Computer Technology and Application 3 (2012) 130-139

Context-Aware Query Control for Secure Spaces

Shun Hattori

School of Computer Science, Tokyo University of Technology, Tokyo 192-0982, Japan

Received: December 10, 2011 / Accepted: December 28, 2011 / Published: February 25, 2012.

Abstract: In public spaces, there are a number of different contents such as visitors, physical information resources, and virtual information resources via their embedded output devices. Therefore, we might unexpectedly enter the public spaces that have our unauthorized contents and/or unwanted characteristics. The author's previous papers have introduced the novel concept of "Secure Spaces", physical environments in which any visitor is protected from being pushed her unwanted information resources on and also any information resource is always protected from being accessed by its unauthorized visitors, and the model and architecture for space entry control and information access control based on their dynamically changing contents. Aiming to build more flexible Secure Spaces, this paper proposes an extended model for context-aware query control and search control based on how preferentially a virtual information resource should be outputted in a Secure Space as well as spatial entry control based on whether a virtual information resource should be granted or denied to be outputted in a Secure Space.

Key words: Access control, authorization, authentication, context-awareness, Web search.

1. Introduction

In recent years, it has become one of the hottest research topics to make physical spaces smarter and more intelligent. Smart Spaces [1-6] are often physically isolated environments such as individual rooms that have been made smart by various information communication technologies and are expected to become increasingly convenient for our information access. Meanwhile, Information Security also becomes very significant and increasingly critical for any people in diverse scenes, especially in public places such as indoor work places, educational facilities, and healthcare centers, and so forth. The amount of physical or virtual information resources which should be protected in the physical world keeps growing exponentially.

Physical environments are becoming smart but not necessarily secure. When a user requests to access a virtual (computational) information resource via an output device, conventional access control systems make a decision by using its access policies on whether the user should be granted or denied to access it and then assuredly enforce the access decision. However, even if the requester is authorized by the resource, it should not be immediately offered to her via the output device, because there might be its unauthorized users as well as the authorized requester around the output device, especially in public places. Meanwhile, when a user enters a physical environment, the user might be unexpectedly forced to access her unwanted information resources (e.g., although she does not want to know about the result of a football game that she had recorded on video to watch later, she unfortunately encounters it in her train), and/or hate its real characteristics (e.g., degrees of dismal and danger).

There are two kinds of conventional access controls for the purpose of protecting information resource security. One approach is Information Access Control. When a user requests to perform an action on a virtual information resource such as a sensitive data file on computer, information access control systems make an authorization decision on whether the access request

Corresponding author: Shun Hattori, Ph.D. (Informatics), Assistant Prof., research fields: Web engineering, database, mobile and ubiquitous computing. E-mail: hattori@cs.teu.ac.jp

should be granted or denied, in order to protect it from its unauthorized users. However, they are not aware of the other users who are surrounding a device outputting it, and thus there might be its unauthorized user(s) in the surrounding area. If there are its unauthorized user as well as the authorized user, both users become able to access it and thus its confidentiality is not always protected. To protect it from its unauthorized users assuredly, they have to ensure that the area surrounding a device which will be granted to output the requested virtual information resource is truly secure, i.e., there is nobody unauthorized in the surrounding area.

Another approach is Space Entry Control. When a user requests to enter a physically isolated space such as a room and a building, physical entry control systems make an entry decision on whether the entry request should be granted or denied, in order to protect any physical information resource inside the space from its unauthorized users. However, they often determine the entry decision statically regardless of what physical or virtual information resources there are actually in the physical space, and thus there might not be any resource which should be protected from her. To ensure effective entry control, space entry control systems must be aware of dynamically changing contents such as visitors, physical or virtual information resources.

My previous papers [7-13] have introduced the novel concept of "Secure Spaces", physically isolated environments where any visitor is protected from being pushed her unwanted information resources on and also any information resource is always protected from being accessed by its unauthorized visitors, and the model and architecture for space entry control and information access control based on their dynamically changing contents.

Aiming to build more flexible Secure Spaces, this paper proposes an extended model for Context-aware Query Control and Search Control based on how preferentially a virtual information resource should be outputted in a Secure Space as well as spatial entry control based on whether a virtual information resource should be granted or denied to be outputted in a Secure Space.

The remainder of this paper is organized as follows. Section 2 introduces the mechanism and formalized model of Secure Spaces. Section 3 and Section 4 propose the space-dependent query control and search control, respectively. Section 5 concludes this paper.

2. Secure Spaces and Entry Control

This section describes the architecture to build Secure Spaces in the physical world and the mechanism and formalized model of Space Entry Control for Secure Spaces by summarizing my previous papers [7-13].

2.1 Architecture

To build Secure Spaces in the real world by using space entry control based on their dynamically changing contents such as their visitors, physical information resources and virtual information resources via their embedded output devices, each Secure Space requires the following facilities (Fig. 1).

- **Space Management**: is responsible for managing a Secure Space, i.e., for constantly figuring out its contents such as its visitors, its embedded physical information resources and virtual information resources outputted via its embedded output devices and also for ad-hoc making an authorization decision on whether an entry request to enter the Secure Space by a visitor or a physical/virtual information resource should be granted or denied, and for notifying the entry decisions to the Electrically Lockable Doors or enforcing entry control over virtual information resources according to the entry decisions by itself.
- **User/Object Authentication**: is responsible for authenticating what physical entity such as a user or a physical information resource requests to enter or exit the Secure Space (e.g., by using Radio Frequency IDentification or biometrics technologies) and also for notifying it to the space management.

- **Electrically Lockable Door**: is responsible for electrically locking or unlocking itself, i.e., for assuredly enforcing entry control over physical entities such as users and physical information resources, according to instructions by the space management.
- **Physically Opaque Wall**: is responsible for physically isolating inside a Secure Space from outside there with regard to information access, i.e., for validating the basic assumption that any user inside a Secure Space can access any resource inside the Secure Space while any user outside the Secure Space can never any resource inside the Secure Space.

To protect us from our unwanted characteristics of physical spaces as well as our unauthorized contents, the following additional facilities are required.

- **Real Sensor**: is responsible for physically sensing inside a Secure Space for its real characteristics to make access decisions in the Secure Space and also for notifying the sensor data stream to the space management. For example, thermometers, hygrometers, cameras.
- **Weblog Sensor** [11,13,14]: is responsible for logically sensing the Weblog for the approximate characteristics of each Secure Space to make access decisions in the Secure Space and also for notifying the Web-mined data to the space management. Note that any Secure Space does not have to equip the extra devices unlike Real Sensors.

2.2 Mechanism

When a user requests to enter a Secure Space, the space entry control system will make an entry decision on whether the entry request should be granted or denied, by checking whether or not the requester is granted to access by all information resources inside the Secure Space and whether or not the Secure Space itself as well as all resources inside the Secure Space are granted to be accessed by the requester, in order to protect her preference as well as information security for all contents of the Secure Space.

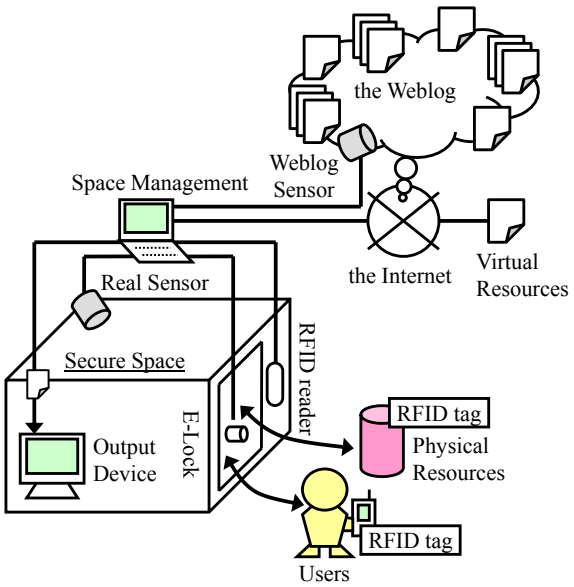

Fig. 1 Architecture of Secure Spaces.

If the Secure Space is not granted to be accessed by the requester because its real characteristics (e.g., degrees of dismal or danger) are unfavorable for the requester, the space entry control system has only one approach of preventing the requester from entering the Secure Space. If the requester is not granted to access by at least one physical information resource inside the Secure Space or if at least one physical information resource inside the Secure Space is not granted to be access by the requester, the space entry control system has also only one approach of preventing the requester from entering the Secure Space (Fig. 2). Reversely, when a physical information resource requests to enter a Secure Space, the space entry control system will also prevent the physical information resource from entering the Secure Space that contains at least one visitor who does not have access right to access the physical information resource (Fig. 3).

Meanwhile, if the requester is not granted to access by at least one virtual information resource via an output device embedded inside the Secure Space or if at least one virtual information resource is not granted to be access by the requester, the space entry control system has two approaches of not only preventing the requester from entering the Secure Space but also permitting the requester to enter there after revoking the virtual information resource (Fig. 4).

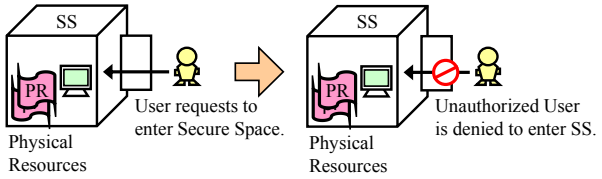

Fig. 2 Entry Control over Users for Physical Resources.

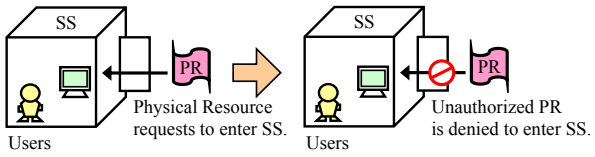

Fig. 3 Entry Control over Physical Resources for Users.

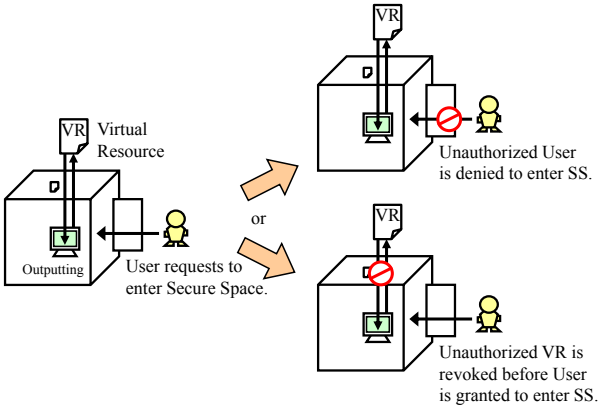

Fig. 4 Entry Control over Users for Virtual Resources.

2.3 Formalized Model

The formalized model of space entry control for Secure Spaces based on their dynamically changing contents such as their visitors, physical information resources and virtual information resources via their embedded output devices, by listing component primitives and by defining the syntax and semantics of the model components.

Definition 1: Model Entities

The space entry control model has the following four kinds of entities and protects all of them with respect to their information security and preferences to the others.

- **Secure Spaces**: are physically isolated environments (e.g., a closed room by opaque walls with electrically lockable doors) whose contents such as users and physical/virtual resources are always protected according to their access policies. The universal set of Secure Spaces and Secure Spaces' Access Policies are denoted by S and SAP.
- **Users**: are physical entities who request to enter or exit a Secure Space and who are assumed to be able to access any resource inside their current Secure Space but not to access any resource outside there. The universal set of Users and Users' Access Policies are denoted by U and UAP.
- **Physical Resources**: are physical information entities (e.g., a hardcopy of sensitive information) which request to enter or exit a Secure Space and which are assumed to be able to be accessed by any user inside their current Secure Space but not to be accessed by any user outside there. In order to assuredly enforce a physical resource's access policies, the space entry control system has to prevent its unauthorized users from entering its current Secure Space at any cost. The universal set of Physical Resources and Physical Resources' Access Policies are denoted by PR and $PRAP$.
- **Virtual Resources**: are virtual information entities (e.g., sensitive information on the Internet) which request to be outputted or revoked via an output device embedded in a Secure Space and which are assumed to be able to be accessed by any user inside their current Secure Space but not to be accessed by any user outside there. In order to assuredly enforce a virtual resource's access policies, the space entry control system has to prevent its unauthorized users from entering its current Secure Space or to prevent itself from being outputted in the Secure Spaces where there are its unauthorized users. The universal set of Virtual Resources and Virtual Resources' Access Policies are denoted by VR and $VRAP$.
- Resources: $R = PR \cup VR$.
- Contents (Contexts): $C = U \cup PR \cup VR$.

Definition 2: Model Functions

The model uses the following functions in order to keep up on the set of ad-hoc entities in each Secure

Space and evaluate the weight of a set of its dynamically changing contents.

- cu: $S \rightarrow 2^U$, is a function mapping each Secure Space s_i, to its current set of Containing Users $\mathrm{cu}(s_i)$.
- cpr: $S \rightarrow 2^{PR}$, is a function mapping each Secure Space s_i, to its current set of Containing Physical Resources $\mathrm{cpr}(s_i)$.
- cvr: $S \rightarrow 2^{VR}$, is a function mapping each Secure Space s_i, to its current set of Containing Virtual Resources $\mathrm{cvr}(s_i)$.
- cc: $S \rightarrow 2^C$, is a function mapping each Secure Space s_i, to its current set of Containing Contents such as Users, Physical Resources, and Virtual Resources $\mathrm{cc}(s_i) = \mathrm{cu}(s_i) \cup \mathrm{cpr}(s_i) \cup \mathrm{cvr}(s_i)$.
- w: $S \times 2^C \rightarrow \mathcal{R}$, is a function mapping a set of contents $\mathrm{cc}(s_i)$ in each Secure Space s_i, to its evaluated Weight $\mathrm{w}(s_i, \mathrm{cc}(s_i))$.
- authU: UER→{grant, deny}, is a function mapping each User's Entry Request uer_j, to the Authorization decision for Users $\mathrm{authU}(uer_j)$.
- authR: RER→{grant, deny}, is a function mapping each Resource's Entry Request rer_j, to the Authorization decision for Resources $\mathrm{authR}(rer_j)$.

Definition 2.1: Content Weighting of Secure Spaces

The weight that evaluates contents such as Users $\mathrm{cu}(s_i)$, Physical Resources $\mathrm{cpr}(s_i)$ and Virtual Resources $\mathrm{cvr}(s_i)$ in each Secure Space s_i could be defined in different manners. Here, I introduce one definition of content weighting function which seems to be more understandable for its space administrator and most often used.

The weight $\mathrm{w}(s, cs)$ of a Secure Space $s \in S$ who has a set of Contents $cs \in 2^C$ is defined as the summation of positive weights $\mathrm{w}(s, u, r)$ that evaluates each User's accessing each Resource in each Secure Space.

$$\mathrm{w}(s, cs) = \sum_{u \in cs \cap U, r \in cs \cap R} \mathrm{w}(s, u, r)$$

Definition 3: Access Policies

The model stores the following four kinds of access policies for Secure Spaces, Users and Physical/Virtual Resources.

- **Secure Space's Access Policy**: is an access policy by a Secure Space, defined as a 3-tuple of the Secure Space, a User/Resource and a set of its containing entities as contextual conditions,

  $SAP \subseteq S \times C \times 2^C$.

  $(s, c, cs) \in SAP$ where $s \in S$, $c \in C$, and $cs \in 2^C$, states that the Secure Space s grants the User/Resource c to enter there when it contains the set of Contents cs.
- **User's Access Policy**: is an access policy by a User, defined as a 4-tuple of the User and her qualified physical/virtual Resource, a Secure Space, and a set of its containing entities as contextual conditions,

  $UAP \subseteq U \times R \times S \times 2^C$.

  $(u, r, s, cs) \in UAP$ where $u \in U$, $r \in R$, $s \in S$, and $cs \in 2^C$, states that the User u grants the Resource r to be pushed on herself in the Secure Space s who contains the set of Contents cs.
- **Physical Resource's Access Policy**: is an access policy by a Physical Resource, defined as a 4-tuple of the Physical Resource, its qualified User, a Secure Space, and a set of its containing entities as contextual conditions,

  $PRAP \subseteq PR \times U \times S \times 2^C$.

  $(pr, u, s, cs) \in PRAP$ where $pr \in PR$, $u \in U$, $s \in S$, and $cs \in 2^C$, states that the Physical Resource pr grants the User u to access itself in the Secure Space s who contains the set of Contents cs.
- **Virtual Resource's Access Policy**: is an access policy by a Virtual Resource, defined as a 4-tuple of the Virtual Resource, its qualified User, a Secure Space, and a set of its containing entities as contextual conditions,

  $VRAP \subseteq VR \times U \times S \times 2^C$.

$(vr, u, s, cs) \in \mathtt{VRAP}$ where $vr \in \mathtt{VR}$, $u \in \mathtt{U}$, $s \in \mathtt{S}$, and $cs \in 2^{\mathtt{C}}$, states that the Virtual Resource vr grants the User u to access itself in the Secure Space s who contains the set of Contents cs.

Definition 4: Entry Requests

The model has the following three kinds of entry requests for Users and Physical/Virtual Resources.

- **User's Entry Request**: is an entry request by a User, defined as a 2-tuple of the User and a Secure Space which she is requesting to enter,

  $\mathtt{UER} \subseteq \mathtt{U} \times \mathtt{S}$.

  $(u, s) \in \mathtt{UER}$ where $u \in \mathtt{U}$ and $s \in \mathtt{S}$, states that the User u requests to enter the Secure Space s and also to access its containing Resources $\mathrm{cpr}(s) \cup \mathrm{cvr}(s)$ inside there.
- **Physical Resource's Entry Request**: is an entry request by a Physical Resource, defined as a 2-tuple of the Physical Resource and a Secure Space which it is requesting to enter,

  $\mathtt{PRER} \subseteq \mathtt{PR} \times \mathtt{S}$.

  $(pr, s) \in \mathtt{PRER}$ where $pr \in \mathtt{PR}$ and $s \in \mathtt{S}$, states that the Physical Resource pr requests to enter the Secure Space s and also to be accessed by the visitors $\mathrm{cu}(s)$ inside there.
- **Virtual Resource's Entry Request**: is an entry request by a Virtual Resource, defined as a 2-tuple of the Virtual Resource and a Secure Space which it is requesting to enter,

  $\mathtt{VRER} \subseteq \mathtt{VR} \times \mathtt{S}$.

  $(vr, s) \in \mathtt{VRER}$ where $vr \in \mathtt{VR}$ and $s \in \mathtt{S}$, states that the Virtual Resource vr requests to enter the Secure Space s and also to be accessed by the visitors $\mathrm{cu}(s)$ inside there.

Algorithm 1.1: Authorization for Users

An entry request $uer = (u, s) \in \mathtt{UER}$ that a User u requests to enter a Secure Space s is granted, if and only if any content inside there grants the User u to access itself and is granted to be accessed by the User u or if the Assumptive Weight $\mathrm{aw}(s, u)$ of the Assumptive Contents $\mathrm{ac}(s, u)$ in case of granting the User u to enter the Secure Space s after revoking any Virtual Resource inside there which denies the User u to access itself or is denied to be accessed by the User u is higher than the Current Weight $\mathrm{cw}(s)$ in case of denying the user to enter there.

$$\mathrm{authU}(uer) = \mathrm{authU}(u, s) = \mathtt{grant}$$
$$\Leftrightarrow (\mathrm{apr}(s, u) = \mathrm{cpr}(s)) \wedge \{(\mathrm{avr}(s, u) = \mathrm{cvr}(s)) \vee (\mathrm{aw}(s, u) \geq \mathrm{cw}(s))\}$$

where $\mathrm{au}(s, u)$, $\mathrm{apr}(s, u)$ and $\mathrm{avr}(s, u)$ is the Assumptive set of Users, Physical Resources or Virtual Resources inside the Secure Space s after granting the User u to enter there and regulating its contents to keep secure, respectively.

$$\mathrm{au}(s, u) = \mathrm{cu}(s) \cup \{u\}$$
$$\mathrm{apr}(s, u) = \{pr \in \mathrm{cpr}(s) | (pr, u, s, \mathrm{ac}(s, u)) \in \mathtt{PRAP} \text{ and } (u, pr, s, \mathrm{ac}(s, u)) \in \mathtt{UAP}\}$$
$$\mathrm{avr}(s, u) = \{vr \in \mathrm{cvr}(s) | (vr, u, s, \mathrm{ac}(s, u)) \in \mathtt{VRAP} \text{ and } (u, vr, s, \mathrm{ac}(s, u)) \in \mathtt{UAP}\}$$
$$\mathrm{ac}(s, u) = \mathrm{au}(s, u) \cup \mathrm{apr}(s, u) \cup \mathrm{avr}(s, u)$$
$$\mathrm{cw}(s) = \mathrm{w}(s, \mathrm{cc}(s))$$
$$\mathrm{aw}(s, u) = \mathrm{w}(s, \mathrm{ac}(s, u)).$$

Algorithm 1.2: Authorization for Resources

An entry request $prer = (pr, s) \in \mathtt{PRER}$ that a Physical Resource pr requests to enter a Secure Space s is granted, if and only if the Physical Resource pr grants any User inside the Secure Space to access itself and also is granted to be accessed by any User inside there.

$$\mathrm{authR}(prer) = \mathrm{authR}(pr, s) = \mathtt{grant}$$
$$\Leftrightarrow \mathrm{au}(s, pr) = \mathrm{cu}(s)$$

where $\mathrm{au}(s, pr)$ is the Assumptive set of authorized Users who have right to access any Resource in the Secure Space s even after granting the Physical Resource pr to enter there.

$$\mathrm{au}(s, pr) = \{u \in \mathrm{cu}(s) | (pr, u, s, \mathrm{ac}(s, pr)) \in \mathtt{PRAP} \text{ and } (u, pr, s, \mathrm{ac}(s, pr)) \in \mathtt{UAP}\}$$
$$\mathrm{apr}(s, pr) = \mathrm{cpr}(s) \cup \{pr\}$$
$$\mathrm{avr}(s, pr) = \{vr \in \mathrm{cvr}(s) | \forall u \in \mathrm{cu}(s), (vr, u, s, \mathrm{ac}(s, pr)) \in \mathtt{VRAP} \text{ and } (u, vr, s, \mathrm{ac}(s, pr)) \in \mathtt{UAP}\}$$
$$\mathrm{ac}(s, pr) = \mathrm{au}(s, pr) \cup \mathrm{apr}(s, pr) \cup \mathrm{avr}(s, pr).$$

Similarly, an entry request $vrer = (vr, s) \in \mathtt{VRER}$ that a Virtual Resource vr requests to enter a Secure Space s is granted, i.e., to be outputted via an output

device embedded in a Secure Space s, if and only if the Virtual Resource vr grants any User inside the Secure Space to access itself and also is granted to be accessed by any User inside there.

$$\text{authR}(vrer) = \text{authR}(vr, s) = \texttt{grant}$$
$$\Leftrightarrow \text{au}(s, vr) = \text{cu}(s)$$

where $\text{au}(s, vr)$ is the Assumptive set of authorized Users who have right to access any Resource in the Secure Space s even after granting the Virtual Resource vr to enter there.

$$\text{au}(s, vr) = \{u \in \text{cu}(s) | (vr, u, s, \text{ac}(s, vr)) \in \texttt{VRAP} \text{ and } (u, vr, s, \text{ac}(s, vr)) \in \texttt{UAP}\}$$
$$\text{apr}(s, vr) = \{pr \in \text{cpr}(s) | \forall u \in \text{cu}(s), (pr, u, s, \text{ac}(s, vr)) \in \texttt{PRAP} \text{ and } (u, pr, s, \text{ac}(s, vr)) \in \texttt{UAP}\}$$
$$\text{avr}(s, vr) = \text{cvr}(s) \cup \{vr\}$$
$$\text{ac}(s, vr) = \text{au}(s, vr) \cup \text{apr}(s, vr) \cup \text{avr}(s, vr).$$

3. Space-Dependent Query Control

This section proposes an extended model of Space-dependent (Context-aware) Query Control for Secure Spaces based on their dynamically changing contents such as visitors, physical information resources, and virtual information resources via their embedded output devices, aiming to apply my developed techniques [15-19] of query refinement for mobile/ubiquitous Web search to Secure Spaces.

Definition 2.2: Weighting of Search Queries

The weight $\text{w}_q(q, s)$ of a search Query $q \in \texttt{Q}$, where $\texttt{Q}$ stands for the universal set of queries to search for virtual information resources, by a Secure Space $s \in \texttt{S}$ who has a set of Contents $\text{cc(s)} \in 2^{\texttt{C}}$, is defined as follows:

$$\text{w}_q(q, s) = (1 - \alpha_q(s) - \beta_q(s)) \cdot \text{w}_q(q, s, \text{cc}(s)) + \alpha_q(s) \cdot \sum_{u \in \text{cu}(s)} \text{w}_q(q, u, s, \text{cc}(s)) + \beta_q(s) \cdot \sum_{r \in \text{cc}(s) \cap \texttt{R}} \text{w}_q(q, r, s, \text{cc}(s))$$

where $\text{w}_q(q, s, cs)$ stands for the weight of the Query q by the administrator of the Secure Space s who has the set of Contents cs, $\text{w}_q(q, u, s, cs)$ stands for the weight of the search Query q by each User u in the Secure Space s who has the set of Contents cs, $\text{w}_q(q, r, s, cs)$ stands for the weight of the search Query q by the administrator of each Resource r in the Secure Space s who has the set of Contents cs, and $\alpha_q(s)$ and $\beta_q(s)$ stand for parameters tailored by the administrator of the Secure Space s.

For example, a User u_A can define his/her weight function of search Queries as follows:

$$\text{w}_q(q, u_A, \forall s, cs) = \frac{\text{df}([q \,\&\, s.\text{name}])}{\text{df}([q])}$$

where $\text{df}([q])$ stands for the Document Frequency of

Fig. 5 Space-dependent Search Queries for Initial "d".

Web documents searched by submitting the query q to Google or Yahoo!, and df($[q \,\&\, s.\text{name}]$) stands for the Document Frequency of Web documents searched by submitting the query q expanded with the name of Secure Space s to Google or Yahoo!.

Fig. 5 shows the top 7 search queries dependent on Secure Spaces' names, such as "bookstore", "cd store", and "school", for their initial "d".

4. Space-Dependent Search Control

This section proposes an extended model of Space-dependent (Context-aware) Search Control for Secure Spaces based on their dynamically changing contents such as visitors, physical information resources, and virtual information resources via their embedded output devices, aiming to build more flexible Secure Smart Spaces (3S).

Definition 2.3: Weighting of Virtual Resources

The weight $\mathrm{w}_s(vr, s, q)$ of a Virtual Resource $vr \in \mathtt{VR}$ for a Query $q \in \mathtt{Q}$ by a Secure Space $s \in \mathtt{S}$ who has a set of Contents $\mathrm{cc}(s) \in 2^{\mathtt{C}}$, is defined as follows:

$$\mathrm{w}_s(vr, s, q) = (1 - \alpha_s(s) - \beta_s(s)) \cdot \mathrm{w}_s(vr, s, q, \mathrm{cc}(s)) + \alpha_s(s) \cdot \sum_{u \in \mathrm{cu}(s)} \mathrm{w}_s(vr, u, q, s, \mathrm{cc}(s)) + \beta_s(s) \cdot \sum_{r \in \mathrm{cc}(s) \cap \mathtt{R}} \mathrm{w}_s(vr, r, s, \mathrm{cc}(s))$$

where $\mathrm{w}_s(vr, s, q, cs)$ stands for the weight of the Virtual Resource vr for the search Query q by the administrator of the Secure Space s who has the set of Contents cs, $\mathrm{w}_s(vr, u, q, s, cs)$ stands for the weight of the Virtual Resource vr for the search Query q by each User u inside the Secure Space s who has the set of Contents cs, $\mathrm{w}_s(vr, r, s, cs)$ stands for the weight of the Virtual Resource vr by the administrator of each Resource r inside the Secure Space s who has the set of Contents cs, and $\alpha_s(s)$ and $\beta_s(s)$ stand for parameters tailored by the administrator of the Secure Space s.

For example, a Secure Space s_1 or s_2 can individually define its weight function of Virtual Resources as follows:

$$\mathrm{w}_s(vr, s_1, q, cs) = 1/\mathrm{googleRank}(vr, [q])$$
$$\mathrm{w}_s(vr, s_2, q, cs) = 1/\mathrm{yahooRank}(vr, [q \,\&\, s_2.\text{name})$$

where $\mathrm{googleRank}(vr, [q])$ stands for the rank of the Virtual Resource vr in the search results by submitting the original Query q to Google without modification, and $\mathrm{yahooRank}(vr, [q \,\&\, s_2.\text{name})$ stands for the rank of the Virtual Resource vr in the search results by submitting the original Query q expanded with the name $s_2.\text{name}$ (e.g., "bookstore") of the Secure Space s_2 to Yahoo!. The former is not space-dependent, while the latter is space-dependent.

Meanwhile, a User u_A or u_B can also individually define his/her weight function of Virtual Resources as follows:

$$\mathrm{w}_s(vr, u_A, q, s_1, cs) = 1/\mathrm{googleRank}(vr, [q])$$
$$\mathrm{w}_s(vr, u_A, q, s_2, cs) = 1/\mathrm{yahooRank}(vr, [q])$$
$$\mathrm{w}_s(vr, u_B, q, \forall s, cs) = 1/\mathrm{yahooRank}(vr, [q \,\&\, s.\text{name}])$$

The former by the User u_A uses space-dependent Web search engines but the space-independent original Query, while the latter by the User u_B uses the space-independent Web search engine but expands the original Query with each Secure Space's name.

Definition 5: Search Requests

The extended model accepts the following two kinds of search requests by Secure Spaces and Users.

- **Secure Space's Search Request**: is a search request by a Secure Space, defined as a 2-tuple of the Secure Space and a search Query,

  $\mathtt{SSR} \subseteq \mathtt{S} \times \mathtt{Q}$

  where $\mathtt{Q}$ stands for the universal set of Queries. $(s, q) \in \mathtt{SSR}$ where $s \in \mathtt{S}$ and $q \in \mathtt{Q}$, states that the Secure Space s requests to search by the Query q for Virtual Resources suitable for itself to output via its embedded public device, implicitly with its current Contents $\mathrm{cc}(s)$ such as Users $\mathrm{cu}(s)$, Physical Resources $\mathrm{cpr}(s)$, and Virtual Resources $\mathrm{cvr}(s)$.
- **User's Search Request**: is a search request by a User, defined as a 3-tuple of the User, a search Query, and a Secure Space in which she is requesting to search,

  $\mathtt{USR} \subseteq \mathtt{U} \times \mathtt{Q} \times \mathtt{S}$.

$(u, q, s) \in \mathtt{USR}$ where $u \in \mathtt{U}$, $q \in \mathtt{Q}$, and $s \in \mathtt{S}$, states that the User u requests to search by the search Query q for Virtual Resources suitable for herself to output via her private (mobile/wearable) device in the Secure Space s, implicitly with its current Contents $\mathrm{cc}(s)$ such as Users $\mathrm{cu}(s)$, Physical Resources $\mathrm{cpr}(s)$, and Virtual Resources $\mathrm{cvr}(s)$.

Algorithm 2.1: Search for Secure Space's Requests

For a Secure Space's Search Request $ssr = (s, q) \in \mathtt{SSR}$, the space-dependent search control system returns a set of Virtual Resources with some kind of weights as its search results. First, each Virtual Resource $vr_i \in \mathtt{VR}$ from among the universal set of Virtual Resources is filtered by the Space Entry Control based on whether it should be granted or denied to be outputted in the Secure Space s. Next, each Authorized Virtual Resource $vr_j \in \mathrm{avr}(s)$ is assigned some kind of weight by the Context-aware Search Control based on how preferentially it should be outputted in the Secure Space s with its set of Contents $\mathrm{cc}(s)$. Finally, the highest-ranked Virtual Resource will be outputted via an embedded public device(s) in the Secure Space s and be PUSHed on its visitors $\mathrm{cu}(s)$.

$$\mathrm{searchS}(ssr) = \mathrm{searchS}(s, q) = \{(vr_j, \mathrm{w}_s(vr_j, s, q, \mathrm{cc}(s))) | vr_j \in \mathrm{avr}(s)\}$$
$$\mathrm{avr}(s) = \{vr_i \in \mathtt{VR} | \mathrm{authR}(vr_i, s) = \mathtt{grant}\}.$$

Algorithm 2.2: Search for User's Requests

For a User's Search Request $usr = (u, q, s) \in \mathtt{USR}$ when the User u requests to search by the Query q in the Secure Space s, the space-dependent search control system returns a set of Virtual Resources with some kind of weights as its search results. First, each Virtual Resource $vr_i \in \mathtt{VR}$ from among the universal set of Virtual Resources is filtered based on whether it should be granted or denied to be outputted in the Secure Space s. And then each Authorized Virtual Resource $vr_j \in \mathrm{avr}(s)$ is assigned some kind of weight on how preferentially it should be outputted to the User u in the Secure Space s with its set of Contents $\mathrm{cc}(s)$. Finally, the top k search results will be outputted via the User's mobile device and some Virtual Resource will be PULLed by herself.

$$\mathrm{searchU}(usr) = \mathrm{searchU}(u, q, s) = \{(vr_j, \mathrm{w}_s(vr_j, u, q, s, \mathrm{cc}(s))) | vr_j \in \mathrm{avr}(s)\}$$
$$\mathrm{avr}(s) = \{vr_i \in \mathtt{VR} | \mathrm{authR}(vr_i, s) = \mathtt{grant}\}.$$

5. Conclusions

In public spaces, there are a number of different contents such as visitors, physical information resources, and virtual information resources via their embedded output devices (e.g., displays and speakers). Therefore, we might unexpectedly enter the public spaces that have our unauthorized contents and/or unwanted characteristics. My previous papers introduced the novel concept of "Secure Spaces", physical environments in which any visitor is protected from being pushed her unwanted information resources on and also any information resource is always protected from being accessed by its unauthorized visitors, and the model and architecture for space entry control and information access control based on their dynamically changing contents. Aiming to build more flexible Secure Spaces, this paper has proposed an extended model for Context-aware Query Control and Search Control based on how preferentially a virtual information resource should be outputted in a Secure Space as well as spatial entry control based on whether a virtual information resource should be granted or denied to be outputted in a Secure Space.

I plan to formalize a hierarchical model, specify its description language to enable administrators to configure and maintain their Secure Spaces and physical/virtual information resources more easily and flexibly, implement a prototype of Secure Spaces and evaluate its effectiveness and functionality by applying it to actual cases in the physical world.

Acknowledgments

This work was supported in part by JSPS (Japan Society for the Promotion of Science) Grant-in-Aid for Young Scientists (B) "A research on Web Sensors to extract spatio-temporal data from the Web" (#23700129, Project Leader: Shun Hattori).

References

[1] L. Rosenthal and V. Stanford, NIST Smart Space: Pervasive Computing Initiative, Proceedings of the 9th IEEE International Workshops on Enabling Technologies: Infrastructure for Collaborative Enterprises (WETICE'00), pp.6−11, 2000.

[2] J. Al-Muhtadi, A. Ranganathan, R. Campbell, and M. D. Mickunas, Cerberus: A Context-aware Security Scheme for Smart Spaces, Proceedings of the 1st IEEE International Conference on Pervasive Computing and Communications (PerCom'03), pp.489−496, 2003.

[3] G. Sampemane, P. Naldurg, and R. H. Campbell, Access Control for Active Spaces, Proceedings of the 18th Annual Computer Security Applications Conference (ACSAC'02), pp.343−352, 2002.

[4] Y. J. Song, W. Tobagus, D. Y. Leong, B. Johanson, and A. Fox, iSecurity: A Security Framework for Interactive Workspaces, Technical Report, Stanford University, 2003

[5] M. J. Covington, W. Long, S. Srinivasan, A. Dey, M. Ahamad, and G. Abowd, Securing Context-aware Applications Using Environment Roles, Proceedings of the 6th ACM Symposium on Access Control Models and Technologies (SACMAT'01), pp.10−20, 2001.

[6] P. G. McLean, A Secure Pervasive Environment, Proceedings of the Australasian Information Security Workshop 2003 (AISW'03), Conferences in Research and Practice in Information Technology, pp.67−75, 2003.

[7] S. Hattori, T. Tezuka, and K. Tanaka, Content-Based Entry Control for Secure Spaces, Proceedings of the International Workshop on Future Mobile and Ubiquitous Information Technologies (FMUIT'06), pp.98, 2006.

[8] S. Hattori, T. Tezuka, and K. Tanaka, Secure Spaces: Physically Protected Environments for Information Security, Proceedings of the Joint 3rd International Conference on Soft Computing and Intelligent Systems and 7th International Symposium on advanced Intelligent Systems (SCIS&ISIS'06), TH-B5-2, pp.687−691, 2006.

[9] S. Hattori and K. Tanaka, Secure Spaces: Protecting Freedom of Information Access in Public Places, Proceedings of the 5th International Conference on Smart Homes and Health Telematics (ICOST'07), LNCS Vol.4541, pp.99−109, 2007.

[10] S. Hattori and K. Tanaka, Towards Building Secure Smart Spaces for Information Security in the Physical World, Journal of Advanced Computational Intelligence and Intelligent Informatics (JACIII), Vol.11, No.8, pp.1023−1029, 2007.

[11] S. Hattori and Katsumi Tanaka, Mining the Web for Access Decision-Making in Secure Spaces, Proceedings of the Joint 4th International Conference on Soft Computing and Intelligent Systems and 9th International Symposium on advanced Intelligent Systems (SCIS&ISIS'08), TH-G3-4, pp.370−375, 2008.

[12] S. Hattori, Context-aware Search Control for Secure Spaces, Proceedings of the Joint 5th Int'l Conference on Soft Computing and Intelligent Systems and 11th Int'l Symposium on advanced Intelligent Systems (SCIS&ISIS'10), SA-D4-2, pp.1348−1353, 2010.

[13] S. Hattori, Secure Spaces and Spatio-Temporal Weblog Sensors with Temporal Shift and Propagation, Proceedings of the 2011 First IRAST International Conference on Data Engineering and Internet Technology (DEIT'11), pp.1042−1047, 2011.

[14] S. Hattori, Linearly-Combined Web Sensors for Spatio-Temporal Data Extraction from the Web, Proceedings of the 6th International Workshop on Spatial and Spatiotemporal Data Mining (SSTDM'11), 2011.

[15] S. Hattori, T. Tezuka, and K. Tanaka, Query Modification Based on Real-World Contexts for Mobile and Ubiquitous Computing Environments, Proceedings of the International Workshop on Managing Context Information and Semantics in Mobile Environments (MCISME'06), p.77, 2006.

[16] S. Hattori, T. Tezuka, and K. Tanaka, Activity-Based Query Refinement for Context-Aware Information Retrieval, Proceedings of the 9th International Conference on Asian Digital Libraries (ICADL'06), LNCS Vol.4312, pp.474−477, 2006.

[17] S. Hattori, T. Tezuka, and K. Tanaka, Context-Aware Query Refinement for Mobile Web Search, Proceedings of the 3rd IEEE International Workshop on Next Generation Service Platforms for Future Mobile Systems (SPMS'07), p.15, 2007.

[18] S. Hattori, T. Tezuka, H. Ohshima, S. Oyama, J. Kawamoto, K. Tajima, and K. Tanaka, ReCQ: Real-world Context-aware Querying, Proceedings of the 6th International and Interdisciplinary Conference on Modeling and Using Context (CONTEXT'07), LNAI Vol.4635, pp.248−262, 2007.

[19] S. Hattori, Alternative Query Discovery from the Web for Daily Mobile Decision Support, Proceedings of the 5th IADIS International Conference on Wireless Applications and Computing (WAC'11), pp.67−74, 2011.