ICT 기기인증 보안기술 현황

박정효
한국인터넷진흥원

요 약

과거의 휴대폰, TV, 전화기 등의 기기들은 아날로그 신호 기반이 주류를 이루었고, 낮은 대역폭, 폐쇄된 네트워크 환경, 낮은 컴퓨팅 사양 등으로 그 적용 범위가 협소하였고, 어느 정도 보안성을 갖추었다고 볼 수 있다. 하지만, 최근 들어 고품질의 서비스를 제공하는 다양한 기기들이 등장하고 네트워크 대역폭과 제공 범위가 확장되면서 정보통신 기기의 중요성과 위협요소가 커지고 있다. 특히, 2010년부터 본격적으로 시작된 스마트폰의 확산으로 태블릿 PC, 스마트 TV, 스마트워크, 스마트그리드 등 스마트 기기 시대가 개막되었음을 알 수 있다. 이에 정보통신기기의 보안은 더 이상 간과할 수 없는 중요한 요소로 자리매김 되었다. 본 고에서는 네트워크에 참여하는 다양한 기기의 안전한 운영을 위하여 해당 기기를 식별하고 진위를 판단할 수 있는 신뢰된 인증방법에 대한 현황을 소개한다.

Ⅰ. 서 론

정보통신기술(ICT: Information and Communication Technologies)이 발달함에 따라, 사람뿐만 아니라 홈 네트워크 기기, 휴대 통신단말기, 의료기기 등 다양한 기기가 정보제공의 주체로 등장하고, 이러한 추세는 지속적으로 확대될 것으로 예상된다. 이와 같은 기기의 이용 증가와 더불어 이들에 대한 정보보호의 중요성도 증대되고 있다. 이에 따라 네트워크에 참여하는 기기에 대한 신뢰된 식별 및 인증체계의 필요성이 부각되고 있다.

예를 들어, 스마트그리드, 스마트워크 등에 참여하는 기기에 대한 진위성 확인 및 인증이 이루어지지 않아 비인가된 기기를 통해 서비스가 제공될 경우, 불법적인 접근 및 정보 유출, 서비스 방해 등 관련 서비스의 신뢰성에 직접적인 위협 및 피해를 유발할 수 있다. 이러한 위협 및 피해에 대응하고 네트워크에 접속하는 기기의 진위성 및 네트워크 접속 권한을 확인하기 위해 기기인증서비스의 이용이 요구되고 있으며, 케이블TV, 셋탑박스, 휴대 통신단말기 등에 기기인증을 이용하는 사례가 점진적으로 증가하고 있는 추세이다.

최근 스마트그리드 및 인터넷전화기 도입 등 국가정보화 사업 등을 통해 다양한 기기가 도입되고, 비인가된 기기에 대한 인증 문제가 대두되면서 국내에서도 기기에 대한 인증의 필요성 및 표준화 수요가 증가하고 있다.

이에 본고에서는 기기인증 기술, 이용분야, 관련 표준화 동향 등에 대해 알아본다.

Ⅱ. 기기인증의 필요성

정보통신기술이 발전함에 따라, 사람과 사람을 대상으로 하던 인증기술의 적용범위가 기기와 기기, 기기와 사람으로 확대되었다. 이러한 기기간의 식별 · 인증 등이 안전하고 신뢰성 있게 이루어지기 위해 보안이 강화된 기기인증 기술이 필요하게 되었다.

표 1. 비인가된 기기로 인한 보안위협

환경	기기	위협
공공	인터넷 전화기	• 통화내용의 도청 • 불법 전화사용에 따른 과도한 벌금
	CCTV	• 데이터 위 · 변조
	RFID/USN	• 데이터 위 · 변조 • 수집정보의 유출 • 서비스 방해
개인 · 가전	디지털 셋탑박스	• 인증 우회를 통한 불법시청 • 과도한 과금 • 개인정보의 유출
	스마트 미터기	• 전력량 이용패턴 등 개인정보 유출 • 비인가 기기 접근에 따른 불법 과금
의료	의료기기	• 의료기기에 대한 데이터 위 · 변조 • 의료기기의 오작동

〈표 1〉과 같이 기기에 대한 식별 · 인증이 이루어지지 않아 비인가된 기기를 통해 서비스에 접근이 가능한 경우, 이들 비인가

된 기기에 의한 잘못된 정보의 전달, 비인가된 휴대단말기 이용에 따른 과도한 요금의 부과, 의료기기의 비인가된 이용에 따른 인간 생명에 치명적인 위협을 초래할 수도 있다.

이러한 기기인증의 중요성에도 불구하고 이를 위한 기술 및 인식 부재 등으로 사물인터넷(IoT: Internet of Things) 환경에서의 관련 서비스가 미흡한 실정이다.

Ⅲ. 기기인증 방법 간의 비교 · 분석

현행 기기에 대한 식별 · 인증을 수행하는 방식으로는 아이디/비밀번호 인증 방식, 암호 프로토콜을 활용한 인증 방식, 공개키 암호화 기술 기반 인증 방식으로 나눌 수 있다. 본 장에서는 각각의 기술을 설명한 후, 장/단점을 비교 · 분석한다.

1. 아이디/비밀번호 인증 방식

아이디/비밀번호 방식은 기기간 혹은 기기-서버간 통신에서 기기는 서버 혹은 다른 기기에 자신의 아이디, 비밀번호를 제공하는 방식이다. 아이디/비밀번호 인증 방식은 다시 2가지로 나눌 수 있다. 기기 고유값을 이용하는 방식과 기기 고유값을 이용하지 않는 방식으로 나눌 수 있다.

1.1 기기 고유값을 이용하는 방식

기기 고유값을 이용하는 방식은 아이디를 MAC(Media Access Control) 주소나 전자식 고유번호(ESN: Electronic Serial Number) 혹은 디바이스 내부 하드웨어 제작 시 들어있는 값을 이용하여 연관시킨다. 비인가된 기기에서 정상 기기의 고유값을 사용하더라 할지라도 특수 하드웨어를 제작하거나 MAC 주소가 달라져 통신을 할 수 없게 되는 등 보안위협에 안전하다고 할 수 있다.

1.2 기기 고유값을 사용하지 않는 방식

기기 고유값을 사용하지 않는 방식은 일반적으로 사용자를 인증하는 방식과 동일하게 아이디, 비밀번호 값만을 이용하는 방식이다. 이러한 인증 방식의 장점은 기존 소프트웨어나 라이브러리를 기기에 그대로 적용할 수 있고 관리가 매우 쉽다는 장점이 있다. 하지만, 아이디 값이 기기 고유값과 연동되지 않는 이러한 방식은 보안에 좀 더 취약하다고 판단되는데, 그 이유는 일반 사용자들이 이용하는 경우에는 아이디/비밀번호가 해킹당했다고 의심되는 경우 손쉽게 아이디/비밀번호를 바꿀 수 있지만, 기기의 경우는 장치의 개수가 너무 많고 개별 장치에 대한 아이디/비밀번호의 해킹여부를 판단하기에는 관리적 측면에서 무리가 있다.

기기 내 고유값을 이용하는 방식은 아이디/비밀번호 방식의 아이디만을 이용하는 방식으로 해석할 수 있으며, 아이디/비밀번호 방식과 비교해보면, 기기 내 고유값을 이용하는 방식은 비밀번호를 사용하지 않기 때문에 반드시 아이디에 해당하는 고유값이 기기의 하드웨어와 연동되어 있어야 안전하다. 즉, 기기가 이더넷을 사용하는 경우 이더넷 인터페이스 카드의 MAC 주소라던가, 휴대폰의 경우 ESN 번호 등과 같이, 기기 고유 장치 혹은 기기의 통신에 필수불가결한 요소와 연관하여 사용하여, 해커나 제3자가 장치를 도용하여 고유값을 탈취한다 할지라도 이를 활용하기 힘들게끔 하여야 한다.

2. 암호 프로토콜을 활용한 인증 방식

기기인증 관련 표준으로는 AAA(Authentication, Authorization, Accounting) 표준과 EAP(Extensible Authentication Protocol) 표준이 있다. AAA 표준은 EAP인증방식을 사용한다. EAP(RFC 2284 and 3748)는 다양한 인증 수단을 복합적으로 사용할 수 있는 인증 프로토콜 프레임워크이다. 즉, EAP 자체로는 인증 프로토콜을 지정하지 않고, 단지 그러한 인증 프로토콜을 사용하기 위한 인프라를 제공할 뿐이다. EAP 방식으로 실제 구현된 인증 방식에는 EAP-TLS, EAP-TTLS, EAP-MD5, EAP-PSK, EAP-IKEv2, PEAP, LEAP, EAP-FAST, EAP-SIM 등이 있다.

위에 열거한 표준 중 EAP-PSK, EAP-MD5, LEAP는 비밀번호 기반 인증 방식을 택하고 있어 아이디/비밀번호 방식과 안전도가 유사하다고 할 수 있으며, EAP-TLS, EAP-TTLS, PEAP 등은 PKI 인증서를 기반으로 하고 있어 인증서 방식과 안전도가 유사하다고 할 수 있다.

3. 공개키 암호화 기술 기반 인증 방식

공개키 암호화 기술(PKI: Public Key Infrastructure) 기반 인증 방식은 현재 기기인증으로 널리 사용되고 있다. PKI 기반 인증 방식의 장점으로는 인증을 확인하는 주체가 상대방 기기가 적법한 기기인지를 판단하기 위하여 대규모 패스워드 데이터베이스나 MAC 주소 데이터베이스 혹은 하드웨어 아이디 데이터베이스 등을 관리할 필요가 없다는 점이다. 기기인증과 사용자 인증이 다른 점은 디바이스 고유의 아이디 및 특성이 기기 인증서 내부에 들어간다는 점이다.

이에, 일반 사용자가 이용하는 인증서를 기기인증에 직접 적용하기에는 무리가 있어, 기기인증 적용 인증서 포맷에 관한 표

준이 제정되고 있다.

PKI 인증서를 이용한 기기인증의 문제점 중 하나는 기기가 인증서와 개인키를 어떻게 관리하는가 하는 문제가 있다. 인증서는 공개키를 서명한 문서이므로 외부에 노출되어도 보안상 문제가 없지만, 이에 관련된 개인키는 누출되면 심각한 위험이 생길 수 있다. 기기(전자기기, 로봇, 홈 디바이스 등)는 일반 사용자와 달리 제3의 해커에게 물리적으로 노출되어 내부 정보가 유출될 위험이 훨씬 많으므로 개인키가 노출되는 것을 물리적으로 막을 수 있는 방안이 절실하다.

이에 셋탑박스나 케이블모뎀 등의 기기에서는 별도의 안전한 기기메모리나 스마트카드 등을 이용하여 기기가 물리적으로 탈취된다 할지라도 해커가 내부의 개인키를 탈취할 수 없도록 하는 하드웨어 기반 안전장치를 구비하고 있다.

〈표 2〉는 방송통신, 임베디드, RFID 등에서 이용되는 기기인

표 2 기기인증 비교 분석

기술 요소	세부 기술요소	방송통신 기기인증			Embedded 기기인증			RFID	
		케이블 모뎀	셋탑 박스	CMLA	WiMAX	CCTV	URC 로봇	태그/ 리더	리더/ 서버
인증 암호 기반 기술	전자서명키 길이	1024	1024	1024	1024, 2048	1024	1024	768	1024
	경량화	O	X	X	X	X	X	O	X
	서명 알고리즘	SHA-1 with RSA	SHA-1 with RSA	SHA-1 with RSA	SHA-1 with RSA	MD5 with RSA	SHA-1 with RSA	SHA-1 with RSA	SHA-1 with RSA
인증서 발급 기술	인증서 프로파일	O	O	O	O	X	X	X	O
	인증서 저장공간	기기메모리, 스마트카드	기기메모리, 스마트카드	기기메모리	기기메모리, 스마트카드	기기메모리	기기메모리	태그메모리	리더메모리
	컴퓨팅 파워	임베디드 (CM)	임베디드 (SB)	임베디드 (DVD-R)	임베디드 (이동단말기)	임베디드 (CCTV)	임베디드 (로봇단말)	X (passive)	임베디드 (RFID리더기)
	전자서명키 생성	제조사	제조사	제조사	제조사	제조사	제조사	제조사	제조사
	인증서 생성	Kablelab CA, 제조사CA	Kablelab CA, 제조사CA	제조사 device CA	제조사 CA, Device sub-CA	제조사 CA, CCTV	제조사 CA	제조사 CA	제조사 CA
	유효기간	30년	30년	20년	7년	1년	10년	1년	10년
인증서 관리 기술	비밀번호 적용	X	X	X	X	X	X	X	X
	비밀번호 암호화	X	X	X	X	X	X	X	X
	인증서 자동갱신	X	X	X	X	X	X	X	X
	CA	Kablelab(TTP), 제조사 CA	Kablelab(TTP), 제조사 CA	CMLA Root CA, Device CA	Device root CA, 제조사 CA, Device sub-CA	제조사 CA	제조사 CA	제조사 CA	제조사 CA
인증 수단 활용 기술	전자서명 생성	O	O	O	O	O	O	O	O
	전자서명 목적	CM인증, 컨텐츠보호	SB인증, 소프트웨어 다운로드	DVD-R인증	이동단말기 인증, 키교환	CCTV 인증, 키교환	로봇단말인증, 키교환	태그인증 (의약품)	RFID리더기 인증, 키교환
	운영 프로토콜	SATP	BPKM	ROAP	WiMAX	SSL	SSL	–	SSL
	인증서 검증	CRL	CRL, OCSP	CRL, OCSP	CRL	X	X	X	CRL, OCSP
	데이터 암호화	O	O	O	O	O	O	X	O
	암호화 대상	기기인증정보, 컨텐츠보호	기기인증정보, 소프트웨어	기기인증정보, 컨텐츠보호	기기인증정보, 키교환	기기인증정보, 키교환	기기인증정보, 키교환	X	기기인증정보, 키교환
	기기인증	O	O	O	O	O	O	O	O

증 기술에 대한 세부 기술요소를 분석하였다.

Ⅳ. 기기인증 기술 관련 국내 · 외 동향

1. 국내 동향

모바일 기기가 현대인의 필수품으로 자리 잡으면서 개인의 신분을 대표하는 수단으로 사용되고 있다. 하지만 모바일 기기 자체에 인증 기능이 있는 것이 아니라 사용자가 입력하는 정보에 따라 인증이 이루어진다. 현재 모바일 기기의 USIM(Universal Subscriber Identity Module)에 공인인증서를 저장하는 방식을 대상으로 PKCS#11(Cryptographic Token interface Standard), PKCS#15(Cryptographic Token Information Format Standard), SCWS(Smartcard Webserver) 기술이 고려되고 있다. 대용량 USIM 등장함에 따라 HTTP 통신에 기반을 둔 SCWS 인증 기술에 대한 표준도 함께 연구 중이다. SCWS 기술은 웹 서버 기능을 USIM에 구현하여, HTTP 프로토콜을 지원하는 단말의 브라우저를 통해 USIM 서비스에 접근하는 방식이다.

한국 디지털케이블연구원(KLabs)에서는 국내 케이블 분야 최상위 인증기관의 역할을 수행하며 미국의 CableLabs와 업무협력으로 PKI 기기 인증서를 발급하고 있다.

한국정보인증은 KLabs의 위탁인증기관으로 셋탑박스와 케이블카드를 연결할 때 기기인증을 위한 PKI 기반 기기 인증서를 발급하고 있다.

홈 네트워크 환경의 국내 인증 표준화는 2004년부터 시작되었고 한국정보통신기술협회(TTA: Telecommunication Technology Association)의 정보보호기반 프로젝트 그룹과 홈 네트워크 시큐리티 포럼을 중심으로 이루어졌다. ITU-T에서 홈 네트워크 환경 표준안이 채택됨에 따라 국내에서도 홈 서버 중심의 홈 네트워크 사용자 인증 메커니즘, 홈 네트워크를 위한 보안기술 프레임워크, 홈 네트워크 등에 적용 가능한 디바이스 인증서 프로파일이 표준안으로 채택되었다.

802.1X EAP 기반 인증은 강력한 무선랜 보안 방식으로 떠오르면서 전문 솔루션들이 시장에 많이 출시되고 있으며, 무선랜을 도입할 때 인증 솔루션을 함께 구축하려는 기업도 늘어나고 있다. 기존의 인증 솔루션들은 무선랜 보안을 위하여 설계된 솔루션들이지만, 무선랜 망에 허가 받지 않은 무선 기기들의 접근을 차단 및 탐지하는 것이 주목적이므로, 이러한 인증 솔루션들 또한 기기인증의 한 부분이라고 말할 수 있다. 국내에서 개발된 대표적인 솔루션들을 살펴보면 다음과 같다. 대표적인 국산 솔루션 중의 하나인 유넷시스템의 "애니클릭 AUS"는 Wi-Fi WPA/WPA2, IEEE 802.11i/802.1X, 국가보안기술연구소 무선랜 보호 프로파일 등 국내 · 외 대표 무선 네트워크 보안 표준을 준용하여 개발된 표준 무선 네트워크 보안솔루션이며, 에어큐브의 "AGS-NPS v4.5"은 무선랜 접근 인증, 무선 구간의 데이터 암호화 강화를 지원하는 솔루션으로 EAP-MD5, EAP-TLS, EAP-TTLS, LEAP, PEAR 등 다양한 EAP 유형과 WPA2을 지원한다.

그밖에 다른 기기 인증에 대한 구체적인 표준안이 아직까지 제시된 것은 없으나, 한국정보통신기술협회에서 기기인증 관련 표준화가 진행될 것으로 예상된다.

2. 국외 동향

2009년 9월 미국에서 Ponemon 협회는 Traverse City에서 소비자들에게 설문 조사를 실시하였다. 설문 조사의 내용은 온라인상에서 소비자가 사용자 인증을 하기 위해서 사용자 이름과 패스워드를 입력하는 것에 대한 불편함을 대체하기 위해 각 개개인의 기기가 대신 인증하는 것에 대한 선호도 조사였다. 그 결과 551명의 설문자 중 70%는 온라인상에서 물건을 구입하기 전에 온라인 상인에 의해 그들의 컴퓨터가 인증되는 것에 대해 찬성하였으며, 그들 중의 75%는 패스워드를 기억하거나 이미 선택된 질문에 대답하는 것보다 컴퓨터 인증 즉 기기 인증을 더 선호하였다. 이에 더하여 기기 인증이 패스워드 인증보다 선호되는 이유가 더 있다.

2007년 Microsoft사의 패스워드 연구에 의하면, 각 사용자당 평균 6.5개의 웹을 위한 패스워드를 가지고 있으며, 각 패스워드는 대략 4개의 웹 사이트에 의해 공유되고 있다. 또한 그 연구는 각 사용자는 패스워드를 요구하는 25개의 계정을 가지고 있으며, 하루 평균 약 8개의 패스워드를 입력한다고 밝혔다. 패스워드에 대한 공유는 자칫 하나의 패스워드 유출로 각 사용자가 사용하는 다수의 계정에 대한 개인 정보가 노출될 수 있는 결과로 이어지므로 소홀한 패스워드 관리는 커다란 보안 위협을 초래할 수 있다. 하지만, 비록 이러한 패스워드 관리의 중요성을 사용자가 인지하고 있다 하더라도 개개인이 기억할 수 있는 패스워드의 수는 한정되어 있기 때문에, 사용하는 패스워드의 수는 제한되어 있다. 결국 각 사용자가 소유하고 있는 계정이 많으면 많을수록 계정들 사이에서 공유하는 패스워드의 수는 증가한다. 따라서 기존의 패스워드 인증이 아닌 기기 인증을 도입하게 되면 사용자는 패스워드를 공유하여 사용할 필요가 없어지게 된다. 이와 같이 기기 인증은 사용자의 편리성과 안정성을 증대한다는 장점 아래 점차 사용자들에 의해 사용자 인증

보다 선호되는 추세이다.

Todos사의 Todos A200은 강력한 기능을 가진 스마트카드 리더기로 케이블 연결 없이 e-banking 시스템과의 강력한 인증을 제공한다. 리더기는 은행으로부터 카드의 바코드를 웹브라우저를 통해 전송 받아 스마트카드를 인증하고, 기기 안의 작은 센서들은 A200을 검증하는 세부항목에 대해 해독한다. Todos A200은 이러한 정교한 시스템으로 중간자공격(MITM: Man-In-The-Middle) 공격과 같은 보안위협을 막을 수 있다.

Accumulate사는 Mobile Everywhere 기술을 개발하였다. 이 기술은 적은 비용으로 효과적인 인증, 확인, 서명이 가능한 보안을 제공한다. Accumulate사는 사용자의 모바일단말로 하드웨어 인증토큰이나 인증서를 이용하여 사용자 인증 및 서명을 수행하는 기술을 적용하였다.

모바일 환경에서의 인증서비스를 살펴보면 유럽의 이동통신사에서 대용량인 1GB USIM이 개발되었고, 지속적인 연구에 따라 USIM의 가격은 내려가며 용량은 더 커질 것으로 보인다.

또한 SUN사에서 USIM에서 구동되는 JavaCard 3.0을 개발하여 다양한 어플리케이션 사용이 가능하다. 즉, 국외에서는 대용량 USIM을 기반으로 한 인프라가 이미 구축된 상태로 USIM 분야 개발이 확장되고 있다. SCWS 표준은 OMA와 ETSI SCP에서 진행하고 있고, SCWS와 단말 또는 서버 등과의 통신 프로토콜 및 HTTP 프로파일링, USIM 내부기능을 구현하기 위한 API 표준이 제정되었다. 이와 별도로 폰에서 사용할 수 있는 인터페이스인 PKCS#11은 RSA Laboratories에서 현재 ISO/IEC 7816-15로 표준화가 된 상태이다.

미국 Verisign사에서는 PKI 인증서를 이용한 기기인증을 케이블모뎀에 적용하였다. 기기 인증서는 케이블모뎀과 케이블 모뎀 터미네이션 시스템과의 인증을 검증하는데 사용된다. 기기 인증서는 케이블모뎀 비활성 메모리 내에 저장되며, 케이블모뎀 인증을 위한 기기 인증서에 관련된 규격은 케이블 모뎀 업계표준 DOCSIS(Data Over Cable Service Interface Specification)을 따른다.

Phoenix사에서는 TrustConnector제품을 출시하였다. 이 제품은 공개키 암호화 기술을 이용해 기기인증을 제공하며, 아이디와 비밀번호가 타인에게 유출되더라도 승인되지 않은 하드웨어는 네트워크에 접속할 수 없도록 차단하는 엔드포인트 보안을 지원한다. 인증기관은 Verisign 이나 Entrust와 같은 외부 인증기관을 사용할 수 있고, Microsoft사의 Standalone CA나 Enterprise CA와 같은 내부 인증기관을 사용할 수도 있다.

그 밖에 방송신호를 수신하여 디스플레이 매체를 통해 볼 수 있도록 신호를 변환하는 장치인 셋탑박스, WiMAX규격의 가입자 단말기(노트북, 휴대폰) 같은 종류의 하드웨어에도 기기 내에 X.509 인증서를 저장하여 인증서비스를 제공하고 있다.

CCTV 업체인 액시스, 소니 등은 PKI 기기 인증서 기반의 기기 인증을 네트워크 카메라에 적용하였다. 기기 인증서를 통하여 카메라에 대한 인증을 하고, 화상정보에 대한 전자서명을 전송하여 정보의 위·변조여부를 확인한다. 기기 인증서는 IEEE 802.v1의 RADIUS(Remote Authentication Dial In User Service) 프로토콜을 따른다. 또한 CCTV와 서버 간 상호 인증을 위하여 HTTPS 기반 보안 프로토콜을 이용한다. 그리고 Cisco의 "Cisco Video Surveillance 2500 Series IP Camera"는 WPA/WPA2를 사용하여 강력함 무선 보안을 제공하며, 802.1x 인증을 위한 다양한 네트워크 프로토콜을 지원한다.

홈 네트워크 환경에서의 기기 인증에 대한 표준은 2005년 ISO에서 댁내 및 댁외 보안에 대한 표준이 지정되었다. 이 표준은 총 3가지로 보안 요구사항, 내부 보안서비스, 외부 보안서비스로 이루어져 있다. 또한 외부공격에 대한 기기의 안전성 확보를 위하여 SCPM(Secure Communication Protocol to Middle-ware)을 적용하여 보안을 향상시켰다. ITU-T SG17 Question9도 2004년부터 표준화가 진행되었다. X-homesec-1,2,3,4 총 4개의 표준이 이루어졌으며 각각 홈 네트워크 보안 기술의 프레임워크, 홈 네트워크용 디바이스 인증서 프로파일, 홈 네트워크 사용자 인증 메커니즘, 홈 네트워크 인가프레임워크에 대하여 정의되어 있다.

CMLA(Content Management Licensing Administrator)는 인텔, 노키아, 파나소닉, 삼성 4개의 회사가 모여 만든 표준화 단체로 안전한 콘텐츠 배포를 위한 OMA DRM 2.0 규격의 표준을 제시하였다. OMA DRM 2.0에서는 PKI 기반 종단간 프로토콜(end-to-end protocol)을 정의하고, 이를 위한 인증서 프로파일 및 인증서 폐지 목록에 대한 규격을 정의하고 있다. OMA DRM 호환 제품의 인증 및 라이센스 관리를 정의한 이 표준에서는 기기가 전송받은 컨텐츠를 재생할 때 기기 내 저장된 CMLA의 PKI기기 인증서를 사용하여 저작권 발급자(Right issuer)로부터 기기의 공개키로 암호화된 RO(Right Object)를 전송받아 암호화된 컨텐츠의 키를 추출한다. 만약 올바른 인증서를 가지고 있다면 컨텐츠를 재생할 수 있게 된다.

EPCglobal은 RFID 표준 개발과 보급을 위해 GS1(Global Standard 1)이 설립한 국제 표준기구이고, 전 세계 모든 상품을 자동으로 식별, 추적할 수 있는 글로벌 네트워크 구축을 목표로 표준화하고 있다. EPCglobal Network에는 각각의 시스템마다 인터페이스가 정의 되어있으며, 인증, 검증, 접근제어와 같은 암호화 기법을 제공하고 있다. EPCI표준(EPC Information Service)간 서비스 요청 시 인증서를 사용하여 인증이 이루어진다. 인증은 EPCI표준인터페이스를 통해서 전송

되어야 하며, RFID 리더 데이터를 주고받을 때 반드시 안전한 미들웨어나 리더기 관리 시스템을 통해야 한다. 여기에서 사용되는 기기 인증서는 X.509 인증 방식과 기존 RFC32ic의 인증서 폐지목록을 따른다.

V. 결 론

기기인증에서 기본적인 아이디/비밀번호 인증 방식은 각 기기가 아이디와 비밀번호를 할당 받고, 할당 받은 아이디와 비밀번호를 기기가 서비스를 받고자 하는 서버(또는 게이트웨이)에게 전송하여 인증을 받는 방식이다. 물론 이러한 방식은 기기 측에서는 아이디와 비밀번호만 저장하면 되고, 기기에게 서비스를 제공하는 서버 입장에서는 각 기기별로 아이디와 비밀번호만을 관리하면 되기 때문에 관리도 쉬울뿐더러, 서버에서 요구하는 자원도 크지 않다. 하지만 문제는 단순히 아이디와 비밀번호 인증만으로 서버가 서비스를 제공할 경우, 서버에 등록되지 않은 기기는 서비스를 받기 전에 무조건 서버에 등록해야 하는 불편함이 존재한다. 더군다나 사용자가 받고자 하는 서비스의 양은 점점 많아지고 있다. 이러한 서비스 다양화 추세에서 각각의 사용자가 사용하는 다수의 기기가 여러 서버로부터 서비스를 받고자 할 때, 각각의 사용자의 기기들은 서비스를 받기 위하여 여러 서버에 이미 등록되어 있어야 한다. 비록 여러 서버가 하나의 기기인증 서버를 설치하여 사용한다 하더라도 기기인증 서버는 기기 접근에 대한 과부하로 제 성능을 발휘하지 못할 것이다. 그리고 이에 더하여 아이디/비밀번호 인증 방식은 부인 방지 기능을 제공하지 못한다. 부인 방지 기능은 유료 서비스를 제공하는 모델에서 필수적으로 요구되는 보안 요구사항 중의 하나이다. 기기가 서버로부터 유료 서비스를 받았음에도 불구하고, 돈을 지불하지 않기 위해 서비스를 받지 않았다고 주장할 때, 이를 거부할 수 있는 증거가 아이디/비밀번호 인증 방식에는 존재하지 않는다. 이러한 문제점은 MAC 주소 인증 기술에도 나타난다. 비록 인증 절차가 아이디/비밀번호 인증 방식보다 비교적 간단하고 빠르지만 MAC 주소 위조가 어렵지 않음은 이미 알려진 사실이다. 게다가 서비스를 제공받는 기기가 추가될 때 마다 기기인증을 위해 개별적으로 MAC 주소를 서버에 등록해야 하는 불편함이 존재한다. 이와 더불어 MAC 주소 인증 방식 역시 아이디/비밀번호 인증 방식처럼 부인방지 기능을 제공하지 못한다. 따라서 아이디/비밀번호 인증 방식과 MAC 주소 인증 방식은 기기인증 방식에 적합하지 않다. 반면 PKI 기반 기기 인증서 인증 방식은 위 문제점들을 해결할 수 있다. PKI 기반 기기 인증서의 가정은 각 기기가 이미 공인된 인증서를 분배 받았다는 하에 시작된다. 각 기기들은 공인된 인증서를 바탕으로 자신들의 적법성을 서비스를 제공받고자 하는 서버로부터 식별 받을 수 있다. 서버는 기기 인증서가 공인된 기관으로 발급받은 것임을 기기 인증서의 서명을 통해 확인하고, 기기가 기기 인증서의 공개키에 속하는 개인키를 가지고 있는 것을 확인함으로써 기기를 적법하게 식별할 수 있다. 즉, 기기 식별을 위한 서버를 따로 설치할 필요가 없다는 것이다. 물론 인증서 폐기 목록 관리를 위한 별도의 서버는 필요하겠지만, 이는 기존의 OSCP를 고용함으로써 해결할 수 있다. 더군다나 PKI 기반 기기 인증서 방식은 앞서 언급한 부인방지 기능을 제공한다. 각 기기는 유료 서비스를 서버로부터 제공받을 때마다 기기의 개인키로 서명된 값을 서버에게 전달함으로써, 차후에 발생할 수 있는 서비스료 지급 거부를 사전에 예방하거나 사후에 이에 대한 증거자료로 활용할 수 있다. 위와 같은 이유로 기기 인증 방식에 가장 적합한 인증 기술은 PKI 기반 기기 인증서 인증 방식이 될 것이다. 단, 기기는 전자 서명을 생성하고 검증할 수 있을 정도의 연산 장치를 지니고 있어야 할 것이다.

참 고 문 헌

[1] 이상원 외 2명, “인증서 기반의 정보통신 기기인증서비스 표준화 추진전략”, 제6회 정보통신표준화우수논문집, pp. 60-75.(http://www.tta.or.kr).

[2] 루멘소프트, “정보통신기기 대상 기기인증서비스 적용방안”, 한국인터넷진흥원, pp. 1-161.(http://www.kisa.or.kr).

[3] 루멘소프트, “기기인증서 기반 서비스 구축 및 운영 가이드라인”, 한국인터넷진흥원, pp. 1-37.(http://www.kisa.or.kr).

[4] 한국정보통신기술협회, “개체 인증에 대한 보증 프레임워크”, 정보통신단체표준, pp. 1-51.(http://committee.tta.or.kr).

[5] 경원대학교, “유비쿼터스 환경에 적합한 인증체계 구축을 위한 법 · 제도 연구”, 한국정보보호진흥원, pp. 1-130.(http://www.kisa.or.kr).

[6] 김수진 외 1명, “사용자 아이디와 패스워드 기반의 휴대인터넷(와이브로) 상호 인증 방법”, IT Standard & Certification, pp. 68-70.(http://www.tta.or.kr).

[7] 한국정보통신기술협회, “TTAS.KO-12.0012/R1, 전자서명 인증서 프로파일 표준”, 한국정보통신기술협회, pp. 1-28.(http://www.tta.or.kr).

[8] 한국정보통신기술협회, "TTAS.KO-12.0001/R1, 부가형 전자서명 방식 표준 2부 : 인증서 기반 전자서명 알고리즘", 한국정보통신기술협회, pp. 1-58.(http://www.tta.or.kr).
[9] Jari Arkko et al., "Weak Authentication How to Authenticate Unknown Principals without Trusted Parties", Lecture Notes in Computer Science, pp. 5-19.(http://link.springer.com).
[10] CableLabs, "CableLabs Certificate Issuance Pricess", CableLabs, pp. 1-8.(http://www.cablelabs.com).

약 력

박 정 효

2009년 숭실대학교 공학사
2011년 숭실대학교 공학석사
2013년 숭실대학교 공학박사 수료
2012년~현재 한국인터넷진흥원 전자인증팀 선임연구원
관심분야: 익명 인증, 다중 인증, 암호 이론