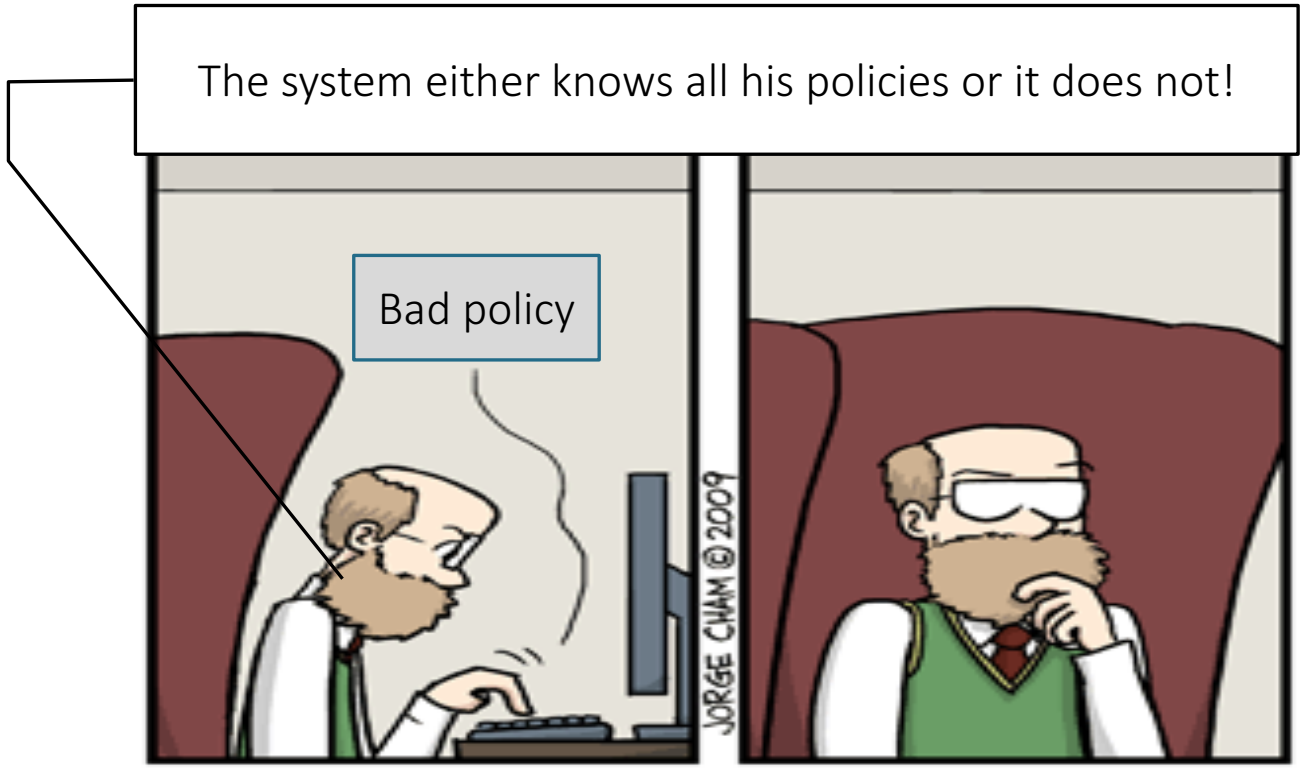
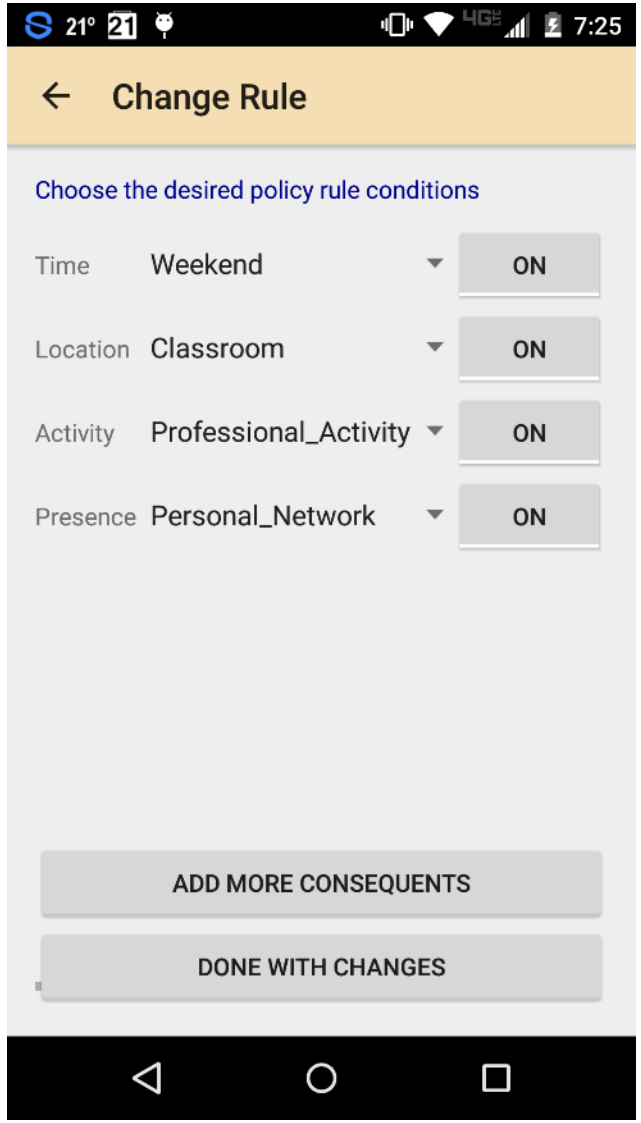


Image courtesy: www.phdcomics.com

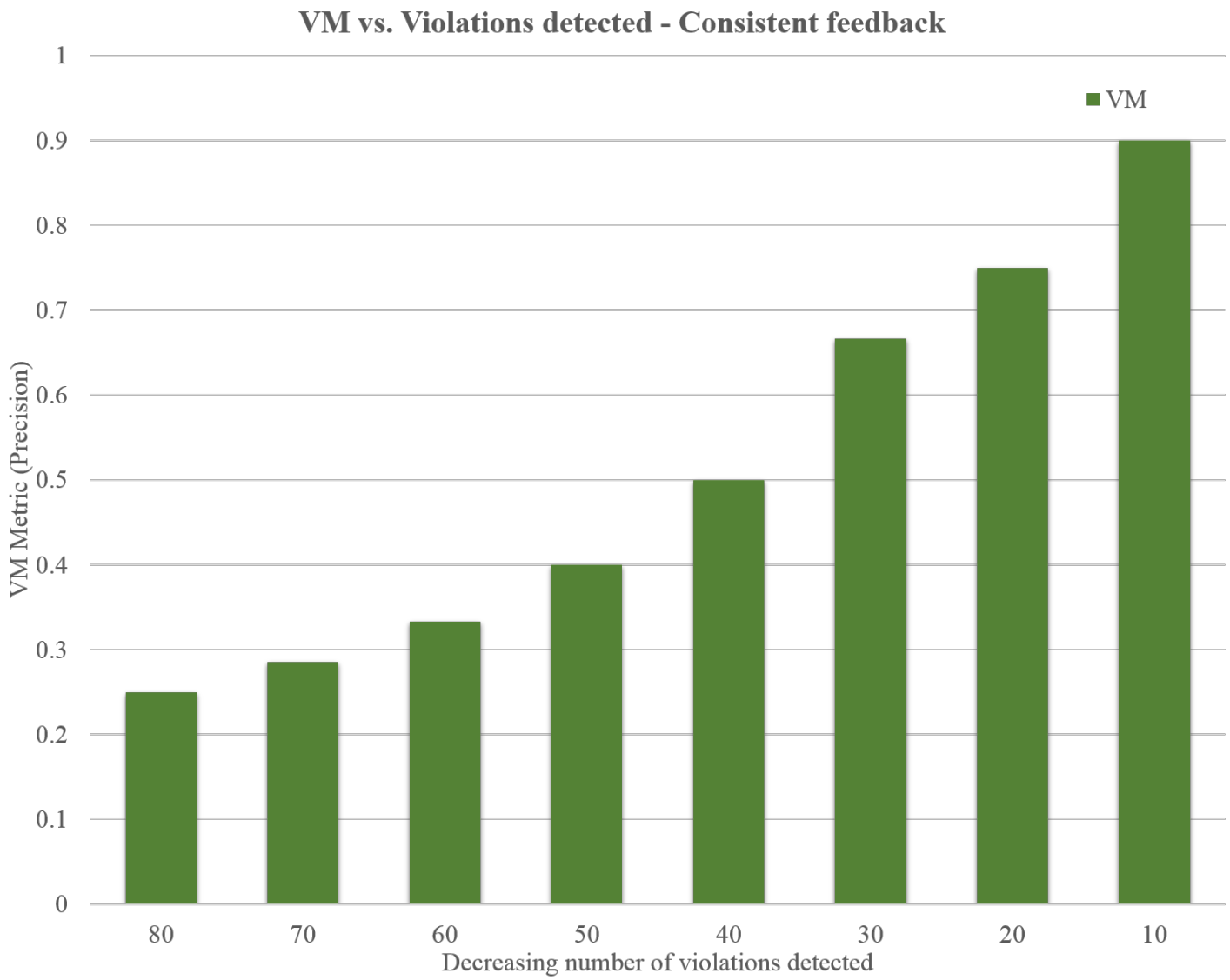


False violation: Use cases

- Rule requires
  - Deletion
  - Antecedent generalization
  - Antecedent specialization
  - Delete conditions
  - Add conditions

Experimental Results

Consistent feedback



Emulating XPrivacy

Source: http://www.xprivacy.eu/
License: GNU General Public License version 3

Future Work

- More experiments validating violation metric
- Finer granularity capture of policy violation
- Possible predictive model for policy generation
  - Using machine learning to generate policies
  - Inducing policy using logic programming

Conclusion

We presented MITHRIL

- Framework for capturing ABAC access control policies
- User-preferred & specific policy capture
- Fine-grained, context-sensitive
- Uses Semantic Web technologies
- Policy enforcement