국가 정보전 관점에서의 부채널 기반 공격 시나리오 및 대응 전략

김동영[1]
[1]경북소프트웨어마이스터고등학교
소프트웨어개발과
dongyoung0912@gmail.com

Side-Channel Scenarios and Countermeasures for National Information Warfare

Dong-Young Kim[1]
[1]Dept. of Software Development,
Gyeong-Buk Software Meister High School

요 약

하드웨어 부채널 공격은 장치가 의도치 않게 흘리는 물리적 신호(전력 소비, 전자기 방사, 연산 시간 등)를 이용해 기밀 정보를 탈취하는 기법이다. 본 논문은 국가 수준 정보전에서 실질적으로 활용 가능한 두 가지 부채널 시나리오(원격 전자기(EM) 도청 및 공급망 개입을 통한 전력 분석)를 제시하고, 각 시나리오의 성공 요건·위험도·탐지 가능성·대응 요건을 비교·분석한다. 또한 차폐, 부채널 무효화 기법, 공급망 보안 강화 등 기술적·정책적 대응책을 통합적으로 제시하며 향후 실험적 검증 및 대응 방향을 논의한다.

1. 서론

현대 전자장비는 암호 알고리즘의 수학적 안전성에도 불구하고 전력 소비 패턴, 연산 지연, 전자기 방사 등 다양한 부수적 신호를 외부로 누설한다. 이러한 부채널(Side-Channel)은 대상과의 직접적 논리적 침해 없이도 기밀을 노출할 수 있기 때문에 국가 수준의 정보전에서 전략적 가치를 가진다. 본 연구는 하드웨어 기반 부채널 공격의 주요 사례를 살펴보고, 국가 정보전 관점에서 부채널 공격의 현실적 시나리오를 구성, 시나리오별 성공/방어 요건을 체계화하여 국가·군사·산업 인프라 보호를 위한 기술적·제도적 대응책을 제안을 위한 기반을 마련한다.

2. 관련 연구 및 기술적 배경

부채널 공격 연구는 오랜 역사를 가진 분야로서 초창기에는 타이밍 공격과 전력 분석이 주를 이루었다. Kocher 등은 연산 시간 차를 이용한 공격을 보고하였고[1], 그 후 전력 분석(DPA), 전자기(EM) 누설·도청(TEMPEST) 등이 공개되었다.[2] DPA는 수천~수만회의 전력 측정에서 통계적 상관관계를 이용해 비밀키를 추정하며, 타이밍 공격은 연산 소요시간의 미세 차이를 이용해 내부 상태를 복원한다. EM 누설 관련 연구는 원격 감청을 통해 암호키나 화면 내용을 복원할 수 있음을 실험적으로 보여주었다.[3] 최근에는 저전력·소형 IoT 장치를 대상으로 하는 EM 기반 공격[4]도 진행된다.

3. 부채널 정보전 시나리오 정의 및 분석

3-1. 원격 EM 도청

원격 EM 도청 시나리오는 목표 주변 특정 지점에서 고감도 안테나 및 신호 수집 장비를 이용하여 장비가 방출하는 전자기 신호를 장시간 관측하고, 수집한 신호를 스펙트럼 정제·동기화·통계 분석 또는 머신러닝 기반 분류 기법을 통해 복원한다. 공격자는 대상 장비의 방출 특성을 사전에 수집하거나, 현장 관측을 통해 실시간으로 파악한 뒤, 고감도 RF 수신기와 노이즈 감소를 위한 신호처리 알고리즘을 이용해 필요한 정보를 분리한다. 이 시나리오의 성공을 위해서는 감도와 신호 대 잡음비(SNR)가 충분히 높아야 하며, 장비 또는 운용 환경에 차폐 목적의 Faraday cage가 없거나 불완전해야 한다. 실행 난이도는 높지만 성공시 은밀하게 정보를 탈취할 수 있다는 이점이 있다. 실제 정보기관들은 수십 년간 이러한 원격 전자기파 수신을 활용해왔으며, 공격 행위 자체가 전자파 수신에 불과해 피공격측에서 탐지하기가 극히 어렵다.

<표 1> 시나리오별 공격 성공, 방어 요건 및 특성

항목	공격 성공 요건	공격 방어 요건	비고
원격 EM 도청	고감도 수신장비, 유리한 SNR, 대상 장비의 차폐 취약성	EM 차폐(Faraday cage), 실시간 EM 스펙트럼 모니터링, Zoning(구역 격리)	접근 없이 정보 유출 가능
공급망 삽입	공급망 침투(제조/유통 단계), 은닉 센서·통신, 전력 상관성 확보	공급망 무결성 검증, 물리적 검사(엑스레이), HW 해시/펌웨어 검증	장기적 정보 유출 위험
탐지 가능성	외부 수신만으로 탐지 어려움	지속적 수집·이상 탐지, 체계적 규제 필요	로그 無
공격 자원	고도의 기술·장비(국가 수준) 또는 내부자 협력 필요 및 대응 필요		국가적 주도

3-2. 공급망 개입을 통한 전력 분석

공급망 개입 시나리오는 제조·조립·검수·유통 단계에서 악성 하드웨어를 은닉하거나, 반도체/모듈 제조 과정에 변형을 가해 제 전류 센서, 데이터 로거, 또는 원격 송수신 모듈을 기기에 은닉하여 출하 후 장기간에 걸쳐 사용자의 연산 패품에 정보 유출 수단을 삽입하는 방식이다. 초소형턴을 수집하거나, 회수하여 분석하는 시나리오가 대표적이다. 기기 자체의 전력선 변동을 감지해 저장한 후 일정 시점에 회수되어 분석된다. 예컨대 특정 암호모듈에 초소형 전류 센서를 부착해 두면, 원격에서 평문 암호키에 따른 소비전력 패턴을 수집하여 키를 차분 전력분석으로 역추적할 수 있다. 이 시나리오의 성공을 위해서는 공급망의 물리적 접근이 가능한 침투 경로가 필요하며(내부자 협력), 은닉 장치가 사용 중 성능에 거의 영향을 주지 않아 검수 과정에서 발견되지 않아야 한다. 또한 전력 패턴과 내부 데이터 간의 상관관계를 확보할 수 있을 만큼 충분한 데이터가 수집되어야 한다. 탐지는 매우 어려운데, 수집 센서는 시스템 동작에는 영향을 주지 않으므로 일반 보안점검으로는 발견되지 않을 수 있다. 실제 냉전 시대에도 상대국 대사관에 납품된 사무기기에 도청 장치를 은닉하여 키 입력 등을 유출시킨 사례[5]가 있다.

4. 대응 방안 및 결론

부채널 공격에 대응하기 위해서는 기술적 대책과 정책적 대책을 병행해야 한다. 기술적으로는 부채널 정보의 누설을 줄이거나 무의미하게 만드는 설계가 핵심이다. 전자기 방사를 차폐하기 위한 TEMPEST 표준을 적용, 장비를 밀폐된 암실이나 Faraday cage 내부에서 운영하여 민감 설비의 EM 누설을 물리적으로 억제하며 전력선 필터링 및 전원 클린업을 통해 전력 기반의 누설 신호를 줄인다. 소프트웨어·하드웨어 레벨에서 마스킹 및 블라인딩 기술을 적용하여 통계적 분석의 유효성을 낮추고 의도적 노이즈 주입을 통해 신호 상관성을 약화시킬 수 있다. 이런 대책들은 성능 오버헤드나 비용 증가를 초래하지만 기밀성 확보를 위해 중요하다. 한편 정책적 대응으로는 민감 정보시설의 운영과 인증, 신뢰할 수 있는 공급망 구축 등이 있다. 핵심 기기에 대해 물리적·논리적 보안 표준을 법적·계약적 의무로 명시하고, 이를 충족하지 못하는 장비는 공공·군사 도입 대상에서 배제하는 제도를 마련해야 한다. 또한 공급망의 투명성 및 추적성을 법적·제도적으로 강화해야 한다. 제조·조립·유통·수리·회수 등 모든 단계에 대한 디지털 기록을 의무화, 부품의 출처와 변경 이력을 추적할 수 있게 하여 공급망 공격에 대응한다.

본 논문은 전략적·개념적 분석에 중점을 두었으므로 몇 가지 한계가 존재한다. 제시된 시나리오의 실험적 재현을 포함하지 않았다. 또한 공급망 침투의 실제 비용·수행 가능성에 대한 정량적 분석이 부족하다. 향후 연구로는 실제 하드웨어 환경에서의 공격과 평가, 그리고 공급망 침투에 대한 경제적·조직적 모델링을 통한 위험평가, 방어책의 비용 효과 분석을 통해 우선순위를 제시가 요구된다.

참고문헌

[1] P. Kocher, “Timing Attacks on Implementations of Diffie-Hellman, RSA, DSS, and Other Systems,” Advances in Cryptology – CRYPTO’96, 1996.

[2] Standaert, F. X., Introduction to Side-Channel Attacks. In: Verbauwhede, I. (ed.), Secure Integrated Circuits and Systems, Boston, MA: Springer, 2010.

[3] Genkin, D.: Detecting Screen Content via Remote Acoustic Side Channels, Proceedings of the 2019 IEEE Symposium on Security and Privacy (SP), San Francisco, USA, 2019, pp. 853 - 869.

[4] Conti, M., Losiouk, E., Poovendran, R., Spolaor, R., Side-channel attacks on mobile and IoT devices for Cyber - Physical systems, Computer Networks, Vol. 207, Article 108858, 2022.

[5] Wright, P., Spycatcher: The Candid Autobiography of a Senior Intelligence Officer, New York: Viking, 1987.