Aiming to Realize Safe and Secure Mobile Phones

Noritaka Koyama Yasuhiro Mitsui

The penetration rate of mobile phones has peaked and the emphasis in the market is now shifting to more substantial functions and the provision of various services. Substantial functions for mobile terminals and the mobile environment due to advancements in wireless broadband in recent years makes us realize that the advent of the so-called ubiquitous society, in which “a comfortable life in a society with information and services provided at any time, anywhere and in a form a user desires” is here. Businesses are also aiming to maximize their profits through speed and efficiency, brought about by maximizing the potential of such infrastructures by handling the information and services necessary for business activities with mobile terminals. This trend, however, accelerates an increased handling of critical information in mobile phones, which increases the potential for unexpected new security issues.

This paper targets the mobile phone, which is the most important information communication device in the ubiquitous society, as well as describes the concept and system overview of the ubiquitous security technology on which the context-aware technology is applied.

Security threats and current measures for mobile phones

Security threats both personal and in business are on the rise due to the increased use of the mobile phone. Measures to thwart such threats are being implemented.

The first specific threat to be mentioned is the loss of mobile phones and thereby electronic valuables (such as electronic money, electronic tickets and electronic content) within mobile phones and straps (for hanging a phone from the neck) are used as an action against such loss. The second specific threat is leaked customer information or confidential information stored on mobile phones and the measures include function locks that are activated when the phone is dialed from other specific phones or the data stored on mobile phones is deleted remotely using the Internet. The third specific threat involves inappropriate use of mobile phones (use of mobile phones at locations where eavesdropping is quite easy), however, for this there are no measures currently in existence.

With regard to actions against the second threat (leaked information stored on mobile phones) similar services other than remote locks are being offered, which are shown in **Table 1**.

Table 1 Security services for mobile phones

Function	Specific examples of methods for realization
Remote function lock in the event of a mobile phone loss.	Functions of the mobile phone are locked when the user dials the lost phone a multiple number of times according to the registered methods of the pre-registered phone.
Remote deletion of data in the event of a mobile phone loss.	Data on the mobile phone is deleted when the administrator operates the phone remotely in response to an instruction from the user.
Automatic data deletion	Presetting storing period or deleting data, which has not been accessed over a specific period of time.
	Linked with application to delete relevant data when each task is completed.
Remote data management	Synchronizing data between the mobile phone and server, as well as backing up of data on the server.
	Remotely initiated data synchronization, transfer and deletion.
	User accesses a dedicated web site to instruct the deletion of data.

What is Context-Aware Technology?

In general, a context for a certain target means a condition surrounding such a target. More specifically, it may be physical conditions, such as a location, time, temperature or acceleration, or whether the target is currently using a specific service or not and the like, covering an extremely wide range of items. It is also possible to combine individual contexts to form composite contexts. For example, it should be possible to form a context of a train interior by combining ambient noise, vibration and acceleration. Furthermore, contexts are not limited to current conditions but can also contain past, present or future conditions, as well as a combination of these.

Next, context-aware technology also represents technology for providing appropriate services suitable for contexts. As an example it may be possible to provide advertisements that will be most effective in line with the current time and location of users. In the ubiquitous society, wherein the computing environment will be available in various conditions, a large demand will exist for the provision of services that suit the conditions and thus context-aware technology may be rightly described as technology that matches the needs of the era.

Context-aware technologies have been researched since the latter half of the 1980s, but it is only over the last few years that a flurry of activity started to take place at domestic and overseas universities, research organizations and business corporations, primarily in Europe and the United States. At the current time most researches are intending to improve the convenience of users by providing services that respond to contexts.

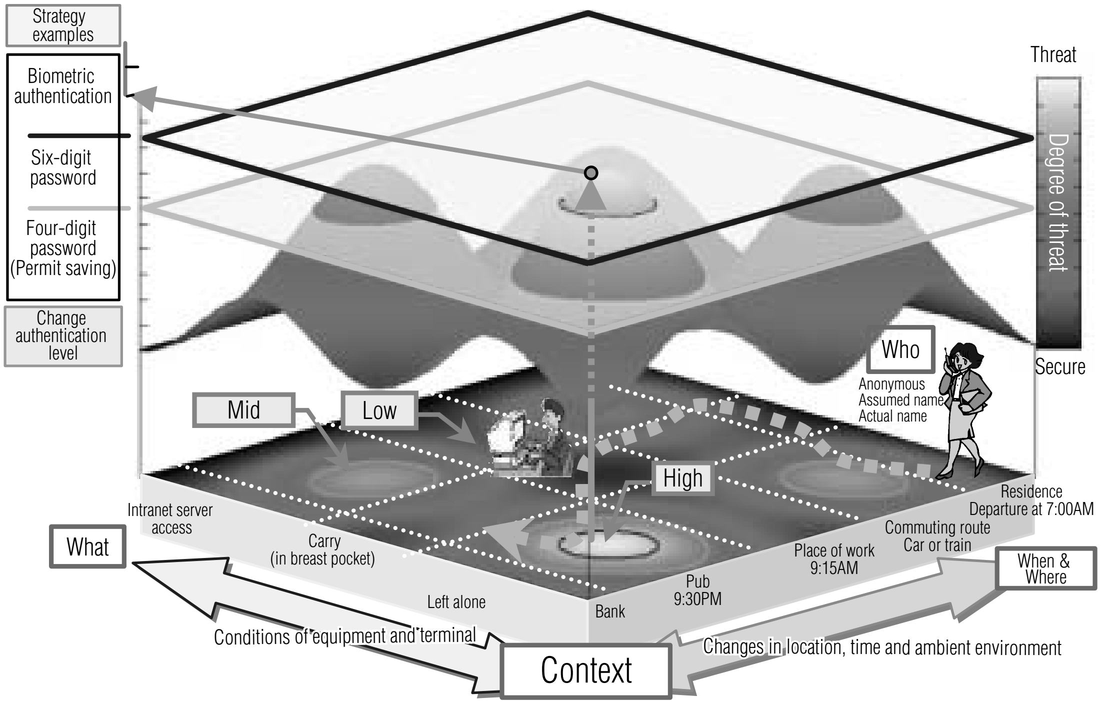

Fig. 1 Image of ubiquitous security

What is ubiquitous security?

Issues with security measures for mobile phones mentioned previously include the following:

a. Intrusive actions against loss inhibit the efficiency of business operations.

b. It is too late to act once a loss has occurred and complicated measures require too much time (incidents may occur during the time it takes to act).

c. It is not possible to completely prevent mistakes arising from the oversight of a user since actions depend on the awareness of the user.

The authors, therefore, have undertaken the development of a technology that will resolve these issues by using a context-aware technology. More specifically, we are developing a context-aware security technology that detects the ambient conditions of the mobile phone, identifies threats, and conducts autonomous preventative and deterrent measures, as well as notifies the server using various information inside and outside the mobile phone. This technology is called “Ubiquitous Security Technology”.

An image of ubiquitous security is shown in **Figure 1**.

This diagram shows that the degree of threat (right hand side vertical axis) varies depending on the behavior of the user, when the condition of the mobile phone is considered to be a combination of “Changes in location, time and ambient environment” and “Conditions of equipment and terminal”. For example, there is adequate security at home or in the office when the user keeps the mobile phone within their vicinity or they carry it in their breast pocket, but the degree of threat is considered to be higher when it is left on a commuting route, in a pub or at a bank, for example. The context-aware ubiquitous security technology automatically identifies such changes in the conditions with regard to the extent of threat and automatically switches over to security measures that correspond to the given condition (left hand side vertical axis).

Functions necessary to realize ubiquitous security will be described next.

With ubiquitous security the context is detected from the mobile phone's various internal and external information and the threat is identified autonomously. The detection of the context involves primarily a sensor built into the mobile phone, external devices or external services. A practical example of a method used to detect a context is shown in **Table 2**.

Table 2 Example of context detection method

Context		Detection method
User leaves the mobile phone alone		Distance from another device carried by the user
Mobile phone in use	Someone holds the phone	Electrostatic capacity and temperature
	Someone flips the phone open	Electrical signal
	Someone views the screen	Camera image & infrared ray
	Someone operates the phone	Key entries
	Someone performs risky operations (e.g: Looks for passwords)	Operating patterns
Location with high degree of threat (e.g: In restaurants and on trains)		Location detection

Threats to mobile phones can be identified by contexts detected in this manner or combinations thereof. It is, for example, possible to identify a threat with a higher certainty by detecting that the phone is being operated by someone other than the user by combining "User leaves the mobile phone alone" and "Someone operates the phone" of **Table 2**.

The mobile phone retains a set of rules for implementing preventative and deterrent measures corresponding to the contexts and combinations thereof. Whenever a context occurs or changes, rules are referenced and security measures corresponding to the rules are performed.

Furthermore, new rules are generated and existing rules are modified in order to successively optimize the rules, through the transmission of contexts and incident information obtained by the mobile phone to the management server, as well as accumulation, later analysis and learning. Rule updates are transmitted from the management server to a mobile phone at the appropriate time and rules are then updated to the mobile phone. Through this process the system prepares to provide a defense against new and unknown threats in the future while repeatedly improving the existing rules.

A concept of the ubiquitous security system is shown in **Figure 2**.

The following measures can be implemented autonomously through the functioning of the ubiquitous security system:

a. Simple deterrence of mobile phone loss without any intrusive measures.

b. Deterrence of leaks or misuse of information on mobile phones even before the user realizes that the phone has been lost.

c. Deterrence of inappropriate use of a mobile phone through the oversight of a user.

System overview

An overview of the system is shown in **Figure 3**.

(1) Function summary of mobile phones

Various contexts are detected and managed with the context management software that operates on the mobile phone, in collaboration with peripheral devices.

- Internal sensors are used to detect touch (touch sensor) and movements (accelerometer).
- Various external sensor values are acquired and the distance from the mobile phone is measured by communicating wirelessly via Bluetooth etc. using external sensors.
- Location is detected using GPS (linked with external services).
- Different types of status monitoring are linked with sensor networks.

(2) Function summary of management server

The management server is used primarily for coordinating with external services and for the management and transmission of rules.

External services represent services, such as application service providers (ASPs). A monitoring service that uses a monitoring camera would be one such example. When the management server receives a context indicating that a suspicious video has been detected, it can be provided to the mobile phone.

The management server manages rules and transmits them to mobile phones at the appropriate time.

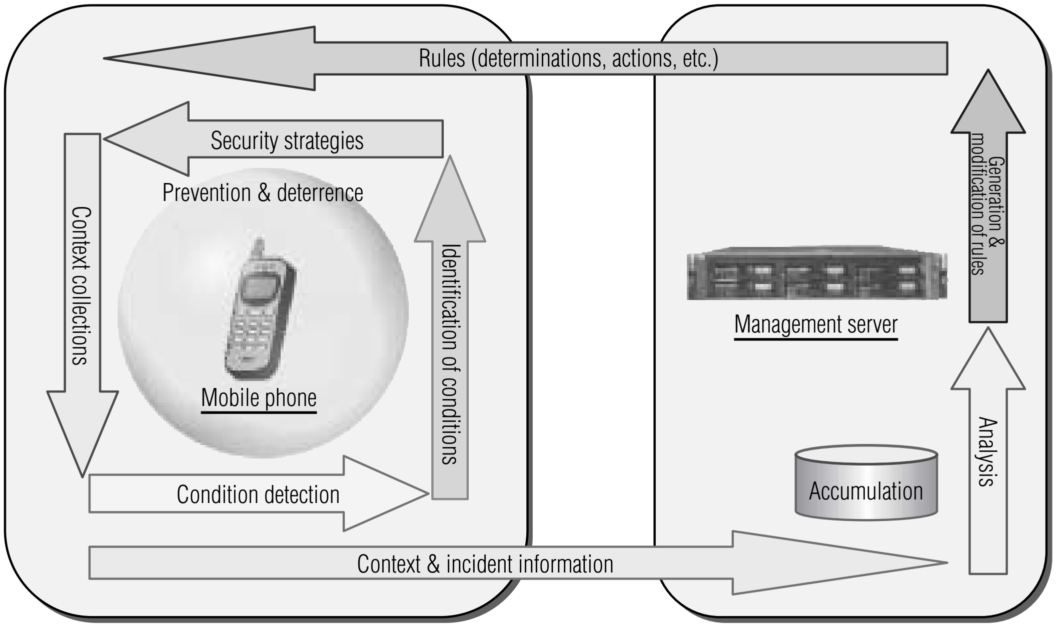
Rules (determinations, actions, etc.)
Security strategies
Prevention & deterrence
Context collections
Mobile phone
Identification of conditions
Condition detection
Context & incident information
Generation & modification of rules
Management server
Accumulation
Analysis

Fig. 2 Ubiquitous security system

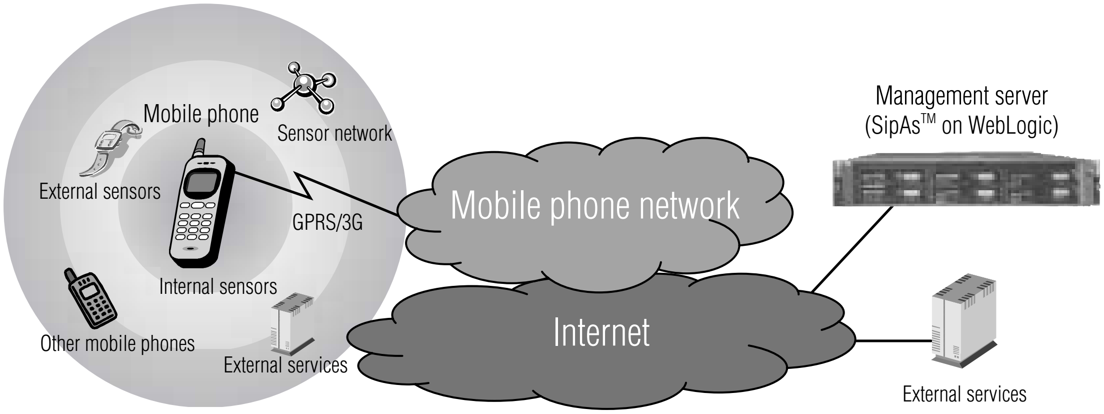

Fig. 3 System overview

(3) Context sharing via networks

Communications between mobile phones and the management server is conducted via mobile phone networks and the Internet. Communication data are rules and various contexts.

Contexts of a mobile phone can be shared with other mobile phones. Sharing contexts makes it possible to use contexts of other mobile phones, as well as use combinations of multiple contexts. The context sharing function can be perceived as a natural extension of the presence function that is used by instant messaging (IM) and has the potential to be widely used in the ubiquitous computing environment in the future as well.

The communication protocol used is the Session Initiation Protocol (SIP), which has attained a status as an international standard, offers real-time and bidirectional characteristics. SIP is used for the incorporation of presence and is believed to have an affinity with context sharing. The platform for the management server will be the SIP incorporated application server developed by Oki Electric, “SipAs^{TM}[*1] on WebLogic[*2]”

Conclusion

We are currently proceeding with developments targeting mobile phone services that offer security and safety, which autonomously deter loss, information leaks and improper use, intended for the business person, who currently carries around critical information on numerous occasions.

More specifically, we are in the process of building a demonstration system for evaluating the effectiveness as well as for marketing this ubiquitous security technology. We intend to incorporate in this system basic functions and an operational flow as indicated in **Figure 2**. We are considering expanding the range of sensors by adding new sensors and using sensors outside the terminal, while analyzing contexts and incident information, as well as automating the generation and modification of rules. We are planning to achieve the following targets through these means:

◆ Proactive security

In general, “the cost for implementing measures before problems occur is lower than the cost for implementing measures after problems occur”, thus prevention at an early stage before a threat occurs is the most effective method. Forecasting foreseeable threats based on past incidents and the results of context identification, suitable security measures are implemented automatically.

◆ Non-Intrusive user interface

Intrusive functions that are not used or alarms that go off as often as the boy who cried wolf will have no meaning. It is, therefore, important that all aspects of convenience, security and privacy protection must meet usability standards. Automated learning functions will be used on the management server to obtain feedback from users to improve usability.

Authors

Noritaka Koyama: Systems Network Business Group, Business Incubation Div., Security Solution Development Dept.

Yasuhiro Mitsui: Systems Network Business Group, Business Incubation Div., Security Solution Development Dept.

[*1] SipAs is a trademark of Oki Electric Industry Co., Ltd.
[*2] BEA WebLogic is a registered trademark of BEA Systems, Inc.