FoMSESS annual meeting 2016

"Self-Disclosure in Social Media: Challenges & Opportunities for Self-Adaptive Systems"

Nicolás E. Díaz Ferreyra and Johanna Schäwel

User-Centered Social Media
Research Training Group

1. Frequent uses of Social Media

- ✓ Users of **Social Network Sites** (SNSs) spend considerable amounts of hours per day exchanging (consuming or sharing) information and using services provided by such platforms.
- ✓ Users ***"voluntarily"*** submit ***personal information*** in order to benefit from the services offered such as maintaining friendship, blogging, sharing photos, music, articles, etc..
- ✓ ***Nothing comes for free!*** SNSs survive at expense of the information that users' upload to their profiles, and the behavior they exhibit while using the different services provided by the sites.
- ✓ Information stored in the ***Facebook*** servers include:
  - *Ads Clicked*
  - *Ad Topics*
  - *Check-ins*
  - *Facial recognition data*
  - *IP Address, log-ins, log-outs, deleted friends…*

2. The richness of information

- ✓ Discovering ***hidden knowledge*** in social networks is a centerpiece in many personalized online services and ad-targeting techniques.
- ✓ Knowledge discovery is basically what makes a SNS ***profitable***.
- ✓ Information about Social Media users can be used to study:
  - People's personal preferences.
  - Patterns of communication.
  - Flow of information.
  - Train predictive models to infer hidden information and improve the user experience within SNS's.
- ✓ Access to this information can bring serious concerns and threats to users' privacy.

EXAMPLE: *College admission officers withdraw students applications using information posted in SNS's.*

3. Privacy breaches in Social Media

Typical actors in Social Media Platforms are the ***Users*** (active or passive), the ***Service Providers*** and ***3rd Parties***.

Each of these players can have ***benevolent*** (GOOD) or ***malevolent*** (BAD) intentions:

- *Users: Interested in sharing and communicating information through online media (benevolent). Scammers, stalkers, and identity thieves (malevolent).*
- *Service Providers: Interested in mining data to provide additional utilities to the users. Extract information to produce goods they can sell to 3rd Parties.*
- *3rd Parties: Individuals or companies who are interested in user data for the purpose of advertising, market research, or collecting and re-selling the data.*

A ***privacy breach*** occurs when a piece of ***sensitive information*** about an individual is disclosed to an ***adversary***.

ADVERSARY: *Someone whose goal is to access information that has not been authorized to access.*

4. Self-Disclosure & Sensitive Information

Exposing ***personal information*** to other persons is referred as individuals' ***self-disclosure***.

Self-disclosure in on-line contexts like Social Media is the precondition for a ***functional social network***, otherwise SNSs would lack of diversity and fail on being interesting enough for the users to engage with.

Self-disclosure and over-exposition can have severe consequences and can put users' integrity into risk.

PRIVACY PARADOX: *Users seem careless when providing* ***sensitive information*** *through SNSs, however they consider privacy protection an* ***important issue***.

SENSITIVE INFORMATION: *Personal attributes that individuals may keep hidden from the public due to potantial harmful consequences.*

- ***European Parliament:*** *Personal data categories protected against public disclosure (e.g. racial or ethnic origin).*
- ***Canadian Personal Information Protection (Act 2000):*** *Any information can be sensitive depending on the context.*

4. Self-Disclosure & Sensitive Information

PROBLEM: *Users find difficult to differentiate sensitive information in their Social Media contributions.*

- ✓ Different legal frameworks propose different approaches for defining "sensitiveness" (EU, Canada, Australia…).
- ✓ Some users have higer or lower risk adversion levels.
- ✓ Sensitiveness modifiers: ***SNS Context*** & ***User's interpretation***

Fig. 1 *Elements for the analysis of sensitive information*

5. Self-adaptive systems

Self-adaptive systems are capable of dealing with the ***uncertainty*** and the ***continuously changing*** nature of the environment

They are also capable of dealing with ***emerging requirements*** that may be unknown at the design time.

Every self-adaptive system is mainly defined by a ***feedback loop*** that controls the self-adaptation process.

MAPE-K MODEL by IBM: *Blueprint for building autonomic systems with an explicit feedback loop architecture (Fig. 2).*

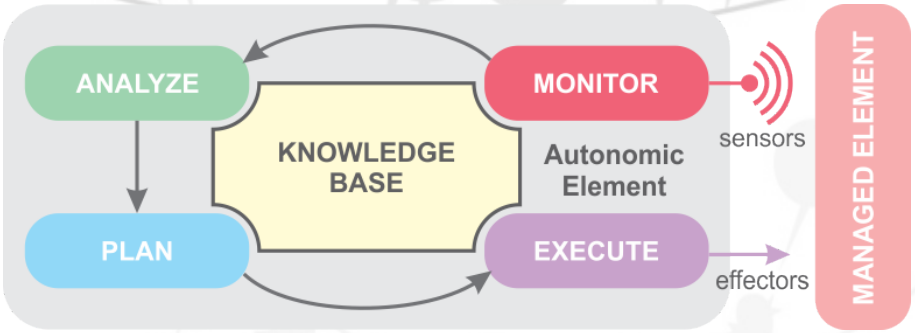

Fig. 2 *MAPE-K MODEL by IBM*

6. MAPE-K adapted to address self-disclosure

- ✓ User-Agent interaction: Recommend not to share potentially sensitive information.
- ✓ This sequence of detection-notification-acceptance defines a feedback loop between the user and the awareness system.
  - ✧ Managed element: User's SNS account
  - ✧ Monitor: Sharing activities of the user
  - ✧ Analyze: Sensitive Information
  - ✧ Plan: Recommendation of not sharing content
  - ✧ Execute: Send recommendation to the user (wait for the user's decision)
  - ✧ Knowledge base: Rules for the classification of sensitive information

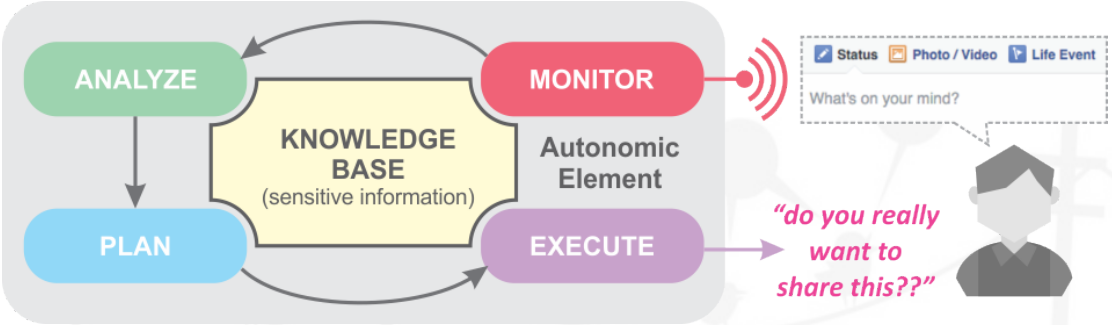

Fig. 3 *Adapted MAPE-K Loop*

7. Deciding the best course of action

- ✓ Self-adaptation brings into account a fundamental reasoning problem: decide which is the best ***course of action*** to follow based on the perceived stimuli from the environment.
- ✓ In Artificial Intelligence this type of reasoning is usually called ***planning***, where the condition to achieve is called ***goal*** and the sequence of actions that will make the goal true is called a ***plan***.
- ✓ ***Situation Calculus*** based on ***First Order Logic (FOL)*** is an adequate candidate to support planning due to its appropriateness for representing dynamically changing worlds.
- ✓ It provides a framework for defining a set of actions, states and changes in the environment, and entails a reasoning mechanism to make inferences.

8. Conclusions and related work

- ✓ Privacy breaches in SNSs have been identified and addressed through different types of privacy-preserving software architectures (e.g. P2P).
- ✓ Some researchers advocate particularly for ***decentralized*** architectures schemas unlike predominant ***centralized*** approaches.
- ✓ Benefits of ***decentralized*** approaches:
  - End-to-end encryption
  - Hidden activity from 3rd Parties
  - Hidden social graph
- ✓ Disadvantages of decentralized approaches: ***Major development effort*** and ***reduced functionalities***.
- ✓ Our approach propose to contribute to privacy from an ***Application Level***.
- ✓ Integrate through the extension points and services of SNSs.