CCTV 환경에서의 키 관리에 관한 연구+

황용운, 이임영
순천향대학교 컴퓨터학과
e-mail:[hwy0123, imylee]@sch.ac.kr

A study on key management in CCTV environment

Yong-Woon Hwang, Im-Yeong Lee
Dept of Computer Science Engineering, Soonchunhyang University

요 약

CCTV는 현재에도 다양한 분야에서 적용되어 활용하고 있다. 하지만 다양한 분야에 설치된 CCTV 시스템에는 다양한 보안 위협이 존재하는데, 공격자는 전송되는 영상데이터를 획득함으로써 카메라에 찍은 사용자의 정보를 획득할 수 있고, 이를 조작하여 사회에 혼란을 줄 수도 있다. 또한 다수의 카메라의 영상을 보관하는 서버가 공격자에 의해 해킹당하면 다수의 카메라는 공격자에 의해 제어 될 수 있다. 본 논문에서는 CCTV의 보안위협을 해결하고자 CCTV 환경에서 프록시 재암호화를 활용하여 키 관리를 함으로써 서버에 저장된 영상을 재암호화하고 원하는 사용자가 암호화된 영상을 획득하여 자신의 비밀키만으로 영상을 안전하게 복호화하여 획득할 수 있다.

1. 서론

CCTV(Closed Circuit Television)는 사건 사고 시 현장을 관찰하거나 현장의 증거자료를 확인, 범죄 예방을 위한 수단, 여성이나 아동, 노약자 등 사회적으로 약한 사람들을 대상으로 사용되며, 마지막으로 회사나 사내 업무에서 근태관리 목적 등으로 활용된다[1]. 현재에도 경찰청, 유치원, 교통분야, 공원 등 다양한 분야에서 CCTV를 활용하고 있다. 하지만 CCTV 시스템은 카메라가 찍은 영상을 서버로 보내지는 구간 이외에도 보안 위협이 존재한다. 이러한 보안위협을 해결하기 위해 본 논문에서는 CCTV의 보안위협을 해결하고자 프록시 재암호화를 활용하여 영상을 암호화하고 원하는 사용자가 암호화된 영상을 획득하여 자신의 비밀키만으로 영상을 안전하게 획득할 수 있는 키관리 기법을 제안한다. 본 논문에서는 디지털 CCTV 환경을 기반으로 무엇보다 영상데이터가 중요한 환경, 예를 들어 범죄수사에 이용되는 경찰청 취조실 CCTV의 증거자료, 허가된 사용자만이 영상정보를 취득할 수 있는 환경을 배경으로 한다.

2. 관련연구

본 장에서는 CCTV의 보안위협 및 키관리 문제를 해결하기 위해 겹선형 사상과 프록시 재암호화에 대해 알아본다.

2.1 겹선형 쌍함수(bilinear pairing)

겹선형 사상은 과거 타원 곡선 암호시스템을 공격하는 도구로 제안되었지만 최근에는 정보보호를 위한 암호학적 도구로 사용된다. 겹선형 쌍함수는 겹선형 사상(bilinear Map)이라고도 한다. 다음과 같은 표기법을 나타낸다.

- q: 매우 큰 소수
- G_1: 위수가 q 인 타원곡선 위의 덧셈군
- G_2: 위수가 q 인 유한체 위의 곱셈군
- $P, Q, R \in {}_RG_1$,
- $a, b, c \in {}_RZ_q^*$

(그림 1) Proxy En-encryption

2.2 프록시 재암호화(Proxy En-encryption)

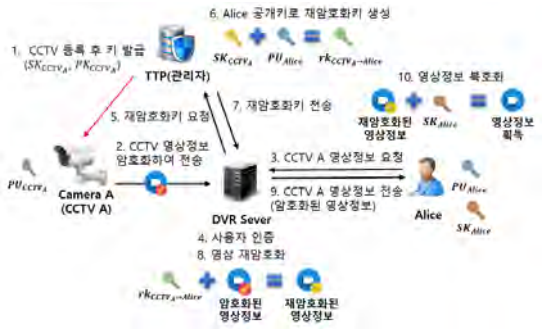
Proxy En-encryption의 기본적인 개념은 (그림 1)과 같다. Alice와 Bob이 서로 통신 시 Alice의 공개키로 암호화된 암호문을 Proxy가 전송받아 Bob의 비밀키로 복호화할 수 있도록 암호문을 변환하는 방식이다. Proxy는 재암호화키를 이용하여 암호문을 재암호화하는데 기존의 암호문을 복호하지 않고 암호문을 변환할 수 있기 때문에 Proxy는 암호화된 데이터의 원본이나 Alice의 비밀키를 알지 못한다[2][3].

3. 보안요구사항

본 연구에서는 CCTV 시스템에서 만족해야 하는 보안요구사항에 대하여 살펴본다[4].

- 재전송 공격 : 공격자가 도청된 영상데이터를 가지고 원하는 사용자에게 다른 영상정보를 전송함으로서 피해를

+이 논문은 연세대학교 바른ICT연구소의 지원을 받아 수행된 연구 결과입니다.



(그림 2) 제안방식 시나리오

줄 수 있기에, 영상데이터의 암호화가 중요하며, 공격자는 영상데이터의 원본을 알 수 없어야 한다.

· 서버의 보안 : 서버가 다수의 CCTV 영상을 저장하고 관리함으로 서버의 보안이 중요하다. 이에 CCTV의 영상을 암호화하여 저장함으로써 공격자가 서버를 해킹하여도, CCTV의 영상을 알 수 없게 한다.

4. 제안방식

본 제안방식은 CCTV 환경에서의 키관리 기법을 제안한다(그림 2). 제안방식은 가정 단계와 CCTV 등록 및 영상암호화 단계, 사용자 영상데이터 획득 단계로 구성된다.

4.1 가정 단계

본 제안방식에서는 다음과 같은 사항을 가정한다.

1. CCTV는 연산량이 충분한 성능을 가지고 있다.
2. TTP는 관리자로서 등록된 다수의 CCTV의 비밀키와 공개키를 생성하고 이를 통해 재암호화키를 생성한다.
3. 영상데이터를 m이라고 가정하고 CCTV는 실시간으로 영상데이터를 암호화하여 DVR Server로 전송한다.
4. Alice와 같은 사용자는 기존의 DVR Server에 등록된 사용자로써 등록된 정보를 통해 사용자 인증을 수행한다.

4.2 CCTV 등록 및 영상암호화 단계

이 단계에서 $CCTV_A$는 초기에 TTP에 등록을 요청하면 TTP는 $CCTV_A$를 등록하고 비밀키와 공개키 쌍을 생성하여 $CCTV_A$에게 공개키를 전송해준다. $CCTV_A$는 받은 공개키를 가지고 영상을 암호화하여 DVR Server로 전송한다. DVR Server는 CCTV마다 별도의 저장공간을 두어 실시간으로 전송받는 암호화된 영상데이터를 저장한다.

4.3 사용자 영상데이터 획득 단계

이 단계에서 사용자는 DVR Server에 원하는 $CCTV_A$의 영상을 요청하면 등록된 사용자 정보를 통해 인증을 수행한다. 인증이 완료되면 DVR Server는 TTP에 재암호화키를 요청하게 되고, TTP는 Alice의 공개키와 $CCTV_A$의 비밀키로 재암호화키를 생성하여 DVR Server에 전송해준다. DVR Server는 전송받은 재암호화키를 사용하여 영상을 재암호화하여 Alice에게 보내주고, Alice는 재암호화된 영상 데이터를 자신의 비밀키로 복호화하여 영상데이터를 획득 할 수 있다.

5. 제안방식 분석

본 장에서는 3장에서 도출된 보안요구사항을 만족한다.

· 재전송 공격 : 재암호화된 영상데이터는 사용자의 비밀키로만 복호화할 수 있기에 공격자는 도청된 영상데이터를 획득하더라도 복호화 할 수 없어 안전하다.

· 서버의 보안 : 기존의 CCTV를 관리하는 서버에 저장된 영상 데이터는 암호화가 재대로 이루어져있지 않기에 공격자가 서버를 해킹하는 경우 다수의 CCTV를 제어할 수 있으며, 영상을 볼 수 있다. 이에 본 제안방식에서 CCTV 영상을 암호화하여 서버에서 관리함으로 다양한 보안위협으로부터 영상데이터를 안전하게 보호한다.

6. 결론

CCTV 시스템에서 발생하는 보안위협을 해결하기 위해 본 논문에서는 CCTV 환경에서 프록시 재암호화 기법을 활용하여 키관리 기법을 제안하였다. 제안방식은 도청, 재전송공격, 위장공격과 같이 CCTV 시스템에서 이루어지는 다양한 보안위협에 대해 안전하며, 무엇보다 서버가 영상데이터 원본을 알 수 없어 공격자가 서버를 해킹하더라도 다수의 CCTV 영상의 원본 데이터는 안전하다. 또한 기존의 통신구간 암호화방식에서의 키관리, 키분배 문제를 해결할 수 있으며, 영상데이터를 원하는 사용자만이 자신의 비밀키로 영상데이터를 볼 수 있어 안전하다.

향후 연구로는 본 논문에서 제시된 프록시 재암호화 기법 외에 좀 더 효율적인 재암호화 기법을 연구하여 논문에서 제시된 보안요구사항 외에 다양한 보안요구사항을 만족 시키는 연구가 필요할 것으로 사료된다.

참고문헌

[1] 서태웅, 이성렬 외 2명 “CCTV 보안관제 취약성 및 성능 분석”, Journal of Korea Multimedia Society, 2012.

[2] 송유진, 박광용, “Proxy Re-encryption 기술”, 정보보호학회지, 2009.

[3] Ateniese, Giuseppe, "Improved proxy re-encryption schemes with applications to secure distributed storage", ACM Transactions on Information and System Security, 2006.

[4] 박태성, 강도운, 전문석, “Network CCTV 환경에서 악의적인 사용자를 차단하기 위한 RTSP 사용자 인증 프로토콜”, 한국산학기술학회, 2011.