Pervasive Computing in general

Computer security May 2006

Introduction.

This report is about security problems in a pervasive computing environment in general.

A part of the report is about possible threats and protection related to pervasive computing that is already reality, which means that security problems are quite well known and dealt with.

But it also deals with potential security problems related to pervasive computing as a complete embedded and invisible technology that may become reality in the future. This technical invisibility may cause less awareness of privacy and security problems, which makes it important to consider consequences in advance.

What is pervasive computing.

Basically pervasive computing means that there are computers everywhere and that the pervasive devices are networked so they can communicate and interact with each other. These devices can access URLs through electronic tags, optical recognition methods and radio frequency transceivers available on PDAs and laptops.

Some examples of pervasive computing applications:

- **Electronic bar-codes.** Widely spread use in the retail trade and production as shoplifting prevention systems, checkouts without cashiers and automatic stock-taking
  RFID could also be used to provide allergi-warnings, food safety etc.
- **Cars.** Embedded and invisible systems such as computer-controlled brakes, cruise-control and automatic alarms where the road is slippery.
- **Healthcare**. Intelligent bandages that can tell how the injury is doing or video consultations with doctors, that can treat patients at home.
- **IT**. Public printers that are accessible with mobile phones and chips in passports.
- **Defence.** E.g. unmanned planes and tanks or weapons that can only be fired by approved users.

Pervasive technology.

In essence pervasive computing uses web technology, portable devices and wireless communication The standard HTTP protocol that the Internet is based on, facilitate such kind of overall access and can be implemented on a variety of devices. This gives mobile users transparent access to resources outside their current environment.
The technology is characterized by the use of units with limited IT capacity in:

- CPU power.
- Memory.
- Bandwidth and limited reach.
- Battery.

Technologies that are already in widespread use:

- Devices.
  RFID (Radio Frequent IDentifikation), Smart cards, PCs, PDAs, digital cameras and printers.
  RFID tags is basically units that can identify themselves either passively (read by scanners) or actively (transmitting a signal - possibly controlled by the user) and can thus have more or less IT capacity in terms of battery and computational power (e.g. support encryption).
- Wireless technology.
  Bluetooth, Wifi, GSM, GPRS, UMTS.
  BlueTooth and GSM support cryptography, but tell the ID code to everyone who asks for it. The use of cryptography is thus not in itself a guarantee that data, e.g. ID codes are protected

IT security in a pervasive computing environment

The concept of pervasive computing range from real and everyday applications over more advanced and only partly realised ones, to total futuristic applications which may never become real. On the other hand security analysis is a specific assessment of threats to computer security. So to relate to security problems on these different levels a distinction in types of applications of pervasive computing is made.

Three categories are defined in accordance to [PC] which in order of increasing technological complexity and realisation are:

- ID-in-everything
- Services-in-everything or The executable Internet
- Agents-in-everything or The extended Internet

Analysis of IT security problems.

The following analysis will identify potential technical security problems in a pervasive computing environment and list threats and protections to these threats in respect to confidentiality (privacy), integrity (authentication) and availablity in each of the named categories.

ID-in-everything.

This type of pervasive computing is characterized by the use of passive units that can only report an ID code and maybe raw sensor input. All other computations are done in the communication infrastructure.

The technology is realized to a great extent, e.g. the use of RFID tags are commercially widespread and some applications are:

- Shoplifting prevention systems.
- Tracking or identification of people with an attached RFID tag.
- Access cards to ski lifts.

Although smart cards, SIM cards and Bluetooth units like RFID tags hold identity data, they are described in the services-in-everything section.

Threats with ID-in-everything. The main security problem is related to identification and privacy. It's obviously a question of how personal information can remain private as the use of these units becomes more widespread.

- Confidentiality (i.e. privacy):
  Tracking or identification by reading of ID codes.
  Unauthorized access to databases with registred ID codes and/or possibly associated data.
- Integrity:
  The falsification of ID codes (spoofing).
- Availability:
  Preventing the unit from transmitting an ID code (kill mode).
  Denial-of-service attack against the scanner (Blocker tags).
  Power failure (sleep deprivation torture).

Protection with ID-in-everything. Concerning privacy it's a weakness to use unique identification. It is not necessary in such technologies and applications, but alternative solutions aren't commercial widespread.

- Confidentiality.
  Regulating the use of the databases containing ID codes and associated data by giving the user control over own data which have already been collected or by giving the user control over which data are transmitted by a unit in a specific situation (although RFID tags can't be turned off, methods such as the “kill mode” and Blocker tags can deactivate them but reduce the functionality).
  Avoiding unique identification.
  All solutions must be easy to use and require RFID tags that can perform some calculations.
- Integrity.
  Using a combination with physical control.
  Using standardised and widespread identification technologies such as BlueTooth and WiFi.
- Availability.
  Partly solutions with RFID tags without battery, but such offer very limited functionality.

Services-in-everything.

These systems are characterised by the use of active units which can perform calculations. Via sensors, actuators and applications the systems carry out actions triggered by the user to provide services via the Internet.

This technology is to some extent realized, e.g. via PDAs, digital cameras and other things that can communicate.

Typical features of the units in this pervasive computing environment:

- Sensors that send data.
- Actuators that receive instructions.
- Local central units, e.g gateways or PDAs.

Although this environment is very flexible (the units can communicate via central points and other units or directly), these systems are relatively closed. I.e. the users know in advance which units will be involved, so it's possible to set them up as part in a known system.

Examples on pervasive computing systems in this category:

- "Intelligent" bandages make it possible to treat diabetic patients with foot wounds at home. The bandage sends various data to a database, and a chief physician at a hospital carry out a video consultations with the assistance of a visiting nurse.
- Electronic patient records.

Threats with services-in-everything.

- Confidentiality.
  Tracking or identification.
  Processing of data (internally and externally between the gateway and central system).
- Integrity.
  Processing of data.
  Unauthorised access.
  Non-repudiation.
- Availability.
  Hardware errors.
  Software errors.
  Malevolent software.

Protection with services-in-everything. Confidentiality and integrity can be secured by storing and/or processing data with the end user instead of in distributed networked systems or central databases. With regard to encryption the main problem is the limited IT capacity in the small units.

- Confidentiality.
  Encryption of stored data.
  Local storing and processing of data.
  Support secure identification to protect access controle.
- Integrity.
  Encryption of stored data.
  Local storing and processing of data.
  Support secure identification to protect access controle.
  Digital signature together with a local set of rules to secure non-repudiation.

- Availability.
  Correct hardware and software, e.g. by means of certification.
  Use of secure operating systems.

Agents-in-everything.

Here the units are active and they are making autonomous decisions, i.e. they process data on their own initiative.As the technical functionalities to a great extent can be implemented by the same technologies as in the services-in-everything systems, the potential computer security problems are similar and already covered by and large.

But some new problems emerge, primarly as a result of the openness of the systems and the use of autonomous, intelligent agents.

Scope of systems. As communication is no longer limited to units that are connected in a closed system, the scope changes because the communicating technology is everywhere: globally wide spread and locally embedded. A complete implementation of the pervasive computing concept.

"Intelligent" and autonomous agents. The use of agents hands a great deal of the responsibility for decisions over to technology e.g. for financial transactions and processing of personal data.

To provide "intelligent" and context aware systems in a pervasive computing environment, it is necessary to build profiles of the data subjects (correlated data that identify and represent a subject, e.g. a person) and to be able to link profiles and data subject correct everywhere. Which is a key point when it comes to privacy and security in pervasive computing.

Even if the data protection legislation grant users complete control of their own data, it would be impossible to hand because of the utter amount of data. So the challenge with respect to securing confidentiality and integrity of data will be to provide technological solutions together with legal regulation, that gives the user real control over own data.

To move data from a central database to a distributed form in the hand of the user, each user must have an identity management device with sufficient IT capacity.

Anonymous credentials. This can provide identity management to support privacy and security but its protocols require devices with great computational capacity. Users are identified by un-linkable pseudonyms (it's possible to have more such virtuel identities without risc of linkink). They are achieved at different organisations (providers of the "intelligent" services) and given credentials signed by the organisations certifying attributes and the user can choose which attributes to show or prove to a given device. Anonymous credentials could be used in contexts where the user wants to maintain a permanent pseudonymous identity and for access control to buildings or rooms or for secure anonymous electronic cash payments.

Threats with agents-in-everything. Legal regulation of data processed in foreign environments will not be unambiguous.

- Confidentiality.
  Processing of data.
  Transmitting ID codes across national borders and different jurisdictions.
- Integrity.
  Non-repudiation.
  Processing of data.
  Unauthorised access.
- Availability.
  The consequences of problems with availability will be much more serious compared to ID- and services-in-everything systems as the everyday life probably will be more dependent on technology.

Protection with agents-in-everything. It is important that agents can be configured and controlled by the end user so everyone only has contact with agents they want to. But this appears to conflict with the basic ideas of autonomous interaction between agents.
Trust Management systems with decentral specifications and independent enforcement of the security politics and sets of assertions for regulating permissions to operations are fit to handle how and how much unknown agents can be trusted in big open dynamic systems.
As opposed to service-in-everything the agents are expected to have enough computing power to use traditional, strong eencryption methods.

- Confidentiality.
  Support end user control over data (local storing and processing of data).
  Encryption of data.
  Secure identification to protect access control (anonymous credentials).
- Integrity.
  Support end user control over data (local storing and processing of data).
  Encryption of data.
  Secure identification to protect access control (anonymous credentials).
  Support of non-repudiatable agreements and control over foreign agents. The use of cryptographic infrastructures To deal with non-repudiatable agreements requires an international digital signature.
- Availability.
  The same as in services-in-everything.

Summary.

In many ways security problems in a pervasive computing environment don't differ significantly from those in a more traditional computing environment. The main difference comes from the use of units with very limited computing power and in the widespread use pervasive computing applications are expected to achieve.

On the basis of the threats and solutions identified in this report so far some potential security problems that are specific to a pervasive environment will be emphasized.

Confidentiality.

The security items are confidentiality of sensitive personal data and ensuring of privacy.

Although encryption could protect sensitive personal data processesd over an open network or a portable device, it is a problem that the units have limited IT capacity so they are not able to carry out sufficient encryption.

Privacy. A main obstacle for a commercial breaktrough of pervasive computing is the concern for privacy. Consequently it's crucical for the implementation of a pervasive computing environment to ensure that privacy are not threatened.

Problems with anonymity and tracking that are specific to pervasive computing are due to the scale in which pervasive technology are implemented, e.g. the use of RFID in the retail trade.
To protect privacy, solutions must support minimal or no registration of data that can be traced. This should should be supported in laws and widely accepted rules and agreements. In a more long-term perspective the technology can be expected to be further developed so that even very small units will be able to perform calculations and support technical solutions.

The concept of anonymous credentials and a proper approach to access control, e.g. with Trust Management are examples of additional methods to ensure confidentiality.

Integrity.

Widespread protocols such as Wifi and Bluetooth provide reasonable security for many practical purposes in a pervasive environment.

Problems with identification often concern inappropriate user behaviour rather than cryptographic protocols. Social engineering and phishing are important problems, but are more specific to a pervasive computing environment in respect to usability.

Non-repudation. Related to autonomous software-agents there is a problem concerning agreements that have to be non-repudiatable. If a final consummation of an agreement has to be controlled by the end user, it appears to conflict with the basic idea of autonomous software agents.

Availability.

Problems are not specific to pervasive computing, but the consequenses of problems will be more serious the more dependent everyday life is on technology.

Usability.

At last some points on usability will be outlined. It is important that the systems are used as they are intended to or else there will be no security.

Examples on troublesome user interfaces in a pervasive computing environment:

- A famous example of inappropriate user behaviour comes from a Danish hospital. Because the staff found too time-consuming to login every time they had to process data in the IT system, one user logged in to all the machines every day on behalf of the rest of the staff granting access to everybody.
  This require better implementation of user authentication and a better awareness of problems related to IT security also in terms of handling passwords sensible.
- Often inexperienced users add devices to the systems on their own. E.g. patients that has to change an "intelligent" bandage on their own or as part of a remote consultation with a doctor has to process measurement data to the system.
- Pervasive computing technology will probably always be stressed to its limits, so its likely that ad hoc applications are added to the systems.
  The certification of units would deal with this to some extent, but subsequently requires management of certificates to be well implemented.
- Existing and usable methods for controlling units that transmit ID codes require that the users managing a key, because these solutions are based on cryptography.

If solutions are based on technically smart solutions this require technically “smart” thinking users. But with widespread and a common accessible technology, this will not be the case. Instead of technology must be simple to use, so the user can spend time on completing the task and not on learning the application and how to configure and troubleshoot it.

In a long-term perspective it is probably more realistic and more necessary to do something about usability problems, because of the more widespread use of pervasive computing. And as it isn't likely that an increasing education of users will solve all problems, another approach has to be taken: the systems must be constructed to fit intuively into their intended application. This are giving rise to pervasive computing as an invisible technology where devices don't have user-interfaces. The disappearing interface which in fact is a main characteristic of the pervasive concept means that technology will be embedded in everyday objects and are working automatically to the extent that people are not aware of it.

Source material.

[PC] **Pervasive computing - IT security and privacy**
http://ec.europa.eu/justice_home/fsj/privacy/docs/rfid/danish-its-consultations_en.pdf

Report on Actual and Possible Profiling Techniques in the Field of Ambient Intelligence
www.fidis.net
fidis-wp7-del7.3.ami_profiling.doc

Dieter Gollmann, Computer Security , second edition

http://www.web-enable.com/business/PervasiveComputing.asp
http://www.web-enable.com/business/EmergingPervasiveTechnologies.asp
http://www.imm.dtu.dk/~cdj