ZIP password cracking (with GPU)

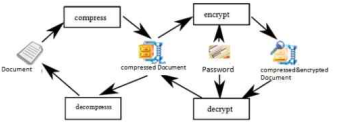
IT융합공학부 윤세영

유투브 주소: https://youtu.be/foVw_os5XcM

목차

Password recovery for encrypted ZIP archives using GPUs (2010)

- “GPU를 활용한 ZIP 암호 해독”
- ZIP 암호화 프로세스: 비밀번호 생성 -> 키 도출 -> 데이터 암호화
- ZIP 복호화 프로세스: 비밀번호 입력 -> 키 도출 -> 데이터 복호화



- 비밀번호 검색 공간 축소 -> GPU를 사용하여 해시 함수 생성

-> 비밀번호 검색 공간에서 동시에 비밀번호 확인

-> 가능성 있는 비밀번호에 대한 AES 암호화 키 생성

- 주어진 비밀번호로부터 해시 함수를 사용하여 AES 키를 생성 (PBKDF2 함수 사용)
- PBKDF2(pw, salt, dkLen), HMAC-SHA1 알고리즘 1000번 수행
- 생성된 AES 키를 사용하여 암호화된 ZIP 파일을 복호화
- 압축 파일에 저장된 MAC 값과 비교되어 비밀번호가 올바른지 여부를 결정하는 확인 값을 생성

Password recovery for encrypted ZIP archives using GPUs (2010)

- 결론
- GPU 기반 알고리즘과 CPU 기반 알고리즘의 성능 비교 (Table 3)
- DOC, PDF 등 암호로 보호된 파일에 대해서도 GPU를 사용해 볼 수 있을 것.
- 위 연구에서는 AES key space을 직접 공격한 것이 아닌 password space를 따로 생성하여 공격함.

-> 사용자의 비밀번호 기억 능력에 관한 심리학적 통계 결과를 사용하여 password space 생성

Table 2: Performance comparison of generating candidate passwords using the exhaustive search algorithm

The limited length of passwords	The number of passwords	CPU	1GPU	2GPUs	4GPUs
1	62	4s	22s	22s	22s
2	3,906	8m	22s	22s	22s
3	242,234	2.25h	180s	92s	48s
4	15,018,570	5.25d	168m	85m	43m

Information Password Recovery with GPU (2015)

- 이전 연구과 동일하게 비밀번호 공간을 축소하기 위해 사전 공격을 사용
- 패스워드 구조 분석 방법을 사용하여 코드 검색 공간을 좁히고*(여기까지 이전 연구와 동일),* WINZIP 헤더에 저장된 two byte의 패스워드 확인 값(PVV)의 정확성을 확인
- 결론: GPU를 사용하여 해시 함수의 복잡한 연산을 수행하고, 동시에 비밀번호 검색 공간에서 가능한 패스워드의 PVV와 AES에서의 암호화된 비밀 키를 확인함.

The length of passwords	The number of passwords	1CPU	1GPU	2GPUs	8GPUs
1	62	5s	20s	20s	15s
2	3,906	7m	43s	43s	31s
3	242,234	2.1h	4m35s	2m20s	55s
4	15,018,570	5.2d	3h	1h35m	28m

d is day, h is hour, m is minute, s is second.

Decryption-Decompression of AES Protected ZIP Files on GPUs (2016)

- 이전 연구들과 동일하게 AES 키 공간에 대한 직접 공격이 아닌 사전 공격 방법을 적용할 수 있도록 새로운 비밀번호 공간을 생성
- 비밀번호 검색 공간의 크기를 줄이기 위해 압축 도구의 특성을 활용하여 ZIP 파일 헤더에 저장된 two byte 패스워드 확인 값(PVV)을 기반으로 잘못된 패스워드를 감지

TABLE I. COMPARISON OF SPEED OF GENERATING KEYS ON CPU/GPUS

The number of CPU/GPUs	The number of keys /s	Time for recovering password
1CPU	35	5.25d
1GPU	1,536	3h5m
2GPUs	3,072	1h32m
4GPUs	6,144	45m48s

- 추후에 다시 볼 연구들

Decryption-Decompression of AES Protected ZIP Files on GPUs (2016)

Speedup and Password Recovery for Encrypted WinRAR3without Encrypting Filename on GPUs (2020)

- 세미나 두 줄 요약
- 1. ZIP 형식의 압축 파일의 비밀번호는 무차별 대입 공격에 대비하여 설계되어 있지만, GPU를 이용하여 유의미한 시간 내에 크래킹 가능하다.
- 2. ZIP 형식의 압축 파일은 AES 암호화를 사용하고 있으며, 대부분의 연구에서 AES 키 공간을 직접 공격하는 것이 아닌, 비밀번호 구조 분석 방법을 이용하여 더 축소된 비밀번호 공간을 공격하였다.

현재 진행중인 부분…

- John the ripper -> 7z2john.pl 있음 https://github.com/openwall/john/blob/bleeding-jumbo/run/7z2john.pl
- Hashcat -> 7-zip 알고리즘에 대한 해시 값을 패스워드로 바꾸는 코드 있음
- https://github.com/hashcat/hashcat/blob/master/src/modules/module_11600.c
- 우분투 환경 -> 인터넷 연결 오류 해결 중
- 윈도우 환경 -> 존더리퍼의 pl 파일 실행 불가 및 해시캣 명령어 오류
- 맥 환경 -> 맥 사용 자체가 서툴러서 시도 안 함