Privacy Patterns

Presented at PST’2016

Professor Clark Thomborson
Computer Science Department
13 December 2016
How can software offer privacy?

- What is privacy?
  - I offer a constructive definition, based on Westin’s 1967 survey
  - I extend Westin’s taxonomy, to cover the “information privacy” of the EU’s Data Protection Directive
- I’ll teach you a bit about object-oriented design along the way…
- Working manuscript: http://arxiv.org/abs/1612.01553
Our starting point: Aristotle(!)

- All humans are mortal
- All Greeks are human
- Therefore: all Greeks are mortal

- In an object-oriented language:
  - Human has a die() method
  - Greek is a subclass of Human
  - Therefore: any Greek can die()

- Not an exact translation
  - Static logic → dynamic system
Extending the design

- Aristotle is-a Greek
  - An “instance” of his class
- I am not representable
  - Clark is-a NZperson
  - Clark2 is-a USperson
  - An instance is a member of *exactly one* class.
- Problem: representing multiple identities
Design Patterns (Gamma, 1994)

- “Design patterns capture solutions that have developed and evolved over time.
  - Hence they aren’t the designs people tend to generate initially.
  - They reflect untold redesign and recoding as developers have struggled for greater reuse and flexibility in their software.
- “Design patterns capture these solutions in a succinct and easily applied form.”
Privacy Patterns

- A subclass of design patterns
  - Foundational patterns, for private identities
  - Privacy affordances, for
    - Solitude
    - Intimacy
    - Anonymity
    - Reserve
    - Confidence

- Your feedback is welcome, this is a work-in-progress
Entity, Aspect, Role, Context

Privacy Patterns
Persona = aspect of a human

- Thousands of years ago, Roman actors wore *persona* (masks) to depict their roles.

- A hundred years ago, Carl Jung asserted that, as social beings, we must hide our true identity:
  - A *persona* is “a compromise between the individual and society as to what a man should appear to be”.

Privacy Patterns
A taxpayer is a persona

- One-way navigability from Human to Persona
  - ssNumber doesn’t reveal irdNumber
  - irdNumber doesn’t reveal ssNumber
Solitude

“The first state of privacy is solitude;
here the individual is separated from the
group and freed from the observation of
other persons.” (Westin, 1967)
- **Context** participates in 1..* Role
- **Isolated** intrudes into Isolate 1
- **Solitude** introspect() and claimSolitude()
- **Isolate** controls, observes Intruder 1
- **Intruder** controls, observes Isolate
- **Isolation** embodies 1
- **Entity**

<<forbiddance>> No entity shall intrude.

<<allowance>> Any entity may intrude in urgent circumstances e.g. when the isolate is at risk of extreme harm.
Intimacy

“In the second state of privacy, intimacy, the individual is acting as part of a small unit that claims and is allowed to exercise corporate seclusion so that it may achieve a close, relaxed, and frank relationship between two or more individuals.” (Westin, 1967)
Context

Secluded

«interface»

Intimacy

revealSecret()
claimIntimacy()

Role

Intimate

«forbiddance>>
No secluded context shall have more than a few intimates.

observes, controls

Seclusion

Secret

«forbiddance>>
No entity shall reveal, to any entity outside this context, any intimate controls, observations, or secrets.

«forbiddance>>
No entity shall have an intimate aspect unless they have been invited to fill this role.

SentientActor

«requirement»
Any entity whose aspect fills a Secret role is owned by an entity whose aspect fills an Intimate role.
Anonymity, Reserve

- "The third state of privacy, anonymity, occurs when the individual is in public places or performing public acts but still seeks, and finds, freedom from identification and surveillance.

- "Reserve, the fourth and most subtle state of privacy, is the creation of a psychological barrier against unwanted intrusion; this occurs when the individual’s need to limit communication about himself is protected by the willing discretion of those surrounding him.” (Westin, 1967)
Context

PublicSphere
  releaseIntoPublicProperty()

Reserve
  isOffensive()
  claimReserve()

Anonymity
  authenticateAnonym()
  claimAnonymity()

Role

Society

PublicProperty

PublicFigure
  name: String

Anon
  observe: String
  observes, controls

Government
  <<forbiddance>>
  Controls, observations, and releases shall not be offensive to a normative public figure.

SentientActor

<<requirement>>
  Any entity playing a PublicFigure role is an Actor.

<<requirement>>
  The entity playing a PublicFigure role is also playing its aliases.

<<allowance>>
  A PublicFigure who uses an alias for offensive controls, observations, or releases may be "named and shamed" in a public release.

<<requirement>>
  The entity playing a Government role is a JudicialAuthority.
Confidence

- I added a fifth state of privacy to Westin’s taxonomy, to handle “information privacy”
  - Formally: this is a subclass of Intimacy
- A private individual enters the state of confidence when they release their personal information to a Trustee e.g.
  - Doctor, lawyer, social network provider.
Any entity whose aspect fills the Asset role is owned by the entity whose aspect fills the Trust role.

Any trustee shall control and observe assets in adiligent and competent pursuit of the purpose of the trust, with beneficence toward the truster(s).

Any entity whose aspect fills the Truster role is a NaturalPerson.

Any entity whose aspect fills the Trustee role is a SentientActor.
Review

■ What is privacy?
  ■ I offered a constructive definition, based on Westin’s 1967 survey
  ■ I extended Westin’s taxonomy, to cover the “information privacy” of the EU’s Data Protection Directive
  ■ I taught you a bit about object-oriented design along the way…

■ Working manuscript: http://arxiv.org/abs/1612.01553