IEEE pervasive COMPUTING
MOBILE AND UBIQUITOUS SYSTEMS
www.computer.org/pervasive

Security and Privacy in Pervasive Computing

Charalampos Patrikakis, Pantelis Karamolegkos, Athanasios Voulodimos, Mohd Helmy Abd Wahab, Nik Shahidah Afifi Mohd Taujuddin, Christina Hanif, Linda Pareschi, Daniele Riboni, Stefan G. Weber, Andreas Heinemann, Sen-ching Samson Cheung, Jayahsri Chaudhari, and Jithendra K. Paruchuri

Vol. 6, No. 4
October–December 2007

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.

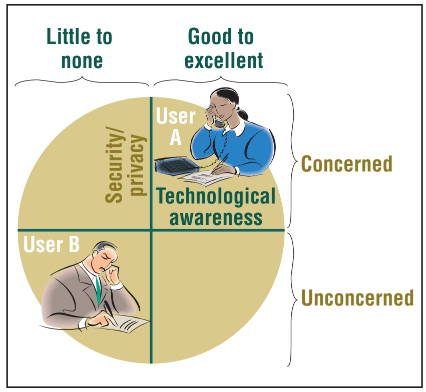

Figure 1. Our model for collecting user feedback regarding privacy concerns and technology awareness.

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 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

WORKS IN PROGRESS

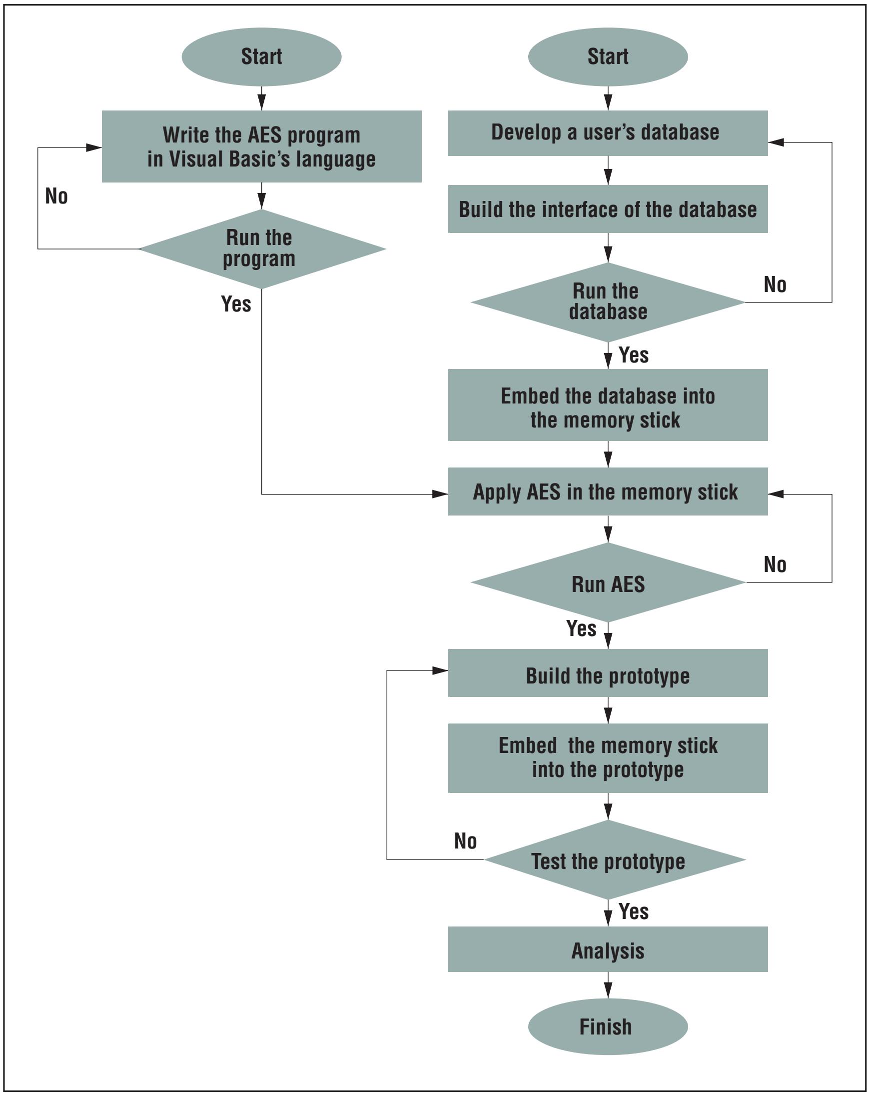

Figure 2. Steps taken in developing the e-passport application.

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*

Privacy is considered fundamental for context-aware services. Indeed, the proliferation of sensing technologies necessitates protecting users from the disclosure of sensitive information such as their location, activity, and physiological parameters.

To address this issue, recent research has concentrated on the use of *k*-anonymity techniques, which aim to hide the user in a set of *k* potential issuers. However, current anonymity techniques are insufficient for a pervasive computing scenario in which users' behavior can be continuously monitored by cameras, sensors, and even people. Indeed, even enforcing *k*-anonymity, in several cases an attacker can recognize the actual issuer by monitoring the potential issuers' behavior with respect to service responses. For example, consider a pervasive gym system that suggests exercises on the basis of gender, age, and physiological data. Even if users are anonymous in a set of *k* potential issuers, the attacker can easily recognize who issued a particular request if, after a reasonable lapse of time, a person starts to use a machine that the system suggested to only one issuer. To our knowledge, no one has yet addressed this class of attacks (which we call *shadow attacks*).

We are defining appropriate defense techniques for shadow attacks and defining a comprehensive measure to express the privacy-threat level deriving from possible users' behaviors on the basis of service responses and environmental conditions.

For more information, contact Daniele Riboni at riboni@dico.unimi.it or see http://webmind.dico.unimi.it/care.

PRIVACY-RESPECTING ATTESTATION IN UBICOMP

Stefan G. Weber and Andreas Heinemann, *Technische Universität Darmstadt*

Ubiquitous computing infrastructures document individuals' everyday lives by collecting large amounts of data. Although privacy concerns and fears of continuous surveillance are obvious, the collected data can help individuals attend to their personal and legal interests. Our project, Privacy vs. Attestation, explores and develops flexible privacy-respecting mechanisms, showing how they can provide new services in ubiquitous computing environments.

We're investigating so-called *attestation services*, which help users prove actions, presence or absence in dispute cases, and damage or loss by harnessing ubiquitous data repositories. For example, imagine that you arrive at a train station but that your train has left too early, causing you to miss a project meeting or an exclusive event. Being able to prove this fact using an attestation service lets you demand compensation or at least appease your employer.

Realizing attestation services in a privacy-respecting and nonrepudiating manner is challenging. We're developing fine-grained and customizable ID management, anonymization, access control, and dissemination control mechanisms, which protect users' privacy and disperse personal data at an individually convincing level. Our work addresses usability issues to manage the fine granularity offered, and it facilitates automated dissemination of requested portions of personal data as parts of these services.

For more information, contact Stefan Weber at sweber@tk.informatik.tu-darmstadt.de or see www.tk.informatik.tu-darmstadt.de/index.php?id=451.

PRIVACY PROTECTION OF HUMAN SPEECH

Sen-ching Samson Cheung, Jayahsri Chaudhari, and Jithendra K. Paruchuri, *University of Kentucky*

Audio is an important medium in pervasive computing environments. The combination of ubiquitous microphone arrays, sophisticated source separation, and speaker identification algorithms let us track and identify individuals using only audio. However, researchers haven't extensively studied audio's privacy protection. An audio privacy-protection scheme aims to hide the speaker's identity while preserving the intelligibility of the speech. The Multimedia Information Analysis Laboratory at the University of Kentucky recently presented results on using a pitch-shifting algorithm for audio privacy protection in a wearable video system.[1] The system segments and distorts the subject's voice by pitch shifting and automatically locates, tracks, and blocks the subject's face. We evaluate the privacy level by checking whether an automatic speaker-identification system can identify a speaker by his or her distorted speech. We measure intelligibility on the basis of the number of errors in the transcription of the distorted speech. Although pitch shifting produces good privacy protection, its intelligibility results are poor, partially owing to the unnaturalness of the distorted speech.

We're developing a more sophisticated voice-morphing scheme that transforms speech from one speaker to another. Our goals are twofold. First, voice morphing likely will produce a more natural-sounding voice, making the resulting speech more intelligible. Second, by using appropriate vocal-tract models, we can better control the output speaker's perceived identity, which lets us place audio privacy protection on a proper data privacy framework such as the *k*-anonymity model.[2]

For more information, contact Sen-ching Samson Cheung at cheung@engr.uky.edu or see the MIA group Web site at www.vis.uky.edu/mialab.

REFERENCES

1. J. Chaudhari, S.-c. Cheung, and M.V. Venkatesh, "Privacy Protection for Life-Log Video," *Proc. IEEE Workshop Signal Processing Applications for Public Security and Forensics*, IEEE Press, 2007, pp. 1–5; www.vis.uky.edu/~cheung/doc/safe07.pdf.
2. L. Sweeney, "K-anonymity: A Model for Protecting Privacy," *Int'l J. Uncertainty, Fuzziness, and Knowledge-Based Systems*, vol. 10, no. 5, 2002, pp. 557–570.