임베디드 시스템에서의 신뢰성 보장형 원격 데이터 삭제 기술 분석 및 보안 요구사항 도출

김시은[O1] 이성기[2] 강태인[2] 김훈규[2] 박기웅[3†]
[1]세종대학교 시스템보안연구실
[2]국방과학연구소
[3]세종대학교 정보보호학과
rlatldms2004@naver.com, seongkeel@add.re.kr, tanekang@add.re.kr, hunk@add.re.kr,
woongbak@sejong.ac.kr

Analysis and Security Requirements of Trustworthy Remote Erasure on Embedded Computing System

Sieun Kim[O1] SeongKee Lee[2] Tae In Kang[2] Hoon Kyu Kim[2] Ki-woong Park[3†]
[1]Sejong Univ. Syscore Lab
[2]Agency for Defense Development
[3]Sejong Univ. Dept. of Computer and Information Security

요 약

최근 IoT 기술이 새로운 컴퓨팅 기술의 패러다임으로 부각됨에 따라, 초소형 임베디드 컴퓨팅 시스템이 군사 영역에서도 활발히 적용되고 있다. 군사 기기에 탑재되는 임베디드 컴퓨팅 시스템 내부에는 군사 기밀 등 보안 데이터가 저장될 수 있기 때문에 해당 기기가 탈취될 경우 국가적으로 큰 손해가 발생할 수 있다. 그러므로 전시상황과 같은 특수한 상황에서 기기 탈취 및 격추를 대비하여 군사 기기의 임베디드 시스템에 내장된 정보를 원격에서 신뢰성이 보장된 방법으로 삭제하는 기법은 매우 중요한 수요기술로 부각되고 있다. 본 논문에서는 보안에 민감한 데이터를 내장한 임베디드 시스템에서 신뢰성이 보장된 원격 데이터 삭제 기술을 실현하기 위해 만족해야 할 요구사항을 도출하고, 관련 연구가 이를 만족하는지를 분석하여 기존 원격 데이터 안전 삭제 방법의 한계점과 앞으로의 연구 방향을 제시하고자 한다.

1. 서 론

임베디드 기기가 사용되는 영역이 일상을 비롯한 군사 영역까지 확장됨에 따라 임베디드 시스템에서의 보안 역시 점점 더 중요해지고 있다. 군사 영역에서 사용되는 무인 항공기의 경우 원거리 핵심표적 타격임무를 수행하는 무기로써 사용되거나 적 핵심시설과 표적에 대한 첩보를 수집하는 등의 임무를 수행한다. 이러한 역할을 수행하는 임베디드 기기는 군사 영역과 관련된 기밀 정보를 담고 있는 경우가 많기 때문에 해당 군사 기기가 탈취 혹은 격추를 당하여 기기에 대한 제어권을 상실하게 되면 저장된 기밀 데이터를 탈취당할 가능성이 높아진다. 따라서 군사 영역에서 사용되는 임베디드 기기가 실소유자 수중을 벗어났을 때 데이터는 복구가 불가능하도록 완전히 삭제되어야 하고 이를 검증할 수 있는 보장시스템이 갖춰져야 한다.

본 논문에서는 임베디드 시스템에서 원격으로 데이터를 삭제할 때 신뢰성이 보장되기 위한 요구사항을 도출하고 관련 연구에 대해 살펴본 후 이를 비교하여 기존 임베디드 시스템에서의 원격 데이터 삭제 방법에 대해 한계점을 제시하고자 한다. 임베디드 시스템에서의 원격 데이터 안전 삭제 방법과 관련된 연구들을 분석하여 해당 방법이 충족해야 하는 요구사항을 다음과 같이 5개로 정의하였다.

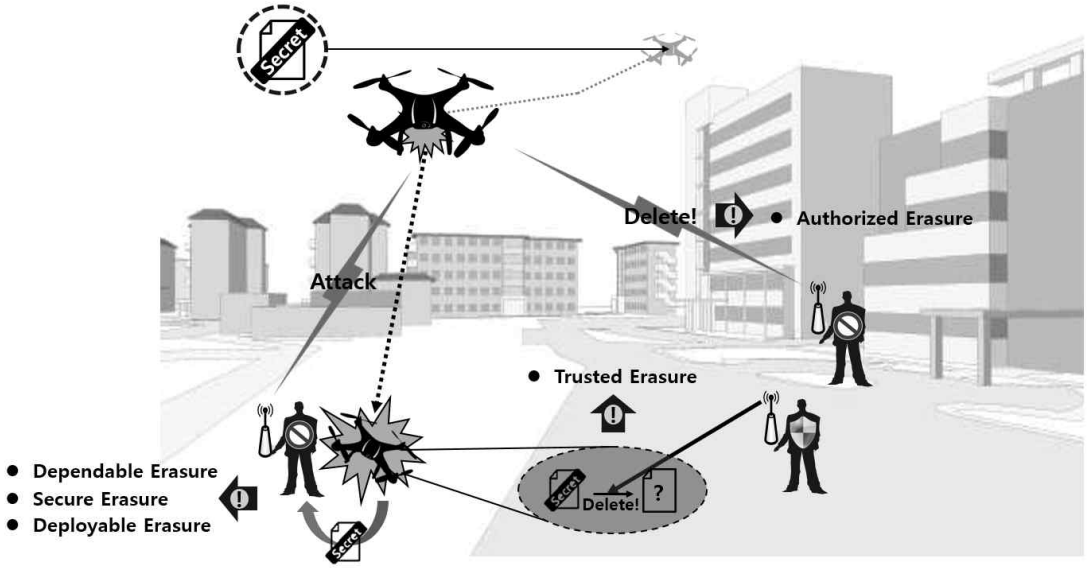
- Dependable Erasure: 실제 기기 소유자의 제어를 벗어난 상태에서도 데이터가 지워질 수 있는 삭제를 의미한다.
- Secure Erasure: 삭제된 데이터가 공격자에 의해 복구되어 도난당하지 않도록 하기 위해 복구가 불가능한 삭제를 의미한다.
- Trusted Erasure: 데이터가 확실하게 삭제되었다는 것을 보장할 수 있는 삭제를 의미한다.
- Authorized Erasure: 기기 실제 소유자가 아닌 공격자가 원격으로 삭제 명령을 내리는 것을 방지하기 위해서 사용자에 대한 인증이 이루어진 삭제를 의미한다.
- Deployable Erasure: 모바일 환경뿐만이 아닌 포괄적인 임베디드 컴퓨팅 시스템에서 적용될 수 있는 삭제를 의미한다.

하나의 예시로써 (그림 1)은 드론에 저장된 데이터에 대해 발생할 수 있는 위협과 그에 따라 필요한 삭제 요구사항들을 보여준다.

---

† 교신저자: 박기웅 (세종대학교 정보보호학과 교수)

이 논문은 한국연구재단 지원사업(2017R1C1B2003957) 및 국방과학연구소에서 수행중인 무기체계용 고신뢰 내장형 실시간 보안 OS 기술 개발과제(UD180001ED)의 지원으로 수행되었음



(그림 1) 드론에 저장되어 있는 데이터에 대한 위협과 그에 따른 요구사항

본 논문의 구성은 다음과 같다. 2장에서 기존에 존재하는 원격 데이터 안전 삭제 방법이 앞서 도출한 요구사항을 만족하는지 살펴보고 3장에서는 2장에서 비교 분석한 결과를 토대로 결론을 제시한다.

2. 원격 데이터 안전 삭제 관련 연구 분석

첫 번째로 모바일 환경에서 적용되는 삭제 방법이 모바일 환경뿐만이 아닌 포괄적인 임베디드 환경에서 적용될 수 있는지를 확인하기 위해 모바일 환경에서의 원격 데이터 삭제 관련 연구들을 조사하였다. 그 다음, 포괄적 임베디드 환경에서 적용될 수 있는 원격 데이터 삭제와 관련한 연구들을 조사하였다. 원격 데이터 삭제 관련 연구의 경우 삭제되었음을 보장하는 과정 즉, Trusted Erasure가 포함되지 않는 경우가 많았기 때문에 Trusted Erasure 과정을 포함하는 연구를 중심으로 선정하여 살펴보았다.

위와 같은 이유로 선정한 관련 연구들이 앞서 도출하였던 요구사항을 만족하는지 조사하여 정리한 후 <표 1>에 나타내었다.

- Dependable Erasure - 2010년 ESORICS에서 발표된 논문에 따르면 Daniele Perito와 Gene Tsudik는 PoSE(Proofs of Secure Erasure)를 이용하여 임베디드 환경에서 안전하게 코드를 업데이트하는 방법을 제안하였다.[1] Prover 장치 측에 있는 ROM은 Verifier와 상호 작용하고 메모리 내용을 지우는 데 필요한 주요 기능을 제공한다. Prover의 메모리에 Verifier가 선택한 난수 값을 채워 전체 메모리를 덮어쓴 후, Prover는 똑같은 난수를 Verifier에게 반환하여 데이터가 지워졌다는 것을 검증한다. 그러나 이 방법의 경우 Verifier가 타겟 기기의 전체 메모리의 크기와 동일한 크기의 난수를 전송해야 하기 때문에 통신 측면에서의 오버헤드가 너무 높아 실용적이지 못하다.

  2018년 ACM에서 발표된 논문에 따르면 Mahmoud Ammar 등은 임베디드 환경에서의 검증 가능한 삭제를 보장하는 접근 방식인 SPEED를 제안한다.[2] 해당 방법은 플래시 메모리의 일부를 격리하여 안전한 삭제에 필요한 기능들을 구현하고 DB(Distance Bounding) 프로토콜을 사용하여 MITM 공격을 방지하는 안전한 삭제 메커니즘을 구축한다. Prover는 Verifier와의 거리를 측정한 후, Verifier가 미리 정해 놓은 범위 내에 있으면 메모리의 삭제를 진행하고 전체 메모리의 Message Authentication Code(MAC)값을 계산하여 Verifier에게 보낸다. Verifier는 이를 확인하여 안전한 삭제가 진행되었음을 확인한다. 그러나 해당 방법은 작동하는 거리에 큰 제한이 있다는 점이 큰 문제가 된다.

  즉 위 두 방법은 실제적인 원격 환경에서 작동하기에는 한계점이 존재한다. 또한 뒤에서 살펴볼 모바일 환경에서의 원격 삭제 방법[3],[4]은 결국 사용자가 원격으로 모바일을 제어해야 한다는 점에서 완벽한 Dependable Erasure를 만족한다 볼 수 없다.

- Secure Erasure - 2012년 Kuppusamy 등은 스마트폰을 도난으로부터 보호하기 위한 모델을 제안하고, SMS(Short Message Service)를 통해 다른 스마트 폰이나 일반 모바일을 통해 스마트 폰에 액세스 할 수 있는 옵션을 제공하는 시스템을 제안하였다.[3] 사용자가 스마트폰을 잃어버린 후 잃어버린 기기에 휴대폰 번호와 원격 연결 명령을 전송하여 잃어버린 기기를 잠그거나 원격으로 제어하여 모든 데이터를 삭제하도록 할 수 있다. 그러나 해당 시스템은 데이터를 삭제하는 방법에 대해 자세히 언급하지 않는다. 즉, 데이터 덮어쓰기나 데이터 암호화를 하여 데이터를 삭제하기 않기 때문에 복구가 가능할 수 있다.

- Trusted Erasure - 2014년 ACM에서 발표된 논문에 따르면 Xingjie Yu 등은 WiFi나 SIM 카드 없이 Cellular Network의 긴급 통화 채널을 통해 원격 명령

<표 1> 임베디드 환경에서의 원격 데이터 안전 삭제 방법에 대한 요구사항

	Secure Code Update of PoSE [1]	SPEED [2]	Remote Access using SMS [3]	Remote wiping using emergency call [4]	One-Time Self-erasing [5]
Dependable Erasure	x	x	△	△	o
Secure Erasure	o	o	x	o	o
Trusted Erasure	o	o	x	x	o
Authorized Erasure	x	△	o	o	x
Deployable Erasure	o	o	x	x	△

을 수신하도록 허용하여 데이터를 삭제하도록 하는 방법에 대해 연구하였다.[4] 스마트폰이 SIM 카드의 제거를 감지하면, 긴급 통화 채널을 통해 전화가 분실되거나 도난당한 것을 확인한 후 지우기 명령을 보내 줄 서비스 제공자와 공격자 몰래 긴급 통화를 시작한다. 해당 방법에서는 데이터 덮어쓰기를 사용하여 데이터 복구가 불가능하도록 한다. 그러나 데이터가 확실하게 삭제되었다는 검증은 하지 않으며, Cellular Network를 사용하기 때문에 휴대폰을 제외한 다른 임베디드 기기에서는 사용이 불가능하다. 또한 앞서 살펴보았던 Kuppusamy의 연구[3] 역시 데이터가 삭제되었음을 보장하는 과정이 없다.

- Authorized Erasure - 앞서 살펴보았던 Daniele Perito의 연구[1]와 뒤에서 살펴볼 Dziembowski의 방법[5]은 사용자에 대한 인증을 따로 하지 않는다. Mahmoud Ammar가 제안한 방법[2]의 경우 거리로써만 사용자를 인증하기 때문에 삭제 명령을 내린 사람이 정확히 명령에 대한 권한이 정확히 있는지는 확인할 수 없다.

- Deployable Erasure - 2011년 TCC에서 발표된 논문에 따르면 Dziembowski 등은 PoSE의 높은 통신 복잡성을 최소화하는 암호 기법을 제안한다.[5] Verifier가 Prover에게 seed로써 약간의 비트를 보내면, Prover는 이 seed를 매우 큰 데이터 구조로 분해한 후 그것을 갖고 있기 위해 모든 메모리를 사용한다. 즉, 모든 메모리를 덮어쓴다. 계산된 해시 값은 한 번만 생성될 수 있기 때문에 삭제의 증거가 된다. 해당 방법은 통신 측면에서의 복잡성은 줄이지만 계산상의 복잡성이 매우 커서 실제 환경에서 사용이 어렵다. 또한 앞서 살펴보았던 모바일 환경에서의 원격 삭제 방법들[3],[4]은 모바일 환경의 특성을 이용하기 때문에 포괄적 임베디드 환경에 적용이 어렵다.

3. 결론 및 추후연구

임베디드 시스템이 군사 영역에서 사용되면서 임베디드 기기에는 특수한 기밀 데이터가 저장되기도 한다. 전시 상황과 같은 특수한 상황에서 임베디드 기기의 제어권을 잃었을 때 저장되어 있는 중요한 데이터를 지키기 위해서는 복구가 불가능하도록 삭제하고 이를 보장할 수 있어야 한다. 본 논문에서는 탈취된 임베디드 기기에 존재하는 데이터가 확실히 삭제되도록 보장하기 위한 5가지 요구사항을 도출하고 관련 연구들이 이를 충족하는지 살펴보았다. 그 결과 앞서 도출한 5가지 요구사항을 모두 만족하는 관련 연구는 없는 것으로 보인다. 그러나 임베디드 시스템이 군사 영역에서 무기 등에 탑재되기 시작하면서 전시 상황과 같은 특정 상황에서의 기밀 데이터 삭제와 그를 보장하는 일은 중요해질 것으로 생각된다. 따라서 원격으로 기기를 제어할 수 없는 상황에서도 기밀 데이터가 삭제될 수 있는 방안과 해당 기밀 데이터가 삭제되었음을 검증하는 방안에 대해 추가적인 연구가 진행되어야 하며 해당 방법이 미래의 무기체계에 탑재된다면 군 기밀 데이터 보안에 큰 기여를 할 수 있을 것으로 생각된다.

참 고 문 헌

[1] Daniele Perito, and Gene Tsudik. “Secure code update for embedded devices via proofs of secure erasure.“ European Symposium on Research in Computer Security. Springer, Berlin, Heidelberg, 2010.

[2] Mahmoud Ammar, et al. “SPEED: Secure Provable Erasure for Class-1 IoT Devices.“ Proceedings of the Eighth ACM Conference on Data and Application Security and Privacy. ACM, 2018.

[3] K. S. Kuppusamy, Senthilraja. R, and G. Aghila. “A model for remote access and protection of smartphones using short message service.“ International Journal of Computer Science, Engineering and Information Technology (IJCSEIT), 2012.

[4] Xingjie Yu, et al. “Remotely wiping sensitive data on stolen smartphones.“ Proceedings of the 9th ACM symposium on Information, computer and communications security. ACM, 2014.

[5] Stefan Dziembowski, Tomasz Kazana, and Daniel Wichs. “One-time computable self-erasing functions.“ Theory of Cryptography Conference. Springer, Berlin, Heidelberg, 2011.