

Security Requirements Analysis on IP Camera via Threat Modeling and Common Criteria

Jisoo Park[†] · Seungjoo Kim^{††}

ABSTRACT

With rapid increasing the development and use of IoT Devices, requirements for safe IoT devices and services such as reliability, security are also increasing. In Security engineering, SDLC(Secure Development Life Cycle) is applied to make the trustworthy system. Secure Development Life Cycle has 4 big steps, Security requirements, Design, Implementation and Operation and each step has own goals and activities. Deriving security requirements, the first step of SDLC, must be accurate and objective because it affect the rest of the SDLC. For accurate and objective security requirements, Threat modeling is used. And the results of the threat modeling can satisfy the completeness of scope of analysis and the traceability of threats .In many countries, academic and IT company, a lot of researches about drawing security requirements systematically are being done. But in domestic, awareness and researches about deriving security requirements systematically are lacking. So in this paper, I described about method and process to drawing security requirements systematically by using threat modeling including DFD, STRIDE, Attack Library and Attack Tree. And also security requirements are described via Common Criteria for delivering objective meaning and broad use of them.

Keywords : SDLC, Threat Modeling, IP Camera, Security Requirements, Traceability

보안위협모델링과 국제공통평가기준을 이용한 IP Camera 보안요구사항 분석

박 지 수[†] · 김 승 주^{††}

요 약

다양한 산업에 걸쳐 IoT 기기의 보급이 급격히 증가하면서 신뢰성, 보안성과 같은 안전한 IoT 기기 및 서비스를 위한 요구가 증가하고 있으며 보안공학에서는 고 신뢰(Trustworthy) 시스템의 설계 및 구현을 위해 안전한 개발 생명주기를 활용한다. 안전한 개발 생명주기는 보안요구사항 도출, 설계, 구현, 운영 단계로 구분되며 각 단계별로 달성하기 위한 목표 및 활동이 존재한다. 그 중 보안요구사항 도출 단계는 가장 첫 단계로 향후 설계, 구현 단계의 목표를 달성을 위해 정확하고 객관적인 보안요구사항을 도출하는 것이 중요하다. 정확하고 객관적인 보안요구사항을 도출하기 위해 보안위협모델링을 활용하며 이를 통해 도출된 보안요구사항은 위협 식별 범위에 대한 완전성과 대응되는 위협에 대한 추적성을 만족시킬 수 있다. 해외에서는 다양한 대상과 보안위협방법론을 활용한 연구가 진행되고 있는 반면 국내 연구는 중요성에 비해 상대적으로 미흡한 편이다. 따라서 본 논문에서는 IP Camera를 대상으로 Data Flow Diagram, STRIDE, Attack Tree와 같은 체계적인 보안위협모델링을 통해 보안요구사항을 도출하는 과정에 대해 설명하고 객관적인 의미 전달을 위해 도출한 보안요구사항은 국제표준인 공통평가기준을 활용하여 표현한다.

키워드 : 안전한 개발생명주기, 위협모델링, IP Camera, 보안요구사항, 추적성

1. 서 론

최근 스마트 그리드, 스마트 홈, 스마트 의료, 스마트 자동차와 같은 IoT(Internet of Things)와 CPS(Cyber Physical

System)를 활용한 서비스가 전 세계적으로 산업 전반에 걸쳐 상용화되고 있다. 이러한 IoT와 CPS는 일상생활 및 산업에 직접적인 영향을 끼치는 서비스를 제공하는 만큼 제작과 활용에 있어 높은 수준의 신뢰성(Trustworthiness)이 요구 된다. ‘신뢰성(Trustworthiness)’있는 시스템은 시스템의 Availability, Reliability, Security, Safety를 모두 고려하여 어떠한 상황에서도 안전하게 목적을 달성할 수 있는 시스템을 의미한다. 신뢰성 있는 시스템을 개발 및 운영하기 위한 일련의 과정을 정보보증(Information Assurance)이라 하며 보안 공학(Security Engineering)에서는 안전한 개발 생명주기(Secure

※ 이 논문(저서)은 2016년 대한민국 교육부와 한국연구재단 지원을 받아 수행된 연구임(NRF-2016S1A3A2924760).

† 준 회 원 : 고려대학교 정보보호대학원 정보보호학과 석사과정

†† 종 신 회 원 : 고려대학교 사이버국방학과/정보보호대학원 정교수

Manuscript Received : November 2, 2016

First Revision : November 29, 2016

Accepted : December 10, 2016

* Corresponding Author : Seungjoo Kim(skim71@korea.ac.kr)

Development Life Cycle, SDLC)를 통해 시스템의 정보보증 달성을 지원한다. 안전한 개발 생명주기는 일반적으로 시스템의 요구사항 도출, 설계, 구현, 운영, 폐기 단계로 구성되어 각 단계별 보증을 달성할 수 있는 행위들이 존재한다. 대규모 IT 서비스 기업 및 제조사는 자사에 적합한 안전한 개발 생명주기를 보유 및 적용하고 있으며 안전한 개발 생명주기를 제품의 신뢰성을 위한 홍보로 사용하기도 한다. 가장 잘 알려진 안전한 개발 생명주기로는 Microsoft사의 Security Development Life Cycle[1]이 있으며 이외에도 Cisco[2], VMware[3], OWASP[4]와 같은 잘 알려진 기업, 단체에 대한 안전한 개발 생명주기가 존재한다.

안전한 개발 생명주기 중 가장 첫 단계는 요구사항 도출 단계로 도출된 요구사항과 설계를 바탕으로 구현, 운영 단계 보증 활동을 진행하기 때문에 가장 중요한 단계이며 정확하고 완전한 요구사항을 도출하는 방법에 대한 연구가 필요하다. 따라서 본 논문에서는 보안성 평가 관점에서 완전성과 추적성을 만족하는 보안요구사항 도출을 위해 IP Camera를 대상으로 보안위협모델링을 통한 체계적인 보안요구사항 도출 방법에 대해 설명한다.

본 논문의 2장에서는 보안위협모델링 및 IP Camera에 대한 관련 연구를 설명하고 3장에서는 IP Camera를 대상으로 보안위협모델링을 수행하는 과정 및 결과에 대해 설명한다. 4장에서는 3장에서 도출한 위협에 대응하는 보안기능요구사항을 도출하는 과정과 결과에 대해 설명한다.

2. 원고 작성

2.1 보안위협모델링

보안위협모델링은 안전한 개발 생명주기(SDLC) 과정 중 구현 단계 이전에 이해관계자들이 모여 공격자의 입장에서 대상에 존재하는 잠재적인 위협을 식별하는 것을 의미한다.

1) 보안위협모델링 역사와 종류

1990년대부터 소프트웨어 개발 생명주기 발전과 함께 다양한 보안위협모델링 방법에 대한 연구가 진행되었다. 1990년대 시스템 설계를 위한 방법으로 설계를 시각화해서 보여주는 UML(Unified Modeling Language) Use case가 사용되었다. 이를 응용하여 노르웨이의 Guttorm Sindre와 Andreas L. Opdahl은 처음으로 시스템에 대한 비정상행위를 표현하기 위한 방법으로 Use case와 반대되는 개념의 Misuse Case를 사용하였다[5, 6]. 이와 함께 Edward G. Amoroso는 1994년 그의 저서 “Fundamentals of Computer Security”에 시스템 안전 공학에 사용된 Fault Tree를 변형시킨 Threat tree를 소개했다[7]. Threat tree는 시스템에 존재하는 위협을 논리적이고 계층 구조로 표현한 것으로 위협들 간의 관계를 시각적으로 이해할 수 있다는 장점이 있다. 이처럼 1990년대에는 시각화하여 위협을 설명하는 방법론을 사용하였지만 점차 소프트웨어의 규모, 복잡도가 증가하면서 표현의 범위, 내용, 구조의 어려움으로 인해 명확성이 떨어지는

어려움이 발생하였다.

1998년 Bruce Schneier는 위와 같은 어려움을 고려하여 “Toward a Secure System Engineering”과 “Attack Trees” 발표에서 Attack Tree 방법을 제안하였다[8, 9]. Attack Tree는 공격자의 최종 목표를 최상위 노드(Root Node), 최종 목표를 달성하기 위한 중간 목표들을 하위 노드(Leaf Nodes)로 설정하여 AND/OR 기호와 함께 공격을 체계적으로 나타낸다. Attack Tree는 시각화뿐만 아니라 글 형식으로도 Tree의 구조적 표현이 가능하다는 장점이 있다. 비슷한 시기인 1999년에 Microsoft 사의 Jason Garms, Praeit Grag, Michael Howard는 자체적으로 사용하는 체계적인 보안위협 모델링 방법을 내부 문서 “The threats to our products”에 정리하여 STRIDE 방법론을 소개하였다[10]. Microsoft 사는 현재까지도 STRIDE 방법론을 지속적으로 발전시키고 있으며 STRIDE 방법론을 지원하는 도구[11]들도 함께 개발하고 있다. STRIDE에 대한 내용은 다음 2.1.2에서 상세히 다룬다. Microsoft 社의 STRIDE 방법론 외에도 개인정보 위협 식별을 위한 “LINDDUN[12]”, Carnegie Mellon University의 Software Engineering Institute의 “OCTAVE[13]”, OctoTrike의 “Trike[14]”, OWASP의 “P.A.S.T.A[15]”, “Threat Risk Modeling[16]”과 같이 조직의 목표, 특성, 위협모델링의 목적을 고려한 다양한 보안위협방법론이 존재한다.

2) STRIDE 보안위협모델링

Microsoft 社의 STRIDE는 시스템 분석 시 고려해야 할 보안속성 6가지[17]에 대해 대응되는 위협들을 식별하는 방법이다. 다음 Table 1은 STRIDE의 6가지 위협과 대응되는 보안속성을 나타낸 표이다.

다음은 STRIDE의 각 속성에 대한 설명으로 STRIDE를 이용하기 위해서는 이에 대한 정확한 이해가 요구된다.

- a) Spoofing(위장) : 허가받지 않거나 인증 받지 않은 주체 또는 시스템 요소가 허가 또는 인증 받은 것처럼 위장하는 위협
- b) Tampering(변조) : 프로세스, 파일, 네트워크 전송 값과 같은 대상의 구성요소를 변조 시키는 위협
- c) Repudiation(부인) : 주체가 대상에 대해 쓰기, 읽기, 접근과 같은 특정 행위를 한 뒤 이를 부인하는 행위
- d) Information Disclosure(정보 노출) : 대상의 민감 또는 중요 정보가 허가되지 않은 대상 또는 사람에게 노출되는 위협

Table 1. STRIDE and Security Property

STRIDE	Security Property
Spoofing	Authentication
Tampering	Integrity
Repudiation	Non-Repudiation
Information Disclosure	Confidentiality
Denial of Service	Availability
Elevation of Privilege	Authorization

- e) Denial of Service(서비스 거부) : 자원소모와 같은 특정 행위를 통해 대상의 정상적인 동작을 방해하거나 중지시키는 모든 위협
- f) Elevation of Privilege(권한 상승) : 접근, 실행 권한이 없는 주체가 주체에 할당된 권한보다 높은 권한이 할당된 대상에 접근하거나 실행하는 위협

또한 STRIDE 방법론은 Data Flow Diagram과 함께 사용할 경우 효과적인 분석을 위해 “STRIDE per Element”, “STRIDE per Interaction”이라는 두 가지 방법을 제안한다[18].

- a) STRIDE per Element : Data Flow Diagram의 요소마다 특정 위협이 더 많이 연관되어 있는 특성을 활용하여 Data Flow Diagram 요소에 집중하여 STRIDE를 분석하는 방법으로 Table 2와 같이 적용
- b) STRIDE per Interaction : Microsoft 社の Larry Osterman, Dogulas MacIver에 의해 개발된 방법으로 (Origin, Destination, Interaction)로 구성된 각 Tuple에 대해 STRIDE를 적용하는 방법

Table 2. STRIDE per Element Reference Table

	S	T	R	I	D	E
Data Flow		X		X	X	
Data Stores		X		X	X	
Process	X	X	X	X	X	X
Interactors	X		X			

2.2 보안위협모델링 활용 연구

최근 IoT, CPS 등장과 함께 해외에서는 다양한 대상에 대한 보안위협모델링에 대한 연구가 진행되고 있으며 보안위협모델링 결과 활용에 대한 연구도 함께 진행되고 있다.

Guttorm Simdre, Andreas L. Opdahl은 2002년[5, 6]에서 Use case 및 Misuse Case를 이용해 표현하는 과정에서 발생하는 추상화 격차를 최소화하기 위한 방법으로 Misuse case에 경로, 요약, 가정 사항, 위협과 같은 상세한 설명을 글로 표현하여 보안요구사항을 체계적으로 도출하는 과정에 대해 설명하였다.

Aaron Marback, Hyunsook Do 외 3명은 [19]에서 효과적인 방법으로 고 신뢰 시스템 및 소프트웨어 개발을 위해 Threat tree를 이용한 Security Test Case를 도출하는 방법을 설명하였다. Threat Tree 작성 시 STRIDE 기법을 함께 이용하여 STRIDE로 도출된 위협 속성을 Threat Tree를 통해 체계적인 구조로 정리하였다.

Inger Anne Tondel, Jostein Jensen, Lillian Rostand는 [20]에서 Misuse Case와 Attack Tree를 함께 이용한 보안위협모델링 방법을 제시하였다. Misuse Case와 Attack Tree는 위협을 표현하는 수준(Level)이 다르기 때문에 Misuse Case로 식별한 위협에 대해 Attack Tree로 상세하게 설명하였다. Attack Tree 작성 시 CAPEC(Common Attack Pattern

Enumeration and Classification)의 공격 내용을 참고하여 효율적이고 정확한 내용을 설명하였다.

Goncalo Martins, Sajal Bhatia 외 4명은 [22]에서 실제 활용하는 무선 철도레일 온도 모니터링 시스템을 대상으로 Data Flow Diagram, STRIDE와 같은 체계적이고 효과적인 보안위협모델링을 활용하여 위협을 식별하였으며 식별한 위협을 NIST(National Institute of Standards and Technology) 표준을 활용해 완화시켰다.

ENISA(European Network and Information Security Agency)에서는 2011년 [23]에서 스마트 폰의 App Store를 대상으로 Data Flow Diagram, STRIDE, Attack Tree와 같은 보안위협모델링을 이용해 위협을 식별하고 식별한 위협에 대한 5가지 완화 방안을 제안하였다.

Tong Xin, Ban Xiaofang은 [24]에서 Online Banking System을 대상으로 STRIDE 및 Threat tree를 적용하여 보안위협모델링을 수행하였다. STRIDE를 통해 식별한 위협을 Threat Tree를 이용하여 체계적으로 제시하여 효과적인 Online Banking System의 보안성 분석을 지원하였다.

Anthony Hadding은 [25]에서 임베디드 시스템에 대해 Data Flow Diagram, Attack Tree를 이용한 보안위협모델링을 수행했다. 기존 관련 연구와 유사하지만 자동차 네트워크 임베디드 시스템을 대상으로 전문적인 보안위협모델링 도구를 사용하여 수행한 것이 특징이다.

Kristian Beckers, Stephan Fabbender 외 2명은 [26]에서 스마트 홈을 대상으로 보안위협모델링 과정에 대해 설명하였다. 규모가 큰 Smart Grid 시스템을 대상으로 Data Flow Diagram, STRIDE per Interaction 방법과 유사한 방법을 활용하였으며 Entry Point라는 데이터의 흐름 및 진입지점을 중점으로 분석하였다. 또한 규모가 큰 시스템의 Data Flow Diagram을 통해 실제 전송되는 데이터 유형 및 시스템 구조를 파악하는 효과적인 방법을 제시하는 것이 특징이다.

Anton Bretting, Mei Ha는 [27]에 자동차 임베디드 시스템의 오픈소스 플랫폼인 AUTOSAR를 대상으로 STRIDE per Element 방법과 STRIDE per Interaction 방법을 모두 사용하여 보안위협모델링을 진행했으며 두 방법에 대한 결과를 비교, 분석하여 설명하였다.

Katrina Mansfield, Timothy Eveleigh 외 2명은 [28]에서 美 국방부의 작전간 스마트 기기의 활용이 증가함에 따라 안전한 스마트 기기 도입을 위한 방법으로 보안위협모델링의 중요성을 강조하며 소프트웨어, 하드웨어가 결합된 UAV(Unmanned Aerial Vehicle) 운영환경에 대한 보안위협모델링을 수행했다. 공격자의 목표를 설정하고, 그에 대한 소프트웨어, 하드웨어, 네트워크 통신에 존재하는 위협에 대해 설명했지만 구체적인 위협 도출 방법은 제시되어 있지 않고 사례중심의 참고 내용으로만 설명하였다.

Mark Yampolskiy, Peter Horvath 외 4명은 [29]에서 사이버 공격에 대한 CPS 응용성(Applicability) 분석을 위해 Data Flow Diagram 기반의 접근 방법을 제안했다. [29]에서는 기존 Data Flow Diagram의 요소로 CPS 환경에 대한 범위 및 데이터를 표현하는데 한계가 있기 때문에 새로운

요소를 추가한 확장된 Data Flow Diagram 요소를 제안하여 UAV의 Data Flow Diagram 작성 후 보안위협모델링을 수행하였다.

2.3 IP Camera 관련 연구

기존 CCTV는 가용성, 효율성과 관련한 연구가 주로 진행되었으나 인터넷에 연결된 IP Camera가 개발 및 보급되면서 보안성과 관련된 연구가 활발히 진행되기 시작하였다. Cletus O. Ohaneme, James Eke 외 5명은 [30]에서 IP Surveillance security system을 설계하고 C#을 이용해 구현하는 과정에 대해 설명하였다. 설계 및 구현 시 암호화, 원격 접속, 무선 기능, 영상 화질 관리와 같은 항목에 대해 고려한 내용을 설명하였다. Craig Heffner는 2013년 해킹·보안 컨퍼런스 블랙햇 2013에서 0-day 취약점을 이용한 원격 공격 및 영상 번조 공격에 대해 설명하며 실제 영화와 같은 원격 감시, 사생활 침해가 가능함을 설명하였다[31]. Sergey Shenkyan, Artem Hartutyunyan은 2013년 보안교육 컨퍼런스인 SecTor 13에서 IP Camera의 Web Application, 펌웨어에서 발생할 수 있는 인증 우회, 권한 상승과 같은 공격방법에 대해 설명하였다[32]. Francisco Falcon, Nahuel Riva는 2013년 Hack.lu 컨퍼런스에서 다양한 IP Camera 제품에 대해 하드웨어를 포함한 다방면의 방법으로 해킹, 공격을 하는 과정을 설명하였다[33]. Lee Tobin은 2014년 [34]에서 디지털 포렌식 관점에서 CCTV를 대상으로 Reverse Engineering 기법을 이용해 효율적으로 데이터를 추출하는 방법에 대해 설명하였다. 시나리오 기반의 실습을 통해 수사 관점에서 효율적으로 데이터 추출할 수 있는 방법을 설명하였다. 보안연구소 NSHC와 KAIST 시스템보안 연구실은 2015년 공동연구를 통해 외산 IP Camera 및 CCTV에 Hidden Backdoor 탐지 연구를 진행하고 두 개의 제품에 대한 Hidden Backdoor 탐지 결과를 보고하였다[35].

3. IP Camera 보안위협모델링

보안위협모델링은 다음과 같이 ‘대상 범위 파악’, ‘대상의 기능 및 데이터 흐름 파악’, ‘보안위협 식별’, 세 가지 단계로 구분할 수 있다. 본 장에서는 IP Camera를 분석 대상으로 선정한 이유 및 위 세 가지 단계에 사용할 적절한 방법론 선정 및 선정 이유와 단계별 적용 결과에 대해 설명한다.

본 논문에서는 다음과 같은 이유로 IP Camera를 분석 대상으로 선정하였다. 첫째, IP Camera는 네트워크에 연결되어 IP Camera가 Server, 사용자가 Client인 Server-Client 구조로 보안 속성 중 무결성(Integrity), 가용성(Availability)을 고려할 수 있다. 둘째, 관리자, 허가된 사용자, 허가받지 않은 사용자와 같은 접근 제어 기능이 존재하는 서비스를 제공하기 때문에 보안 속성 중 허가(Authorization), 인증(Authentication)을 고려할 수 있다. 셋째, 데이터 저장 및 네트워크를 통한 전송 기능이 존재하므로 Data Store, Network Transfer를

고려할 수 있다. 마지막으로 IP Camera의 제조사는 온라인으로 설명서, Client Application 및 Firmware와 같은 분석에 참고할 수 있는 요소를 제공하므로 획득 및 분석이 용이하다는 장점이 있다. 본 논문에서는 2015년 시장 점유율 1, 2위 제조사 제품 4대 및 다수의 IP Camera의 매뉴얼 및 기술보고서를 바탕으로 분석을 진행하였다.

3.1 보안위협모델링 범위 및 구성 요소 식별

첫 번째 단계로 범위 및 구성요소 식별에 앞서 분석을 위한 공격자의 목표를 식별하고 가정 사항을 식별한다. 이후 공격자의 목표 및 가정 사항을 반영하여 보안위협모델링 범위와 범위 내 구성 요소들 간의 관계를 파악한다.

1) 공격자 목표 식별 및 가정 사항 설정

공격자의 목표는 다음과 같이 IP Camera 촬영화면 획득, IP Camera 제어권 획득, IP Camera 서비스 거부 공격 수행으로 총 세 개의 공격 목표를 설정한다. 분석 가정 사항으로는 Cloud 및 Social Network Service는 분석 대상에 포함하지 않고 IP Camera 자체에서 제공하는 서비스만을 대상으로 한다. 또한 정상적인 사용자는 관리자, 일반 사용자로 구분하고 이 외의 접근하는 주체에 대해서는 허가받지 않은 사용자로 간주한다.

2) Context Diagram, Data Flow Diagram 작성

본 논문에서는 Diagram을 이용하여 IP Camera의 분석 범위 및 구성 요소를 식별하였다. Diagram을 활용할 경우 분석해야 할 대상의 요소에 집중하여 가지적으로 파악할 수 있는 장점이 있다. Context Diagram은 상세한 Diagram을 작성하기 전 분석 대상과 외부 요소들과의 관계를 추상적으로 식별할 수 있는 Diagram으로 보안위협모델링에 참여하는 모든 이해관계자의 공통적인 분석 대상 범위 및 요소들의 관계에 대한 이해를 돕는다. 다음 Fig. 1은 IP Camera 운영에 대한 Context Diagram이다.

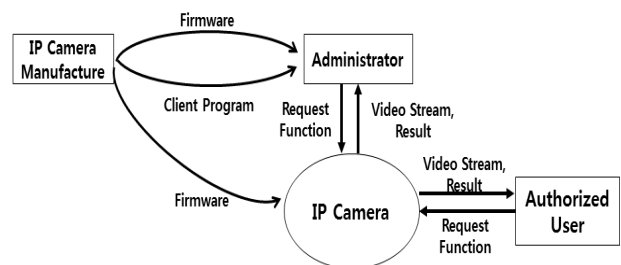



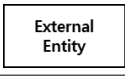



Fig. 1. Context Diagram of IP Camera

IP Camera 제조사는 IP Camera를 위한 Firmware를 제공하고 관리자에게는 관리용 Client Program을 제공한다. 관리자와 인가된 사용자는 IP Camera의 기능을 사용하고 비디오영상을 시청할 수 있다. 작성한 Context Diagram을

Table 3. Elements of Data Flow Diagram

Element	Symbol	Description
Process		Any running code
Data Store		Communication between processes, or between process and data stores
Data Flow		Things that store data
External Entity		People, or code outside your control
Trust Boundary		Where program data or execution changes its level of "trust"

바탕으로 구체적인 구성요소와 데이터 흐름을 나타낼 수 있는 Data Flow Diagram(DFD)을 작성하였다. 공격자는 대상의 기능 및 데이터, 신뢰 구간(Trust Boundary)을 고려하여 공격 방법 또는 지점을 식별하기 때문에 정확한 DFD를 작성할 경우 보안위협을 식별하기 용이하다는 장점이 있다. DFD는 다음 Table 3과 같은 요소를 활용하여 작성한다[18].

DFD는 동일한 대상 범위에 대한 구체화 정도에 따라 레벨을 구분하여 작성할 수 있다. Figs. 2와 3은 각각 IP Camera의 Level 0과 Level 1 DFD를 나타낸 것으로 Microsoft사에서 제공하는 공개 소프트웨어인 Microsoft Threat Modeling Tool 2016[11]을 사용하여 작성하였다. 다음 Table 4는 Level1 DFD(Fig. 3)의 각 Element에 대해 설명한 표이다.

Table 4. Description of Level1 DFD Element

Element Type	No	Name	Description
Entity	E1	Administrator	User who can control and manage the IP Camera with initial set-up
Entity	E2	Authorized User	User who can watch video and control some functions depending on his/her authority
Process	P1	Login	A process that checks who he/she is and his/her authority
Process	P1.1	Authenticate	A process that checks who he/she is. Usually ID and PW are used
Process	P1.2	Authorize	A process that checks authority given by the administrator. (Admin, User, etc)
Process	P1.3	Show Web Page	After P1.1, P1.2, Admin or user can access web pages that the IP Camera provides
Process	P2	Configure System Files	A process that can configure system file
Process	P2.1	Manage File Systems	A process that can manage file systems. For example, allowing FTP, Telnet, etc.
Process	P2.2	Record video	A process related to function about recording video
Process	P2.3	Update Firmware	A process that can update firmware.
Process	P2.4	Manage Accessible IP address	A process related to filtering IP address
Process	P2.5	Manage Users	A process that can manage IP camera users. It include add, modify, delete etc.
Process	P3	Show Video Stream	A process that can make video stream to user wanted protocol
Data Store	D1	File System	File system for IP Camera. It include System File, Embedded Server, Account Information, etc.
Data Store	D1.1	User Account	A data store for user information such as ID, Password, Authority
Data Store	D1.2	System File	System files that used to operate IP Camera. Most embedded devices use embedded linux
Data Store	D1.3	IP Address List	A data store for accessible or inaccessible IP address
Data Store	D2	Flash Memory	A data store for bootloader
Flow	F1.1	Admin ID, PW	ID, PW for IP Camera administrator
Flow	F1.2	User ID, PW	ID, PW for IP Camera users who have authority to access
Flow	F1.3	Command for Configure	Command for managing User
Flow	F1.4	Command for IP Configure	Command for managing IP Address list
Flow	F1.5	Firmware	Firmware file from official provider
Flow	F1.6	Command for Record	It contains command about recording function
Flow	F2.1	ID, PW	ID and PW that combined with other property for system, security
Flow	F2.2	User Info	User information for checking authority of the user

Element Type	No	Name	Description
Flow	F2.3	Result and Request command	After authority checking, result and request are provided to System file data store
Flow	F2.4	Web Page	After login, system file give web pages that can monitor and control
Flow	F2.5	IP List, State	IP address that are accessible to IP Camera or denied, Function to add, remove, modify
Flow	F2.6	Bootloader	Bootloader of Firmware file
Flow	F2.7	System data	System data for specific function
Flow	F2.8	File System	File system of Firmware file
Flow	F3.1	Video Stream	Raw Video frame from System files
Flow	F3.2	Video Stream	Video stream which modified with transfer protocol
Flow	F4.1	Web Page for Admin	A web page for administrator, it has both monitor and control functions for the IP camera system
Flow	F4.2	Web Page for User	A web page for users, it has only functions for monitoring

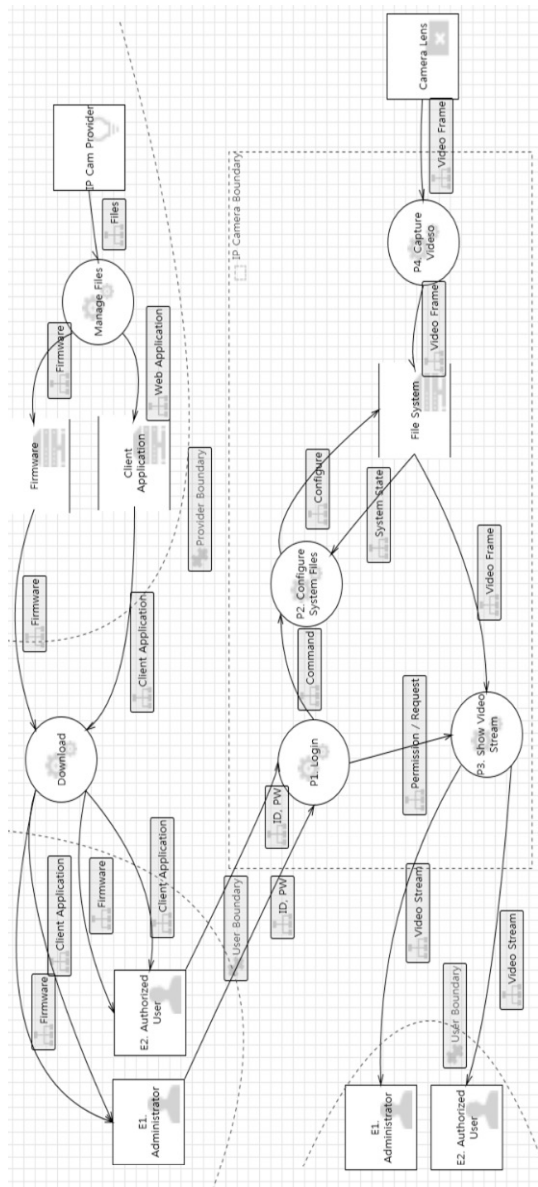


Fig. 2. IP Camera Level0 Data Flow Diagram

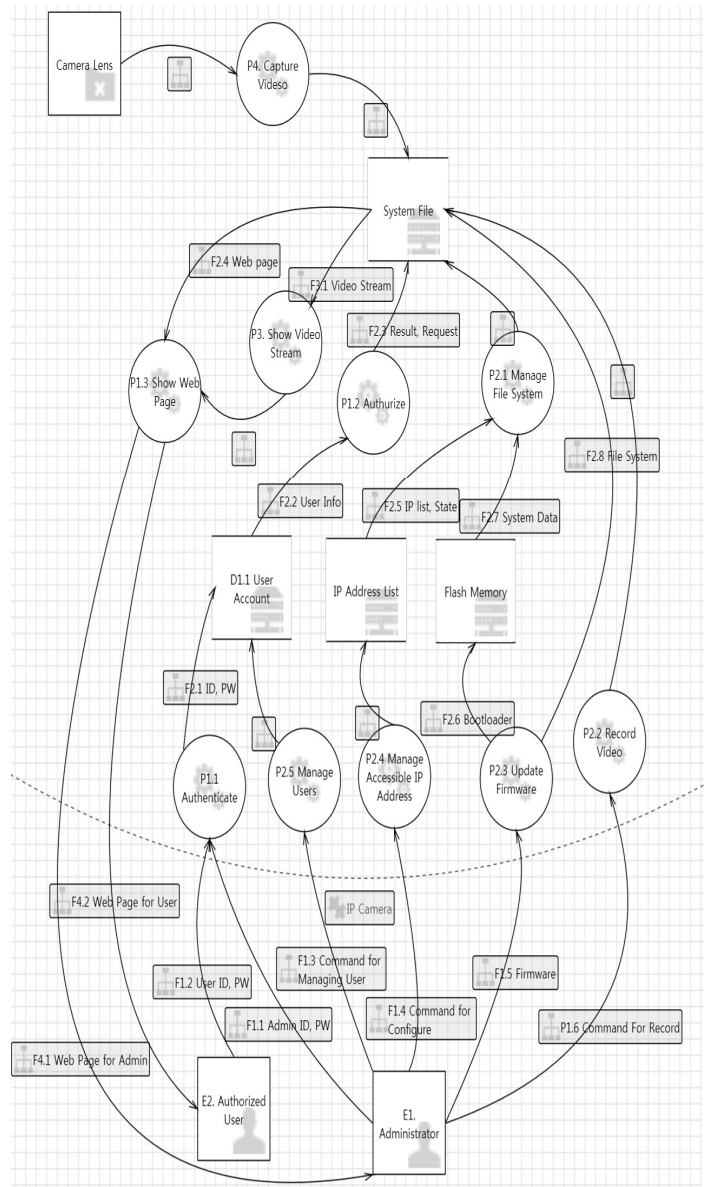


Fig. 3. IP Camera Level1 Data Flow Diagram

3.2 STRIDE를 이용한 위협 식별

IP Camera 분석 범위, 기능, 데이터 흐름을 나타낸 DFD를 바탕으로 Process, Data Flow, Data Store, External Entity와 같은 DFD Element에 존재하는 보안위협을 식별한다.

본 논문에서는 Microsoft에서 개발한 보안위협모델링 방법인 STRIDE를 사용하여 보안위협을 식별하였다. STRIDE를 보안위협식별을 위한 방법으로 선택한 이유는 Authentication, Integrity, Non-repudiation, Confidentiality, Availability, Authorization과 같은 보안 속성을 고려한 위협식별 방법이고 DFD와 연계하여 효과적인 위협분석이 가능하기 때문이다. 본 논문에서는 IP Camera Level 1 DFD에 STRIDE per

Element 방법을 적용하여 총 136개의 보안위협을 식별하였다. 다음 Table 5는 IP Camera Level 1 DFD에서 STRIDE를 이용한 위협 식별 결과 일부를 나타낸다.

IP Camera Level 1 DFD의 모든 Element에 대해 STRIDE per Element 방식을 적용하여 위협을 식별한 결과 총 136개의 보안위협이 식별 되었지만 이는 보안위협을 단순 열거한 것에 불과하다. 따라서 식별한 보안위협이 앞서 설정한 공격자의 공격목표를 달성하는데 어떻게 적용될 수 있는지 체계화시켜야 한다. 본 논문에서는 Attack Library와 Attack Tree를 이용하여 식별한 보안위협을 체계화하여 공격 목표 달성에 영향을 끼치는 보안위협을 도출하였다.

Table 5. STRIDE per Element for IP Camera Level 1 DFD

Element Type	No	Name	STRIDE	Threat Description	Threat No
Entity	E1	Administrator	S	Threats to non-administrator claim that he/she is an admin	T1
			R	Attacker deny his/her access try or access	T2
Entity	E2	Authorized User	S	Attacker pretend that he/she is an authorized user	T3
			R	Attacker deny his/her access try or access	T4
Process	P1.1	Authenticate	S	Attacker make fake login page and wait	T5
			S	ARP Spoofing, IP Spoofing, DNS Spoofing, IP redirection	T6
			T	Tampering authentication parameters	T7
			R	Attacker repudiate sniffing authentication parameter	T8
			I	Input parameter for Authentication can be disclosed	T9
			I	Any parameter added to Input parameter for authentication can be disclosed	T10
			I	Sensitive information can be disclosed by error message	T11
			D	Attacker can make login function lock by trying and exceeding available number of login attempt	T12
			D	Attacker can make access login page impossible.	T13
			E	Attacker can access to admin page by using non-admin user authentication parameter	T14
			E	Attacker can access to specific page by bypassing authentication and entering well-known page name	T15
Process	P1.2	Authorize	S	Non-admin users can admin authority by pretending his/her parameters are for admin	T16
			T	Attacker can modify the result of authentication	T17
			R	Attacker deny that he/she got the authentication result of P1.1	T18
			I	Authentication result can be disclosed	T19
			I	Authorization result can be disclosed	T20
			D	Attacker can make authentication and authorization functions impossible	T21
Process	P1.3	Show Web Page	E	Threats that assign higher authorization level than normal level	T22
			S	Threats that make fake login page and print it	T23
			T	Threats that tamper the login result or web page	T24
			R	Threats that deny result of login or trying to login	T25
			I	Threats that unauthorized web pages are exposed to attacker	T26
			I	Threats that sensitive server information is disclosed to attacker	T27
			D	Threats that Admin/User can not access web pages after login	T28
			E	Threats that user can access web pages for admin only	T29

Element Type	No	Name	STRIDE	Threat Description	Threat No
Process	P2.1	Manage File Systems	S	Threats that attacker's malicious file systems can be used as normal file systems	T30
			T	Threats that tamper normal file systems	T31
			R	Threats that repudiate malicious activities such as unauthorized access, tampering	T32
			I	Threats that important file or information of system are exposed	T33
			D	Threats that make it impossible to access, execute file in the system	T34
			E	Threats that access files which are assigned higher authorization level than users assigned.	T35
Process	P2.2	Record video	S	Threats that attacker can make fake video frames or files and transport them to users	T36
			T	Threats that tamper recording configurations	T37
			I	Threats that recording data or recording configurations are exposed	T38
			D	Threats that make it impossible to record	T39
중략					
Flow	F4.2	Web Page for User	T	Threats that tamper user's pages	T134
			I	Threats that user's pages are exposed	T135
			D	Threats that make it impossible to transport user's web pages	T136

3.3 Attack Library 수집 및 구축

STRIDE를 통해 식별한 보안위협은 추상적으로 작성되어 다른 위협들과 연관 지어 공격자의 공격 목표 달성을 위한 Attack Tree의 체계적인 적용 및 구성이 어렵다. Attack Library는 STRIDE로 식별된 보안위협을 구체화하고 올바르게 보안위협을 식별했는지 판단할 수 있는 근거를 제시하는 역할을 한다. 이를 위해 다양한 자료를 수집하여 Attack Library를 제작할 수 있으며 본 논문에서는 IP Camera, CCTV, Embedded System과 관련된 논문과 신뢰할 수 있

는 저자 또는 기관의 기술보고서, 저명한 해킹·보안 컨퍼런스의 발표, 공신력 있는 공격 패턴, 약점, 취약점 데이터베이스, IP Camera와 관련된 표준을 수집하여 제작하였다. 다음 Table 6은 IP Camera의 Attack Library로 완전한 Attack Library는 본 논문의 부록으로 작성하였다.

구축한 Attack Library를 활용하여 Attack Tree를 작성할 경우 구체화 시키는 장점 외에도 현재까지 알려진 가능한 모든 약점, 취약점, 공격 패턴을 반영할 수 있는 장점이 있다.

Table 6. Attack Library for IP Camera

Type	Category	Title	Author
Paper	Firmware	Embedded Devices Security and Firmware Reverse Engineering	Jonas Zaddach
	Firmware	When Firmware modification attack: A Case study of embedded Exploitation	A Cui
	Firmware	When Firmware modification attack: A Case study of embedded Exploitation	Ang Cui,
	File System	Reverse Engineering a CCTV system, a case study	Lee Tobin
	File System	Analysis of CCTV digital video recorder hard disk storage system	N.R. Poole
	File System	Forensic imaging of embedded systems using JTAG(boundary-scan)	Ing,M.F. Breeunsmma
	File System	Case Study: Forensic analysis of a Samsung digital video recorder	Wouter S. van Dongen
	File System	Digital Camcorder Forensics	Aswami Ariffin
	All	Design and Implementation of an IP-Based Security Surveillance System	Cletus O.Ohaneme

Type	Category	Title	Author
Technical Report	Hardware	Reverse Engineering Serial ports	Craig
	Hardware	Hacking Embedded Devices : UART Consoles	MWR LABS
	Flash Memory	Reverse Engineering Flash Memory for Fun and Benefit	Jeong Wook Oh
Conference	중략		
Public Program or Project	All	Validating Security Configuration and Detecting in New Network Devices	
	Attack Pattern	CAPEC - Mechanisms of Attack	MITRE
	Weakness	CWE - Fault Pattern Cluster	MITRE
	All	Embedded Application Security	OWASP
Standard	IP-based surveillance	ONVIF(Open Network Video Interface Forum) - Security Recommendations	ONVIF
	Network	RTSP(Real Time Streaming Protocol) - RFC 2326	IETF
	Network	RTP : A Transport Protocol for Real-Time Applications - RFC 3550	IETF
	IP-based surveillance	PSIA(Physical Security Interoperability Alliance)	PSIA

3.4 Attack Tree 작성

STRIDE를 통해 도출한 위협과 공격자의 공격 목표 달성을 위한 방법과의 연관성을 파악하고 체계화하기 위해 Attack Tree를 작성하였다. IP Camera 공격자의 공격 목표에 대한 Attack Tree 그림은 크기와 양 제한으로 인해 부록에 별도로 첨부하였다. Attack Tree를 글로 나타낼 경우 다음 Table 7과 같이 나타낼 수 있으며 STRIDE에서 도출한

위협을 함께 연결 지어 나타내었다.

Attack Tree를 작성한 결과 STRIDE를 통해 도출된 보안위협이 실제 공격자 공격 목표에 영향을 끼치는 보안위협이 될 수 있는지 확인할 수 있었다. 다음 4장에서는 3장에서 식별된 보안위협에 대응하기 위한 보안기능요구사항을 도출하는 과정에 대해 설명한다.

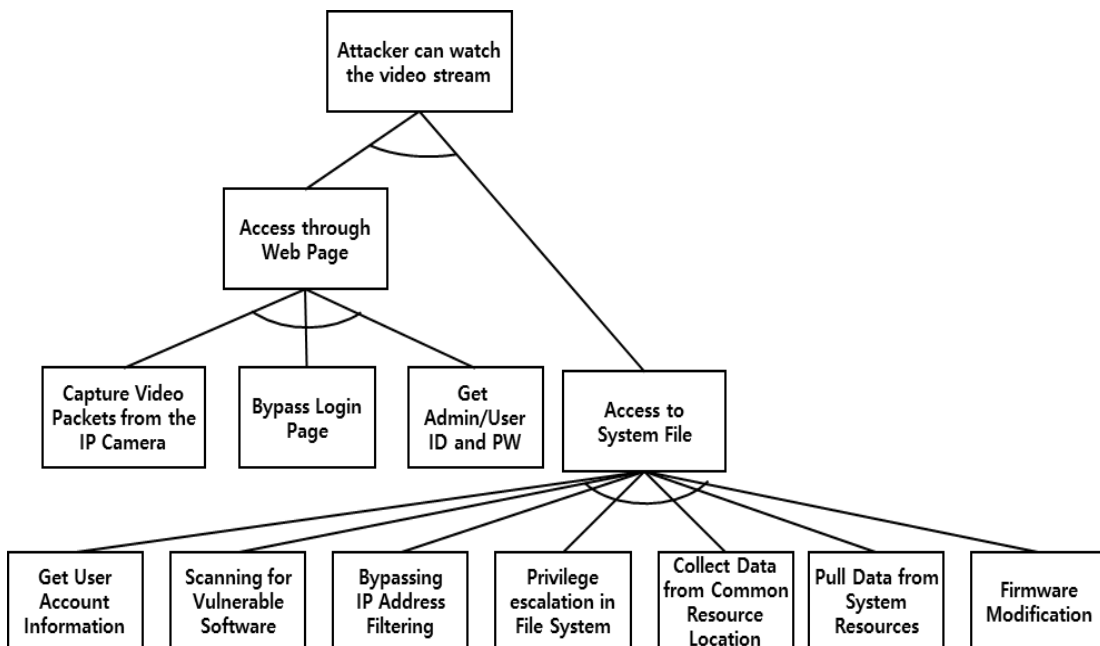


Fig. 4. Example of IP Camera Attack Tree

Table 7. Mapping Attack Tree and STRIDE threats

Attack Tree				Threats
1	Attacker can watch the video stream			
OR	1.1	Access through Web page		
	OR	1.1.1	Capture Video packets from the IP Camera	
		OR	1.1.1.1 Protocol Analysis	T9, T10, T11, T84, T87, T125, T126, T128, T129
	OR	1.1.2	Bypass Login page	
		OR	1.1.2.1 Authentication Abuse	T1, T2, T3, T4, T7, T13, T14,
		OR	1.1.2.2 Detect Unpublicized Web Pages	T15, T29, T110, T111, T131, T132,
		OR	1.1.2.3 Explore for Predictable Temporary File names	T134, T135
	OR	1.1.3	Get Admin/User ID and PW	
		OR	1.1.3.1 Get from Provider's Initial setting ID/PW	
		OR	1.1.3.2 Get information when Admin/User login	T1, T2, T3, T4, T5, T6, T9, T10,
		OR	1.1.3.3 Functionality Misuse	T11, T12, T16, T17, T18, T19, T20,
		OR	1.1.3.4 Guessing	T21, T22, T23, T24, T25, T26,
		OR	1.1.3.5 Query System for ID and PW	T27, T29, T90, T93
OR	1.2	Access to System File		
	OR	1.2.1	Get User Account information	
		OR	1.2.1.1 Query System for ID and PW	T1, T2, T3, T4, T14, T54, T55,
		OR	1.2.1.2 Sniffing Network Traffic	T56, T57, T59, T60
		OR	1.2.1.2 Sniffing Network Traffic	T1, T2, T3, T4, T9, T10, T11,
		OR	1.2.1.2 Sniffing Network Traffic	T19, T20, T26, T27, T32
	OR	1.2.2	Scanning for Vulnerable Software	
	OR	1.2.3	Bypassing IP Address Filtering	
		OR	1.2.3.1 Input data manipulation	T49, T70, T71, T76, T83, T86,
		OR	1.2.3.2 Variable Manipulation	T92, T113
		OR	1.2.3.2 Variable Manipulation	T49, T70, T71, T76, T113
		OR	1.2.3.3 Configuration/Environment Manipulation	T49, T70, T71, T76, T113
		OR	1.2.3.4 Web Service Protocol Manipulation	T49, T70, T71, T76, T113
		OR	1.2.3.5 Accessing Functionality not properly constrained by ACL	T49, T70, T71, T76, T113
	OR	1.2.4	Privilege escalation in file system	
		OR	1.2.4.1 Target Programs with elevated privileges	T29, T35, T47, T52, T53
	OR	1.2.5	Collect Data from Common Resource Locations	
		OR	1.2.5.1 Detect Unpublicized Web services	T30, T36, T37
		OR	1.2.5.2 Access Flash memory	T30, T31, T32, T33, T35
	OR	1.2.6	Pull Data from System resources	
		OR	1.2.5.2 Access Flash memory	T30, T31, T32, T33, T35
	OR	1.2.7	Firmware modification	
		OR	1.2.5.2 Access Flash memory	T30, T31, T32, T33, T35
		OR	1.2.7.2 Update with modified firmware	T40, T41, T42, T43, T44, T47, T116,
		OR	1.2.7.2 Update with modified firmware	T117, T119, T120, T122, T123
Attack Tree				Threats
2	Attacker can control IP Camera system			
중략				
3	Attacker can perform denial of service attack			
OR	3.1	Access to System file		
	OR	3.1.1	Firmware modification	
		OR	3.1.1.1 Update with modified firmware	T45, T46, T52, T58, T64,

4. IP Camera 보안기능요구사항 도출

본 장에서는 3장에서 단계별 방법론 적용을 통해 도출한 보안위협에 대응하는 보안기능요구사항을 국제표준인 공통 평가기준 (Common Criteria, 이하 CC) 형식에 맞춰 도출한다. 첫 번째로 3장에서 식별한 보안위협 내용을 활용하여 보안문제를 정의하고 두 번째로 정의한 보안문제에 대응하는 보안목적을 정의하여 마지막으로 보안기능요구사항을 도출한다.

4.1 보안문제 정의

CC에서 보안문제(Security Problem)란 평가대상에서 다루려는 보안 특징 및 범위를 정의한 정형화된 방식의 표현을 의미하며 대응할 위협, 보안정책, 가정 사항을 포함한다.

1) 위협

3장의 STRIDE 및 Attack Tree에서 도출한 발생할 수 있는 위협을 위협원, 자산, 악의적 행동의 관점을 고려하여 다음 Table 8과 같이 정리하였다.

Table 8. Threat in Security Problem

Category	Threat	Attack Tree Node
Unauthorized Access	T.Replay	1.1.1.1, 1.1.3.2, 1.2.1.2, 1.2.3.1~1.2.3.4
	T.Weak_Password	1.1.3.1, 1.1.3.4, 3.1.3.1
	T.Admin_Session_Hijack	1.1.1.1, 1.1.1.2, 1.1.3.2
	T.Retry_Auth_Attempt	1.1.3.2~1.1.3.5
	T.Impersonation	1.1.3.2, 1.2.7.2
Traffic Bypass	T.Traffic_Bypass	1.1.2.1, 1.1.2.3
Information Disclosure	T.Transmission_Disclose	1.1.1.1, 1.1.2.1, 1.1.3.2, 1.2.3.1~1.2.3.5, 1.2.4.1
	T.Stored_Data_Damage	1.1.2.2, 1.1.2.3, 1.2.4.1, 1.2.5.1, 1.2.5.2, 3.1.4
	T.Untrusted_Path	1.1.1.1, 1.1.2.1, 1.1.3.2, 1.2.3.1~1.2.3.5, 3.1.2.1~3.1.2.5
	T.Weak_Crypto_Protocol	1.1.1.1, 1.1.2.1, 1.1.3.2, 1.2.3.1~1.2.3.5,
Compromise	T.TSF_COMPROMISE	1.2.4.1, 1.2.5.2, 1.2.7.1, 3.1.4
	T.Modified_Update	1.2.7.1
Function Bypass	T.Traffic_Control_Bypass	1.2.3.1~1.2.3.5
Network Service Disability	T.Exhaustsed_Resource	3.1.2.1~3.1.2.5, 3.1.4
	T.Service_Unavailable	3.1.2.1~3.1.2.5, 3.1.4

2) 조직의 보안정책

조직의 보안정책에는 IP Camera를 운영하는데 관련된 모든 요소들의 보안규칙, 절차, 지침을 고려하여 작성하며 Table 9와 같이 작성하였다.

Table 9. Organization Security Policy

Category	Policy
Organization Security Policy	P.Correct_Operation
	P.Audit
	P.Cleartext_Transmission
	P.Confidentiality
	P.Crypto_Strength

4.2 보안목적

보안목적은 보안문제에 서술된 문제에 대한 해결책을 간결하고 추상적인 문장으로 표현한 것을 의미한다. 보안목적은 4.1에서 정의한 위협, 조직의 보안정책에 대해 완전하고 추적 가능해야 한다. 따라서 Table 10과 같이 위협 및 보안정책에 대응하는 보안목적 표를 작성하여 식별된 위협 및 보안정책이 모두 다 보안목적에 대응하는지 확인하여 완전성과 추적성을 만족함을 확인했다. 보안목적은 Object의 앞 글자를 이용하여 'O.보안목적', 운영환경에 대한 보안목적은 'OE.보안목적'으로 나타낸다. 다음은 각 보안목적에 대한 설명이다.

- 1) O.Traffic_Control : 정보흐름 통제를 나타내는 보안목적으로 통신상대간의 정보흐름을 증쇄해야 한다.
- 2) O.Abnormal_Packet_Block : IP Camera는 IP Camera에 전달되는 비정상 패킷에 대해 차단해야 한다.
- 3) O.I&A : IP Camera에 접속하거나 기능을 수행하려는 경우 인가된 사용자를 유일하게 식별하고 안전하게 인증해야 한다.
- 4) O.Password_Management : IP Camera는 인가된 사용자의 패스워드를 보호하고 관리할 수 있는 수단을 제공해야 한다.
- 5) O.Session_Control : 접속과 관련된 정보에 근거하여 세션을 통제 및 관리하고, 인가된 사용자 세션을 통해 전송되는 데이터를 보호해야 한다.
- 6) O.Security_Management : IP Camera는 보안기능 및 보안기능과 관련된 데이터를 관리하는 방안을 제공하고 이에 대한 접근 및 설정을 인가된 관리자로 제한해야 한다.
- 7) O.Audit : IP Camera의 보안관련 모든 행위에 대한 추적이 가능하도록 사건을 기록 및 유지해야 하며 이를 검토할 수 있는 수단을 제공해야 한다.
- 8) O.Update : IP Camera는 현재 버전을 확인할 수 있는 기능을 제공하고 업데이트 시 업데이트 파일에 대한 유효성을 검증해야 한다.
- 9) O.Stored_Data_Protection : IP Camera의 데이터는 인가되지 변경 또는 유출로부터 보호되어야 한다.
- 10) O.Self_Protection : IP Camera 구동 시 하드웨어 및 주요 보안기능에 대한 정상동작 여부를 시험해야 하고 인가된 관리자가 시험결과를 확인할 수 있어야 한다.
- 11) O.Key_Management : IP Camera는 암호화에 사용되는 키를 안전하게 생성, 분배, 파괴해야 하고, 마스터키의 인가되지 않은 노출, 변경, 삭제로부터 보호해야 한다.
- 12) O.Admin_Role_Control : IP Camera의 사용자 역할을 관리자 및 일반 사용자로 구분하여 역할에 따른 보안정책 및 보안기능을 제공해야 한다.

Table 10. Security Problems and Security Objective Mapping table

		O. Traffic Control	O. Abnormal Packet Block	O. I & A	O. Password Management	O. Session Control	O. Security Management	O. Audit	O. Update	O. Stored Data Protection	O. Self Protection	O. Key Management	O. Admin Role Control	O. Data Protection	O. DoS Protect	OE. Trusted Admin	OE. Patch Management	OE. Log Backup
Unauthorized Access	T.Replay			X														
	T.Weak_Password			X	X													
	T.Admin_Session_Hijack					X												
	T.Retry_Auth_Attempt			X														
	T.Impersonation			X														
Traffic Bypass	T.Traffic_Bypass		X															
Information Disclosure	T.Transmission_Disclose					X								X				
	T.Stored_Data_Damage									X				X				
	T.Untrusted_Path					X												
	T.Weak_Crypto_Protocol					X				X	X			X				
Compromise	T.TSF_COMPROMISE			X		X				X		X	X	X				
	T.Modified_Update								X	X						X	X	
Function Bypass	T.Traffic_Control_Bypass	X																
Network Service Disability	T.Exhausted_Resource		X												X			
	T.Service_Unavailable														X			
Organization Security Policy	P.Correct_Operation			X		X		X	X	X			X			X	X	
	P.Audit							X										X
	P.Cleartext_Transmission	X																
	P.Confidentiality	X																
	P.Crypto_Strength					X								X				

- 13) O.Data_Protection : IP Camera는 저장 및 전송 데이터에 대해 인가되지 않은 노출 또는 변경으로부터 보호해야 한다.
- 14) O.DoS_Protect : IP Camera는 네트워크를 통한 서비스 거부 공격 시 IP Camera를 데이터를 보호할 수 있는 적절한 대응책을 마련해야 한다.
- 15) OE.Trusted_Admin : IP Camera 관리자는 IP Camera의 기능에 대해 잘 알고 있으며 관리규정에 따라 운영한다.
- 16) OE.Patch_Management : IP Camera 관리자는 검증된 펌웨어 및 소프트웨어에 대한 최신 패치를 정기적으로 적용하고 패치 이후 기존에 설정한 보안 서비스의 정상 동작 여부를 확인한다.
- 17) OE.Log_Backup : IP Camera 관리자는 감사 기록 저장소의 여유 공간을 주기적으로 확인하고 감사기록 백업을 수행한다.

4.3 보안기능요구사항

4.2에서 도출된 보안목적에 대해 보안목적을 만족시킬 수 있는 보안기능요구사항을 도출한다. 마찬가지로 보안기능요구사항을 도출할 때 4.2의 보안목적과의 추적성을 고려하여야 하며 CC 1부를 참고하여 다음과 같은 사항을 고려하였다.

- a) 각 보안기능요구사항은 적어도 하나의 보안목적으로 추적
- b) 각 보안목적은 최소한 하나의 보안기능요구사항으로 추적

다음 Table 11은 4.2에 도출한 보안목적에 대응하는 보안기능요구사항 목록이며 상세한 결과는 [36]에 작성된 내용을 참고한다.

Table 11. Security Functional Requirements

Class	Component
Security Audit	FAU_ARP.1, FAU_GEN.1, FAU_GEN.2, FAU_SAA.1, FAU_SAR.1, FAU_SAR.2, FAU_SAR.3, FAU_STG.2, FAU_STG.4
Communication	FCO_NRO.1, FCO_NRR.1
Cryptographic Support	FCS_CKM.1, FCS_CKM.2, FCS_CKM.3, FCS_CKM.4, FCS_COP.1
User Data Protection	FDP_ACC.1, FDP_ACF.1, FDP_IFC.1, FDP_IFF.1, FDP_ITC.1, FDP_ITC.2, FDP_ITT.1, FDP_ROL.1, FDP_SDL.1, FDP_UCT.1, FDP_UIT.1
Identification and Authentication	FIA_AFL.1, FIA_ATD.1, FIA_SOS.1, FIA_SOS.2, FIA_UAU.1, FIA_UAU.2, FIA_UAU.3, FIA_UAU.4, FIA_UAU.7, FIA_UID.1, FIA_UID.2, FIA_USB.1
Security Management	FMT_MOF.1, FMT_MSA.1, FMT_MSA.3, FMT_MTD.1, FMT_REV.1, FMT_SMF.1, FMT_SMR.1
Protection of the TSF	FPT_FLS.1, FPT_ITA.1, FPT_ITC.1, FPT_ITL.1, FPT_ITT.1, FPT_RCV.2, FPT_STM.1, FPT_TST.1
Resource Utilization	FRU_RSA.1
TOE Access	FTA_MCS.2, FTA_SSL.1, FTA_SSL.3
Trusted Path/Channels	FTP_ITC.1, FTP_TRP.1

5. 결 론

보안기능요구사항 도출에 관한 국내 관련 연구에는 분석 범위의 완전성과 내용의 추적성을 보장하고, 현재까지 알려진 모든 약점, 취약점을 반영한 체계적인 보안위협모델링에 대한 연구가 없었다. 이에 본 논문에서는 IP Camera를 대상으로 보안위협모델링을 통해 체계적인 보안기능 요구사항을 도출하는 과정을 설명하였다. 또한 본 논문에서 도출한 보안기능요구사항은 정확성과 활용성, 객관적인 의미 전달을 위해 주관적인 표현 방법이 아닌 국제 표준제도에서 활용하는 분류, 표현 방법을 활용하였다.

암호 알고리즘, 로그인 시도 횟수, 무결성 검사 방법과 같은 보안기능요구사항에 대한 세부적인 내용은 IP Camera 특성에 따라 다르게 구현할 수 있다. 따라서 IP Camera 제조사들은 본 논문의 보안기능요구사항을 활용하여 자사의 제품에 알맞은 보안기능을 구현할 수 있는 체크리스트 제작이 가능할 것으로 판단된다. 또한 본 논문에서 제시하는 분석 과정을 다른 대상에 활용할 경우 마찬가지로 분석의 완전성과 추적성을 만족하는 결과를 얻을 수 있을 것으로 보인다. 하지만 본 논문은 요구사항을 도출하는 과정에 다양한 이해관계자들의 참여가 제한되었으며 추후 보안에 대한 전문적인 지식이 없는 이해관계자들도 함께 참여하여 진행할 수 있는 보안기능요구사항 도출에 관한 연구가 향후 과제로 남아있다.

References

- [1] Microsoft, Security Development Lifecycle [Internet], <https://www.microsoft.com/en-us/sdl/>.
- [2] Cisco, Cisco Secure Development Lifecycle(SDL) [Internet], <http://www.cisco.com/c/en/us/about/security-center/security-programs/secure-development-lifecycle.html>.
- [3] VMware, VMware Security Development Lifecycle [Internet], <http://www.vmware.com/security/sdl.html>.
- [4] OWASP, OWASP Secure Development Lifecycle Cheat Sheet [Internet], https://www.owasp.org/index.php/Secure_SDLC_Cheat_Sheet.
- [5] Guttorm Sindre and Andreas L. Opdahl, "Capturing Security Requirements through Misuse Cases," in *Proceedings of the Norsk Informatikkonferanse*, Bergen, 2001.
- [6] Guttorm Sindre and Andreas L. Opdahl, "Eliciting security requirements with misuse cases," *Requirements Engineering*, Vol.10, Issue 1, pp.34-44, 2005.
- [7] Edward G. Amosoro, "Fundamentals of computer security technology," AT&T Bell labs, 1994.
- [8] Chris Salter, O. Sami Saydjari, Bruce Schneier, and Jim Wlner, "Toward A Secure System Engineering Methodology," in *Proceedings of the 1998 Workshop on New Security Paradigms*, pp.2-10, 1998.
- [9] Bruce Schneier, Attack Trees [Internet], https://www.schneier.com/academic/archives/1999/12/attack_trees.html.
- [10] Adam Shostack, "Experiences Threat Modeling at Microsoft," Microsoft, 2008.
- [11] Microsoft, Microsoft Threat Modeling Tool 2016 [Internet], <https://www.microsoft.com/en-us/download/details.aspx?id=49168>.
- [12] DistriNet Research Group, LINDDUN [Internet], <https://distri-net.cs.kuleuven.be/software/linddun/contributors.php>.
- [13] CERT, Software Engineering Institute, Carnegie Mellon University, OCTAVE [Internet], <http://www.cert.org/resilience/products-services/octave/>.
- [14] Octotrike, Trike [Internet], <http://octotrike.org/home.shtml>.
- [15] Tony UcedaVelez, "Real World Threat Modeling using the PASTA Methodology," in *Proceedings of OWASP AppSec Research 2012*, Athens, 2012.
- [16] OWASP, Threat Risk Modeling [Internet], https://www.owasp.org/index.php/Threat_Risk_Modeling.
- [17] Donn B. Parker, "Our Excessively Simplistic Information Security Model and How to Fix it," *ISSA Journal of Requirements Engineering*, Springer-Verlag, 2010.
- [18] Shostack, Adam, Threat Modeling: Designing for Security," John Wiley & Sons, 2014.
- [19] Aaron Marback, Hyunsook Do, Ke He, Samuel Kondamarri, and Dianxiang Xu, "Security Test Generation using Threat Trees," in *Proceedings of Automation of Software Test on ICSE Workshop*, 2009.
- [20] Inger Anne Tondel, Jostein Jensen, Lillian Rostad, "Combining misuse cases with attack trees and security activity models," in *Availability, Reliability, and Security on ARES'10 International Conference*, 2010.
- [21] Goncalo Martins, Sajal Bhatia, Xenofon Koutsoukos, Keith Stouffer, CheeYee Tang, and Richard Candell, "Toward a Systematic Treat Modelling Approach for Cyber-Physical Systems," in *Proceedings of National Symposium on Resilient Critical Infrastructure*, Philadelphia, 2015.
- [22] Dr. Marnix Dekker and Dr.Giles Hogben, "Appstore security - 5 lines of defence against malware," European Network and Information Security Agency(ENISA), 2011.
- [23] Tong Xin and Ban Xiaofang, "Online Banking Security Analysis based on STRIDE Threat Model," *International Journal of Security and its Applications* 8, pp.271-282, 2014.
- [24] Anthony Hadding, and Dr. J. Zalewski, "Threat Modeling in Embedded Systems," Dissertation, Florida Gulf Coast University, 2012.
- [25] Kristian Beckers, Stephan Fabbender, Maritta Heisel, and Santiago Suppan, "A Threat Analysis Methodology for Smart Home Scenarios, Technical Report," in *Proceeding of the International Workshop on Smart Grid Security*, Munich, pp.94-124, 2014.
- [26] Anton Bretting and Mei Ha, "Vehicle Control Unit Security using Open Source AUTOSAR," M.S. disseration, University of Gothenburg, Gothenburg, Sweden, 2015.

- [27] Katrina Mansfield, Timothy Eveleigh, Thomas H. Holzer, and Shahryar Sarkani, "DoD Comprehensive Military Unmanned Aerial Vehicle Smart Device Ground Control Station Threat Modeling," Defense ARJ, USA, 2015.
- [28] Mark Yampolskiy, Peter Horvath, Xenofon D. Koutsoukos, Yuan Xue, and Janos Sztipanovits, "Systematic Analysis of Cyber-Attacks on CPS-Evaluating Applicability of DFD-based Approach," in *Proceedings of the International Symposium on Resilient Control System*, Salt Lake City, pp.55-62, 2012.
- [29] Cletus O. Ohaneme, James Eke, Augustine C. O. Azubogu, Emmanuel N. Ifeagwu, and Louisa C. Ohaneme, "Design and Implementation of an IP-Based Security Surveillance System," *International Journal of Computer Science Issues*, Vol.9, No.5, Sept., 2012.
- [30] Craig Heffner, "Exploiting Surveillance cameras, Like a Hollywood Hacker," Tactical Network Solutions, 2013.
- [31] Sergey Shekryan and Artem Hartutyunyan, "Watching the watchers: hacking wireless IP Security Cameras," Shape Security and Qualys Inc., 2013.
- [32] Fransico Falcon, Nahuel Riva, Do you know who's watching you? An in-depth examination of IP Camera attack surface [Internet], <https://www.coresecurity.com/corelabs-research/publications/examination-ip-cameras-attack-surface-ekoparty2013>.
- [33] Lee Tobin, "Reverse Engineering a CCTV system, A case study," *Digital Investigation*, Vol.11, No.3, pp.179-186, 2014.
- [34] Red ALert, SysSec Lab, "Security threat report Foreign-made CCTV, IP-Camera," NSHC and KAIST, 2015.
- [35] CCMB, "Common Criteria for Information Technology Security Evaluation - Part 1 : Introduction and general model," Version 3.1 Revision 4, CCRA, 2012.
- [36] CCMB, "Common Criteria for Information Technology Security Evaluation - Part 2 : Security functional components," Version 3.1 Revision 4, CCRA, 2012.
- [37] James Ransome and Anmol Misra, "Core Software Security, Security at the source," CRC Press, 2013.
- [38] Jae-ki Kim, Jeong-Hoon Shin, and Seung-joo Kim, "Study on the Femtocell Vulnerability Analysis Using Threat Modeling," *The KIPS Tr. Comp. and Comm. Sys.* Vol.5, No.8 pp.197-210, 2016.
- [39] Suvda Myagmar, Adam J.Lee, William Yurcik, "Threat Modeling as a Basis for Security Requirements," in *Symposium on Requirements Engineering for Information Security*, Pittsburgh, 2005.
- [40] Vineet Saini, Qiang Duan, Vamsi Paruchuri, "Threat Modeling Using Attack Tree," *Journal of Computing Science in Colleges*, Vol.23, Issue 4, pp.124-131, 2008.
- [41] Steven F Burns, "Threat Modeling: A Process to Ensure Application Security," OWSP, 2005.
- [42] Caroline Mockel and Ali E. Abdallah, "Threat modeling approaches and tools for securing architectural designs of an E-banking application," in *Proceedings of the Information Assurance and Security*, pp.149-154, 2010.
- [43] Sathya Prakash Kadhivelan and Andrew Soderberg-Rivkin, "Threat Modelling and Risk Assessment within Vehicular Systems," M.S. dissertation, Chalmers University of Technology, Goteborg, Germany, 2014.
- [44] Jia Di and Scott Smith, "A Hardware Threat Modeling Concept for Trustable Integrated Circuits," in *Proceedings of the Region 5 Technical Conference*, 2007.
- [45] Marwan Abi-Antoun, Daniel Wang, and Peter Torr, "Checking Treat Modeling Data Flow Diagrams for Implementation Conformance and Security," in *Proceeding of the International conference on Automated Software Engineering*, pp.393-396, 2007.
- [46] ITSCC, "Supporting Document for Korean National Protection Profile for Network Device," V1.0, 2016.
- [47] ITSCC, "Supporting Document for Korean National Protection Profile for Virtual Private Network", V1.0, 2016.
- [48] ITSCC, "Supporting Document for Koeran National Protection Profile for Firewall", V1.0, 2016.



박 지 수

e-mail : jisoo8881@korea.ac.kr
 2015년 동국대학교 컴퓨터공학과(학사)
 2015년~현 재 고려대학교 정보보호
 대학원 정보보호학과 석사과정
 관심분야 : Information Assurance,
 Common Criteria, Threat
 Modeling



김 승 주

e-mail : skim71@korea.ac.kr
 1994년 성균관대학교 정보공학과(학사)
 1996년 성균관대학교 정보보호학과(석사)
 1999년 성균관대학교 정보보호학과(박사)
 1998년~2004년 KISA 팀장
 (舊한국정보보호진흥원)
 2004년~2011년 성균관대학교 정보통신공학부 조교수, 부교수
 2011년~현 재 고려대학교 사이버국방학과/정보보호대학원
 정교수
 관심분야 : Security Engineering, Security Threat-Risk
 Modeling, Security Testing, Security Evaluation,
 Usable Security