무인 원격 감시시스템의 데이터 암호화 및 Review 프로그램

이철용, 신희성, 김호동
한국원자력연구원, 대전광역시 유성구 대덕대로 1045
lcy@kaeri.re.kr

1. 서론

미국의 LANL(Los Alamos National Labortory)는 무인 원격 감시(Unattended and Remote Monitoring; UNARM) 시스템을 개발하여 사용하고 있다. 안전조치의 신뢰성 향상을 위해 UNARM의 모든 데이터는 암호화되어야 하며, 데이터 통신은 암호화된 데이터를 사용하여야 한다. DES(Data Encryption Standard)는 NIST(National Institute of Standards Technology)에 의해 국제 표준화되어 오랫동안 사용되었으며, DES의 강화된 알고리즘인 TDES(Triple Data Encryption Standard) 가 이용되기도 하였다. 그러나 국제 표준화 기간 만료와 강화된 데이터 암호화 알고리즘의 요구로 인해 새로운 국제 표준화 알고리즘이 필요하게 되었다. 이에 NIST는 새로운 국제 표준화 암호 알고리즘을 공개적으로 공모하였으며, 2001년에 비로소 AES(Advanced applied Standard) 알고리즘을 승인하였다. 본 논문에서는 AES 알고리즘을 UNARM 시스템의 데이터에 적용하고, XOR 암호화 알고리즘을 비교하였다.

2. 데이터 암호화 알고리즘

가. AES 암호화 알고리즘의 적용

AES 암호화 알고리즘은 공개된 프로그램으로 소스를 인터넷상에서 확인할 수 있다. 본 논문에서는 Rijndael 의 AES block 암호화 알고리즘인 VB class 를 프로그램에 사용하였다. Collect 컴퓨터의 암호화 알고리즘 적용과정은 다음과 같다. 영상 정보는 임시 디렉토리에 파일로 저장되고 이 파일은 AES_ENC 모듈에 의해 암호화 된 파일로 새롭게 저장된다. 암호화된 영상 파일은 MicXfer 프로그램에 의해 Review 컴퓨터로 전송된다. 이때 원래의 영상파일의 크기는 45 kbyte 였지만, 암호화된 파일의 크기는 거의 2배인 87 kbyte가 된다. Review 프로그램에서는 Collect 컴퓨터에서 수신된 암호화 파일을 원래 파일로 복원하여야 한다. 그림1은 원래의 ReviewInformation.txt 파일의 내용이며, 이 텍스트 파일을 AES 알고리즘으로 암호화하면 그림 2와 같이 변환된다. 원래의 파일을 이진 파일로 읽어 Block 단위로 암호화되며, 마찬가지로 암호화 후에는 이진 파일로 저장된다. Review 프로그램을 수행시키면 암호화된 영상파일은 자동적으로 복호화 되어 메인 화면의 preview 영역에 표시된다. 암호화 과정을 거치지 않은 Review 프로그램과 비교하면 review 속도면에서 차이가 있다. 이것은 전술한 바와 같이 거의 2배로 암호화된 파일을 복호화하는 과정으로 생기는 당연한 결과이다.

그림 1. AES 적용 ReviewInformation.txt

그림 2. AES 에 의한 ReviewInformation.txt

나. XOR 암호화 알고리즘의 적용

AES 알고리즘은 암호화와 복호화시 약간의 시간이 소요된다. 따라서 암호화와 복호화시 실시간으로 동작되는 알고리즘이 필요하다. XOR 알고리즘은 간단하고 유용하다. 원래 XOR 은 "exclusive OR" 이라는 의미로 정보값 중 하나의 true가 있으면 결과값이 true로 된다. XOR 알고리즘은 매우 간단하지만 암호화한 후 파일 크기의 변화가 없다. 따라서 암호화된 파일을 원래의 파일로 복원화 하는데 매우 유리하다. 그림 3은 2 kbyte 의 ReviewInformation.txt 파일을 16bit XOR 알고리즘으로 암호화한 결과이다. UNARM 시스템도 암호화 및 복호화 알고리즘이 적용되어야하며, 앞에서 검토한 바와 같이 실제적인 측면에서 XOR 알고리즘이 가장 적합한 것으로 사려된다. LANL의 UNARM 시스템을 Upgrade 하고 새로운 Review 프로그램을 개발하였다. 여기에 텍스트 데이터와 영상데이터를 XOR 알고리즘으로 적용시킨 프로그램을 개발하였는데, 그림 4는 이에 대한 결과이다.

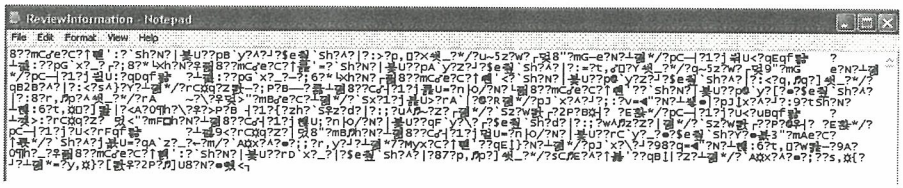

그림 3. XOR 알고리즘으로 암호화된 ReviewInformation

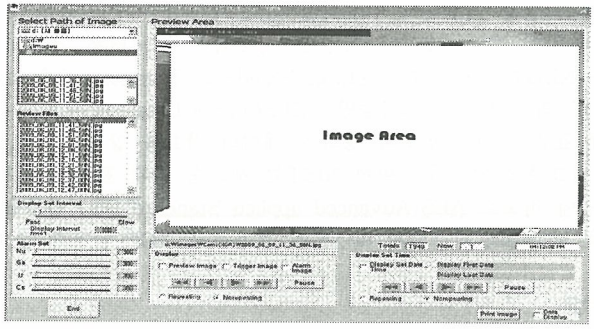

그림 4. XOR 알고리즘이 적용된 Review 프로그램

3.. 결론

LANL의 UNARM 시스템의 문제점을 분석하고 IP 카메라를 사용하는 최적화 시스템으로 Upgrade 하였다. 그리고 Upgrade 시스템에 맞추어 암호화 및 복호화 모듈로 AES 알고리즘과 XOR 알고리즘이 적용된 새로운 Review 프로그램을 개발하였다. 프로그램 성능평가 결과 XOR 알고리즘이 적용된 Review 프로그램이 UNARM 시스템에 가장 합당하다.

참고문헌

1. J.Halbig, "Overview of an Unattended Monitoring System", LA-UR-01-4547, 2001.
2. K.Alvar, "UNARM an Overview of Los Alamos Activities", LA-UR-01-3609, 2001.