Thin-Client 로봇 보안 프레임워크에 관한 연구

김건우*, 한종욱

*한국전자통신연구원

Study on Security Framework of Thin-Client Robot

Geon-woo Kim*, Jong-wook Han

*Electronics and Telecommunications Research Institute

E-mail : kimgw@etri.re.kr

요 약

RUPI 기반 로봇 서비스는 다양한 성능을 지원하는 로봇과 서버간의 연동을 통해서 융통성과 확장성을 보장하는 로봇 기반 서비스를 제공한다. 높은 H/W 성능과 계산 능력을 보장하는 Rich-Client 로봇과 달리 Thin-Client 로봇은 제한된 성능만을 제공하기 때문에, 상대적으로 높은 연산량을 요구하는 보안 알고리즘을 수행하기에는 어려움이 있다. 따라서 본 논문에서는 Thin-Client 로봇의 보안 위협과 요구사항, 및 보안 기능을 포함하는 Thin-Client 로봇 보안 프레임워크를 제안한다.

ABSTRACT

RUPI-based robot service provides a variety of robot services guaranteeing extensibility and flexibility by communications between heterogeneous robots and servers. Unlike rich-client robot of high H/W performance and computing ability, as thin-client robot supports limited capability, it has some difficulty in performing security algorithms requiring relatively high computation power. Therefore, in this paper, we propose security framework of thin-client robot containing security threats, security requirements, and security functions.

키워드

로봇 보안, Thin-client 보안 프레임워크

Ⅰ. 서 론

홈네트워크는 이동통신, 초고속 인터넷 등 유·무선 통신 네트워크를 기반으로 가정 내의 A/V, 데이터통신 및 정보가전 기기들이 네트워크로 상호 연결되어 기기·시간·장소에 구애받지 않고 다양한 서비스를 제공받을 수 있는 가정 환경을 구축하여 국민들에게 편리하고, 안전하고, 즐겁고, 윤택한 삶을 제공할 수 있는 새로운 IT 기술 이용 환경이라 할 수 있다[1].

이러한 홈네트워크 서비스의 하나로서 로봇에 관한 많은 연구와 개발이 현재 활발히 진행 중이다. 로봇 서비스는 인터넷과의 연결로 인하여 인터넷에서 발생되고 있는 다양한 사이버 공격에 그대로 노출되어 있어 해킹, 악성코드, 웜 및 바이러스, 서비스 거부 공격, 통신망 도·감청 등에 보안 취약성을 내포하고 있다[2]. 또한 정상적인 홈네트워크 사용자일지라도 사용자의 권한과 특성을 고려해서 서로 다른 서비스를 제공해야 할 필요성이 있다. 또한 제한된 성능을 지원하는 Thin-client 로봇에는 기존 보안 메커니즘을 그대로 적용하기에는 많은 어려움이 있다.

따라서 본 논문에서는 로봇 서비스 환경에서 발생할 수 있는 보안 위협을 정의하고, 이를 방어하기 위한 보안 요구사항, 보안 기능을 포함하는 Thin-client 로봇 보안 프레임워크를 제안한다.

II. 본 론

RUPI 기반 로봇 시스템은 시간과 장소에 구애받지 않고 다양한 콘텐츠를 전송해서, 원격에 위치한 로봇에서 이를 실행할 수 있다.

RUPI 기반 로봇 시스템의 구성을 보면 그림 1과 같다.

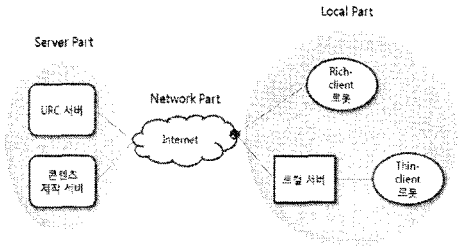

그림 1. 로봇 시스템 구성

네트워크 로봇 서비스의 구성을 보면, 크게 3부분으로 구분할 수 있다. 모든 로봇을 관리하고 콘텐츠를 제작하고 분배하는 기능을 수행하는 server part, 두 부분간 통신 기능을 수행하는 network part, 및 다운로드받은 콘텐츠를 수행하고 고유 로봇 기능을 수행하기 위한 local part로 구성된다.

Rich-client 로봇은 컴퓨터와 유사한 성능을 제공하기 때문에 server part와 직접 네트워킹이 가능하지만, Thin-client 로봇은 자체 운영체제도 탑재되지 않는 경우가 대부분일 정도로 제한된 성능만을 지원한다. 따라서 원거리의 서버와 직접 통신하기에는 무리가 있으며 동일 서비스 도메인에 위치한 로컬 서버를 통해서 원격 서비스를 제공받는다.

2.1 보안 위협

RUPI 기반 로봇 서비스는 인터넷에 직접 노출되어 있기 때문에, 기존 시스템에서 발생할 수 있는 모든 보안 위협이 존재한다. 또한 로봇 기기가 개인 프라이버시 정보를 다수 포함하고 있는 경우가 많아, 외부에 노출될 경우 심각한 보안 위협에 처할 수 있다.

다음은 RUPI 기반 로봇 서비스에서 발생할 수 있는 보안 위협을 나타낸다.

- Eavesdropping/Disclosure/Interception: 네트워크를 통해서 전송되는 데이터가 외부로 불법 노출되면 심각한 개인 프라이버시 침해를 노출할 수 있을 뿐 아니라, 제작된 콘텐츠의 저작권을 침해할 수있다.
- Interruption/Communication jamming: 외부에 의한 통신 장애는 정상적인 로봇 서비스에 방해한다.
- Injection and modification of data: 전송 또는 저장되어 있는 데이터에 대해서 불법적으로 수정이 발생할 경우, 정상적인 서비스를 방해할 수 있다.
- Unauthorized access: 인가되지 않은 접근은 개인 프라이버시를 침해할 수 있다.
- Repudiation: 전송된 데이터 송/수신 부인을 통해서 로봇 시스템 서비스 방해와 신뢰로 저하를 초래한다.
- Shoulder surfing: 개인 정보의 유출로 인하여 불법 서비스 접근을 허용한다.
- Lost robot device: 개인 정보의 유출을 초래한다.
- Stolen robot device: 개인 정보의 유출을 초래한다.
- Packing abnormal-forwarding: 로컬 서버에 발생할 수 있는 문제로서 Thin-client 로봇의 오동작을 유발한다.

2.2 Thin-client 보안 요구사항

2.1절에서 정의된 보안 위협으로부터 Thin-client 로봇 시스템을 안전하게 보호하기 이한 보안 요구사항은 다음과 같다.

- Confidentiality: 서버와 로봇, 및 로봇간 전송되는 데이터의 기밀성 보장
- Integrity: 전송되는 데이트의 무결성
- Authentication: 네트워크 통신 당사자의 인증
- Non-repudiation: 부인 방지
- Access control: 접근 제어
- Availability: 가용성
- Privacy: 개인 프라이버시 정보 보호

위의 요구사항들 중에서 Thin-client 로봇의 특성을 고려해서 Thin-client에서 반드시 보장되어야 할 보안 요구사항은 Integrity, Authentication이다.

2.3 보안 위협과 보안 요구사항 관계

표 1은 로봇 시스템에서 정의된 보안 위협과 보안 요구사항간의 관계를 보여준다.

표 1. relationship between security threats and security requirements

Requirements / Threats	Confidentiality	Integrity	Authentication	Non-repudiation	Access control	Availability	Privacy
Eavesdropping	Y		Y		Y		Y
Interruption			Y		Y		

Modification	Y	Y	Y		Y		
Unauthorized access	Y		Y		Y		Y
Repudiation				Y			
Shoulder surfing							
Lost/Stolen			Y		Y		Y
Packet abnormal forwarding		Y				Y	

2.4 Thin-client 로봇을 위한 보안 구조

로봇의 안전성을 보장하기 위해서는 앞에서 정의된 보안 요구사항을 만족할 수 있어야 한다. 하지만, 제한된 성능을 지원하는 Thin-client 로봇이 모든 보안 요구사항을 만족시키기는 쉽지 않다. 따라서 본 절에서는 Thin-client 로봇의 보안 구조를 도식화하고, 필요한 보안 요구사항을 구분한다.

그림 2는 Thin-client 로봇을 위한 보안 구조를 나타낸다.

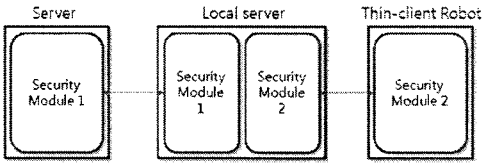

그림 2. Thin-client 로봇 보안 구조

Thin-client 로봇에 서비스를 제공하는 구조는 그림 2과 같이 크게 3개의 노드로 구성되어 있다. Thin-client 로봇을 관리하고 콘텐츠를 제공하는 server, 외부로는 server와 통신하고 내부적으로는 Thin-client 로봇에 서비스를 제공하는 local server, 및 Thin-client 로봇으로 구성된다. 즉 필요한 네트워크는 server와 local server간의 통신, local server와 Thin-client 로봇간의 통신이다.

Server와 local server는 각각 높은 성능을 보장하고, 이들 간의 통신은 인터넷을 경유하기 때문에 상대적으로 높은 보안성을 요구하는 반면, local server와 Thin-client 로봇간의 통신은 Thin-client 로봇의 성능과 댁내와 같은 비교적 접근에 제한된 망을 사용하는 것을 고려하면, 기본적인 보안 기능만을 제공하는 것을 요구한다.

Security module 1이 제공해야 할 보안 요구사항은 다음과 같다.

- Confidentiality
- Integrity
- Authentication
- Access control
- Non-repudiation
- Availability
- Privacy

이에 반해, Security module 2가 반드시 제공해야 할 보안 요구사항은 다음과 같다.

- Authentication
- Integrity

그림 3은 Security module 1/2에서 사용될 키 관리 구조를 보여준다.

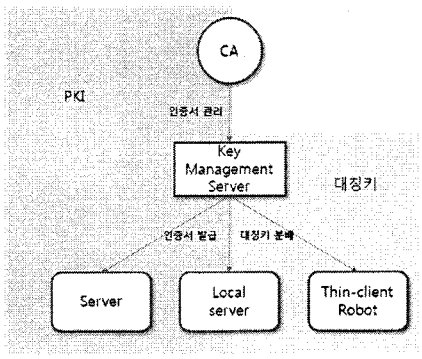

그림 3. Thin-client 로봇 키 관리 구조

RUPI 기반 로봇 서비스 구조에서는 공개키 방식과 대칭키 방식을 동시에 적용하는 것이 효율적이다. 즉, 인터넷과 같은 외부망에서 동작하는 노드(Server, Local server, Rich-client 로봇 등)는 공개키 방식을 사용한다. 반면에 내부 망에서 동작하는 Thin-client 로봇의 경우에는 대칭키를 사용하는 것이 바람직하다.

Thin-client 로봇이 외부 인터넷과 연동할 때에는 반드시 local server를 통해서 동작하므로 local server는 Thin-client 로봇의 신뢰할 수 있는 외부 인터페이스 역할을 수행한다.

III. 결 론

로봇에 대한 다양한 연구와 개발이 활발히 진행되고 있으며, 사용자에게 친숙한 서비스와 어플리케이션을 개발하기 위해서 많은 노력이 이루어지고 있다. 로봇은 다양한 H/W 성능과 제약 사항을 가지고 있다. 또한, 외부에 노출되어서는 안되는 개인 프라이버시 정보를 관리하기 때문에 안전성을 보장하기 위한 모듈이 필수적이다.

따라서 본 논문에서는, 제한된 성능만을 보장하는 Thin-client 로봇에서 발생할 수 있는 보안 위협을 정의하고, 이를 위한 보안 요구사항을 정의한다. 또한 이들 간의 연관관계를 보여주고, Thin-client 로봇 보안 구조를 제안한다.

참고문헌

[1] 김정원, 정보통신부, "홈 네트워크 산업 활성화 정책 방향", 정보과학회지, 2004, 09, 제 22권 제 9호 통권 제 184호

[2] 한종욱, 김도우, 주홍일, 한국전자통신연구원, "홈 네트워크 보안 프레이워크 구축을 위한 고려사항", 정보과학회지 2004, 09, 제 22권 제 9호 통권 제 184호