악의의 위탁 컴퓨터로부터 씬 클라이언트 보호를 위한 Virtual private computing

박종열* 이동익* 김형천** 장인숙** 박중길**
*광주과학기술원 정보통신공학과
국가보안기술연구소
jypark@kjist.ac.kr

Virtual private computing for thin client against malicious surrogate

Jongyoul Park* Dong-Ik lee* Hyoung-Chun Kim** In-Sook Jang** Joong-Gil Park**
*Kwang-Ju Institute of Science and Technology
** National Security Research Institute

요 약

Pervasive 컴퓨팅은 다양한 분야에서 다양한 방향으로 연구가 진행 중에 있다. 제안된 모델 중에 CMU에서 제안한 위탁형 컴퓨팅 모델은 앞으로의 연구에 대한 한 방향을 제시하고 있다. 이 모델은 사용자가 요청하는 작업을 휴대하는 컴퓨터에서 처리하는 것이 아니라 주위에 뛰어난 성능을 가진 컴퓨터에게 작업을 위탁하는 방법이다. 이 방법은 기존 단말에서 작업을 처리 하는 것에 비해 뛰어난 성능을 보이지만 위탁 컴퓨터에 의한 공격에 취약한 단점을 가지고 있다. 본 논문에서는 이러한 단점을 보완하기 위해서 Virtual Private Computing이라고 하는 개념을 제안 한다.

1. 서론

Ubiquitous 컴퓨팅은 Xerox Park의 Mark Weiser에 의해서 처음 제안되었다[1]. ubiquitous는 pervasive 컴퓨팅이라고도 불리며 미국 NIST에서는 다음과 같은 특징들로 정의하고 있다[2].

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

Pervasive 단어의 의미에서 알수 있듯이 많은 컴퓨터들이 서로 연결되어 있고, 사용자는 그 컴퓨터들을 실제로 인지하지 않아도 자신이 원하는 작업을 언제 어디서나 서비스 받을 수 있는 컴퓨팅 환경을 말한다.

뛰어난 성능의 PDA의 등장과 무선랜, 블루투스, 적외선 통신과 같은 무선 통신 기술이 발전하면서 pervasive 컴퓨팅 기술은 차세대 컴퓨팅 환경으로 인식되고 있다. 특히 스마트 가전기술의 발전은 활용 가능성에 대한 비전을 제시했다. 다양한 이름으로 개발되고 있는 pervasive 컴퓨팅은 UC Berkely의 Endeavour[3], MIT의 Oxygen[4], CMU의 Aura[5], U. of Washington의 Portolano[6]가 대표적인 연구 사례이고 산업계에서는 영국 AT&T Research in Cambridge, IBM T.J Watson Research Center와 HP가 공동으로 연구하는 cooltown, Microsoft의 EasyLiving의 연구가 진행 중에 있다.

Pervasive 컴퓨팅을 위한 많은 기술 중에 사용자의 인터페이스는 기존의 시스템과 많은 부분에서 다르다. 이동이 쉽고 사용자가 특별히 인지하지 않아도 되는 특징은 많은 기능을 모두 포함해야 하는 기존의 컴퓨터와는 다른 작은 컴퓨터를 요구하게 된다. 이러한 작은 컴퓨터들은 사용자가 필요로 하는 모든 프로그램과 기능을 갖추는 것은 힘든 일이며 비 효율적이다. 따라서 pervasive 컴퓨팅 환경에서 사용자는 주위의 산재되어 있는 컴퓨팅 자원을 필연적으로 이용하게 된다[7]. 이 경우 산재된 자원은 개인의 소유가 아닌 다수 혹은 다른 사람의 컴퓨터일 가능성이 높고 사용자의 요청한 작업을 안전하게 수행한다는 보장을 받기 힘들다.

본 논문에서는 사용자가 산재된 컴퓨터로 작업을 위탁하는 경우 악의를 가진 위탁 컴퓨터의 공격으로부터 작업을 보호하기 위한 방법을 제시한다.

2. Pervasive 컴퓨팅 기술과 문제점

Pervasive 컴퓨팅은 그림 1과 같이 기반 구조, 분산서비스, 사용자인터페이스의 3개 영역으로 구성[6]이 된다. 기반구조는 전체 시스템을 가능하게 하는 기반기술들의 집합으로 통신시스템, 파일 시스템, 자원관리와 같은 가장 기본적인 기능을 제공하는 영역이다. 분산 서비스는 기반 구조에서 제공하는 통신, 자원, 데이터를 이용하여 구체적인 서비스를 제공하는

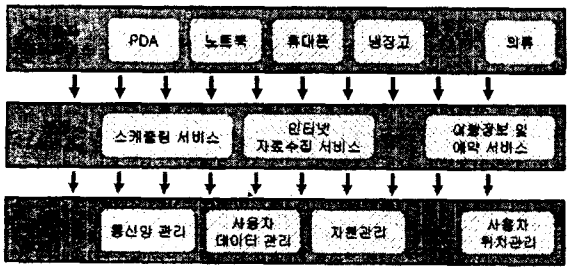

그림 1 Pervasive 컴퓨팅 구조

영역이며 개인 사용자의 스케줄이나 인터넷에서 자료를 수집하는 구체적인 기능을 수행한다. 마지막으로 사용자 인터페이스는 사용자의 입력을 받아 적절한 출력을 보이는 장치를 의미한다. 노트북과 같은 완전한 컴퓨터로부터 휴대폰, PDA와 같은 휴대 단말뿐만 아니라 우리가 일상적으로 입고 다니는 의류[8]까지 다양한 인터페이스들이 제공된다. 사용자는 항상 자신의 위치와 기본적인 정보를 저장하고 처리하기 위해서 위에 나열된 인터페이스 중에서 하나를 항상 휴대 한다. 이 인터페이스는 기본적인 연산 능력과 메모리를 가지게 되며 독립적인 연산뿐만 아니라 주변의 기기들과의 통신 기능을 제공한다.

물론 다양한 pervasive 컴퓨팅 시나리오들이 존재하기 때문에 우리가 가정하고 있는 연산 능력을 구비하지 않을 수도 있다. 하지만 본 논문에서는 사용자 인터페이스에는 PDA 수준의 연산능력과 메모리를 가지고 있다고 가정한다.

Pervasive 컴퓨팅은 다양한 가상 시나리오가 가능하지만 다음과 같은 상황을 고려해 보자(그림 2). 홍길동은 아침 7시 미국 출장을 위해서 인천국제공항 21번 게이트 앞에서 탑승을 기다리고 있다. 아직 임원들은 아무도 출근을 하지 않은 상황이다. 그는 방새워 작성한 기획 안을 올리고 미국행 비행기를 탑승하려고 한다. 홍길동의 시계는 가상 스크린과 가상 키보드를 가지고 있으며 PDA 수준의 프로세서를 가지고 있다. 시계는 홍길동이 이동함과 동시에 위치를 파악하고 적외선 통신을 이용해서 가장 가까운 컴퓨터와 연결되어 있는 상태이다. 지금은 21번 게이트에 있는 항공사의 단말기를 위탁 컴퓨터로 할당받고 있다. 홍길동의 시계는 pervasive 네트워크에 접속하기 위해서 인증 과정을 완료했다. 홍길동은 가상모니터를 이용해서 방금 완료한 기획안을 회사의 컴퓨터에 접속하여 결제를 받아야 한다. 하지만 기획안에는 회사내의 제정에 관련된 중요한 내용을 담고 있어 외부에 공개되어서는 안 된다. 홍길동은 게이트에 있는 단말기를 믿을 수 없기 때문에 결국 전송을 포기하게 된다. 결국 LA에 도착한 홍길동은 자동차로 3시간 떨어진 샌디에이고 지사에서 작업을 완료한다.

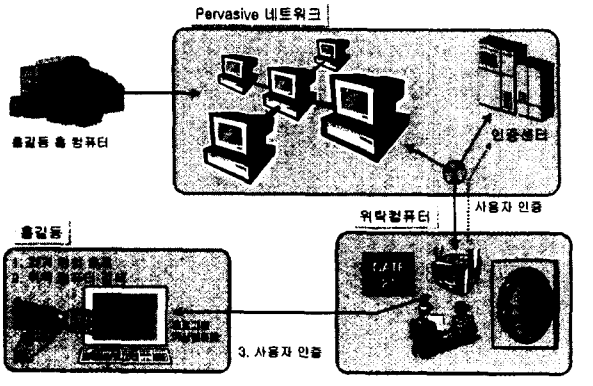

그림 2 위탁 컴퓨팅 시나리오

우리가 가정한 Pervasive 컴퓨팅은 사용자가 직접 pervasive 네트워크에 접속하는 것이 아니고 위탁 컴퓨터를 통해서 접속하기 때문에 위탁 컴퓨터에 의한 공격에 취약한 특징을 가지고 있다. 위탁 컴퓨터는 위탁 컴퓨터에 연결되어 있는 사용자의 모든 업무를 위탁 수행하기 때문에 도청/감청뿐만 아니라 심지어는 거짓 정보를 제공하는 것까지 가능하다.

3. 작업 위탁과 Private Virtual Computing

2장에서는 pervasive 컴퓨팅에서 사용자가 직면할 수 있는 하나의 문제를 보여 주고 있다. 이러한 문제는 사용자의 인터페이스가 네트워크에 직접 연결되지 않고 위탁 컴퓨터를 이용하기 때문이다. 이러한 위탁 모델을 사용하는 이유는 다음과 같은 장점이 있기 때문이다.

- **효율적인 처리 능력**: CMU에서 발표한 논문[7]을 보면 실제로 직접 네트워크에 연결하여 작업을 수행하는 경우와 위탁 컴퓨터를 이용하여 작업을 수행하는 경우의 성능을 비교하고 있다. 위탁 컴퓨터를 활용하는 경우 약 64%로 작업 시간이 단축되는 것을 볼 수 있다.
- **관리비용의 절감**: 네트워크에 직접 접속하는 경우 시스템이 발전하면서 사용자의 인터페이스 기능도 같이 업데이트 혹은 업그레이드를 필요로 하게 된다.

실제로 위탁 컴퓨팅을 구현하는 과정에서 보안상의 문제들이 지적되고 있다. 이는 작업을 위탁받는 컴퓨터가 실행 주체이기 때문에 생기는 문제이다. 또한 위탁 컴퓨터가 특별히 지정되거나 검증된 컴퓨터가 아니고 어느 컴퓨터나 위탁 작업을 수행할 수 있기 때문이다. 지금까지 pervasive 컴퓨팅 환경에서의 보안 문제는 사용자의 인증과 외부 도청을 어떻게 막는가에 초점이 맞춰져 있어서 아직까지 적절한 대응책이 제시되지 못하고 있다.

그림 3 Virtual Private Computing 프로토콜

우리는 이 문제를 풀기위해서 다음과 같은 가정을 하였다.

- ◆ 공개키 기반 구조를 가진다.
- ◆ 자신이 신뢰하는 컴퓨터(홈 컴퓨터)를 가지고 있다.

그림 2에서 홍길동은 자신의 개인 컴퓨터(H)를 가지고 있고 pervasive 네트워크에 연결되어 있다. 위탁 컴퓨터는 21번 게이트의 단말기(B)로 지정하고 자신의 인터페이스인 시계(A)를 사용해서 지시한다.

그림 3과 같이 홍길동은 전송할 문서(DOC)와 함께 홈 컴퓨터에서 수행을 하고자 하는 코드(M_Code), 난수(R_1, R_2), 개인 식별자 ID_A, 일회용 비밀번호 OTP_A[9]를 홍길동 개인 컴퓨터 H의 공개키로 암호화(E_{KUb}) 하고 R_1과 함께 위탁 컴퓨터의 공개키로 다시 암호화(E_{KUh}) 하여 위탁 컴퓨터에게 전송한다. 위탁 컴퓨터는 R_1 값을 기억하고 나머지 값을 홈 컴퓨터(H)에게 그대로 전송한다. 홈 컴퓨터는 메시지를 복호화하고 OTP_A를 확인한 후에 전송된 코드와 데이터를 이용하여 지시된 작업을 수행한다. 앞의 예에서는 홍길동의 기획 서류를 회사의 결제 시스템에 연동 시키는 프로그램이다.

여기서 홈 컴퓨터는 믿을 수 있는 컴퓨터들을 총칭한다. 믿을 수 있는 컴퓨터란 홍길동의 신뢰를 받고 있는 컴퓨터들의 집합으로 다음과 같은 특징을 가지는 컴퓨터들 의미한다.

- ◆ 동일한 공개키 혹은 그룹키를 사용
- ◆ 사용자의 OTP를 검증 가능

홈 컴퓨터는 개인이 소유한 컴퓨터가 될 수도 있지만, 개인이 속한 조직이나 특정 네트워크로 한정할 수 있다. 일반적으로 같은 조직에 있는 컴퓨터가 되며, 홍길동의 경우에는 회사망 안에 있는 컴퓨터가 된다.

모든 작업을 마친 홈 컴퓨터는 결과(RTN_H)를 난수 R_2와 함께 홍길동의 공개키로 암호화(E_{KUA})하고 R_1과 함께 위탁 컴퓨터의 공개키로 다시 암호화(E_{KUh})한다. 위탁 컴퓨터는 메시지를 수신하고 처음에 자신이 홍길동으로부터 받은 난수값(R_1)과 일치하는지 확인한다. 일치하는 경우 난수 이외의 데이터를 홍길동에게 전달하게 된다. 최종적으로 홍길동은 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

3장에서 제시한 프로토콜은 다양한 공격의 가능성이 있으며 그 공격이 성공하기 위한 조건들은 다음과 같다.

- ◆ **A→B 과정에서 B에게 혹은 B→H 과정에서 H에게 거짓 정보 제공**: 공격 메시지의 생성은 가능하지만 OTP_A를 생성하지 못하기 때문에 H 에서 원하는 코드를 수행할 수 없다.
- ◆ **H→B 과정에서 B에게 거짓 정보 제공**: 공격 메시지의 생성은 가능하지만 R_1값을 알지 못하기 때문에 유효한 공격 메시지의 생성이 불가능하다.
- ◆ **B→A 과정에서 A에게 거짓 정보 제공**: 공격 메시지의 생성은 가능하지만 R_2값을 알지 못하기 때문에 유효한 공격 메시지의 생성이 불가능하다.
- ◆ **B에 의한 공격**: 위탁 컴퓨터 B 역시 H 에서 코드를 수행시키기 위해서는 OTP_A를 알아야 하고 A에게 거짓 정보를 전송하려고 하면 R_2값을 알아야 한다.

5. 결론

본 논문에서는 위탁 컴퓨터를 이용하는 경우 안전한 작업을 수행하기 위한 Virtual Private Computing을 구현하기 위한 한 방법을 제안하고 분석하였다. 아직은 홈 컴퓨터를 이용하는 한정된 사례가 연구되었지만 앞으로 범용으로 사용 가능한 시스템의 연구를 진행할 예정이다.

6. 참고문헌

[1] M. Weiser, " The Computer for the 21st Century," Sci. Amer., Sept.,1991.
[2] NIST, http://www.nist.gov/pc2001/
[3] Endeavour, http://endeavour.cs.berkeley.edu/
[4] Oxygen, http://oxygen.lcs.mit.edu/
[5] Aura, http://www.cs.cmu.edu/~aura/
[6] M. Esler, J. hightower, T. Anderson, G. Borriello, " Next Century Challenges: Data-Centric Networking for Invisible Computing," In Proceedings of MOBICOM' 99, Seattle, Washington, August 1999.
[7] 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.
[8] Wearable, http://www.media.mit.edu/wearables/
[9] N. Haller, C. Metz, " A One-Time Password System," RFC 1938, 1996.