



University of Cambridge
Computer Laboratory

Context-Adaptive Information Security for UbiComp Environments

Boris Dragovic and Jon Crowcroft

{firstname.lastname}@cl.cam.ac.uk



Motivating Observation

- Information in a UbiComp system is, throughout its lifetime, while being in possession of or accessed by legitimate users, exposed to variable levels of security and privacy risks through the degree of its potential exposure to the surrounding.



Motivating Observation

- Most obvious: User Interfaces
 - Personal Server (Intel), Virtual Network Computing, Steerable User Interfaces etc.
- But.. applicable throughout information life cycle
 - Lost/stolen laptops/PDAs, insecure communications links etc.
- Information availability vs. security



The Aim

- Develop a framework to mitigate security and privacy risks present for a piece of information, through its perceived exposure level, in an environment through a set of protective mechanisms, maximizing its availability to legitimate users.
- ... in a “cooperating user” scenario, i.e. representing an aid in protecting information security and privacy.



A comparison: Access Control

- Access Control
 - Point of system-level access, [subject, object, <context>].
 - Uniform, coarse grained decisions.
- Our paradigm
 - Continual, life-long protection, [context LoE, object].
 - (Also at the point of Access Control.)
 - Maximize availability through a spectrum of protective actions.

Orthogonal – complementary, not competing, paradigm.



Protective actions

- Two classes:
 - Data manipulation:
 - Restricting information content (format adaptation)
 - Choice of appropriate data set (e.g. Chalmers et al.: map adaptation work)
 - Container “hopping”:
 - Transferring data objects among container of a same class but different type. e.g. full size display vs. mobile phone's screen.



Levels of Exposure (LoEs)

- Quantify the perceived extent to which data is accessible to its “surrounding”.
- Example:
 - A two level LoE model:
 - “visible” - credible threat of exposure
 - “non-visible” - absence of the threat
- LoEs model uniform across the system.
- LoE activation triggered by a set of contextual attributes.



Context, as we see it

- Example:
 - Two instances of a data object: A and B.
 - A is being displayed on an LCD panel.
 - B is on a storage device.
 - The “visible” LoE triggered by:
 - Instance A: e.g. Presence of a third party within a visibility range.
 - Instance B: e.g. Proximity of the device to the owner.
 - Different LoE triggers depending on the device data exists within - containment.



Containment

- Split the notion of context:
 - Environment – the traditional view
 - Containment
- A Container – immediate physical enclosure in which an data object exists
 - e.g. A display, a storage device, a communications link etc.
- Container classification:
 - “type” and “class”



Collaboration groups

- Trust-based, intra-PAN or with dedicated services
 - e.g. Resurrecting Duckling (Stajano) etc.
- Remote operation:
 - Context sensing
 - Increased confidence
 - Wider LoE establishment capabilities
 - Protective actions
 - Resource preservation/exploitation



Prototype

- Explore the issues and build the framework through an incremental prototype:
 - User Interface application (e.g. VNC, Personal Server etc.)
 - Expansion for different container classes.
 - Collaboration group: extension to PAN e.g. simple laptop – mobile phone.
 - GPRS-WLAN-LAN-Bluetooth testbed.



A number of issues

- Policy & profiles
- Meta-data model
- Application awareness
- Complexity
- Cognitive load, user acceptance
- Scalability
- Manageability
- etc.