# Confidence Value Based Multi Levels of Authentication for Ubiquitous Computing Environments[† †]

He Zheng*, Jin Kwak*, Kyungho Son**, Wansuk Lee**, Seungjoo Kim*, and Dongho Won*,†

*School of Information and Communication Engineering,
Sungkyunkwan University

**Korea Information Security Agency

요 약

New computing paradigm in ubiquitous computing environments is revolutionizing the way people interact with computers, services and the surrounding physical spaces. In order to provide stronger authentication, MIST proposed an authentication framework for ubiquitous computing environments and assigned confidence values to some authentication methods to facility the combining. However, the assigned confidence values lack sufficient evidence. In this paper reliable confidence values for each authentication method used in MIST is proposed. These confidence values can combine multiple confidence values in some manner, producing a more accurate net confidence value. Authentication entities with confidence values allows the authentication framework to blend nicely into ubiquitous computing environments.

## I. Introduction

Major advances in distributed systems and mobile computing have converged to enhance global interconnectivity. This has fueled the idea of ubiquitous computing and active information spaces where users can access services, run programs, utilize resources, and harvest computing power at any time and at any location.

The vision of Active Information Spaces is not far fetched; the Gaia [1] project at the Department of Computer Science, University of Illinois at Urbana-Champaign, attempts to develop a component-based, middleware system, which provides support for building, registering and managing applications that run in the context of Active Information Spaces. In addition, they proposed the MIST [2] a communication infrastructure, preserving location privacy in ubiquitous computing environments, while simultaneously allowing entities to be authenticated.

In this paper, a multi level authentication mechanism that provides reliable levels of confidence is proposed.

The remainder of this paper is divided as follows. Section 2 talks about related work. Section 3 describes the details of the proposed mechanism. Finally, Section 4 concludes this paper.

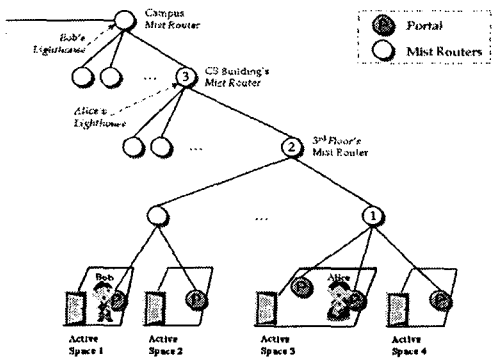
## II. Related Work

### 2.1 MIST

MIST is a communication infrastructure

† Corresponding author : 원동호(dhwon@security.re.kr)
† † This work was supported by the University IT Research Center Project funded by the Korean Ministry of Information and Communication.

that preserves location privacy in ubiquitous computing environments, while allowing entities to be authenticated at the same time in Gaia. The following figure demonstrates how MIST consists and how it is formulated.




(그림 1) The MIST Hierarchy

MIST consists of a privacy-preserving hierarchy of MIST Routers that form an overlay network. This overlay network allows users to communicate privately.

MIST Routers at the leaves of the hierarchy represent "Portals." Portals are viewed as the gateways that bridge the virtual world to the physical one.

The point at issue is that the authentication with single factor is not sufficiently strong. Therefore, MIST suggests multiple authentication with "confidence" values, a measure of how "confident" the system is that the user is authenticated.

When a user initiates more than one authentication method, MIST suggests a confidence-builder module which eventually produces a net confidence value employing the simple probability-based formula $C_{net} = 1 - (1-C_1)(1-C_2)...(1-C_n)$.($C_1$, $C_2$,.., $C_n$ are the confidence values of each authentication method)

2.2 Authentication Mechanisms in MIST

The following authentication devices are applied narrowly to focus on the password system, active badges, and biometric system.

2.2.1 Password

The password which includes single words, phrases, and personal identification numbers (PINs) is a closely kept secret used for authentication.

The main problem is not with a single password, but with multiple passwords. Users have difficulty remembering all their passwords, therefore they choose easy-to-guess passwords or they write them down and do not safeguard the paper on which they are written.

2.2.2 Active Badges

As an identity token, the active is a physical device that performs or aids authentication.

The two main disadvantages of an active badge are inconvenience and cost. The equipment cost is greater than that of a password, but comparable to a biometric that requires a reader. Due to the vulnerability relating to theft, a single-factor token should only be used in special circumstances, such as behind a first line of defense (within a house or restricted office building).

2.2.3 Biometric

A biometric characteristic is a feature measured from the human body that is distinguishing enough to be used for user authentication. However, stable biometric signals(e.g. fingerprint, face, hand, iris and retina) can be stolen and copied (either now or with higher probability within the lifetime of an implemented system), a biometric

identification device should not be deployed in single-factor mode.

## III. Multi-level Authentication Mechanism

In a ubiquitous computing environment, multi-level authentication is used to create a strong system which is resistent to most kinds of attacks. In order to capture this, MIST assigns confidence values to different authentication methods. However, the values which is defined by MIST are not well-grounded.

### 3.1 SOF Analysis of Single Authentication Mechanism

In CEM, the strength of the function is retrieved by calculating the attack potential considered by vulnerability. In order to calculate attack potential, five factors should first be considered, Elapsed Time, Expertise, Knowledge of TOE, Access to TOE and Equipment.

#### 3.1.1 SOF Analysis of Password Mechanism

SOF of password mechanism is influenced by five factors the number of password characters, limitation of password(e.g. must not be a common word, a word in any existing password dictionaries, or a word easily guessed), range of password character, expertise level of the attacker and ratification counter.

**Elapsed Time.** In order to calculate the elapsed time, the following variables are established.

Number of password character: $N$

Number of numeric character: $N_n$

Number of special character: $N_s$

Range of special character: $S$

Guessing speed of attacker: $V$

Two general functions which are used to calculate the elapsed time in all password cases are defined.

Elapsed Time:

$$\frac{10^{N_n} \times S^{N_s} \times (62+S)^{N-N_n-N_s}}{2} \times V$$

**Expertise.** Expertise level is related to the guessing speed. Laymen always guess the password by hand and this guessing speed can be assumed to be 5 seconds/(password guess). Proficient and expert guessing of the password by creating a password crack program. By referencing Security Target [3](ST), proficient guessing of the password, can guess the password at 0.001 second/(password guess) at most and the expert can guess password at 0.001 second/(password guess) at least.

**Knowledge of the TOE.** Much knowledge of the password mechanism can be gained through the internet. Therefore, it is recommended to set the level as "public".

**Access to TOE.** In order to exploit the password mechanism, an attacker must retrieve the IP address of TOE and a user ID of TOE. It is only possible when one use an external IP address.

**Equipment.** There is relationship between Equipment and Expertise. It is suggested that an ordinary individual cannot use any equipment, a proficient individual can use standard equipment(e.g. PC) and an expert individual can use standard, specialised(e.g. parallel computer) or bespoke equipment(e.g. super computer).

This methodology can be applied to an example, to achieve the Strength of Function.

1. There are 72 possible characters.
2. Each password must have at least six

characters.

3. Each password must contain at least one numeric and one special character. In this case, ''alphabetic'' means upper and lower case letters. Numeric or special character means any digit or special character on a standard keyboard above a digit.

4. Each password must differ from the word in password dictionary. It is assumed that the number of word in dictionary is 200,000.

5. A expert person could create a program to guess passwords with a standard equipment. The guessing speed is assumed as 0.001 second/(password guess).

6. Assume that attacker can retrieve the IP address of TOE and the user ID of TOE in less than one month.

The average total time to guess the correct password can be estimated 15 days.

The attack potential table(Table 3 in CEM 2.3) yields the following:

<표 1> Table of calculating exploitation

| Factor | Level | Exploitation |
|---|---|---|
| Elapsed Time | < 1 month | 5 |
| Expertise | Expert | 4 |
| Knowledge of TOE | Public | 2 |
| Access to TOE | < 1 month | 6 |
| Equipment | Standard | 2 |
| Total | | 19 |

From the rating of vulnerabilities table(Table 4 in CEM 2.3) (sum = 19), the SOF rating is SOF-medium. In applying the previous evaluation process to various passwords, the following table can be obtained.

<표 2> SOF evaluation criteria for password

| Number of password characters | SOF rating |
|---|---|
| ≦ 4 characters | SOF-basic |
| 5 - 6 characters | SOF-medium |
| ≧ 7 characters | SOF-high |

It is recommend that the configuration of the ratification counter will increase the strength of function at least one level, because of its effect to the strength of the function.

3.1.2 SOF Analysis of Random Number Generator

As small smart cards, the SOF of active badges is decided by the SOF of a Random Number Generator(RNG). Because RNG is not a probabilistic or permutation function, the SOF rating of RNG based on AIS 20 [4].

3.1.3 SOF Analysis of Biometric

Strength of Function(SOF) is an important part of the evaluation of a biometric device. It is related to the False Accept Rate(FAR), however, the relationship between FAR and SOF is not simple or clearly defined [5].

In order to establish the SOF of the biometric device with a FAR of 0.01, it is assumed that an expert uses specialised equipment(e.g. biometric DB) to attack a device like a door lock. Considering an attacker has a biometric DB, he can easily success can easily be achieved within half an hour. Since knowledge of TOE can be obtained through the Internet, the level can be considered as "public".

From the attack potential table(Table 3 in CEM 2.3), we can calculate the total exploitation. The total exploitation is 12. Consequently the SOF rating is SOF-basic. In applying the previous evaluation process to

biometric devices with 0.0001 FAR and 0.000001 FAR, the following table can be obtained.

<표 3> SOF evaluation criteria for biometric

| FAR of biometric device | SOF rating |
|---|---|
| ≦ 0.01 | SOF-basic |
| ≦ 0.0001 | SOF-medium |
| ≦ 0.000001 | SOF-high |

3.2 Multi-level Authentication Mechanism

When a user uses more than one authentication method, the overall level of confidence increases. .In this case, the confidence-builder module which is proposed by MIST is used. In order to make the confidence value more reasonable, the value according to the SOF rating is assigned in the following table.

<표 4> SOF rating and its confidence value

| SOF Rating | Confidence Value |
|---|---|
| SOF-basic | 0.55 |
| SOF-medium | 0.75 |
| SOF-high | 0.95 |

The confidence-builder module employs some algorithms for combining multiple confidence values, and is implemented as a module to plug-in different algorithms for combining. The following probability-based formula for calculating the net confidence value: $C_{net} = 1 - (1-C_1)(1-C_2)...(1-C_n)$.

Where $C_{net}$ is the net confidence value of a person who has authenticated himself using n methods whose individual confidence values are $C_1$, $C_2$,.., $C_n$. The product of all $(1-C_i)$ terms gives the probability that the user was incorrectly authenticated by all methods used. Therefore, finally $C_{net}$ provides the "probability" that this did not occur.

## IV. Conclusion

In order to achieve a stronger authentication method, we should combine some methods. In this paper we present a confidence value which is assigned to each authentication method. The confidence values are based on the SOF rating, a reliable evaluation done by CEM.

## [References]

[1] Renato Cerqueira, Christopher K. Hess, Manuel Roman, Roy H. Campbell, "Gaia: A Development Infrastructure for Active Spaces," Workshop on Application Models and Programming Tools for Ubiquitous Computing (held in conjunction with the UBICOMP 2001), September 2001.

[2] Jalal Al-Muhtadi, Anand Ranganathan, Roy Campbell, M. Dennis Mickunas. " Flexible, Privacy-Preserving Authentication Framework for Ubiquitous Computing Environments," Proceedings. 22nd International Conference on Distributed Computing Systems Workshops (ICDCSW '02), pp.771 - 776, July 2002.

[3] Cray Incorporated, "Cray UNICOS/mp Operating System Version 2.4.15 on Cray X1 hardware Security Target," August 2004. http://www.commoncriteriaportal.org

[4] Certification body of the BSI, "Functionality classes and evaluation methodology for deterministic random number generators," Application Notes and Interpretation of the Scheme(AIS), December 1999.

[5] Common Criteria Biometric Evaluation Methodology Working Group, "Biometric Evaluation Methodology," August 2002.