TOWARDS SITUATION-BASED IT MANAGEMENT DURING NATURAL DISASTER CRISIS

SECURWARE 2020

Abdelmalek Benzekri, **Romain Laborde**, Arnaud Oglaza, Maleerat Sodanil and Hatahairat Ketneechairat

Romain LABORDE - Short Resume

- Maître de conférences (similar to Associate Professor) at University Paul Sabatier – Toulouse III, France since 2006
- Head of the Computer Science Dept at the University Paul Sabatier Institute of Technology since 2019
- 9 Ph.D supervision
- ~90 articles published in international journals/conferences/workshops
- More info on my personal web page:
  - https://www.irit.fr/~Romain.Laborde/index_en.php

Romain LABORDE – Research topics

- Research workgroup : SIERA
- Research interests: Identity and access management
  - Privacy Management
  - Self-sovereign Identity
  - Dynamic security management (topic of this article)
- Current Research Projects:
  - H2020 – Cybersec4Europe
    - https://cybersec4europe.eu/
  - H2020 – LeADS (Legality Attentive Data Scientists)

Natural Disasters – Asia Pacific

The Asia-Pacific region experiences over 70% of the world's natural disasters.

Major Natural Disasters in Recent Years

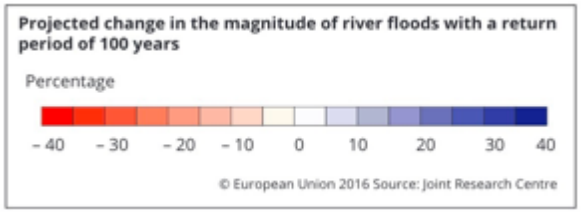
Earthquake (Chile) 2010
Tennessee Floods (USA) 2010
The Great East Earthquake (Japan) 2011
Floods (Thailand) 2011

Tornado (USA) 2011
Loreto Floods (Peru) 2012
Hurricane Sandy (USA) 2012
Typhoon Haiyan (the Philippines) 2013

APEC - https://www.adrc.asia/acdr/2015/documents/PF520_05_ABAC.pdf

Natural disasters - Europe

Climate change will impact other regions



https://www.eea.europa.eu/publications/climate-change-adaptation-and-disaster/

ICT infrastructure contribute to saving lives during natural disasters

Damage Prevention

- ✓ Urgent earthquake detection alarm system

- ✓ Earthquake early warning mobile phone alert

Rescue

- ✓ Twitter-led rescue
- ✓ Online disaster message board service

Communication Tool

- ✓ Mobile phone station vehicles

- ✓ Satellite phones

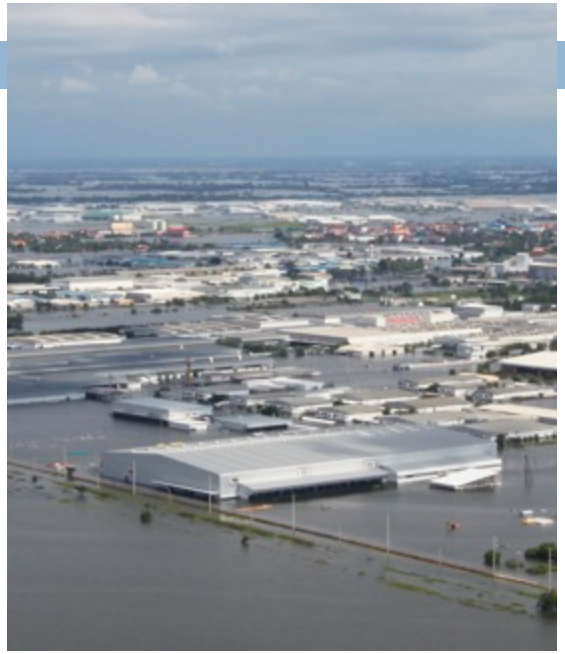
Reliable Information Source

- ✓ Distribution station information for evacuees
- ✓ Information sharing for volunteers

APEC - https://www.adrc.asia/acdr/2015/documents/PF520_05_ABAC.pdf

ICT infrastructure shall be disaster resilient

- Example : Thailand Floods in 2011
- What happended
  - Occurred during Aug-Dec. 2011, lasted for 5 months in some areas
  - The worst flooding in 50 years for Thailand
  - Over 800 deaths and 13.6 million people were affected
  - Over US$45.7 bil. economic damages and losses
- Impact ICT
  - Flooding caused power outage, leaving people without power generators unable to charge their mobile phones
  - Server hubs were flooded and mail systems were malfunctioned for days



ICT infrastructure shall be disaster resilient

- Crisis management processes involve complex management decisions to automatically adapt the deployed IT systems
  - Eliciting/expressing/validating adaptive systems requirements.
  - Expressing/managing/validating adaptive security and/or management policies.
  - Dynamically enforcing adaptive security and/or management policies.

Situational Awareness

- Situational Awareness describes the idealized state of understanding what is happening in an event involving many actors and other moving entities
- Context [DEY, 2001]
  - *context is any information that can be used to characterize the situation of an entity.*
- Situation [Barwise and J. Perry, 1980]
  - *The world consists not just of objects, or of objects, properties and relations, but of objects having properties and standing in relations to one another. And there are parts of the world, clearly recognized [...]. These parts of the world are called situations.*
- Situational awareness [Endsley, 1988]
  - *the perception of the elements in the environment within a volume of time and space, the comprehension of their meaning, and the projection of their status in the near future.*

Difficult Situations Fun Deck

Situational awareness in dynamic IT crisis management

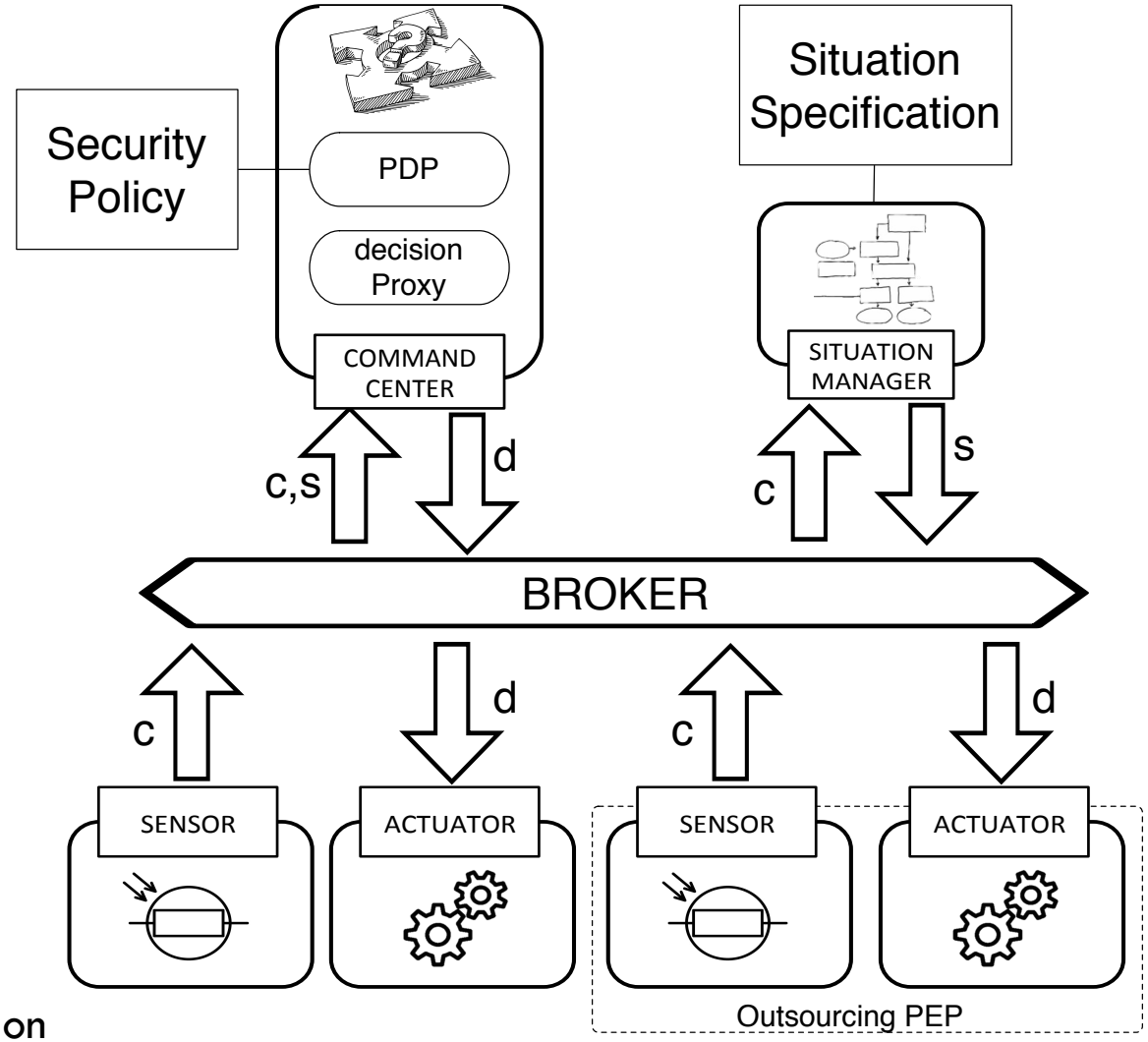
- Anticipating how individuals, groups and communities can use information contributed by others especially in a social media context
- How to launch situation characteristics extraction as well as situational updates labelling from, for instance tweets in the Thai language?
- How to dynamic adapt the ICT infrastructure to crisis management?

DynSMAUG – A situation driven security management framework

- We developed DynSMAUG
  - Objective = Dynamic security management
  - Already applied to:
    - Virtual organizations management
    - Health ICT management (Break the Glass)
    - Mobile device management
    - Etc.
- Can we use DynSMAUG to adapt the deployed IT systems during crisis management ?

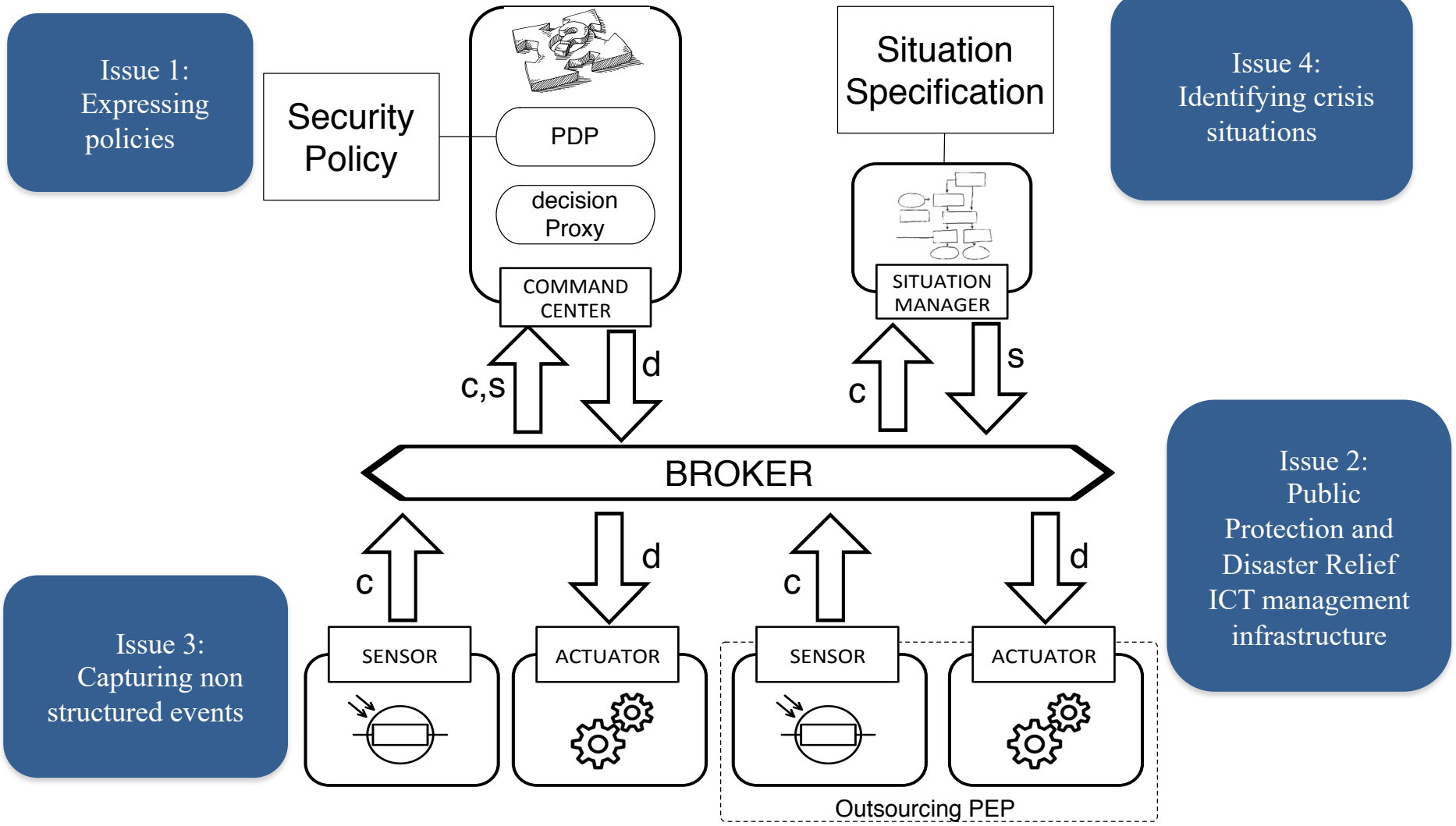
MANY OPEN QUESTIONS !

DynSMAUG – A situation driven security management framework



C: context
S: situation
D: security decision

DynSMAUG – A situation driven security management framework



Issue 1 : Expressing emergency/crisis procedures

- How to write policies to dynamically manage IT systems during natural disaster crisis?
- Machine-readable crisis procedures
  - McHugh and Sheth defined a process to develop flow charts for emergency procedures
  - Hanachi et al. go further "transforming a plan into a process providing an accurate and machine-readable specification of actions to be done in the field, a better common understanding between stakeholders responsible for these actions and a means to analyse, simulate and evaluate the crisis response before launching it…"
- DynSMAUG policies = Situation-Based Security policy
  - **when** *situation* **and** *some condition* **then** *authorization decision and/or obligation(s)*
- DynSMAUG policies are
  - close to the decision crisis cell needs, reduces the gap between policies requirements and the effective policy enforced by stakeholders, and then limits the policy translation errors
  - minimizes the impact of changing mechanisms and simplifies the policy life cycle management

Issue 2: adapt the network to natural disaster crisis environment

- Resilience of networks = one objective of 5G networks
  - enabling the automation of network service provisioning and management as software functions running on commodity hardware to support efficient network resource utilization, quicker operational changes, and faster service provisioning cycles
- Self-organized Public Protection and Disaster Relief (PPDR) network
  - Act as primary user in the frequencies allocated to it for mission-critical application such as voice
  - Act as secondary user to enable new applications, such as the exchange of high-definition videos and images (e.g., sent by drones, etc)
- We plan to use dynSMAUG dynamic management capabilities to:
  - Conceive algorithms able to dynamically and quickly make decisions on optimal number and locations of resources to be allocated. In case of emergency, mobile access network elements (mainly BS elements carried by drones and ground mobile BSs) can be utilized for better spectrum management and throughput delivery.
  - Design of a mechanism that, depending on the traffic's quality of service requirements and possibly on external events (e.g. an emergency situation), can decide dynamically whether to transmit the traffic over the PPDR dedicated frequencies, thus setting the radio to act as primary user, or over spectrum accessed opportunistically, setting the radio to act as secondary user
  - Dynamic reconfiguration of network components (such as edge gateways) and can be implemented as part of a Network Functions Virtualization (NFV) architecture deployed at the PPDR level

Issue 3: capturing non structured context events

- Social media = good crisis context sensors
- But ..
  - Social media streams = unstructured information
    - Natural Language Processing (NLP) to transform it into structured information
      - Many works applied to tweeter
    - No NLP model for tweets in thai language
      - Thai has specific features such as not marking word boundaries
  - Social media are not trustworthy
    - Fake news

Issue 4: calculate a natural disaster crisis situation

- A situation
  - has a beginning and an end
  - is a correlation of multiple context information
- In DynSMAUG, we use a Complex Event Processing (CEP) approach for computing the beginning and the end of situations.
  - *set of tools and techniques for analyzing and controlling complex series of interrelated events*
  - ESPER
    - Event Processing Language
    - SQL + time-windows, timed-data arithmetic definition
    - Good performance
- CEP is a specification-based identification approach that does not scale
  - situations identification rules become too hard for being written by a human in such a Big data context that includes plenty of sensors and very complex situations
- Apply machine learning to identify situations
  - Dataset such as The Humanitarian Data Exchange that provides open crisis data

Conclusion

- Crisis management = a big data issue given the incredible diversity, heterogeneity and number of channels that can contribute to a crisis resolution
- Situational awareness theory provides the concepts for expressing and deploying the machine-readable crisis policies
- Using the dynSMAUG system as a concrete example, we highlighted open questions in building an effective decision support system to help crisis cells