Annual Spring Conference of KIPS

서명 및 암호화를 통한 펌웨어 보안 시스템 구축

김나현, 이연준

한양대학교 ERICA 소프트웨어학부

요약

최근 펌웨어를 겨냥한 공격이 늘어나고 있다. 기기에 수정된 펌웨어 주입이 가능하다면 장치를 무력화하거나 데이터 유출, 디도스 등의 공격이 가능하다. 본 연구는 펌웨어 보안을 위해 펌웨어 서명 및 암호화 시스템을 구축하였다. 또한 STM32MP1-DK2보드의 리눅스 커널 코드를 수정하여 이를 검증하였다.

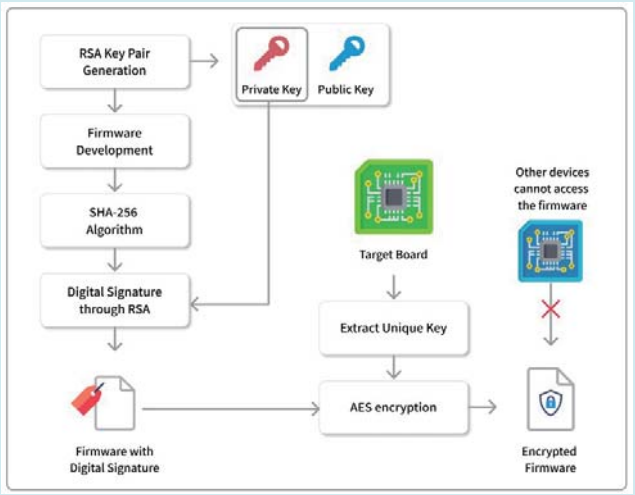
서론

2021년 3월, 마이크로소프트에서 작성한 'Security Signals'보고서의 1000명의 보안 분야 결정권자들을 대상으로 한 조사에 따르면 80%가 넘는 기업들이 지난 2년 동안 한 번 이상의 펌웨어 공격을 받았다고 한다. 이를 통해 최근 펌웨어를 겨냥한 공격이 늘어나고 있다는 것을 알 수 있다.

공격자는 펌웨어에 접근하여 암호화폐 채굴, 장치 무력화, 기기 장악을 통한 디도스, 역공학을 이용한 펌웨어 기술 유출 등의 심각한 피해를 입힐 수 있으며 펌웨어 공격이 의료기관이나 금융 기관과 같은 민감한 데이터를 다루는 조직을 대상으로 이뤄진다면 데이터 유출로 인한 치명적인 피해가 야기될 것이다.

본 연구에서는 이러한 문제를 인식하고 펌웨어 서명 및 암호화 시스템을 구축하여 펌웨어 보안을 한단계 높이고자 하였다. 이를 위하여 RSA를 이용한 펌웨어 서명 생성 및 암호화를 위한 AES 암호화 코드를 작성하였고 펌웨어 인증 및 복호화를 위하여 커널 코드를 수정하였다.

연구 내용



<그림 1> 서명 및 암호화 과정 다이어그램

본 연구에서는 펌웨어 서명 및 암호화 시스템을 구축하기 위해 인증되지 않은 펌웨어의 실행을 막도록 펌웨어 서명을 펌웨어에 추가하였고 이를 암호화하여 공격이 어렵게 만들었다.

서명 및 암호화는 다음과 같은 과정으로 진행되었다.

1. RSA키 생성 알고리즘을 통해 서명에 필요한 공개키와 개인키 쌍을 생성한다.
2. 펌웨어 인증을 위해 펌웨어 서명을 펌웨어 상단에 추가한다. 펌웨어 서명을 생성하기 위해 SHA256알고리즘을 이용하여 펌웨어 해쉬를 생성하고 이를 RSA암호화한다.
3. 보드 내 레지스터의 값을 추출하여 고유키를 만들고 AES 암호화를 진행한다.

이렇게 하여 보드마다 고유한 암호화 키를 가질 수 있다. 또한 암호화한 펌웨어를 실행하기 위해 리눅스에 복호화 코드를 추가하여 부팅 시 펌웨어가 복호화될 수 있도록 하였고 따라서 펌웨어 암호화가 진행된 보드에서만 복호화가 가능하다.

연구 결과

본 연구에서 제안한 펌웨어 암호화 및 인증 시스템을 검증하기 위한 타겟 보드로 STM32MP1-DK2를 사용하였으며 연구 내용에서 밝힌 방식으로 펌웨어 서명 및 암호화를 진행하였다.

암호화된 펌웨어에 다른 보드로가 접근이 가능한지 테스트하기 위해 타겟 보드에서 SD-card를 추출한 후 다른 보드에 이식하여 암호화된 펌웨어 사용을 시도해보았으나 해당 보드에서 암호화된 펌웨어를 실행할 수 없음을 확인했다. 암호화에 참여하지 않은 보드는 펌웨어를 복호화 할 수 없기 때문이다.
이를 통해 본 연구에서 제안한 펌웨어 보안 방식이 핵심 펌웨어 기술이 유출되는 것을 막는 데 효과가 있음을 알 수 있다.

결론

본 연구에서 기본적인 펌웨어 보안을 위한 펌웨어 암호화 및 인증 시스템을 제안하였으며 STM32MP1-DK2보드를 통해 이를 검증하였다.

본 연구에서 제안한 펌웨어 서명 및 암호화 시스템은 타겟 보드에서 SD-card를 추출해서 다른 보드에 이식하는 등 외부 접근이 발생했을 때 외부 장치에서 해당 펌웨어를 제약 없이 사용할 수 있었던 기존의 취약점을 보완하여 해당 펌웨어를 복호화할 수 있는 타겟 보드만이 펌웨어에 접근할 수 있도록 함으로써 기본적인 펌웨어 보안을 달성한다.

토론

현재 암호화된 펌웨어의 실행 과정은 리눅스에서 커널이 호출된 후 커널이 펌웨어를 복호화 및 실행하는 방식으로 되어있지만 이는 커널이 공격당할 경우 펌웨어가 함께 위험해질 수 있는 문제점이 있다. 이러한 한계를 해결하기 위해 펌웨어의 복호화 및 실행 과정이 커널이 아닌 bootloader인 U-boot에서 진행되도록 변경하여 커널이 공격받더라도 펌웨어가 보호될 수 있도록 하는 것을 추후 과제로 남겨둔다.

참고문헌

- S. Frankel, R. Glenn, S. Kelly " The AES-CBC Cipher Algorithm and Its Use with IPsec " RFC 3602 September 2003