ChipWhisperer를 이용한 패스워드 기반 인증 방식의 단순 전력 분석 검증[1)]

최낙준* 이지은** 김광조*,**

KAIST *정보보호대학원 **전산학부

Simple Power Analysis on Password-based Authentication using ChipWhisperer

Nakjun Choi* Jeeun Lee** Kwangjo Kim*,**

*Graduate School of Information Security **School of Computing, KAIST

요 약

사용자가 입력한 문자열과 서버에 저장된 문자열의 일치여부만을 확인하는 패스워드 기반 인증 방식은, 그 간편성으로 인해 인터넷상의 각종 정보통신 서비스에서 광범위하게 사용되고 있다. 따라서 우리는 패스워드 기반 인증 방식의 서버와 사용자 간 전송 채널 상에서 획득한 부채널 정보(특히, 전력 소모 정보)를 이용하여 공격이 가능함을 검증하고자 한다. 본 논문에서는 캐나다 NewAE Technology(사)의 ChipWhisperer와 단순 전력 분석(Simple Power Analysis) 스크립트를 이용하여 부채널 공격을 수행한 결과, 간단하게 공격이 가능함을 보이고 추후 연구 방안을 제시한다.

I. 서론

패스워드 기반 인증 방식은 개인의 정보보호를 위한 다양한 방법 중 가장 기초적이고 간단한 방법이다. 추가적인 인증 없이 문자열의 일치 여부만 확인하는 간편함 덕분에 온라인 계정 로그인, 디지털 도어락, 은행 계좌 관리 등 온·오프라인을 가리지 않고 광범위하게 사용되고 있다. 하지만 패스워드 기반 인증 방식이 널리 사용되는 만큼, 이를 무너뜨리기 위한 새로운 공격 방법 또한 꾸준히 개발되고 있다. 만약 패스워드 기반 인증 방식이 이러한 공격에 취약한 내부적 결함을 가지고 있다면 이는 사회 전반적인 보안에 직접적인 영향을 미칠 것이 분명하다. 따라서 높은 안전성을 갖춘 고성능 패스워드 기반 인증 방식을 개발하는 것이 매우 중요하다.

1) 이 논문은 SK Telecom Network R&D Center의 지원을 받아 수행된 연구임.

웹 보안의 경우, 사용자가 패스워드 인증 방식을 통과하더라도 추가적인 인증 과정을 거쳐야 로그인이 가능하도록 시스템을 구성하는 경우가 있지만, 대부분의 하드웨어 기반 패스워드 인증 방식은 패스워드가 일치할 경우 곧바로 데이터에 접근이 가능하다. 또한 하드웨어의 물리적인 특성으로 인해 타이밍 공격(Timing Attack) 또는 오류 주입 공격(Fault Injection Attack) 등 부채널 공격의 위험에 항상 노출되어 있다. 따라서 패스워드 기반 인증 방식의 보안성이 인정받기 위해서는 해당 시스템이 부채널 공격에도 안전함을 보여야 한다.

본 논문에서는 캐나다의 NewAE Technology(사)에서 제공하는 패스워드 기반 인증 방식과 단순 전력 분석(Simple Power Analysis, SPA) 스크립트를 이용하여 부채널 공격을 구현해보고 이를 토대로 부채널 공격 대응 연구의 중요성에 대해 논한다 [1].

본 논문의 구성으로 Ⅱ장에서는 부채널 공격에 속하는 전력 분석 공격과 타이밍 공격에 대해 간단하게 설명하고, Ⅲ장에서는 실험을 진행한 환경에 대해서 서술한다. Ⅳ장에서는 이번 실험의 공격 대상인 패스워드 기반 인증 방식에 대해 설명하고, Ⅴ장에서 구체적인 공격 방법 및 결과에 대하여 서술한다. 마지막 Ⅵ장에서는 결론 및 이를 토대로 한 향후 연구 계획에 대해 논한다.

II. 배경지식

2.1 전력 분석 공격

[2]에서 처음 소개 된 전력 분석 공격은 공격 대상에 직접적인 손상 또는 변형을 가하지 않기 때문에 수동(Passive) 공격 및 비침입 공격으로 분류된다. 전력 분석 공격은 크게 단순 전력 분석과 차분 전력 분석(Differential Power Analysis, DPA)으로 나뉜다.

단순 전력 분석은 암호 장치의 연산 과정에서 소비되는 전력 변화를 측정 후 분석하여 비밀키 등의 유용한 정보를 얻어내는 공격 방법이고, 차분 전력 분석은 측정된 전력 소모량의 통계적 특성을 비교하여 비밀키를 추정해내는 방법이다. 본 논문에서는 단순 전력 분석 공격을 통하여 실험을 진행하였다. 전력 분석 공격을 막기 위해서는 연산에 소모되는 소비전력에 무작위성을 부여하거나 중간 값을 감추는 마스킹 기법 등이 사용되어야 한다.

2.2 타이밍 공격

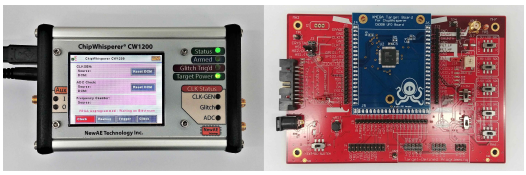
타이밍 공격은 알고리즘 연산에 소요되는 시간을 측정하여 유용한 정보를 얻어내는 공격으로서 부채널 공격 중 가장 기본이 되는 공격 방법이다. [3]에서 처음 소개된 타이밍 공격은 전력 분석 공격과 마찬가지로 수동 공격 및 비침입 공격으로 분류된다.

비교적 간단한 방법으로 공격을 구현할 수 있지만 연산과정에 의도적인 시간 지연을 발생시키는 방법으로 대부분의 타이밍 공격에 대한 방어가 가능하다. 본 논문에서 사용할 패스워드 기반 인증 방식 또한 타이밍 공격에 대한 방어 기법을 갖추었다.

III. 실험 환경

3.1 실험 장비 및 소프트웨어

본 실험에서는 캐나다의 NewAE Technology(사)에서 제작한 ChipWhisperer-Pro (CW1200)를 사용하여 전력 분석 공격을 구현하였다 [4]. ChipWhisperer-Pro는 오픈 소스 임베디드 보안 분석 플랫폼으로서 FPGA(Field Programmable Gate Array) 기반 펄스를 생성하여 클록 및 전압 오류 주입 공격 등 다양한 부채널 공격이 가능하도록 해준다.



[그림 1] ChipWhisperer-Pro(CW1200, 왼쪽), CW308 UFO 보드와 CW308T XMEGA 타겟 보드(오른쪽)

실험에 사용한 패스워드 기반 인증 방식은 프로그래밍이 가능한 FPGA 보드 중 하나인 CW308T XMEGA 타겟 보드에 소스코드를 업로드 하는 방법으로 구현하였다. [그림 1]은 우리가 실제로 실험에 사용한 ChipWhisperer 장비와 FPGA 보드를 나타낸다.

또한 소모되는 전력을 기록 및 분석하기 위해서 NewAE Technology(사)에서 기본적으로 제공하는 'ChipWhisperer Capture' 오픈 소스 소프트웨어를 사용하였다.

3.2 공격 모델

본 실험에서는 공격 대상인 패스워드 인증 방식의 소스코드를 공격자가 모두 확인 할 수 있고 이를 이용하여 전력 소모량이 변화하는 지점을 찾아내었기 때문에 화이트 박스 모델에 가깝다고 할 수 있다. 하지만 공격자가 소스코드에 접근 할 수 없다고 하더라도, 패스워드의 첫 문자에 전수공격을 가하는 방법을 통해 전력 소모량이 변화하는 구간을 찾아낼 수 있다. 따라서 블랙 박스 모델에도 동일한 공격 방식을 충분히 적용시킬 수 있지만 본 실험에서는 다루지 않았다.

IV. 패스워드 기반 인증 방식

본 실험에서는 NewAE Technology(사)가 기본적으로 제공하는 패스워드 인증 방식 소스코드를 토대로 시스템을 구현하였다. 원활한 실험을 위하여 다섯 자리의 문자열인 'ciscw'를 최초 패스워드로 설정 한 뒤, CW308T XMEGA 타겟 보드에 해당 소스코드를 업로드 하였다. [그림 2]는 패스워드 인증 방식의 실행 결과를 나타낸다. 사용자가 잘못된 비밀 번호인 'abcd'를 입력할 경우엔 패스워드가 일치하지 않는다는 메시지를 출력하고, 올바른 패스워드를 입력할 경우엔 접근이 허용되었다는 메시지가 출력된다.

[그림 2] 패스워드 인증 방식의 실행 결과

본 실험에서 사용한 패스워드 인증 방식은 입력 받은 패스워드를 1 Byte씩 비교하는 알고리즘을 취하고 있다. 즉, 사용자가 'abcd'를 입력하였을 경우, 패스워드 인증 시스템은 'abcd' 전체가 아닌 'a' 하나의 일치여부를 먼저 확인한다. 불일치할 경우 나머지 4 Byte의 확인 과정을 생략할 수 있기 때문에 연산 속도를 높일 수 있다는 장점이 있지만, 이는 연산 시간과 전력소비의 차이를 발생시키는 원인이 되기 때문에 타이밍 공격과 전력 분석 공격에 취약해질 수 있다. 본 실험에서 사용한 패스워드 인증 방식은 타이밍 공격에 대응하기 위하여 패스워드 불일치 시 랜덤한 시간 지연을 발생시키는 소스코드를 탑재하고 있고 이는 [그림 3]과 같다. 하지만 전력 분석 공격에 대한 대응 기법은 적용 되어 있지 않기 때문에 본 실험에서는 해당 패스워드 인증 방식에 단순 전력 분석 공격을 수행하였다.

```
if (passbad){
    //Stop them fancy timing attacks
     int wait = rand() % 100000;
    for(volatile int i = 0; i < wait; i++){
        ;
    }
    delay_200_ms();
    delay_200_ms();
    my_puts("PASSWORD FAIL\n");
    led_error(1);
```

[그림 3] 타이밍 공격에 대응하기 위한 랜덤 시간 지연 소스코드

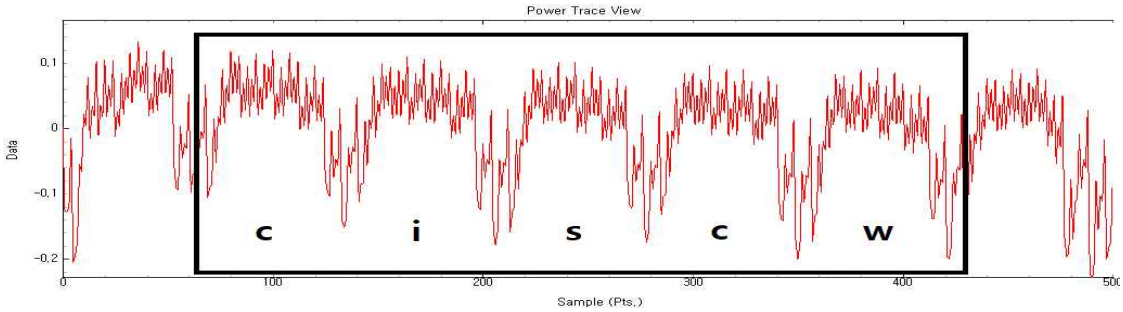
V. 단순 전력 분석 공격

우리는 ChipWhisperer Capture 소프트웨어를 이용하여 패스워드 인증 방식의 연산 시 소모되는 전력을 측정하였다. [그림 4]는 올바른 패스워드인 'ciscw'를 입력했을 때의 전력 소모량을 나타낸다. 시간이 흐름에 따라 전력소모량이 변화하는 것이 명확하게 나타나기 때문에 단순 전력 분석 공격을 통해 유용한 정보를 얻어 낼 수 있음을 쉽게 예상할 수 있다.

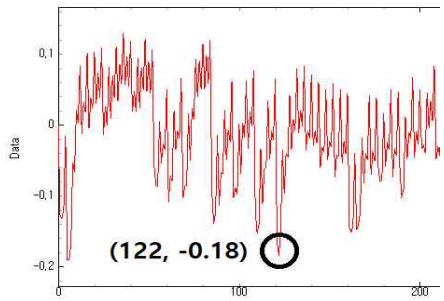
실제 공격을 구현하기 위하여 우리는 NewAE Technology(사)가 제공하는 단순 전력 분석 공격 스크립트를 사용하였고 공격 방법은 다음과 같다 [5].

1) 전력 소모 그래프에서의 타겟 포인트 결정
2) 패스워드의 첫 번째 Byte가 일치할 때와 일치 하지 않을 때의 타겟 포인트 변화량 측정
3) 매 Byte 마다 타겟 포인트 지점 전력이 일정 값을 초과 하는지 확인
4) 초과할 경우 올바른 Byte, 미만일 경우 잘못된 Byte로 판별
5) 모든 Byte를 진행 후 최종 패스워드를 출력

패스워드를 찾아내기 위해선 먼저 전력 소모 그래프에서 확연하게 구별이 가능한 타겟 포인트를 결정해야 한다. [그림 5]는 패스워드의 첫 번째 Byte가 일치하지 않을 때의 전력 소모량을 나타내는데, 검은색 원으로 표시한 122 포인트 지점이 상대적으로 낮은 전력소모량을 보이기 때문에 타겟 포인트로 결정하였다.



[그림 4] 올바른 패스워드 입력 시 전력 소모 그래프



[그림 5] 첫 번째 Byte 불일치 시 타겟 포인트

패스워드의 첫 번째 Byte가 일치하면 타겟 포인트는 194 지점으로 이동하는데 이를 통해 타겟 포인트 변화량이 74인 것을 알아 낼 수 있다. 즉, 우리는 122 포인트를 시작으로 74 포인트씩 이동한 지점의 전력 소모량이 일정 값을 초과하는지 확인해보는 방법을 통해 패스워드 일치 여부를 결정 할 수 있다. 본 실험에서는 측정되는 전압 -0.15mV를 기준으로 패스워드를 판별하였다.

타겟 포인트 변화량을 측정한 이후에는 단순 전력 분석 공격 스크립트 의해, 패스워드 인증 시스템에 'a'부터 '0'까지의 문자 및 숫자가 순차적으로 대입된다. 앞선 방법으로 패스워드의 첫 번째 Byte인 'c'를 찾아낸 후에는 다시 'ca'를 시작으로 'c0'까지 대입을 반복하며, 최종적으로 'ciscw'의 패스워드를 확정 한 후 공격이 종료된다.

만약 패스워드의 첫 번째 Byte가 일치하지 않았을 때 연산을 즉시 종료하지 않고 나머지 Byte의 비교 연산을 계속 수행하도록 알고리즘을 변경해준다면 성공적으로 단순 전력 분석 공격을 막아 낼 수 있다.

VI. 결론 및 향후 연구

본 논문에서는 NewAE Technology(사)에서 제공하는 패스워드 인증 방식과 단순 전력 분석 공격 스크립트를 이용하여 부채널 공격 방법을 구현하였다. 공격자가 패스워드 인증 방식의 전력 소비량 변화를 확인할 수 있다면 간단한 공격을 통하여 패스워드를 획득 할 수 있음을 보여주었다. 이는 패스워드 인증 방식을 광범위하게 사용하는 현대 보안산업에 큰 위협이 될 수 있다. 따라서 다양한 부채널 공격에 대응 할 수 있는 기법을 개발 및 적용하는 것이 매우 중요하다.

향후 연구 과제로는 난수 발생기 중 하나인 Xorshift128+에 다양한 부채널 공격을 시도하여 난수성을 낮추는 연구를 진행할 예정이다.

[참고문헌]

[1] NewAE Technology, https://newae.com/

[2] Power analysis attack, http://softknow.com/up2/file/20130930/20130930141438_0781.pdf

[3] P. C. Kocher, Timing attacks on implementations of Diffie-Hellman, RSA, DSS, and other systems, *Annual International Cryptology Conference*. Springer, 104-113. 1996.

[4] ChipWhisperer-Pro, https://wiki.newae.com/Main_Page. https://newae.com/tools/chipwhisperer/

[5] https://wiki.newae.com/Tutorial_B3-1_Timing_Analysis_with_Power_for_Password_Bypass