경량 IoT 를 위한 안전한 무선 펌웨어 업데이트 메커니즘

이승은[1], 이진민[2], 이일구[3]
[1] 성신여자대학교 융합보안공학과 학부생
[2] 성신여자대학교 미래융합기술공학과 박사과정
[3] 성신여자대학교 융합보안공학과/미래융합기술공학과 교수
rose6825@gmail.com, csewa56579@gmail.com, iglee@sungshin.ac.kr

Secure FOTA Update Mechanism for Lightweight IoT

Seung-Eun Lee[1], Jin-Min Lee[2], Il-Gu Lee[1,2]
[1]Dept. of Convergence Security Engineering, Sungshin Women's University
[2]Dept. of Future Convergence Technology Engineering, Sungshin Women's University

요 약

최근 전 산업 분야에서 사물인터넷 (Internet of Things, IoT) 기술이 활용되면서, 안전하고 편리한 펌웨어 업데이트 기술의 중요성이 커지고 있다. 그러나 종래의 FOTA (Firmware Over-The-Air) 기술은 단일 경로로 펌웨어를 업데이트하여 보안이 취약하고, 강력한 암호 기술을 활용할 수 없는 문제가 있다. 본 연구에서는 경량 IoT 를 위한 안전한 FOTA (Secure FOTA, S-FOTA) 메커니즘을 제안한다. 실험 결과에 따르면 제안하는 S-FOTA 는 암호화된 파일이 60 개이고 공격자 수가 100 명일 때 종래의 FOTA 대비 공격자의 공격 성공률을 89.84% 줄일 수 있었다.

1. 서론

최근 사물인터넷 (Internet of Things, IoT)이 전 산업 분야에 널리 사용되면서 IoT 펌웨어 업데이트 메커니즘의 보안이 중요해지고 있다. IoT 펌웨어는 FOTA (Firmware Over-The-Air)를 활용하여 무선으로 업데이트될 수 있다. 종래의 FOTA 메커니즘은 클라이언트 장치가 단일 경로를 활용하여 업데이트하므로 탈취 공격에 취약하다는 문제점이 있다. 이 문제를 해결하기 위해 SSS (Shamir's Secret Sharing)은 펌웨어 업데이트 파일을 조각으로 분할하고 다중 경로로 전달할 수 있지만, SSS 은 일정 개수의 분할 파일을 공격자가 획득하면 공격자도 원본 파일을 복구할 수 있는 문제가 있다. 따라서 본 논문에서는 SSS 에서 분할한 파일의 일부를 암호화하여 전달하는 안전한 FOTA (Secure FOTA, S-FOTA)를 제안하고, 종래의 방식과 보안성, 복잡도 측면에서 비교 및 분석한다.

본 논문의 주요 기여점은 다음과 같다.

- 경량 IoT 를 위한 부분 암호화 기반의 SSS 을 활용한 S-FOTA 메커니즘을 제안했다.
- 기존의 FOTA 와 제안하는 S-FOTA 의 보안성, 평균 소요 시간을 비교 평가하는 프레임워크를 제안했다.
- 제안하는 S-FOTA 는 암호화된 파일이 60 개, 공격자가 100 명일 때 기존의 FOTA 대비 공격자의 공격 성공률을 89.84% 줄였다.

본 논문의 구성은 다음과 같다. 2 장에서는 기존의 다중 인자 공유 선행연구를 보안성 관점에서 분석한다. 3 장에서는 제안하는 S-FOTA 를 설명하고, 4 장에서는 제안 방식과 종래 방식의 성능을 비교 및 분석한다. 마지막으로 5 장에서는 결론을 맺는다.

2. 관련연구

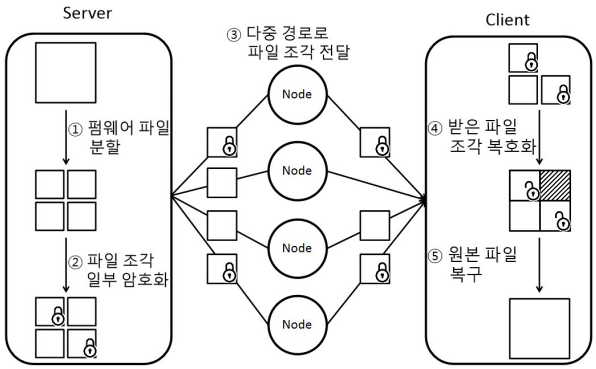
Abdel Hakeem, S.A.[1] 외 1 인은 HMAC (Hash-Based Message Authentication Code)과 SSS 기반 임계 공유 비밀 프로토콜을 제안하였으나, 공격자가 분할 공유되는 키를 탈취하여 복구할 수 있다는 한계점이 있다.

Duan, J.[2] 외 2 인은 비밀 공유 기반 개인 정보 보호 분산 학습 프레임워크를 제안하였으나, 공격자가 다수인 경우를 고려하지 않았다는 한계점이 있다.

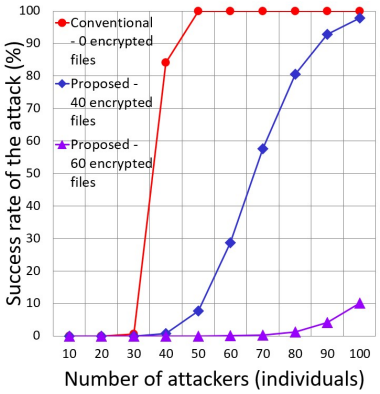
Subrahmanyam, R.[3] 외 2 인은 타원 곡선 기반 분산 환경의 비밀 공유 체계를 제안하였으나, 소요 시간을 기존 방식과 비교 분석하지 않았다는 한계점이 있다.

3. 안전한 무선 펌웨어 업데이트 메커니즘

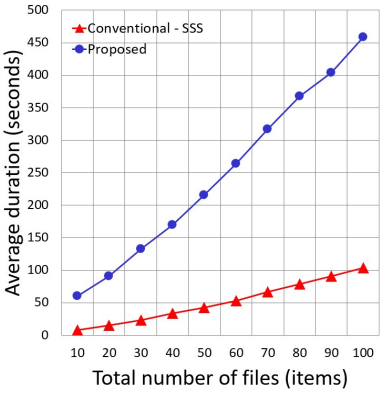
기존의 SSS 은 분할 파일을 일정 개수 이상 획득하면 공격자도 원본 파일을 복구할 수 있다. 따라서 본 연구에서는 펌웨어 분할 파일 중 일부를 암호화하여 전달함으로써 공격자가 원본 파일을 복구할 수 없는



(그림 1) 제안 방식.



(그림 2) 공격자 수에 따른 공격자 공격 성공률.



(그림 3) 분할 파일 수에 따른 평균 소요 시간.

S-FOTA 를 제안한다.

그림 1 은 제안 방식의 동작 과정이다. 클라이언트 업데이트 시 서버는 SSS 을 이용하여 펌웨어 파일을 분할하고 암호 알고리즘으로 일부 파일을 암호화하며, 부분 암호화된 분할 파일을 다중 경로로 분산하여 전달한다. 클라이언트는 사전에 서버와 합의한 키로 전달받은 파일을 복호화하여 펌웨어를 업데이트한다.

4. 실험환경 및 결과

본 실험에서는 기존의 SSS 과 제안 방식을 비교하기 위해 FOTA 업데이트 환경을 모델링하여 시뮬레이션하였다. 제안 방식의 암복호화는 경량 암호인 LEA (Lightweight Encryption Algorithm)-128 을 적용하였다.

그림 2 는 제안 방식과 기존 방식을 공격자 수에 따른 공격 성공률 측면에서 비교한 실험 결과이다. 공격 성공률은 공격자가 원본 파일 복구를 성공할 확률이다. 실험에서는 원본 파일을 총 100 개의 분할 파일로 나누었으며, 원본 파일 복구에 필요한 분할 파일의 수는 30 개로 고정하였다.

실험 결과, 공격자 수가 100 명일 때 암호화된 파일이 40 개인 제안 방식은 기존 방식 대비 공격 성공률을 2.21% 약화시킬 수 있었다. 그리고 암호화된 파일이 60 개인 제안 방식은 공격자 수가 100 명일 때 공격 성공률을 89.84% 약화시켰다. 실험을 통해 제안 방식이 기존 방식보다 공격 성공률을 약화시켜 보안성이 향상됨을 확인하였다.

그림 3 은 제안 방식과 기존 방식의 전체 분할 파일 개수별 소요 시간을 비교한 실험 결과이다. 분할 파일 수가 10~100 개일 때, 복구에 필요한 파일 수는 분할 파일 수의 50%, 제안 방식의 암호화 파일 수는 분할 파일 수의 20%로 설정하였다.

실험 결과, 분할 파일이 100 개일 때 제안 방식의 평균 소요 시간이 기존 방식 대비 343.07% 더 걸렸다. 실험을 통해 제안 방식은 SSS 에 부분 암호화가 적용되어 기존 방식보다 시간이 더 소요됨을 확인하였다.

5. 결론

FOTA 메커니즘은 파일이 단일 경로로 전달되어 탈취될 위험성이 있으므로, SSS 에서는 파일을 분할하여 다중 경로로 전달한다. 하지만 SSS 은 공격자가 일정 개수의 분할 파일을 수집하면 원본 파일을 복구할 수 있다는 문제점이 있다. 본 연구에서는 FOTA 업데이트 시 SSS 방식으로 파일을 전달할 때 공격자가 원본 파일을 복구할 수 없도록 분할 파일 일부를 암호화하는 S-FOTA 를 제안하였다. 실험 결과에 따르면 제안 방식은 암호화 파일 수가 60 개인 경우, 공격자 수가 100 명일 때 기존 방식 대비 공격 성공률을 89.84% 낮추어 기존 방식보다 보안성이 뛰어남을 확인하였다. 분할 파일이 100 개일 때 기존 방식 대비 제안 방식의 평균 소요 시간은 343.07% 더 소모되었다. 향후 연구에서는 제안 방식의 복잡도를 낮추어 소요 시간을 줄이고 테스트베드를 구축하여 실험할 계획이다.

Acknowledgement

본 논문은 2024 년도 정부재원(과학기술정보통신부 여대학원생 공학연구팀제 지원사업)으로 과학기술정보통신부와 한국여성과학기술인육성재단의 지원(WISET 계약 제 2024-138 호), 산업통상자원부 및 한국산업기술진흥원의 지원(No. RS-2024-00415520)과 과학기술정보통신부 및 정보통신기획평가원의 지원 (No. IITP-2022-RS-2022-00156310)을 받은 연구결과로 수행되었음.

참고문헌

[1] Abdel Hakeem, S.A., Kim, H., "Centralized Threshold Key Generation Protocol Based on Shamir Secret Sharing and HMAC Authentication", Sensors, 22, 1, 331, 2022

[2] Duan, J., Zhou, J., Li, Y., "Privacy-Preserving distributed deep learning based on secret sharing", Information Sciences, 527, 108-127, 2020

[3] Subrahmanyam, R., Rekha, N.R., Rao, Y.V.S., "Authenticated Distributed Group Key Agreement Protocol Using Elliptic Curve Secret Sharing Scheme", IEEE Access, 11, 45243-45254, 2023