JKIICE Journal of the Korea Institute of Information and Communication Engineering

한국정보통신학회논문지(J. Korea Inst. Inf. Commun. Eng.) Vol. 18, No. 1 : 169~176 Jan. 2014

N-스크린서비스 환경에서 웹콘텐츠 이동/결합/분리를 고려한 보안 기술 분석 및 협업 서비스 프레임워크 개발

이호원*

Research on Technical Requirements of Security for Migration, Combination, and Separation of Web-Contents and Development of Cooperation Service Framework in N-Screen Services

Howon Lee*

Department of Electrical, Electronic and Control Engineering & IITC, Hankyong National University, Anseong 456-749, Korea

요 약

스마트 디바이스의 수가 급증함에 따라 다양한 스크린들 간의 협업을 통하여 사용자들에게 새로운 사용자 경험(User Experience)을 제공할 수 있는 N-스크린서비스에 대한 수요가 급증하고 있으며, 이는 사용자들에게 기술적 풍요를 제공하는 동시에 새로운 보안상의 약점을 유발하게 되었다. 본 논문은 기존의 다양한 웹 공격유형에 대하여 분석하고, 미래 N-스크린서비스 시나리오들을 기반으로 웹콘텐츠의 이동/결합/분리를 위한 새로운 보안 요구사항을 제안하고 이를 구체적으로 정리하고 분석해 본다. 또한, N스크린 환경에서 웹콘텐츠의 이동을 통하여 사용자의 개인 정보가 공공 디바이스를 통해 외부로 공개되는 것을 방지할 수 있는 방안이 적용된 N스크린 협업서비스 프레임워크에 대해서 살펴본다.

ABSTRACT

According to explosion of smart-devices, demands on N-screen services based on cooperation of multiple screens are rapidly increasing. These N-screen services can provide new user-experience (UX) to users. That is, it can provide technical advances to users. On the other hand, it causes new security problems. In this paper, we analyze conventional web-security attacks, and we propose and analyze new security requirements for migration, combination, and separation of web-contents based on N-screen service scenarios. Also, we develop N-screen cooperation service framework in order to ensure user security.

키워드 : N-스크린서비스, 웹콘텐츠, 보안 기술, 서비스 프레임워크

Key Words : N-Screen Service, Web Content, Security Requirement, Service Framework

접수일자 : 2013. 07. 06 심사완료일자 : 2013. 12. 17 게재확정일자 : 2013. 12. 30

* **Corresponding Author** Howon Lee (E-mail:hwlee@hknu.ac.kr, Tel:+82-31-670-5198)
Department of Electrical, Electronic and Control Engineering & IITC, Hankyong National University, Anseong 456-749, Korea

Open Access http://dx.doi.org/10.6109/jkiice.2014.18.1.169 print ISSN: 2234-4772 online ISSN: 2288-4165

Ⅰ. 서 론

최근 스마트 디바이스의 수가 급증함에 따라 사용자들은 자신이 보유한 콘텐츠를 여러 디바이스를 통해서 동시에 끊김없이 재생하거나 디바이스-협력적 콘텐츠 재생을 통한 사용자 경험(User Experience)의 극대화를 위한 요구가 늘어나고 있다. 일반적으로 N-스크린서비스란 개인이 가지고 있거나 혹은 개인 주변에 있는 다양한 스크린들(스마트 TV, 스마트폰, 데스크톱 PC, 스마트패드, 게임기 등)을 통해 콘텐츠를 끊김없고(seamless) 실감나게(real) 재생할 수 있는 서비스를 말한다[1-3].

예를 들면, 옥외에서 자신의 스마트패드로 보고 있던 동영상이 실내로 이동할 경우 거실의 스마트 TV와 홈 오디오 시스템을 통해 재생되고 있던 시간 이후부터 연속적으로 재생되는 서비스를 의미한다. N-스크린서비스는 다양한 스크린들 간의 협업을 통해 사용자들에게 새로운 사용자 경험을 제공하며, 사용자들에게 끊김없는 서비스를 제공하는 동시에 시간과 공간의 제약을 넘어서 자유로운 콘텐츠 공유 및 이용을 가능하게 한다[4-5]. N-스크린서비스는 스마트교육, 스마트워크, 디지털 사이니지, 스마트의료 등 다양한 IT융합 산업에 활용될 수 있는 핵심 서비스 기술이다.

새로운 기술의 등장으로 인한 체계의 변화는 필연적으로 이에 따른 새로운 보안상의 약점 노출을 유발하게 된다. 특히, 다양한 접속방식 및 범용성을 가지는 웹 기술의 경우 이러한 약점을 노출할 가능성이 높은 편이다. 안정적인 웹서비스를 위해서는 사용자의 서비스 이용에 대한 기밀성(Confidentiality), 무결성(Integrity), 그리고 가용성(Availability)이 보장되어야만 한다[6]. 따라서 새로운 웹 기반 서비스를 제공하기에 앞서, 서비스의 기능성 및 보안성, 그리고 기술 개발 시 고려해야 할 사항에 대한 철저한 분석이 필요하다[7-8].

본 논문의 II장에서는 기존의 웹 기반 공격방식에 대해서 조사하고, III장에서는 이동형 웹 콤포넌트를 고려한 보안 대비방안에 대하여 알아보도록 한다. IV장에서는 N-스크린서비스 시나리오들에 대한 각각의 보안 요구사항에 대하여 분석하고 제안하며, V장에서는 보안기술이 적용된 N스크린 협업서비스 프레임워크에 대해 알아본다. VI장에서 본 논문을 마무리한다.

Ⅱ. 기존연구조사: 웹기반 공격방식조사

본 장에서는 다양한 웹기반 공격방식에 대해 살펴보고 각각을 위한 대비방법에 대하여도 간략히 알아보도록 한다[9-10].

1) Cross-Site Scripting (XSS): 클라이언트 측 공격으로, 동적 페이지에 스크립트를 삽입하여 공격하는 방법이다. 요즘의 웹 사이트들은 Flash, IMG 등의 동적인 페이지를 제공하므로 XSS에 취약하다. XSS는 바이러스로 변하면 심각한 문제를 일으킬 수 있다.

2) Redirection Attacks: 사용자의 브라우저로 하여금 요청된 URL (Uniform Resource Locator)과 다른 URL로 방문하도록 지시하는 것을 redirection이라고 한다. Redirection 공격의 취약성은 어플리케이션이 사용자가 조작 가능한 입력을 취하고, 이를 redirection 수행에 사용할 때 발생한다.

3) HTTP Header Injection: HTTP의 헤더에 데이터를 삽입하는 방법이다. HTTP Header Injection의 취약성은 사용자가 직접 조작 가능한 데이터가 어플리케이션에 의해 반환되는 HTTP 헤더에 불안전한 방법으로 삽입될 때 발생한다. Location과 Set-Cookie 헤더에서 흔히 취약성이 발견된다.

4) Frame Injection: Frame Injection이란 말 그대로 프레임에 어떤 데이터나 내용을 쓰는 것이다. Frame injection의 취약성은 주로 웹 사이트가 이름 속성을 가진 프레임을 생성할 때 발견된다. 프레임에는 이름 속성이 있으며, 이를 익명 혹은 특정한 이름으로 설정할 수 있다.

5) Cross-Site Request Forgery (XSRF): XSRF란 사용자가 자신의 의지와는 무관하게, 공격자가 의도한 행위(수정, 삭제 등)를 특정 웹사이트에 요청하게 되는 공격 방식이다. 공격자가 작성해 놓은 악성 코드를 통해 일어나는 공격이며, stored XSS와 유사하다. 하지만, XSRF는 인증 완료된 사용자의 권한으로 악성 스크립트를 서버에 요청한다는 면에서 XSS와는 다르다.

6) JSON Hijacking: JSON은 임의의 데이터를 직렬화하고, JavaScript interpreter에 의해 직접 실행될 수 있는 간단한 데이터 전송 포맷이다. JSON hijacking은 XSRF 공격의 특별한 버전이다.

7) Session Fixation: 웹 세션 보안은 공격자가 웹 서버에서 발행된 세션 ID를 얻지 못하게 하는데 주로 초

점이 맞춰져 있다. 사용자가 로그인 시, 세션 ID가 임의적으로 만들어지는 것 대신에 공격자가 사용자의 세션 ID를 설정하게 된다.

8) Attacking ActiveX Controls: ActiveX는 기술적 제약이 적어서 자신도 모르는 사이 악성 소프트웨어가 유입될 수 있고, 호환성 문제도 있어서 최근 선호도가 줄고 있다.

Ⅲ. 이동형 웹콤포넌트 보안 방안

그림 1. 웹 콤포넌트에서의 보안 유의사항 3요소
Fig. 1 3 Primary Elements of Web Security

이동형 웹 컴포넌트 기술은 웹 융합 콘텐츠를 N스크린 환경에서 활용함으로 그 사용성을 극대화 할 수 있는 기술이며, 사용자는 본 기술을 바탕으로, 웹 환경에 끊김없는 접근이 가능하다. 그림 1은 N스크린 환경에서 이동형 웹 서비스가 안정적으로 운영되기 위해 보장해야 할 기본적인 보안 요구사항 3요소에 대해서 나타내고 있다.

- 기밀성 (Confidentiality): 본 서비스의 제공에 있어서, 사용자의 단말 내 존재하거나 네트워크를 통해 전달되는 사용자의 데이터는 데이터의 특성에 따라 다른 시스템에 노출되지 않아야 한다.
- 무결성 (Integrity): 사용자의 끊김없는 웹 연결을 위해서는, 단말 간에 접속정보에 대한 이동이 필요하다. 이 때, 이동 되는 데이터는 다른 시스템에 의해 변경되지 않아야 한다.
- 가용성 (Availability): 단말간의 서비스 이동을 위해서는, 단말 사이의 컨트롤 정보의 이동이 필수적이다. 본 컨트롤 정보는 단말 간의 동기화 혹은 연속적 정보 전달을 위한 신호로 사용된다. 본 서비스를 이용하는 사용자는 다른 시스템의 방해 없이, 원하는 장소, 시간에 서비스를 사용 받을 수 있어야 한다.

Ⅳ. N-스크린 협업서비스 시나리오 기반 보안 요구사항 제안 및 분석

본 장에서는 N-스크린 환경에서 발생할 수 있는 다양한 협업서비스 시나리오들을 분석하고 이를 위한 보안 요구사항들을 제안하고 분석한다. 각각의 시나리오에서 발생할 수 있는 취약성을 분석함으로써, 웹 및 네트워크 공격에 대해 안정적인 서비스를 제공하는 것이 본 IV장의 중요 목표이다.

4.1. K-pop 시나리오

4.1.1. 시나리오 설명

(a) 이동 웹 컴포넌트 기술이 반영된 스마트 TV에서 친구와 함께 소녀시대의 뮤직 비디오 감상, 스크린 하단에 소녀 시대에 대한 한 줄 기사를 보고, 사용자는 뮤직 비디오 화면에 방해를 받지 않는 환경에서 기사를 보고 싶어 한다.

(b) 본 기사를 사용자의 휴대 단말에서 확인하기 위해, TV에서 사용자 휴대 단말을 선택하고, 해당 단말에서 서비스 요청을 확인한다.

(c) 사용자 휴대 단말에서 TV에서 노출된 해당 기사를 받아서 읽는다.

(d) 사용자는 소녀시대의 음악이 마음에 들어, 구매를 요청하였고, 본 구매 프로세스는 사용자의 휴대 단말로 이동되어 진행되었다.

4.1.2. 보안 요구사항

표 1. K-Pop 시나리오 보안 요구사항
Table. 1 Service Requirement of K-Pop Scenario

ID	요구사항	공격 유형	대응방안
SEC-1.001	이동 컨텐츠는 허용된 인증된 사용자만 접근할 수 있어야 한다.	ARP Spoofing, Switch jamming등을 이용한 도청	인증 및 암호화

SEC-1.002	구매 프로세스 시, 전달되는 구매자의 정보는 노출되지 않아야 한다.	ARP Spoofing, Switch jamming등을 이용한 도청	접근 통제 암호화
SEC-1.003	구매 프로세스 시, 휴대 단말은 안전한 사이트로 연결되어야 한다.	Redirection 공격, Frame injection 등을 이용한 피싱	해시 기반 전자 서명
SEC-1.004	휴대 단말에 연결 요청은 상호 인증된 사용자의 접속만을 허용한다.	Service Request Flooding	비정상 Request 탐지, 인증

4.2. 공공 디스플레이 광고 시나리오

4.2.1. 시나리오 설명

(a) 카페 광고를 위해, 사용자는 이미지 저작 웹 어플리케이션을 통해 광고 포스터를 제작하고, 본인의 휴대 단말기에 입력한다.

(b) 사용자는 공공 디스플레이 앞에 도착한 후, 휴대 단말을 통해 웹 응용을 실행시킨다.

(c) 사용자는 이동형 웹 컴포넌트 기술을 기반으로 광고 디스플레이와 본인의 휴대 단말에 있는 웹 응용의 디스플레이를 연계시킨다. 광고 디스플레이의 터치 스크린을 통해 본인이 원하는 광고 영역만큼을 확대 및 축소시킨다.

4.2.2. 보안 요구사항

표 2. 공공 디스플레이 광고 시나리오 보안 요구사항
Table. 2 Service Requirement of Public Display Advertisement Scenario

ID	요구사항	공격 유형	대응방안
SEC-2.001	광고주의 아이디 도용을 막아, 불법 과금 체계를 방지한다.	도청 공격 및 XSS 공격	안전한 사용자 인증 및 사이트 설계
SEC-2.002	광고 플랫폼 관리 서버는 사용자 정보를 안전하게 보관해야 한다.	관리 서버에 대한 SQL injection, 파라미터 변조 등을 통한 해킹	분산 웹서버 시스템, 특수문자 방지, 안전한 사이트 설계
SEC-2.003	사용자의 광고 영역은 사업자와의 계약기간 동안 안전하게 보존되어야 한다.	관리 서버에 대한 SQL injection, 파라미터 변조 등을 통한 해킹	안전한 사이트 설계, 웹서버 권한 관리
SEC-2.004	사용자의 광고 디스플레이 파일은 다른 시스템에 의해 노출되거나 변조되어서는 안 된다.	ARP Spoofing, Rogued AP, MITM (Man In The Middle) attack 등의 도청 및 변조	암호화 및 디지털 서명, AP인증

4.3. 오피스 미팅 시나리오

4.3.1. 시나리오 설명

(a) 팀장 A와 팀원 B, C, D는 신제품 개발을 위한 브레인스토밍을 하기 위해 A, B, C는 한 자리에 모였으며, D는 온라인으로 회의하기로 하였다.

(b) 팀장과 각 팀원들은 협업 캔버스 기능이 가능한 공용 스마트 스크린에 각자의 스마트폰의 브라우저를 통해 접속하였다.

(c) 각 팀원들은 각자 단말을 이용하여 필요한 자료를 검색하였고, 팀장은 협업 캔버스를 통해 이를 모니터 하고, 공용 공간에 중요한 자료들을 뽑아 작업하였다.

4.3.2. 보안 요구사항

표 3. 오피스미팅 시나리오 보안 요구사항
Table. 3 Service Requirement of Office Meeting Scenario

ID	요구사항	공격 유형	대응방안
SEC-3.001	오피스 미팅을 지원하는 웹 사이트는 사용자의 개인 정보를 보호해야한다.	SQL injection 등의 해킹과 내부자 공격	안전한 사이트 설계, 접근 권한 관리
SEC-3.002	웹에서 사용자 간 서로 주고 받는 자료는 외부에 노출되지 않아야 한다.	ARP Spoofing, Rogued AP, MITM Attack 등의 도청 및 변조	데이터 암호화 및 인증
SEC-3.003	협업 캔버스에는 각 사용자가 허용하는 정보만이 노출되어야 한다. 또한 주고 받는 자료 안에 악성코드가 포함되어있으면 안 된다.	시스템 해킹, 악성코드	접근 권한 관리, 침입탐지 시스템
SEC-3.004	회의가 끝난 후, 협업 캔버스에는 각 사용자의 쿠키 정보 등이 삭제되어야 한다.	개인정보 탈취	보안 코딩

4.4. 이동식 동영상 재생 시나리오

4.4.1. 시나리오 설명

(a) 학교 컴퓨터에서 인터넷으로 동영상을 감상하던 사용자는 집으로 돌아가려한다. 현재 컴퓨터에서 보던 동영상을 자신의 휴대 단말기에서 끊김없이 감상한다.

(b) 집에 돌아온 사용자는 휴대단말의 작은 화면에 불만을 느껴 집 안의 스마트 TV에 동영상을 옮기고, 자신의 휴대단말로 텍스트를 출력하고 TV 화면을 컨트롤한다.

4.4.2. 보안 요구사항

표 4. 이동식 동영상 재생 시나리오 보안 요구사항
Table. 4 Service Requirement of Video Scenario

ID	요구사항	공격 유형	대응방안
SEC-4.001	각 디바이스간의 호출은 다른 시스템에 의해서 접근되거나 방해받지 않아야한다.	IP Spoofing, Request Flooding	상호 인증을 통한 접근 관리
SEC-4.002	컨트롤 정보에 포함된 세션 유지 정보는 외부로 노출되지 않아야한다.	ARP Spoofing, Rogued AP 등의 도청 공격, Session Hijacking	암호화 및 정교한 사용자 인증기법
SEC-4.003	컨트롤 정보에 포함된 세션 정보는 변조, 조작 되어서는 안된다.	Frame Injection, Redirection, 사회공학적 피싱	해쉬기반의 무결성 보장 및 암호화
SEC-4.004	재생이 끝난 후, 공용 TV에서는 각 사용자의 쿠키 정보 등이 삭제되어야 한다.	개인정보 탈취	보안 코딩

4.5. 피겨스케이팅 시나리오

4.5.1. 시나리오 설명

(a) 사용자 A는 피겨 스케이팅을 친구와 함께 감상 중인데, 한 친구 B가 TV의 화면 분할을 이용하여 검색을 수행한다. 사용자 A는 친구 B에게 스케이팅 보는데 방해된다며, B의 개인단말에서 검색해줄 것을 요청한다.

(b) 친구 B는 공용 TV에서 검색하던 검색 브라우저의 상태를 개인 휴대 단말에 바로 가져와 연속적인 검색을 수행한다.

(c) 친구 B는 검색 중, 아사다마오의 트리플 악셀에 관한 자료를 발견했으며, 사용자 A도 검색 결과에 대해 궁금해 한다.

(d) 친구 B는 공용 TV에 본인의 검색 결과를 화면에 띄워 A와 함께 그 검색 결과를 공유한다.

4.5.2. 보안 요구사항

표 5. 피겨스케이팅 시나리오 보안 요구사항
Table. 5 Service Requirement of Figure-Skating Scenario

ID	요구사항	공격 유형	대응방안
SEC-5.001	공용 TV에서는 허용된 사용자만이 접근 및 조정 가능해야만 한다.	권한 위반	보안 코딩
SEC-5.002	TV에서 휴대 단말로 브라우징 상태가 외부에 노출 없이 전달되어야한다.	무선 도청, ARP Spoofing 등	암호화 통신 및 사용자 인증
SEC-5.003	각 사용자 단말 간에 받는 자료안에 악성코드가 포함되어있으면 안 된다.	악성코드 전파	침입탐지 시스템

4.6. 보안기술 요구사항 정리 및 분석

표 6은 각각의 시나리오들의 요구사항을 보안 유의사항의 요소별로 정리하는 동시에 각각의 요구사항의 특징들을 뽑아 정형화된 요구사항으로 정리한 것이다.

표 6. 보안 요구사항 정리
Table. 6 Summary of Service Requirements

No.	요구사항	ID	유형
1	서비스 사용을 위해 전달되는 사용자 개인 정보(사용자 ID, 구매정보, 사용자 위치, 서비스 종류 등)는 외부로부터 보호받아야 한다.	SEC-1.001 SEC-1.002 SEC-2.004 SEC-3.002 SEC-4.002 SEC-5.002	기밀성
2	각 단말간에 주고 받는 정보들은 외부로부터 변조되지 않고 그대로 전송 되어야 한다.	SEC-1.003 SEC-2.004 SEC-4.003	무결성
3	사용자 단말 간에 주고 받는 정보를 통해 악성 코드 등이 전파되지 않아야 한다.	SEC-3.003	무결성

4	공공의 목적으로 사용되는 협업 스크린은 이를 이용하는 사용자의 개인 정보가 노출되지 않도록 해킹 등으로부터 안전해야 한다.	SEC-3.003 SEC-3.004 SEC-4.004	기밀성
5.	사용자의 단말들간의 연계를 담당하는 제어서버는 외부 침입으로부터 안전하게 설계되어야 하며, 서버 내의 사용자 DB는 강력히 암호화 되어야 한다.	SEC-2.002 SEC-3.001 SEC-4.002	기밀성
6	사용자의 단말간의 연계를 담당하는 제어서버는 저장된 자료의 손실을 막기 위한 백업 기능을 제공해야한다.	SEC-2.005 SEC-3.005	기밀성 가용성
7	사용자의 단말에 대한 서비스 요청은 인증 및 허용된 단말기만이 가능하도록 하여, 불필요한 서비스 요청으로 인한 사용자의 불편을 최소화하여야한다.	SEC-1.004 SEC-4.001 SEC-5.001	가용성
8	각 사용자의 권한에 대한 적절한 통제를 하여, 사용자의 권한 남용을 막는다.	SEC-2.003 SEC-5.001	기밀성
9	아이디의 도용을 막아, 서비스를 이용하는 고객에 대한 불법 과금을 막아야한다.	SEC-1.005 SEC-2.001	사용자 인증 (기타)

그림 2로부터 우리는 N스크린 환경에서 공격 유형의 발생빈도를 살펴 볼 수 있다. N스크린 환경에서 웹콘테츠의 이동/결합/분리를 고려한 시스템을 개발할 경우, 보안 측면에서 ARP Spoofing, SQL Injection, Rogued AP, Eavesdropping등의 요소가 우선적으로 고려되어야 함을 볼 수 있다. 또한 Redirection Attack, Frame Injection, Service Request Flooding, Parameter Variation, Malicious Code Dissemination 등도 개발 시 중요하게 고려되어야 하는 요소임을 확인할 수 있다.

Ⅴ. 보안 요구사항을 고려한 N-스크린 협업서비스 프레임워크 구현

Ⅴ장에서는 N스크린 환경에서 웹콘텐츠의 이동을 통하여 사용자의 개인 정보가 공공 디바이스를 통해 외부로 공개되는 것을 방지할 수 있는 방안이 적용된 N스크린 협업서비스 프레임워크에 대해서 알아본다. 지금까지의 HTML 표준 기반 웹 콘텐츠 렌더링(Web Content Rendering)은 단일 페이지에서의 렌더링 상황을 기준으로 설계되어 있어 단일 콘텐츠 서비스 분리에는 적합하지 않다. 따라서, 본 연구에서는 웹 콘텐츠를 랜더링하고 있는 소스 스크린에서 다른 가능한 네트워크 단말간 영상을 스크린 영역 내의 일정 부분에 랜더링하고 입력 이벤트를 전달할 수 있는 방법인 HTML 스트리밍 기술 기반으로 보안 요구사항을 고려한 N스크린 협업서비스 프레임워크를 개발하였다. 또한, 단일 웹페이지에서 일정 영역을 분리 가능하게 만드는 웹 조각화(Web Fragmentation) 기술도 함께 적용하였다.

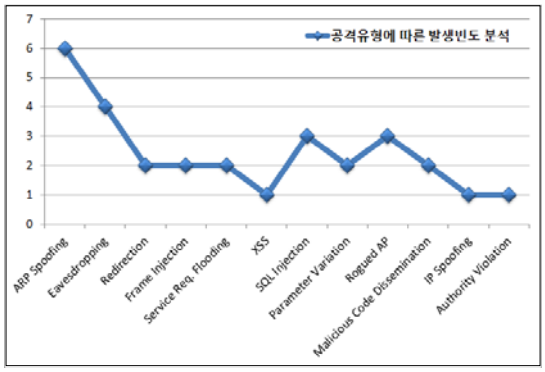

그림 2. 공격유형에 따른 발생빈도 예측 분석
Fig. 2 Occurrence Analysis of Attack Type

그림 3은 N스크린 협업서비스 프레임워크의 구조도이다. 단말에서의 웹 렌더링 결과는 크게 디바이스를 통해 직접적으로 출력되는 부분과 웹 스트림 매니저(Web Stream Manager)를 통해 다른 디바이스로부터 중계되어 렌더링되는 부분으로 나뉜다. 이 때, 출처가 다른 디바이스간의 렌더링 결과는 스크린 관리자(Screen Manager)에 의해 관리된다. 분리된 웹 컴포넌트간 입출력 교환은 입출력 관리자(Input/Output Manager) 모듈을 통해 이루어진다. 교환되는 정보의 타입은 크게 입출력 정보와 자바스크립트(JavaScript) 정보로 나뉜다. 구현된 N스크린 협업서비스 프레임워크은 크게 이종 단말 간 HTML 스트리밍 기능과 사용자 입력 기반 웹 조각화 기능을 가지고 있다. 이종 단말 간 HTML 스트리밍 기능은 단말에서 랜더링 되고 있는 웹 페이지 정보에 대한 스트리밍 (웹페이지의 부분적 영역의 이미지 Stream 전송)을 통해 웹 부분 이동을 지원하고 입출력

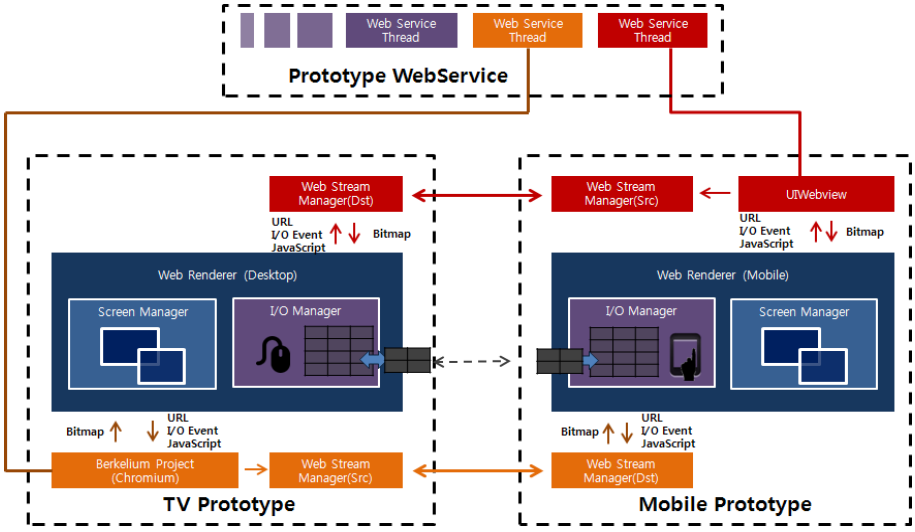

그림 3. 보안 요구사항을 고려한 N스크린 협업서비스 프레임워크 구조도
Fig. 3 Architecture of N-screen Cooperation Service Framework Considering Security

정보를 연동을 지원하는 것이다. 사용자 입력기반 웹 조각화 기능은 사용자의 입력정보 (분할하고자 하는 웹 페이지의 특정 부분을 지정하는 터치스크린 입력 등)를 기반으로 연결 대상 디바이스에서 렌더링 되고 있는 웹 페이지에 대한 동적인 영역 분할 및 이동을 지원하는 것이다. 입출력을 연계하는 과정에서 대형 스크린을 가지고 있는 PC에 개인의 정보가 공개되는 것을 방지하기 위해서 우리는 아래와 같이 User Interface 보안 방안을 적용하였다.

그림 4. N스크린 협업서비스 프레임워크 시연
Fig. 4 N-screen Cooperation Service Framework Demo

TV의 보안 관련 영역이 해당영역을 선택하는 순간 스마트 디바이스로 이동하여 다른 사람들에게 개인의 정보가 공개되는 것을 방지할 수 있다. 그림 3에서는 ID와 Password를 입력하는 부분이 TV에서 스마트 디바이스로 이동해 있는 것을 볼 수 있다. 이와 같이, HTML 스트리밍을 기반으로 하는 웹콘텐츠의 이동기술과 보안 기술이 융합되어 사용자의 정보가 공공 디바이스를 통해서 방지되는 것을 막을 수 있다.

VI. 결 론

본 논문에서는 다양한 N-스크린서비스 시나리오들에 대하여 콘텐츠 이동/결합/분리를 고려한 웹보안 기술 요구사항에 대하여 분석하고 제안하였다. 웹콘텐츠 이동/결합/분리를 고려한 미래의 N스크린 서비스 시나리오를 미리 살펴보고, 이를 위한 보안 위협 상황을 종합적으로 분석하여, 보안 기술이 개발될 때 고려해야 할 사항들을 미리 살펴보았다. 또한, 웹콘텐츠 이동기술과 보안기술의 결합을 통해 사용자의 개인정보를 효과적으로 보호할 수 있다는 것도 확인할 수 있었다.

이동형 웹 컴포넌트는 상호간의 소통이 필수적이며, 단말 간의 경계가 불분명하고 투명하다. 따라서, 기밀

성(Confidentiality), 무결성(Integrity), 가용성(Availability) 보장으로 대표되는 서비스 보안을 필수적으로 지키고, 웹 콤포넌트 간의 이동/결합/분리의 허용으로 얻어지는 사용자 경험은 극대화 하되, 고객의 보안 안정성도 함께 고려하는 방향으로 기술이 개발되어야 한다.

REFERENCES

[1] Ho-Won Lee, Soo-Bin Lee, "Research on N-Screen Cooperative Service Scenarios and Framework Considering Dynamic Reconfiguration of Web Contents", *Global e-Business Association e-Business Study*, Vol. 13, No. 3, pp. 461-480, Sep. 2012.

[2] H. R. Mun, S. H. Kim, and B. H. Chung, "Analysis on Trends for Contents Sharing Technology", *ETRI Electronics and Telecommunications Trends*, Vol. 25, No 4, Aug. 2010.

[3] Kim, J., D. Lee, B. C. Jung, and J. Ahn, "Ontology based information distribution in the pervasive display environment", *IEEE PERCOM'2010 Workshops*, pp.171- 175, 2010.

[4] Kim, J., U. Farman, S. Lee, S. Jo, H. Lee, and W. Ryu, "Dynamic addition and deletion of devices in N-screen environment", *ICUFN*, pp. 118-122, 2012.

[5] Yoon, C., T. Um, and H. Lee, "Classification of N-Screen Services and its standardization", *ICACT*, pp. 597-602, 2012.

[6] J. G. Choi, B. N. Noh, "Security Technology Research in Cloud Computing Environment", *Journal of Security Engineering*, Vol. 8, No. 3, Jun. 2011.

[7] J. S. Park, E. K, Cho, and S. G. Kang, "Security Technology for World Wide Web", *ETRI Electronics and Telecommunications Trends*, Vol. 11 No. 4, Dec. 1996.

[8] G. B. Cho, "A Survey of Information Security Technology in the Ubiquitous Environments", *Samsung SDS Consulting Review*, No. 3, 2005.

[9] Michael, C., *Developer's Guide To Web Application Security*, Syngress, 2007.

[10] Shreeraj, S., *Web 2.0 Security: Defending Ajax, RIA, and SOA*, Thomson, 2007.

이호원(Howon Lee)

2009년 전기및전자공학과 박사
2009년~2010년 KAIST IT융합연구소 선임연구원
2010년~2012년 KAIST IT융합연구소 팀장/연구조교수
2012년~현재 국립한경대학교 전기전자제어공학과 조교수
2012년~현재 KAIST IT융합연구소 겸직교수
※관심분야 : 차세대 이동통신 시스템, D2D 통신, 최적 CSMA, 지식융합기술 등