Security and Privacy issues in Ubiquitous Computing

- Bharat Singh

Ubiquitous Computing

- Computing is made to appear everywhere and anywhere
- Ubiquitous computing can occur using any device, in any location, and in any format
- What happens to my privacy?

What is privacy?

The right to select what personal information about me is known to what people

Types of privacy

- Media privacy – peeping, clicking pictures
- Territorial privacy – your house
- Communication Privacy – phone lines
- Bodily privacy
- Information privacy – NSA

First 4 are established in most legal frameworks

Fair Information Practices

- Openness and transparency: There should be no secret record keeping
- Individual participation: The subject of a record should be able to see and correct the record
- Collection limitation: Data collection should be proportional and not excessive compared to the purpose of the collection.
- Data quality: Data should be relevant to the purposes for which they are collected and should be kept up to date.
- Use limitation: Data should only be used for their specific purpose by authorized personnel.
- Reasonable security: Adequate security safeguards should be put in place, according to the sensitivity of the data collected.
- Accountability: Record keepers must be accountable for compliance with the other principles

European Union's Directive 95/46/EC

- Protection of individuals with regard to the processing of personal data and on the free movement of such data
- Limits data transfers to non-EU countries only to those with "an adequate level of privacy protection."
- Personal data may only be processed if the user has unambiguously given his or her consent

Issues

- Feasibility: All laws and legislation require enforceability. If privacy violations are not traceable, the much stressed point of accountability becomes moot
- Convenience: the advantages of free flow of information outweighs the personal risks in most cases
- Communitarian: personal privacy needs to be curbed for the greater good of society (trusting the NSA)
- Egalitarian: if everybody has access to the same information, it ceases to be a weapon in the hands of a few well-informed

Aspects of ubiquitous computing

- Ubiquity: Ubiquitous computing is everywhere
- Invisibility: We want them to actually disappear from our views
- Sensing: The ability of sensors to accurately perceive certain aspects of the environment increases
- Memory amplification: Advancements in speech and video processing
- Mobility: Pervasive computing environment should be as mobile as its users (Omnipresent)

-- Add more adjectives

Privacy in Ubiquitous computing

Notice:

- Ubiquitous computing ideally suited for covert operation and illegal surveillance, e.g.: secret coffee mug
- Depending on the type of device, different announcement mechanisms would need to be found, e.g.: radio emergency frequency, robots.txt www search
- The Platform for Privacy Preferences project allows Web sites to describe their data collection practices in a machine readable way, it may be something which can be used

Choice and Consent

- Requires collectors to receive explicit consent from the data subject - announce and declare data collection not enough
- Hand written signature is most common, not possible in electronic transactions
- No public-key-infrastructure (PKI) has achieved widespread usage, makes verification of signatures difficult (not that important!)
- Did the user had any knowledge of whether he signed it, may not be physically possible and might be unusable, e.g.: hundreds of sensors asking to say ok

Anonymity and Pseudonymity

- Anonymity can be defined as “the state of being not identifiable within a set of subjects.” The larger the set of subjects is, the stronger is the anonymity
- Asserting explicit consent in electronic communications is difficult
- Direct communications on the other hand often disclose my real identity – MAC address, soln: use one time addresses
- Real-world appearance, unlike my cyberspace one, cannot be disguised that easily (video cameras can get a picture of your face)

Pseudonymity

Pseudonymity is an alternative that allows for a more fine grained control: a certain ID to a certain individual, this person can be repeatedly identified until s/he changes to a different ID

Proximity and Locality

- The idea of proximity is basically a practical solution to much of what makes notice and consent hard
- One would require that information is not disseminated indefinitely, even not across a larger geographic boundary, such as buildings or rooms
- Anybody interested in this information would need to be actually physically present in order to query it
- No additional authentication would be required anymore – e.g.: printer in a hallway can tell which documents were printed last night to any passer by

Adequate Security

- The significance of security is often perceived much higher than that of privacy
- New set of constraints, mainly in the areas of power consumption and communication protocols
- Reduce much of this complexity by employing robust security only in situations with highly sensitive data transfer
- Principles like proximity, locality, and proportionality, much of our basic infrastructure could indeed function without any explicit security model at all
- Security might not be the panacea it appears to be, and it might not need to be that panacea either

Access and Recourse

- Requires a set of regulations that separate acceptable from unacceptable behavior
- A reasonable mechanism for detecting violations and enforcing the penalties set forth in the rules
- Augmenting a P3P-like protocol with something like digital signatures would allow for non-repudiation mechanisms
- Database technology could provide data collectors with privacy-aware storage technology

Collection and Use Limitation

- Only collect data for a well-defined purpose (no “in-advance” storage)
- Only collect data relevant for the purpose (not more)
- Only keep data as long as it is necessary for the purpose

Bottom-Line

- Formalized privacy
- Privacy from an information point of view
- Raised privacy issues in the context of ubiquitous computing – most important
- Proposed a solution for the issues using “coulds” and “mights”

Security and Privacy in Pervasive Computing, Challenges

Extending Computing Boundaries:

- Beyond the computational infrastructure, it attempts to encompass the surrounding physical spaces

- Prone to more severe security threats that can threaten people and equipment in the physical world as much as they can threaten their data and programs in the virtual world

User Interaction

- Security Issues: Users in the space cannot easily be prevented from seeing and hearing things happening in it, so this has to be taken into account while designing access control mechanisms

Security Policies

- Help to specify, implement, and enforce rules to exercise greater control over the behavior of entities
- The policy management software maintains an exhaustive database of corresponding device and resource interfaces, complexity increases

Info Ops

- Actions taken that affect adversary information and information systems while defending one's own information and information systems
- Pervasive computing gives extreme leverage and adds much more capabilities to the arsenal of info warriors, making info ops a much more severe threat

Security Requirements (somebody asked a security expert to describe “Superman”)

- Transparency and Unobtrusiveness: Should be transparent, blending into the background without distracting users
- Multilevel: One size does not fit all
- Flexibility and Customizability: adapt to environments with extreme conditions and scarce resources
- Scalability: Able to support huge numbers of users with different roles and privileges

Security Requirements

- Interoperability: Assumption that a particular security mechanism will eventually prevail is flawed, necessary to support multiple security mechanisms
- Extended Boundaries: Security was restricted to the virtual world, security now should incorporate some aspects of the physical world, preventing intruders from accessing physical spaces

Security Requirements

- Context-Awareness: Security is somewhat static and context insensitive, Pervasive computing integrates context and situational information, transforming the computing environment into a sentient space

Case Study: Gaia OS Security

A component-based, middleware operating system that provides a generic infrastructure for constructing pervasive computing environments

Components

A surround audio system, four touch plasma panels with HDTV support, HDTV video wall, X10 devices, electronic white boards, IR beacons, Wi-Fi and Bluetooth access points, video cameras, and flat panel desktop displays, group meetings, seminars, presentations, demos, and for entertainment purposes

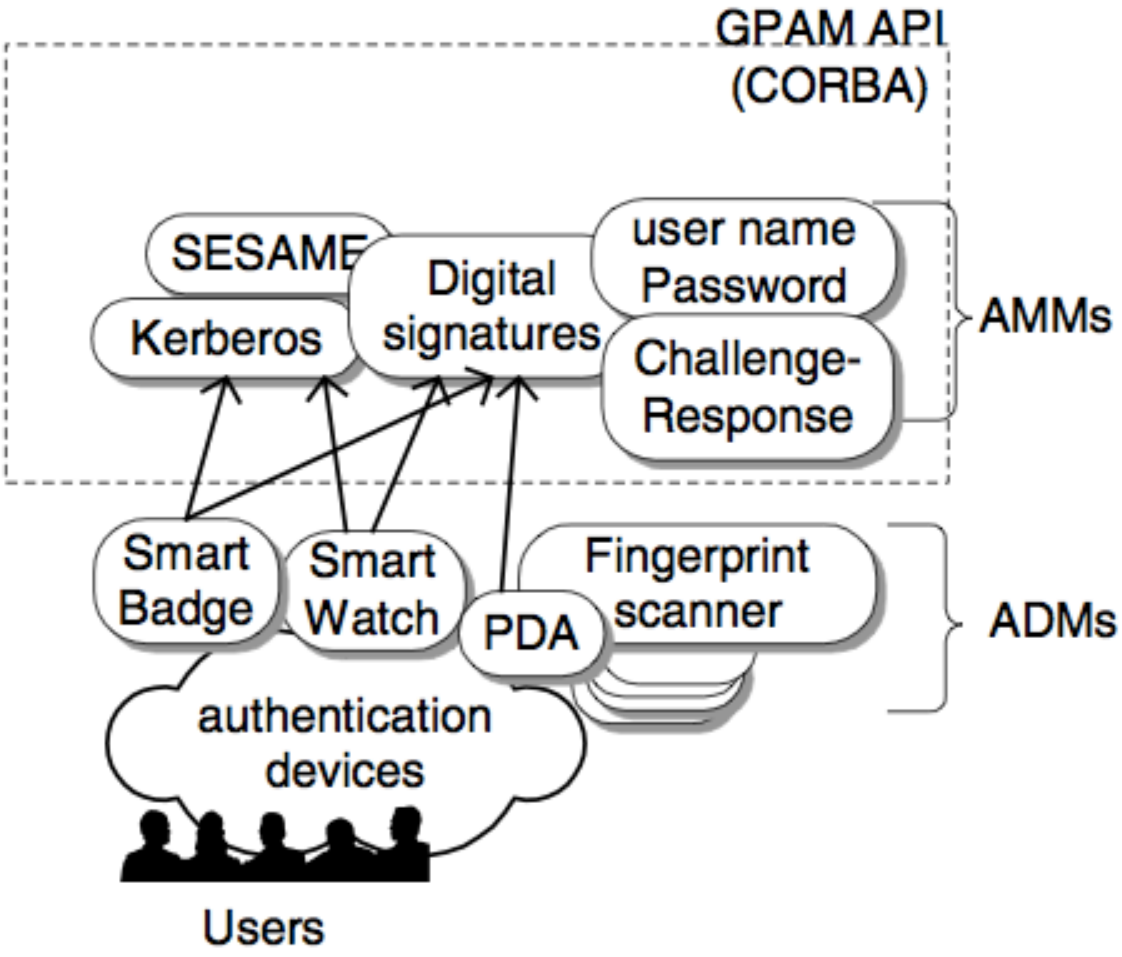
Authentication

- Balance between authentication strength and non-intrusiveness
- Let context decide how strong the authentication
- Associate confidence values to each authentication process (face recognition, smart badges, fingerprint, retinal scans, etc)

Authentication

- PAM (Pluggable Authentication Module) provides an authentication method that allows the separation of applications from the actual authentication mechanisms
- Gaia Authentication Mechanisms Modules (AMM), which implement general authentication mechanisms or protocols that are independent of the actual device being used for authentication
- Authentication Device Modules (ADM) are independent of the actual authentication protocol; instead, they are dependent on the particular authentication device

Authentication



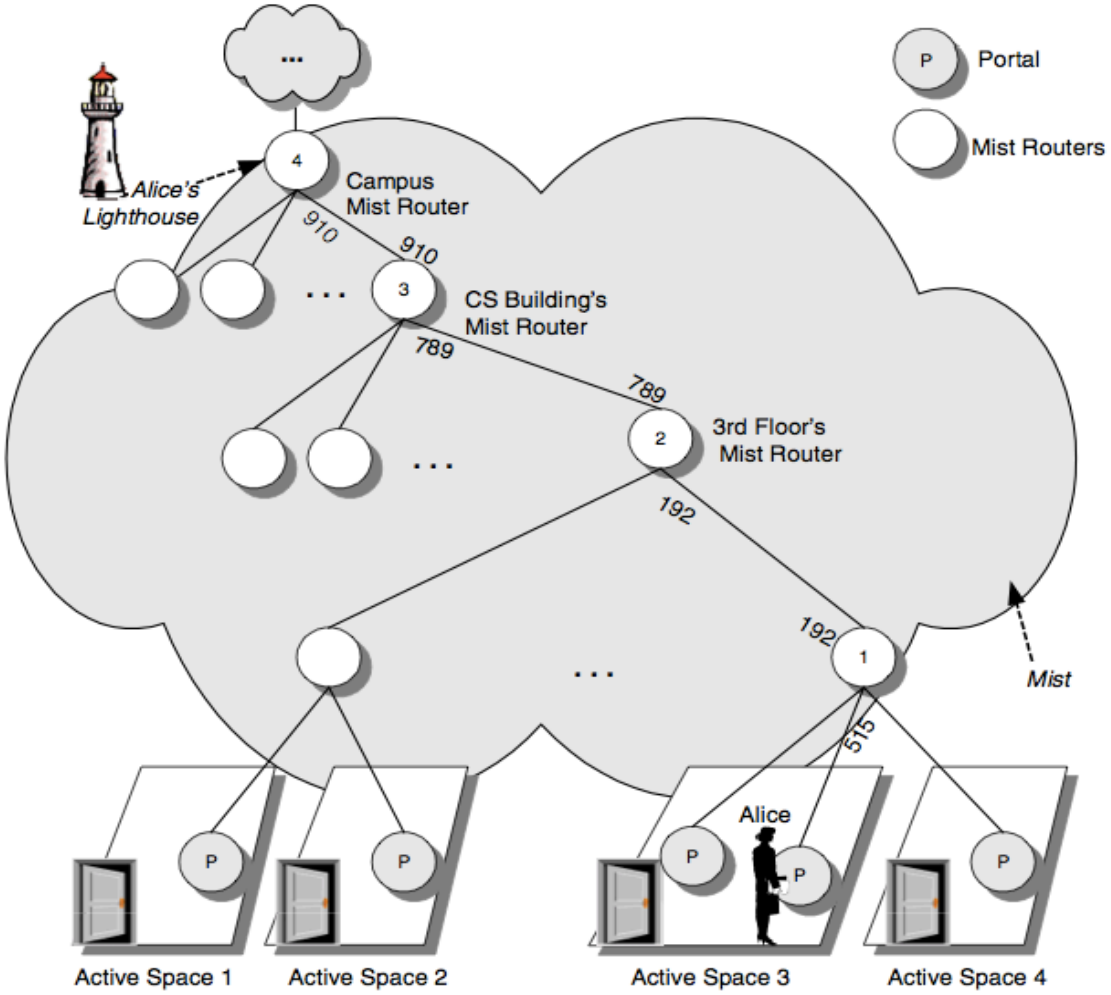
Mist Privacy Communication

- Facilitates private communication by routing packets using a hop-by- hop, handle-based routing protocol
- Portals are devices capable of detecting the presence of people and objects through the use of base stations or sensors, incapable of positively identifying the users

Mist Privacy Communication

- Special Mist Router referred to as a Lighthouse, exists at a “higher level” in the hierarchy, high enough not to be able to deduce the actual physical location of the user

Mist Privacy Communication



Dynamic Security Policies

- Designed with explicit knowledge of system behavior, focusing on the interactions between various system objects

- Set of access rights triples (subject, object, permissions) forms a conceptual access control matrix

Access Control

- Smart rooms are typically shared by different groups of users for different activities at different points in time
- Access control policies and mechanisms are necessary to ensure that users only use the resources in an active space in authorized ways
- RBAC model for policy configuration, and implements both discretionary and mandatory access controls

Takeaway

- Unless security concerns are accommodated early in the design phase, pervasive computing environments will be rife with vulnerabilities and exposures

- There is no single “magical” protocol or mechanism that can address all the security issues and meet the requirements and expectations of secure pervasive computing

- Access control, information flow, availability, secure protocols for authentication, non-repudiation, confidentiality ,integrity (more adjectives) can be specified in terms of system properties

THE END