Handling Privacy as Contextual Integrity in Virtual Communities

Yann Krupa[a], Laurent Vercouter[a], Jordi Sabater-Mir[b]

[a] École des Mines de St-Étienne, Centre G2I, Département ISCOD,
158, cours Fauriel, F-42023 Saint-Etienne, France

[b] IIIA - Artificial Intelligence Research Institute
CSIC - Spanish National Research Council
Campus UAB, 08193 Bellaterra, Catalonia, Spain

October 2010

Outline

1. Introduction
2. Contextual Integrity
3. Framework

Introduction

1. Introduction
2. Contextual Integrity
3. Framework

Question

Privacy is usually handled by security measures, e.g.:

- Trusted Computing (Sticky Policies[Mont03], Piolle[Pioll09], ...)
- Access Control (Bell-Lapadula[Bell73], PBAC[Byun05]...)
- Intrusive Control

Question

Privacy is usually handled by security measures, e.g.:

- Trusted Computing (Sticky Policies[Mont03], Piolle[Pioll09], ...)
- Access Control (Bell-Lapadula[Bell73], PBAC[Byun05]...)
- Intrusive Control

How to minimize privacy violations when standard security measures are unapplicable?

Virtual Communities

Main application domain is Virtual Communities:

- Virtual enterprise
- Decentralised social networks

Properties:

- Open systems
- Decentralized
- Autonomous agents

Proposition

Detect privacy violation from the agent point of view.

- Propose a privacy violation formalism
- Specify an interaction framework
- Define norms for privacy enforcement

Contextual Integrity

1. Introduction
2. Contextual Integrity
3. Framework

Contextual Integrity: Nissenbaum 2004

- Usually, private/public paradigm:
  - private: transmission/use restrictions applies
  - public: no restrictions
- Contextual integrity: no private/public, it only depends on the transmission context
  - every transmission can trigger a violation

Contextual Integrity: Nissenbaum 2004

“whether a particular action is determined a violation of privacy is a function of :

- the nature of the situation/context
- nature of the information with regard to the context
- roles of agents receiving the information
- relation of agents to information subject
- terms of dissemination defined by the subject”

Contextual Integrity: Nissenbaum 2004

“whether a particular action is determined a violation of privacy is a function of :

- the nature of the situation/context
- nature of the information with regard to the context
- roles of agents receiving the information
- relation of agents to information subject
- terms of dissemination defined by the subject”

Formalize it to check if a transmission is a violation or not.

Framework

1 Introduction

2 Contextual Integrity

3 Framework

Main Idea

Agents have to reason:

- Before sending a message (propagator)
- Upon reception of a message (receiver)

Message Structure

A message is composed by unspecified information and the following meta-informations:

- Context Tags
- Target Tags
- Privacy Policies
- Transmission Chain

All meta-informations are signed by their author.

Appropriateness-laws

From Contextual Integrity theory, we say that a transmission is **appropriate** if:

1. Transmission context correspond to the information nature
2. Receiving agent has a role within the transmission context
3. Target’s preferences are respected

```
appropriate(M):-
   fitcontext(C,M),
   fitrole(C,M),
   fitpolicy(M).
```

A-laws : fitcontext

Transmission context must correspond to the information nature.

```
fitcontext(C,M):-
   information(M,I),
   propagator(P,M),
   context(C,I),
   contexttag(C,P,M).
```

A-laws : fitrole

Agent must have a role within the transmission context.

```
fitrole(C,M):-
   receiver(Rc,M),
   role(Rc,R),
   rolecontext(R,C).
```

A-laws : fitpolicy

The target’s preferences must be respected.

```
fitpolicy(M):-
   information(M,I),
   policy(P,T,I),
   target(T,I),
   policyvalid(P,I).
```

Enforcement?

What should an agent do to enforce these laws?

Privacy Enforcing Norms (PENs)

1. Respect the Appropriateness laws
2. Sign the transmission chain before sending
3. Do not send information to untrusted agents
4. Delete information from untrusted agents
5. Punish agents violating PENs (this one included)

Privacy Enforcing Norms (PENs)

1. Respect the Appropriateness laws Contextual Integrity
2. Sign the transmission chain before sending
3. Do not send information to untrusted agents
4. Delete information from untrusted agents
5. Punish agents violating PENs (this one included)

Privacy Enforcing Norms (PENs)

1. Respect the Appropriateness laws Contextual Integrity
2. Sign the transmission chain before sending Responsibility
3. Do not send information to untrusted agents
4. Delete information from untrusted agents
5. Punish agents violating PENs (this one included)

Privacy Enforcing Norms (PENs)

1. Respect the Appropriateness laws Contextual Integrity
2. Sign the transmission chain before sending Responsibility
3. Do not send information to untrusted agents Social Exclusion
4. Delete information from untrusted agents
5. Punish agents violating PENs (this one included)

Privacy Enforcing Norms (PENs)

1. Respect the Appropriateness laws Contextual Integrity
2. Sign the transmission chain before sending Responsibility
3. Do not send information to untrusted agents Social Exclusion
4. Delete information from untrusted agents Avoiding Violation
5. Punish agents violating PENs (this one included)

Privacy Enforcing Norms (PENs)

1. Respect the Appropriateness laws Contextual Integrity
2. Sign the transmission chain before sending Responsibility
3. Do not send information to untrusted agents Social Exclusion
4. Delete information from untrusted agents Avoiding Violation
5. Punish agents violating PENs (this one included) Self Consistency

Future Works

- Formalize trust/framework interaction
- Define good agents
- Do a testbed
- Show that agents violating the PENs are excluded from the system

Conclusion

- Framework for privacy in open and decentralized MAS (1st stage)
- Based on Contextual Integrity theory
- Agents are both actors and judges in the system

Some issues to address:

- The minimum percentage of norm enforcing agents
- "Journalist problem"
- Reputation Paradox

Thank You

Thank you for your attention.