제20회 한국정보처리학회 추계학술발표대회 논문집 제10권 제2호 (2003. 11)

유비쿼터스 컴퓨팅에서 안전한 위탁을 위한 Private Virtual Computing

박종열* 이동익* 김형천** 박중길** 이진석**
*광주과학기술원
**국가보안기술연구소
e-mail : jypark@kjist.ac.kr

Private Virtual Computing for the Secure Surrogate in Ubiquitous Computing

Jongyoul Park*, Dong-Ik Lee*, Hyoung-Chun Kim**, Joong-Gil Park**, Jin-Seok Lee**
*Kwang-Ju Institute of Science and Technology
**National Security Research Institute

요 약

유비쿼터스 컴퓨팅의 발전은 사용자에게 컴퓨터가 단순한 도구가 아닌 삶의 일부가 되는 커다란 변화이다. 하지만 대부분의 사용자는 자신이 악의적인 주변의 컴퓨팅 자원에 의해서 위협 받고 있다는 사실을 모르고 있다. 사용자가 수행하는 작업을 안전하게 완료하기 위해서는 자신의 작업공간이 주변의 컴퓨팅 자원에 의해서 간섭 받거나 훼손되지 않아야 한다. 본 논문에서는 이러한 안전한 작업공간을 제공하기 위해서 Private Virtual Computing 을 제안한다.

1. 서론

유비쿼터스 컴퓨팅의 개념은 Xerox Park 의 Mark Weiser[1]에 의해서 처음 제안되었으며 일반적으로는 다음과 같은 특징을 갖는다[2].

- ✓ 산재하고, 쉽게 접근 가능하고, 때로는 보이지 않는 컴퓨팅 디바이스들
- ✓ 이동이 쉽고 때로는 환경에 내장되어 있는 것들
- ✓ 산재된 통신 구조에 연결된 것들

이 내용에서도 알 수 있듯이 많은 컴퓨터들이 서로 연결되어 있고, 사용자는 그 컴퓨터들을 실제로 인지하지 않아도 자신이 원하는 작업을 언제 어디서나 서비스 받을 수 있는 컴퓨팅 환경을 말한다.

무선 통신 기술이 빠르게 발전하게 되면서 유비쿼터스 컴퓨팅 기술은 차세대 컴퓨팅 환경으로서의 확고부동한 자리를 점하게 되었다. 유비쿼터스 컴퓨팅의 가장 큰 변화는 사용자가 휴대하는 휴대 단말에 있다. 개인의 휴대 단말은 이동이 쉽고 사용자가 특별히 인지하거나 관리하지 않아도 빠르게 서비스 하여야 한다. 이는 기존의 컴퓨터가 가지고 있는 범용성이 아닌 특화된 컴퓨터 기능을 요구한다. 작은 컴퓨터들이 사용자가 필요로 하는 모든 프로그램과 기능을 갖추기 보다는 특성화된 기능과 주위에 산재되어 있는 컴퓨팅 자원을 활용하는 것이 보다 효율적이기 때문이다[3,4]. 여기서 산재된 자원은 자신이 소유하는 것이 아니라 다수가 공유 혹은 다른 사람의 개인 컴퓨터를 빌려 사용하기 때문에 산재된 자원 속에서 자신의 코드를 안전하게 수행한다는 것은 어려운 일이다.

산재되어 있는 컴퓨팅 공간 속에서 자신의 작업을 외부에 공개하지 않고 안전하게 수행하기 위해서는 자신의 비밀 작업공간이 필요하다. 이러한 가상의 비밀 작업 공간을 PVC(Private Virtual Computing)라 한다.

본 논문에서는 PVC 를 구현하기 위해 사용자의 작업을 안전하게 수행 할 수 있는 신뢰 서버들의 인증과 사용자 작업을 안전하게 위탁하기 위한 위탁 프로토콜을 설계하였다.

2. Private Virtual Computing 의 요구사항과 관련연구

PVC 란 익명의 산재되어 있는 컴퓨팅 자원 속에서 안전한 서버를 찾아 자신의 업무를 위탁하고 결과를

안전하게 전송 받는 시스템을 말한다. 다수의 익명성을 가진 서버들 중에서 안전한 서버라는 것은 다분히 주관적인 판단이기 때문에 본 논문에서는 별도의 관리기관인 CA(인증기관)을 정의하고 여기서 관련된 모든 내용을 총괄한다고 가정한다.

PVC 는 크게 두 가지 부분으로 구분되어 구성된다. 하나는 "**신뢰 그룹 관리**"로 신뢰 그룹을 정의하고 사용자가 쉽게 작업을 위탁할 수 있도록 위탁 키를 관리하는 기능이다. 다른 하나는 "**작업의 안전한 위탁**"으로 사용자의 휴대 단말에서 신뢰 서버까지 위탁 업무를 외부에 유출하지 않고 안전하게 전송하고 수행될 결과를 안전하게 전송 받는 것이다. 다음은 각각의 기능과 그 요구사항들이다.

2.1. 신뢰 그룹 관리

PVC 에서 사용자는 자신의 작업을 위탁하기 위해서 신뢰할만한 위탁 컴퓨터를 찾아야 한다. 이를 위해서 사용자가 신뢰할만한 서버들이 별도 관리 되어야 하며, 사용자의 주변에 산재된 서버들 중에서 쉽게 찾을 수 있어야 한다. 이를 위해서 PVC 에서 구성원은 두 가지의 그룹으로 구분된다. 하나는 신뢰 서버들로 구성된 서버 그룹이며 다른 하나는 클라이언트들로 구성된 클라이언트 그룹이다. 서버 그룹은 서로 동일한 그룹 키와 비밀키를 가지며 클라이언트가 작업을 위탁하는 경우 어떤 구성원이라도 메시지를 해독할 수 있어야 한다. 이와 관련된 연구는 그룹통신을 위한 키 관리가 있다. 이중에서 텍사스 대학의 키 그래프를 이용한 그룹통신 방법은 대규모의 구성원을 가지는 그룹에게 안전하고 효율적으로 키를 전송하고 갱신하는 방법을 제안하고 있다[6]. 이 방법은 그룹통신을 위해서 생성된 그룹키를 분배하기 위해서 기존의 개별적인 키 분배 방식을 소그룹 단위로 키 분배와 갱신을 하여 작업의 양과 시간을 대폭 축소하였다.

2.2. 작업의 안전한 위탁

클라이언트는 폐쇄적인 공간에 있을 때조차 신뢰할 수 있는 서버 그룹의 공개키로 위탁 메시지를 생성하여 주변의 유비쿼터스 컴퓨터(중계 컴퓨터)에게 전송한다. 주변에 산재되어 있는 컴퓨터들은 메시지를 해독하고 자신이 해독하지 못하는 경우 주변의 다른 컴퓨터에게 메시지를 전송하여 적절한 위탁 컴퓨터를 찾게 된다. 이때 중간에 전송한 컴퓨터들은 위탁 메시지를 해독할 수 없어야 한다. 클라이언트가 위탁한 내용은 외부에 공개되지 않아야 하며, "클라이언트-중계 컴퓨터-위탁 컴퓨터"의 연결이 설정되고 수행된 결과는 이 연결을 통해 안전하게 전송 되어야 한다. 미국의 카네기 멜론 대학에서 제안하였던 위탁 컴퓨팅(Surrogate)에서 보여주듯이 적은 자원의 사용자 디바이스는 필연적으로 주변의 컴퓨터를 이용하게 된다[3,5]. 이 과정에서 휴대 단말은 자신과 직접 연결되어 있는 컴퓨터를 통해서 작업을 수행하기 때문에 개인 사생활이 침해될 수 있고 수행한 작업이 완전하다고 판단하기 어려운 문제점을 가지고 있다.

3. 작업 위탁과 Private Virtual Computing

그림 1 은 PVC 를 위한 시스템의 구성을 보여주고 있다. 그림에서 서로 다른 역할을 하는 4 개의 객체가 존재하며 그들의 정의와 역할은 다음과 같다.

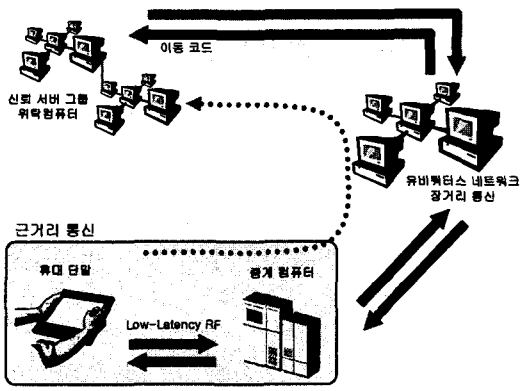

그림 1 Private Virtual Computing 시스템 구성

- ◆ **휴대 단말**: 유비쿼터스 단말기로 사용자의 입력과 기본적인 정보처리를 담당한다.
- ◆ **중계 컴퓨터**: 휴대 단말이 직접 연결된 유비쿼터스 컴퓨터로 사용자의 요청을 중계하는 역할을 한다.
- ◆ **유비쿼터스 네트워크**: 유비쿼터스 컴퓨터들의 모음을 하나의 네트워크로 정의한다.
- ◆ **신뢰그룹의 위탁컴퓨터**: 사용자 혹은 사용자가 소속된 네트워크에서 정의한 신뢰 서버들 중의 하나로 사용자의 작업을 위탁 받아 수행한다.

유비쿼터스 컴퓨팅은 다양한 가상 시나리오가 가능하고 그에 따라 구현방향도 각기 다르지만 여기서는 다음과 같은 상황을 가정하여 설명한다. 홍길동은 자신의 휴가 기간을 아마존의 오지 탐험을 위해 쓰기로 하고 브라질로 떠났다. 급한 회사의 업무는 유비쿼터스 컴퓨팅을 이용하여 휴대 단말로 처리할 예정이기 때문에 아무 걱정이 없었다. 홍길동이 아마존 강 근처의 마나우스 공항에 도착하자 휴대 단말은 긴급한 내용을 표시하고 있다. 홍길동이 만든 회사 방화벽의 보안정책이 문제가 발생하여 긴급히 수정을 해야 한다는 내용이다. 홍길동은 문제점을 파악하고 새롭게 수정된 보안정책을 회사에 전송해야 한다. 하지만 홍길동의 휴대 단말은 수정한 보안정책을 검증할 수 있는 기능이 없다. 따라서 홍길동은 보안정책과 보안정책을 검증할 수 있는 코드를 유비쿼터스 컴퓨터에 위탁해서 처리 해야만 한다. 지금 홍길동은 아마존의 유비쿼터스 네트워크에 연결되어 있고 마나우스 공항의 공공 단말기(그림 1 의 중계 컴퓨터)에 연결되어 있지만 공공 단말기를 통해서 이 일을 처리 할 수는 없다. 위탁하려는 업무가 회사에서 매우 중요한 작업이기 때문에 외부에 유출되거나 거짓으로 검증 되어서는 안되기 때문이다. 결국 홍길동은 휴가를 포기하고 바로 귀국하여 보안정책을 회사에서 수정하였다.

만약 홍길동이 브라질에서 아마존의 유비쿼터스 컴퓨터를 이용하더라도 안전하게 작업을 수행하고 결과를 전송할 수 있었다면 휴가를 잘 보냈을 것이다. 즉 홍길동의 현재 위치에서 신뢰할 수 있고 가장 가까운 곳에 위치한 서버를 통해 보안정책을 검증하고 그 결과를 안전하게 전송할 수 있다면 문제는 해결되는 것이다. 그림 1 에서 휴대 단말은 자신이 독립적인 통신 인터페이스를 가지고 있지 않기 때문에 주변의 중계

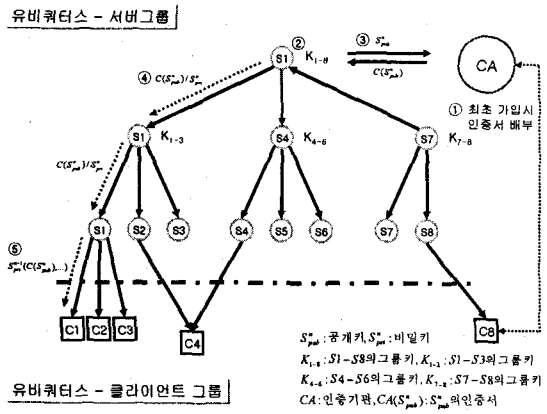

그림 2 그룹키 분배 구조

컴퓨터에 접속하여 작업을 처리한다. 중계 컴퓨터는 휴대 단말을 대신하여 다양한 통신환경과 작업 인터페이스를 제공한다. 하지만 중계 컴퓨터는 휴대 단말이 신뢰하는 서버가 아니기 때문에 중계만 할 뿐 작업을 위탁하거나 전송 정보를 볼 수 없다. 위탁 작업은 중계 컴퓨터를 거쳐 중계 컴퓨터가 속한 네트워크를 지나 신뢰할 수 있는 서버로 까지 흘러 들어 가게 된다. 신뢰 서버로 흘러 들어간 작업은 안전하게 수행이 되고 그 결과를 중계 컴퓨터를 거쳐 휴대 단말로 전송되는 시나리오이다.

위 시나리오에서 휴대 단말은 신뢰 서버를 검색하는 대신에 자신이 신뢰하는 신뢰 그룹의 공개키로 암호화 하여 중계 컴퓨터에게 전송을 하면 중계 컴퓨터가 위탁 작업을 수행할 위탁 컴퓨터를 찾게 된다. 여기서 신뢰 그룹의 서버 구성원이라면 누구나 휴대 단말이 암호화한 메시지를 풀 수 있다. 휴대 단말을 포함한 모든 그룹의 구성원은 다음과 같이 두 가지의 그룹으로 분류된다.

- **서버 그룹**: 많은 컴퓨팅 자원을 가지고 항상 네트워크에 연결되어 있다. 그룹에서 위탁 작업을 수행하며 그룹의 비밀키를 가진다.
- **클라이언트 그룹**: 적은 컴퓨팅 자원을 가지고 있고 때에 따라서는 오프라인 작업을 하기도 한다. 그룹에서 작업을 위탁하는 위치이며 그룹의 공개키를 가진다.

본 논문에서는 그룹 전체를 총괄하기 위해서 인증기관의 존재를 가정한다. 인증기관은 서버 그룹의 구성원을 결정 하고 클라이언트에게 인증서를 발급해 준다. Private Virtual Computing 환경에서 인증기관은 개인, 기업, 정부기관, 네트워크 제공자(Network Provider) 등 필요에 따라서 다양하게 정의하여 사용할 수 있다.

그림 2 는 이와 같이 클라이언트 그룹과 서버 그룹에게 공개키와 비밀키를 어떻게 배분하는 지를 보여주고 있다. 우선 서버 그룹의 키 분배는 텍사스 대학의 키 그래프를 이용한 방법[6]과 동일하다. 최초 1 개의 서버가 그룹을 만들고 서버가 하나 추가되면 추가 프로토콜을, 삭제하면 삭제 프로토콜을 수행하여

추가 프로토콜

S1→{S1 ~ S8}: $E_{K1\text{-}8}[K_{1\text{-}9}], C(S^n_{pub}) / S^n_{pri}$

S1→ S9: $E_{K9}[K_{1\text{-}9}, K_{789}], C(S^n_{pub}) / S^n_{pri}$

삭제 프로토콜 (S9 를 삭제)

S1→{S1 ~ S3}: $E_{K123}[K_{1\text{-}8}], C(S^n_{pub}) / S^n_{pri}$

S1→{S4 ~ S6}: $E_{K456}[K_{1\text{-}8}], C(S^n_{pub}) / S^n_{pri}$

S1→{S7 ~ S8}: $E_{K78}[K_{1\text{-}8}], E_{K7}[K_{78}], E_{K8}[K_{78}], C(S^n_{pub}) / S^n_{pri}$

S_n: n 번째 신뢰서버 K_n: n 을 위한 그룹키

$E_{Kn}[\ldots]$: K_n 으로 암호화

그림 3 그룹의 추가/삭제 프로토콜

그룹 전체의 대칭키(그림 2 의 $K_{1\text{-}8}$)를 생성한다. 다만 본 논문에서는 기존의 키 그래프 방법에 추가로 공개키/비밀키 쌍을 같이 전송한다. 그림 3 은 새로운 서버의 추가 와 삭제 프로토콜을 보여 준다. 새로운 서버가 추가되는 경우 기존의 멤버들에게 이전 그룹의 그룹키(대칭키)로 새로운 키를 전송하고 서버가 삭제되는 경우에는 삭제된 서버가 속한 소그룹의 그룹키를 생성(K_{78})하여 각자의 키(K_7, K_8)로 암호화 하여 소그룹의 그룹키를 분배한 다음에 전체 그룹의 새로운 그룹키($K_{1\text{-}8}$)를 각 소그룹의 그룹키(K_{123}, K_{456}, K_{78})로 암호화 하여 분배 한다. 각 프로토콜에서 새로운 그룹키를 생성할 때 공개키/비밀키 쌍을 같이 생성하고 공개키는 인증센터에서 인증서로 발급 받는다. 이때 새로운 그룹키와 함께 공개키 인증서, 비밀키를 같이 배분한다. 그룹의 각 서버는 그룹키, 공개키 인증서, 비밀키를 수신하여 그룹키와 비밀키는 보관하고 공개키 인증서는 연결되어 있는 클라이언트 그룹에게 $S^{n-1}_{pri}(C(S^n_{pub}),\ldots)$ 형태로 전송해 준다. 이때 새로운 공개키 인증서는 이전 그룹의 비밀키(S^{n-1}_{pri})로 암호화하여 전송하기 때문에 그룹의 이전 공개키(S^{n-1}_{pub})를 아는 클라이언트만 수신을 할 수 있다. 그룹에 처음 가입하는 클라이언트는 인증센터로부터 직접 공개키 인증서를 발급 받는다. 키 분배 과정을 마치면 신뢰 그룹은 항상 다음과 같은 상태를 유지한다.

- 서버 그룹: 현재 서버그룹의 그룹키, 전체 그룹의 비밀키, 공개키를 가진다.
- 클라이언트 그룹: 현재 클라이언트 그룹의 공개키 인증서를 가지고 있다.

서버 그룹과 클라이언트 그룹은 한쌍의 비밀키/공개키를 나누어 가지게 되어 클라이언트 그룹의 구성원이 공개키로 암호화한 내용을 서버 그룹의 어느 컴퓨터나 복호화 할 수 있다. 다시 말해 서버 그룹과 클라이언트 그룹이 공개키 쌍을 나누어 가지게 됨으로 해서 클라이언트는 위탁할 작업을 자신이 가진 공개키로 단순 암호화하여 전송하면 대응되는 비밀키를 가진 서버만이 해독을 할 수 있게 되어 신뢰 그룹에 속한 서버에게 안전하게 작업을 위탁하게 된다.

휴대 단말인 클라이언트가 작업을 신뢰 서버에 위탁하기 위해서는 중계 컴퓨터를 거쳐야 한다. 중계 컴퓨터는 휴대 단말에게 다양한 통신기능과 대리자의 역할을 수행하기 때문에 악의적인 공격이 가능하다.

Private Virtual Computing을 가능하게 하기 위해서는

$A \rightarrow B$: $E_{KUb}[E_{KUg}[DATA||M\_Code||ID_A||R_1||R_2],R_1]$
$B \rightarrow G$: $E_{KUg}[DATA||M\_Code||ID_A||R_1||R_2]$
$G \rightarrow [H_1,\ldots,H_n]$: M_Code
$G \rightarrow B$: $E_{KUb}[E_{KUa}[RTN_g||R_2],R_1]$
$B \rightarrow A$: $E_{KUa}[RTN_g||R_2]$

A: 클라이언트	DATA: 홍길동의 데이터
B: 중계컴퓨터	M_Code: 수행할 명령어(코드)
G: 신뢰서버	ID_A: 홍길동의 개인 식별자
H_n: 범용서버	RTN_g: 신뢰서버의 수행 결과
R_1, R_2: 난수	

그림 4 위탁컴퓨팅 프로토콜

작업을 위탁하고 결과를 수신하는 과정에서 발생할 수 있는 다양한 공격을 제거 해야 한다. 그림 4 는 이러한 공격을 막기 위해서 휴대단말⇔중계컴퓨터⇔신뢰서버⇔범용서버 사이의 통신 프로토콜을 보여주고 있다. 그림 4 에서 홍길동은 새로 작성한 보안정책을 회사내의 N 개의 서버에 전송하여 설치 및 실험해 보고자 한다. 휴대단말에서 수정된 보안정책(DATA), 수행코드(M_Code), 개인 식별자(ID), 난수 R_1, R_2 를 신뢰그룹의 공개키로 암호화(E_{KUg})하고 난수 R_1 를 다시 추가하여 중계 컴퓨터의 공개키로 암호화[1](E_{KUb})하여 $E_{KUb}[E_{KUg}[DATA||M_Code||ID_A||R_1||R_2],R_1]$를 중계 컴퓨터에 전송한다. 중계 컴퓨터는 수신한 메시지를 복호화하여 $E_{KUg}[DATA||M_Code||ID_A||R_1||R_2]$와 R_1 값을 얻게 된다. $E_{KUg}[DATA||M_Code||ID_A||R_1||R_2]$를 유비쿼터스 네트워크에 전송하고 R_1 값은 따로 저장 한다. 유비쿼터스 네트워크는 서버들을 검색하여 가장 가까운 신뢰 서버를 찾아 이 메시지를 전송한다(이 경우에는 신뢰 그룹이 홍길동의 회사 컴퓨터들로 정의한다.). 메시지를 수신한 신뢰 서버는 메시지를 복호화하여 보안정책, 수행코드, 식별자, 난수를 얻어 수행코드를 수행한다. 수행코드는 이동코드로 작성되어서 스스로 검증하고 회사내의 여러 서버($H_1,\ldots,H_n$)를 이동하면서 새로운 보안 설정을 설치 한다. 수행코드가 모든 작업을 마치고 처음의 신뢰서버(G)로 돌아오면 신뢰서버는 결과값과 R_2 값을 그룹의 비밀키로 암호화 하고 다시 R_1 값을 첨가하여 중계 컴퓨터의 공개키로 암호화하여 전송한다. 중계 컴퓨터는 자신의 비밀키로 복호화하여 자신이 저장한 R_1 값과 일치하는지를 검사한 다음 휴대 단말에 결과를 전송($E_{KUa}[RTN_g||R_2]$)한다. 최종적으로 휴대 단말은 메시지를 복호화하고 수신된 난수가 자신이 처음에 보낸 수(R_2)인가를 확인한다. 단 여기서 난수는 시간정보를 포함하며 충돌이 생기지 않을 만큼 충분히 긴 수이다.

4. 안전성 분석

3 장에서 제시한 Private Virtual Computing 은 그룹키 분배 와 위탁컴퓨팅 프로토콜로 구성된다. 그룹키 분배는 모든 과정이 이전 그룹키로 이루어 지기 때문에 키의 유출이 없는 한 안전하다. 반면 위탁컴퓨팅 프로토콜은 악의를 가진 중계 컴퓨터를 경유하여 전송되기 때문에 위험 가능성이 있다. 다음은 다양한 공격의 가능성을 살펴보고 그 공격이 성공하기 위한 조건들을 나열하였다.

- ◆ A→B 과정에서 B 에게 혹은 B→G 과정에서 G 에게 거짓 정보 제공: 그룹의 공개키/비밀키가 유출되지 않는다면 거짓 정보를 생성하는 것은 불가능 하다.
- ◆ G→B 과정에서 B 에게 거짓 정보 제공: 수행 결과에 대한 응답 메시지를 기존의 다른 것으로 재생(replay) 공격의 가능성이 있지만 응답 메시지에 난수 R_1, R_2 를 삽입하여 가능성이 없다.
- ◆ B→A 과정에서 A 에게 거짓 정보 제공: 사용자가 같은 중계 컴퓨터를 계속 이용하는 경우 B 가 G 에게 메시지를 전달하지 않고 이전에 수행한 결과를 재생(replay) 공격할 가능성이 있지만 내부에서 사용되는 난수 R_2 가 충돌이 생기지 않을 만큼 충분히 크기 때문에 그 가능성이 없다.
- ◆ B 에 의 한 공격: 중계 컴퓨터가 T1 메시지를 중계하고 이어서 T2 메시지 중계하였는데 T1 의 결과가 자신에게 더 유리한 경우 다시 T1 메시지를 중계할 수 있다. 이러한 공격의 경우 신뢰서버는 T1 이 정상적인 메시지 때문에 T1 을 수행한다. 이러한 공격을 막기 위해서 난수 값에 시간 정보를 포함시켰다.

5. 결론

유비쿼터스 컴퓨팅 환경은 편리한 만큼 개인 사생활을 해칠 가능성이 크다. 특히 중계 컴퓨터를 이용하는 경우 작업을 안전하게 수행하기 어렵다. 이러한 문제를 해결하기 위해서 본 논문은 Private Virtual Computing 개념을 제안하고 이를 구현하기 위한 구체적인 방법을 제시하였다. 앞으로는 하나의 휴대 단말이 여러 신뢰 그룹에 속한 경우 효율적인 통합 방법과 이동코드 기술을 접목한 분야를 연구할 예정이다.

참고문헌

[1] M. Weiser, "The Comptuer for the 21st Century," Sci. Amer., Sept., 1991.

[2] NIST, http://www.nist.gov/pc2001/

[3] R. K. Balan, J. Flinn, M. Satyanarayanan, S. Sinnamohideen, H. Yang, "The Case for Cyber Foraging," In Proceedings of the 10th ACM SIGOPS European workshop, Saint-Emilion, France, September 2002.

[4] R. Campbell, D. Sturman, T. Tock, "Mobile Computing, Security and Delegation," the International Workshop on Multi-Dimensional Mobile Communications, 1994.

[5] J. Park, D. Lee, H. Kim, I. Jang, J. Park, "Virtual private computing for thin client against malicious surrogate", Spring Korea Information Science Society Conference, 2003.

[6] C. Wong, M. Gouda, S. Lam, "Secure group communications using key graphs," IEEE/ACM Transactions on Networking, Volume. 8, Issue 1, p. 16-30, Feb. 2000.

[7] Mignotte, M., "How to share a secret?," Cryptography – Proceedings of the Workshop on Cryptography, Burg Feuerstein, Germany, p. 371. Springer-Verlag, Berlin, 1983.

[1] 중계 컴퓨터와 휴대 단말 사이의 비밀통신을 위한 것으로 반드시 공개키 방식을 사용할 필요는 없다.