



Works in Progress

Editor: Anthony D. Joseph ■ UC Berkeley ■ adja@cs.berkeley.edu

Security and Privacy in Pervasive Computing

EDITOR'S INTRO

In this issue's Works in Progress department, we have six projects. The first two projects address an individual's privacy concerns and preferences. The next entry discusses a project on data protection for electronic passports. The remaining three projects are investigating various types of privacy protection mechanisms for data collected in pervasive computing environments, by attestation services, and by voice recording systems. —Anthony D. Joseph

PERSONALIZATION ACCORDING TO PRIVACY CONCERNS AND TECHNOLOGICAL AWARENESS

Charalampos Patrikakis, Pantelis Karamolegkos, and Athanasios Voulodimos, School of Electrical and Computer Engineering, National Technical University of Athens

In a user's online profile, the information considered private varies according to the user's privacy concerns and the information's importance. On the other hand, a user's technological knowledge affects the level of information he or she directly manages and the level of abstraction that the system should offer. To address these issues, we're evaluating a methodology for designing services that meet user needs for privacy and technology awareness. The methodology uses as input a service description consisting of distinct features, for which the setup interface is determined by the user's particular privacy concerns and technology awareness level. This selection of the way that each service feature will be offered forms different service versions that correspond to different user profiles.

On the basis of a set of predefined service profiles, we provide best matching between the differentiated user

needs and the most relevant profile. To identify each user's preferences, we record the user's feedback for each specific service feature (see figure 1).

Each service feature is mapped to a related graph, and we ask the users to identify their preferences for that particular service feature. Using a k -means clustering algorithm (where we use the identified service profiles as centroids), we identify the service version that most closely matches the user preferences. Reversing the process, we can collect input from several questioned users and, on the basis of that input, design a service that will satisfy as many users as possible.

For more information, contact Charalampos Patrikakis at bpatr@telecom.ntua.gr or see www.telecom.ntua.gr/~bpatr.

MEASURING PRIVACY THROUGH ENTROPY IN CONTEXT-AWARE MOBILE SERVICES

Charalampos Patrikakis and Athanasios Voulodimos, School of Electrical and Computer Engineering, National Technical University of Athens

Offering high-quality, context-aware mobile services is closely related to reporting data that describes the user's

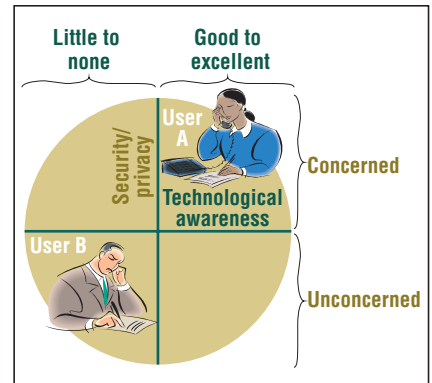


Figure 1. Our model for collecting user feedback regarding privacy concerns and technology awareness.

environment, situation, preferences, and status. On one hand, access to accurate, detailed information about the user's status helps mobile (especially location- and context-aware) service providers provide high-quality answers to user queries. On the other hand, it raises issues of information misuse, such as unwanted "personalized" advertising or surveillance of users' whereabouts.

Researchers have attempted to depersonalize the user information, mostly by using central anonymizer servers that blend information from several users (that is, k -anonymity models). In our present work, we use entropy (H) as the measurement of diversity and, therefore, difficulty in identifying a user's personal preferences, parameters, and whereabouts. On the basis of Claude Shannon's theoretical mathematical framework, we quantify an information source's uncertainty. Our work focuses on providing different abstraction levels of the user's reported information when requesting context-aware mobile services, each of which corresponds to a different entropy

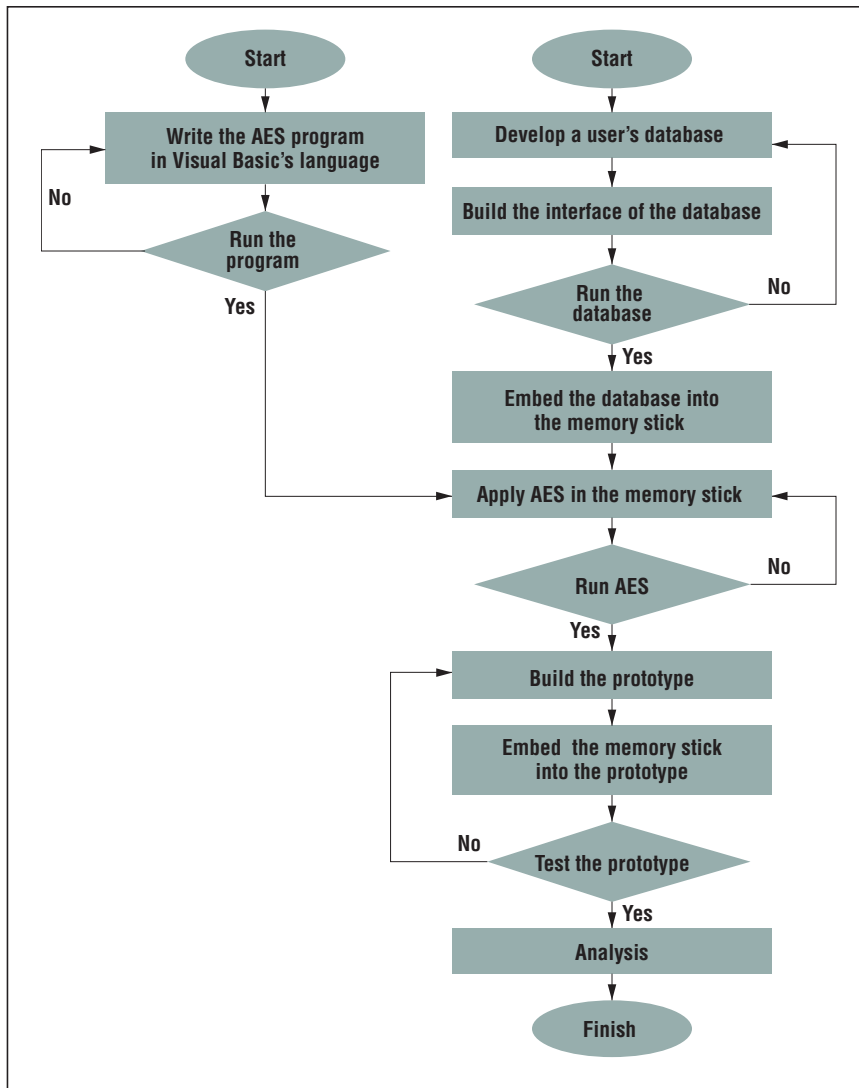


Figure 2. Steps taken in developing the e-passport application.

level. Because the reported information's privacy and accuracy are counterbalancing forces, we identify minimum and maximum entropy levels that identify the corresponding privacy and accuracy levels of user-reported personal data. We apply the model to geographical user information, on the basis of a quad-tree model of organizing map data, and to user preferences, on the basis of spectral (or hierarchical) clustering of user preferences such as for films, music, and other entertainment types.

The PLASMA (Personalized, Location-Aware Services over Mobile Architectures) project is an attempt to materialize the above ideas in a fully functional

prototype. For more information, contact Charalampos Patrikakis at bpatr@telecom.ntua.gr or see www.telecom.ntua.gr/~bpatr.

THE ADVANCED ENCRYPTION STANDARD ALGORITHM IN E-PASSPORT APPLICATIONS

Mohd Helmy Abd Wahab, Nik Shahidah Afifi Mohd Taujuddin, and Christina Hanif, *Universiti Tun Hussein Onn Malaysia*

The Advanced Encryption Standard is expected to become the accepted means of encrypting digital information, such

as financial, telecommunications, and government data (Merike Kaeo, *Designing Network Security*, Cisco Press, 1999). The AES is a cryptographic algorithm that protects electronic data. It has symmetric-key block ciphers that can use 128-, 192-, and 256-bit keys and that can encrypt and decrypt data in blocks of 128 bits (16 bytes). We successfully implemented the prototype using Visual Basic.

In our research at InfoSec Group, we use AES to protect the information in an e-passport. This project will use a collective passport for groups of five to 20 people traveling to countries in the Association of Southeast Asian Nations. Figure 2 shows the steps for developing the e-passport application.

Figure 3 shows the main interface for the e-passport application. This system provides four main services:

- user profiles,
- a traveling record,
- visa information, and
- data safety, which encrypts the database to protect data from unauthorized persons.

By using a memory stick, you can view and check the passport holder's information faster than by reading it page by page. In addition to security concerns, we're considering the algorithm's availability and integrity. Only authorized administration personnel can access and change the e-passport information, which makes the prototype safe and reliable. We plan to further improve the e-passport's security system. For example, we plan to use a microchip to store all the passport holders' information because it's smaller than the memory stick, provides a higher capacity, and can be read faster.

For more information, contact Mohd Helmy Abd Wahab at helmy@uthm.edu.my.

PRESERVING ANONYMITY IN PERVASIVE ENVIRONMENTS

Linda Pareschi and Daniele Riboni, *University of Milan*

