CCTV 유효성 검증 시스템

김현우[O], 박재경[*], 안명진[**]
[O]성균관 정보통신 대학원
[*]한국 폴리텍 대학
[**]성균관 정보통신 대학원
e-mail: babisss@skku.edu[O], jakypark@kopo.ac.kr[*], xovudch@naver.com[**]

CCTV validation System

Hyun-Woo Kim[O], Jae-Kyung Park[*], Myung Jin An[**]
[O]Graduate School of Information Communication, Sungkyunkwan University
[*]Korea Polytechnic University
[**]Graduate School of Information Communication, Sungkyunkwan University

● 요 약 ●

최근 방범 및 보안등의 이유로 CCTV는 그 수를 판단할 수 없을 정도로 빠르게 늘어나고 있다. 네트워크의 발전으로 인해 동축 케이블에서 IP를 이용한 CCTV로 발전되었으며 이는 사업체,주택 등 다양한 곳에서 사용되고 있다. 그에 따라 IP를 기반으로 한 다양한 위협에 노출이 되고 있으며 이를 해결하기 위해 공공기관 및 업체에서도 활발히 연구가 진행되고 있다. 본 논문에서는 IP 기반 CCTV의 위협을 방지하기 위하여 시그니쳐 기법을 통한 검증 시스템을 제안한다.

키워드: 위협(Threat) ,탐지(Detection), 시그니쳐(Signature)

I. 서 론

최근 CCTV의 보급 및 발전은 갈수록 진행되고 있으며 그에 따라 악의적인 행위도 늘어나고 있다. 특히 저 전력, 저 비용 및 소형화 CCTV의 증감함에 따라 개인 정보 유출 및 시스템 공격 피해사례가 갈수록 증가하고 있으며, 해당 위협에 대비하기 위해 CCTV를 보안할 수 있는 다양한 방법이 주목 받고 있다. 이에 따라 본 논문에서는 CCTV의 인증 및 상태를 검사할 수 있는 탐지 시스템을 제안하고자 한다. 시스템은 기존 모니터링 시스템과 달리 시그니쳐 기반의 인증뿐만 아니라 랜덤한 nonce 값을 이용하여 재전송 공격에 대응하여 CCTV를 통해 기업 내부 공격을 미연에 방지할 수 있게 하였다

II. 관련 연구

공격자의 악의적인 행위는 다양한 방법으로 진화되고 있으며 그에 따라 물리적 보안 기술인 CCTV의 중요성은 갈수록 커지고 있다. CCTV는 실시간 녹화 및 사용자 검증에 대하여 사용이 되는데 공격자는 이런 부분을 우회하기 위해 CCTV 자체에 악성코드를 심거나 기기자체를 변조하여 악의적인 피해를 입힐 수 있다. 이러한 CCTV의 취약점을 보완하기 위하여 CCTV를 실시간 검증할 수 있는 자동화된 시스템이 요구되고 있다. 현재 네트워크 시스템을 검증하는 방법은 SYSLOG 및 SNMP 등의 모니터링 프로토콜이 있다. 하지만 기존 프로토콜에서 전해주는 정보는 CCTV 검증을 하기에는 한계가 있기 때문에 네트워크 정보 및 nonce 값을 이용한 CCTV 검증 시스템을 제안한다.

III. 본 론

CCTV 악성행위 탐지 시스템은 현재 사용하는 CCTV가 허가된 CCTV인지 유무를 탐지하는 장비이다. 본 장비는 실시간으로 CCTV와 통신을 수행하여 CCTV의 네트워크 정보를 확인하며 CCTV의 네트워크 정보를 토대로 시그니처를 생성하여 CCTV의 정상 유무를 판단한다. 또한 TCP/IP를 사용하는 CCTV를 대수에 상관없이 폴링 기법을 통하여 주기적으로 분석 및 탐지하여 CCTV를 통하여 내부로 들어오는 악성행위를 미연에 탐지한다.

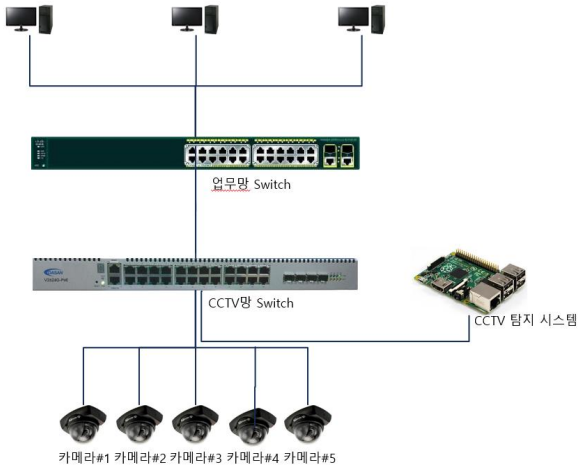


Fig. 1.CCTV 탐지 시스템 망 개념도

[그림1]은 CCTV 탐지 시스템 설치 시 망 개념도를 표현한다. 그림1은 L2 스위치를 통하여 CCTV와 같은 망에 설치되어 있지만 네트워크 통신이 가능하다면 라우팅을 통해서 CCTV와 다른 망에 설치가 되어도 무관하다. 악의적인 공격자는 기존 설치되어 있는 CCTV와 동일한 기종의 CCTV를 교체하여 내부로 접속할 수 있기 때문에 등록되어진 CCTV 검증을 통하여 실시간 악성행위를 탐지해야 한다.

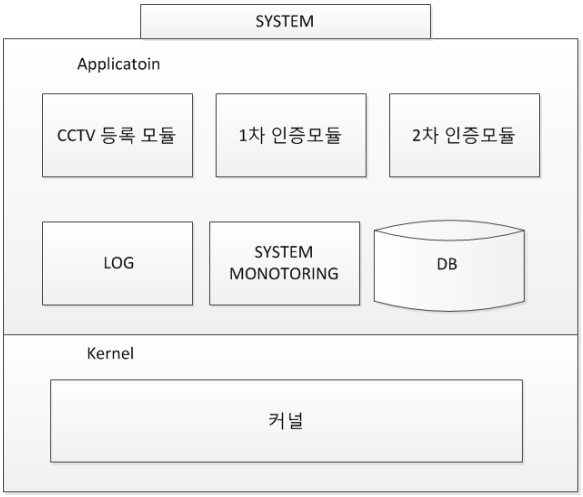


Fig. 2. 시스템 구성도

시스템은 [그림2]와 같이 구성되어 있다. CCTV 등록 모듈은 CCTV의 검증하기 위하여 사용하는 시그니처의 정보를 취합 및 해당 정보를 토대로 시그니처를 생성, DB에 저장한다.

1차 인증 모듈은 생성된 시그니처를 통하여 CCTV를 검사하는 모듈이며 2차 인증 모듈은 nonce를 통하여 CCTV의 허가유무를 검사한다.

Log 모듈은 각각의 모듈에 발생된 로그를 취합하여 저장하는 기능을 수행하며 시스템 모니터링은 주기적으로 시스템의 상태를 검사하여 이상현상 시 이벤트를 발생 시킨다.

3.1 CCTV 등록모듈

CCTV 등록 모듈은 1차 검사와 2차 검사를 수행하기 위하여 사용자가 정보를 입력 및 해당 입력을 토대로 검사를 수행하기 위한 값을 도출하는 기능을 수행한다.

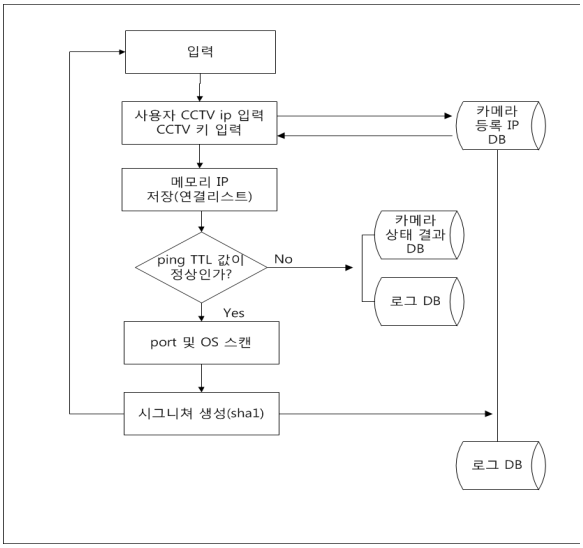


Fig. 3. CCTV 등록모듈 절차도

사용자는 허가된 CCTV를 등록하기 위하여 ip 주소와 mac주소를 입력한다. 또한 2차 검사를 하기 위한 키 값을 등록한다.

시스템은 입력받은 IP에 icmp packet을 보내 네트워크 상태를 점검한다. 네트워크가 정상적으로 작동할 시 네트워크 정보를 토대로 시그니처를 생성하며 생성 조건은 아래와 같다.

- OS 정보
- open port 정보
- TCP window size
- TCP MSS
- IP/MAC 주소
- ICMP TTL 값

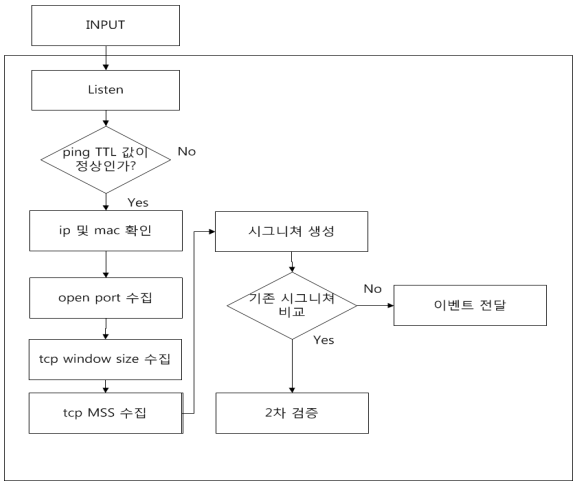
생성 조건들의 값을 취합하여 hash로 단방향 암호화를 수행하여 시그니처를 생성 및 DB에 저장한다.

Fig. 4. CCTV 등록 시 생성된 해시값

CCTV 등록 모듈은 CCTV를 교체하거나 IP 변경 시 최초 한번만 수행하며 등록 이후에는 1차 검사와 2차 검사를 주기적으로 반복한다.

3.2 시그니쳐 기반 1차 검사

시그니쳐 1차 검사는 등록 모듈에서 수행된 작업과 동일하다. 등록 시 진행 되었던 시그니쳐 생성 위한 행위를 동일하게 반복하여 해시를 추출 하며 추출된 해시값과 등록시 저장 되었던 해시값을 비교 및 CCTV의 허가 유무를 검사한다.



Flg. 5. 시그니쳐 기반 1차 검사 절차도

기존 등록 되어진 해시값과 저장되어 있는 해시 값이 다를 시 사용자에게 실시간 이벤트를 전달한다. 저장되어진 해시값과 동일하면 추가 검사를 수행하기 위하여 2차 검사 모듈로 전달 해당 IP를 전달한다.

3.3 nonce 값 기반 2차 검사

1차 검사에서 분석 되어진 시그니쳐가 등록 시 저장된 값과 동일하면 2차 검사를 수행한다. 1차 검사에서 나오는 값은 항상 동일하기 때문에 악의적인 공격자로부터 재전송 공격을 당할 수 있다. 그렇기에 재전송 공격을 방지하기 위하여 2차 검사를 추가로 실시한다.

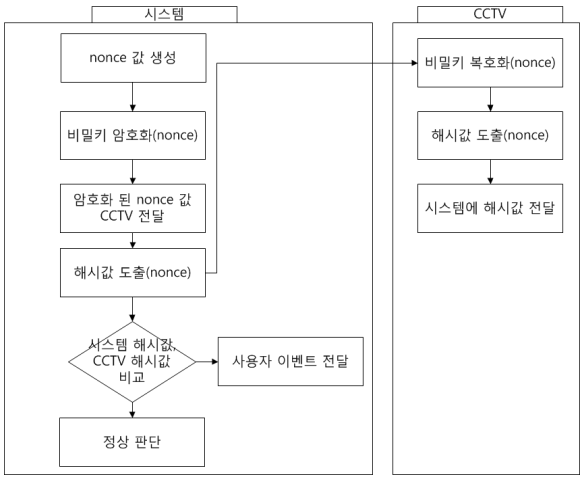


Fig. 6. nonce 값 기반 2차 검사 절차도

1차 검사는 CCTV의 개입없이 시스템에서 시스템의 네트워크 정보를 토대로 검사를 하였다면 2차 검사는 시스템 및 CCTV에 등록되어진 키 값을 이용하여 검사를 수행한다.

CCTV가 임의적 값인 nonce 값을 등록되어진 키를 이용하여 암호화를 수행 및 암호화 된 nonce 값을 CCTV에 전달한다. CCTV는 키를 이용하여 복호화를 수행하여 얻어진 nonce 값을 해시 알고리즘을 이용하여 해시값을 도출한다. CCTV는 도출 되어진 해시값을 시스템에 전달한다. 시스템은 자신이 보낸 nonce 값의 해시값과 CCTV에서 전달해온 nonce 값의 해시값이 일치하는 비교하여 값이 동일하면 허가된 CCTV로 판단하며 값이 일치 하지 않을 시 잘못된 CCTV 판단, 사용자에게 이벤트를 전달한다.

IV. 결 론

본 논문에서는 CCTV의 악성행위를 사전에 차단하기 위하여 CCTV를 유효성을 주기적으로 검증하기 위한 분석 시스템을 제시하였다. 공격자는 악의적인 행위를 하기 위하여 CCTV를 통하여 내부망 으로 접근 할 수 있다. 공격자는 공격을 수행하기 위해 악성코드가 삽입된 동일한 기종의 CCTV를 변경하여 마치 허용된 CCTV인 것처럼 위장 할 수 있다. 또한 검증 부분이 공격자에게 노출 시 이에 대하여 재전송 공격도 할 수 있기 때문에 1차와 2차로 나누어 검증을 수행하였다. 1차적으로 인증에 대한 검사를 수행하여 CCTV의 유효성을 판단할 수 있으나 재전송 공격에 취약한 단점이 있다. 이를 해결하기 위하여 2차 nonce 기반의 검사를 수행하여 비밀 키와 해시값을 이용하여 재전송 공격을 방지 하였다. 또한 시스템은 지속적인 검사 및 분석을 수행하여 실시간 대응이 가능하다.

CCTV 유효성을 검증하는 기술을 더욱 향상 시켜 더욱 세분화된 분석기술을 지속적으로 진행하여 현 시스템에 적용한다면 향후 악성코드에 의한 피해를 효율적으로 효과적으로 차단 할 수 있는 시스템이 될 것으로 기대한다.

REFERENCES

[1] 채영진,. “스마트폰을 이용한 ID/PW 기반 강화된 사용자 인증 시스템 설계 및 구현,”. 배재대학교 석사학위논문, 2016.

[2] 한군희, 배우식,. “M2M 통신환경에서 안전한 P2P 보안 프로토콜 검증,”. 디지털컨버전스학회논문지, Vol.13, No.5, pp. 213-218, May, 2015.

[3] 네이버 지식백과,. “사물인터넷 기술의 유래 및 정의,”. http://terms.naver.com/entry.nhn?docId=2851164&cid=56756&categoryId=56756.

[4] 배상희,. “이석우 美 NITS CPS 담당 부국장...IOT 융합한 제조업 혁신 방향 제시,”. http://www.ajunews.com/view/20151014182407820.

[5] 배규민,. “생활속 사물인터넷 성큼,”. http://www.mt.co.kr/vi

ew/mtview.php?type=1&no=20140611105512071 04&outlink=1.

[6] 강근주,. “서울시, 아시아 최초로 도로조명에 사물인터넷 적용,”.http://www.ekn.kr/news/article.html?no=129121.

[7] 윤혜연,. “해킹 위험 커지는 IoT, 철통 보안시스템 갖춰야,”. http://sunday.joins.com/archives/124654.

[8] Canming jiang, Bao Li and Haixia Xu,. “An efficient Scheme for User Authentication in Wireless Sensor Networks,”. 21st International Conference on Advanced Information Networking and Applications Workshops, pp. 438-442, May. 2007.

[9] Guanglei Zhao, Xianping Si, Jingcheng Wang, Xiao Long and Ting Hu,. “A novel mutual authentication scheme for Internet of Things,”. 2011 International Conference on Modeling Identification and Control, pp. 563-566, 2011.