scrypt

IT융합공학부 윤세영

유투브 주소: https://youtu.be/8VpJI-nEQm8

목차

scrypt 란?

- 기존의 키 유도 함수(KDF, Key Derivation Function)는 다량의 반복 횟수로 무차별 대입 공격 시 연산 시간이 오래 걸리는 데 안정성을 기반함
- 그러나 기존의 KDF는 요구하는 메모리 자원이 낮기 때문에, 충분한 메모리 자원을 가진 공격자가 대규모 병렬 공격을 시도해 볼 수 있는 위험이 있음
- scrypt는 알고리즘의 메모리 사용량을 증가시켜 공격자로 하여금 큰 (메모리)비용을 부담하게 하는 기법임
- 비밀번호를 cracking하는 데 같은 시간이 걸린다고 가정했을 때 scrypt는 bcrypt보다 약 4000배, PBKDF2보다 20000배 더 큰 비용이 들어간다고 추정함. (출처: https://www.tarsnap.com/scrypt.html)

scrypt – Parameter 및 Input / Output

Parameter: PRF, hlen, MF, MFLen

PRF: 의사 난수 함수

hlen: PRF에 의해 생성된 출력 길이

MF: 순차 메모리 하드 함수

MFLen: MF로부터 흡합된 블록의 길이

MF 범위: $\mathbb{Z}_{256}^{MFLen} \times \mathbb{N}$ 부터 $\mathbb{Z}_{256}^{MFLen}$ 까지

Input, (P, Salt, N, r, p, dkLen)

P: password / passphrase, 해시할 문자열

Salt: 해시하기 전에 추가로 입력되는 랜덤 데이터

N: CPU, 메모리 비용 매개변수 (2의 거듭제곱)

r: 블록사이즈 결정 매개변수(일반적으로 8, 순차 메모리 읽기 크기와 성능을 미세 조정하는 매개변수)

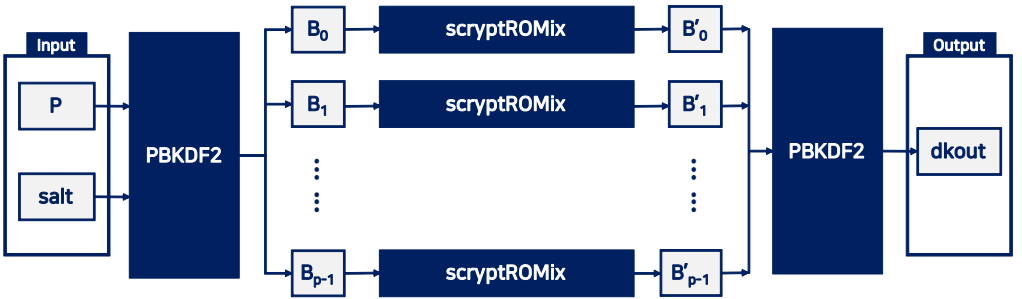
p: 병렬화 매개변수(양의 정수)

dkLen: derived key의 의도된 출력 길이

Output, DK

DK: 길이가 dkLen인 derived key

scrypt – 구성(알고리즘 진행 과정)



[표 1] 함수별 사용 Cycle

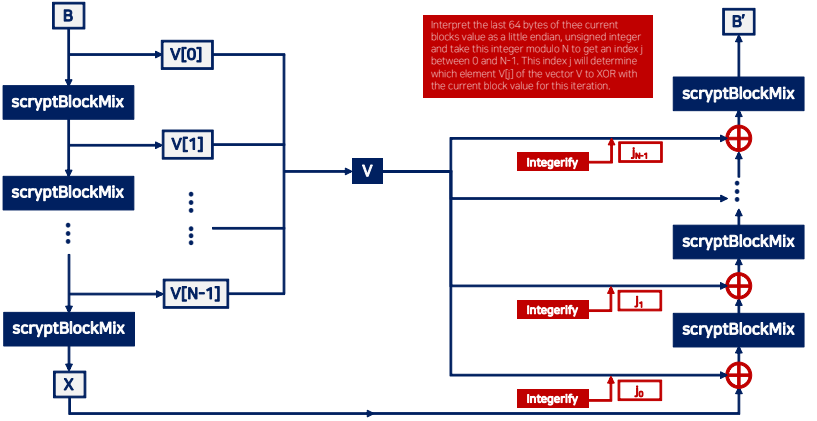
Algorithm	Cycle(Clock)	Ratio
PBKDF2(블록 생성)	166,833	1.02
scryptROMix	16,141,658	98.58
PBKDF2(파생키 생성)	65,009	0.39
Total	16,373,500	100

(r = 8, p = 2, N = 1024, dkLen = 64)

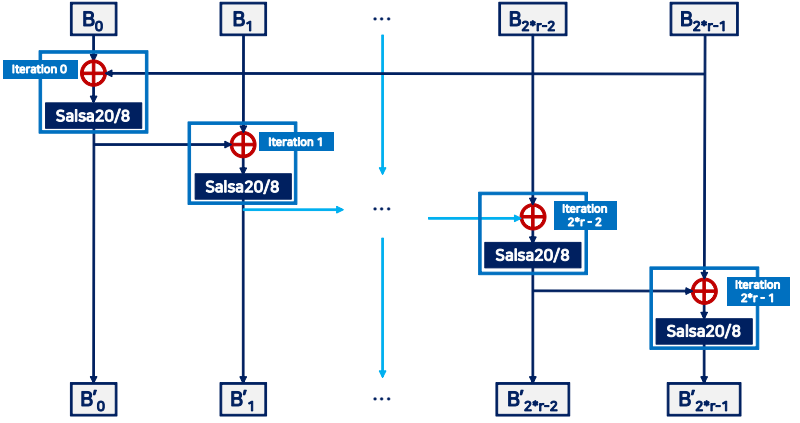
참고사이트: https://www.pointsoftware.ch/2014/10/01/the-importance-of-hashing-passwords-part-4-the-hardware-threat/

참고논문: 최성준 외 2명, "GPU 환경에서의 Scrypt 알고리즘 병렬 구현 최적화 연구", 한국정보보호학회 하계학술대회 논문집 Vol.33, p106-110, 2023.

scrypt – 구성(알고리즘 진행 과정) scryptROMix



scrypt – 구성(알고리즘 진행 과정) scryptBlockMix



Cracking

Brute-force attack

- 추측 암호를 고유한 알고리즘으로 해싱하여 저장된 해시값과 반복적으로 비교한다.

KDF	6 letters	8 letters	8 chars	10 chars	40-char text	80-char text
DES CRYPT	< $1	< $1	< $1	< $1	< $1	< $1
MD5	< $1	< $1	< $1	$1.1k	$1	$1.5T
MD5 CRYPT	< $1	< $1	$130	$1.1M	$1.4k	1.5×10^{15}
PBKDF2 (100 ms)	< $1	< $1	$18k	$160M	$200k	2.2×10^{17}
bcrypt (95 ms)	< $1	$4	$130k	$1.2B	$1.5M	$48B
scrypt (64 ms)	< $1	$150	$4.8M	$43B	$52M	6×10^{19}
PBKDF2 (5.0 s)	< $1	$29	$920k	$8.3B	$10M	11×10^{18}
bcrypt (3.0 s)	< $1	$130	$4.3M	$39B	$47M	$1.5T
scrypt (3.8 s)	$900	$610k	$19B	$175T	$210B	2.3×10^{23}

Fig. 1: Estimated hardware cost to crack hashed passwords in 1 year as per 2002 [21]

- 해시된 비밀번호를 1년 동안 crack하는데 필요한 하드웨어의 비용을 추정한 것

PBKDF2는 적은 메모리 자원을 요구하므로 굳이 GPU를 쓰지 않아도 되지만, bcrypt와 scrypt 같은 경우에는 요구하는 메모리 자원이 크다는 것을 알 수 있음

참고 논문: https://arxiv.org/abs/1602.03097

Cracking

In addition, recent work on GPU- and FPGA-facilitated cracking of bcrypt and scrypt hashes has shown scrypt can be attacked quite efficiently for smaller parameters using GPUs and bcrypt can be attacked rather efficiently using FPGAs, as shown in figure 2.

	Cost		Target (CPU) runtime			
	HW	Energy	1ms	10ms	100ms	1000ms
bcrypt						
– zedboard	$319	$7.41	28.3 H/$s	2.81 H/$s	0.303 H/$s	0.0304 H/$s
– GTX 480	$517	$759	2.25 H/$s	0.250 H/$s	0.0264 H/$s	0.00212 H/$s
scrypt						
– GTX 480	$517	$759	33.4 H/$s (t=1)	1.83 H/$s (t=2)	0.0384 H/$s (t=8)	0.000287 H/$s (t=4)

Fig. 2: Hashes per dollar-second taking energy and hardware cost for two years into account as per 2015 [20]

참고 논문: https://arxiv.org/abs/1602.03097

참고문헌

참고논문(원본)[1]: https://www.tarsnap.com/scrypt/scrypt.pdf

참고자료[2]: https://datatracker.ietf.org/doc/html/rfc7914

참고자료[3]: https://www.tarsnap.com/scrypt/scrypt-slides.pdf

참고사이트[4]: https://en.wikipedia.org/wiki/Scrypt

참고사이트[5]: https://stytch.com/blog/what-is-password-hashing/

참고사이트[6]: https://security.stackexchange.com/questions/234558/why-isnt-it-more-popular-to-increase-the-p-parallelization-parameter-of-scryp

참고논문[7]: 최성준 외 2명, "GPU 환경에서의 Scrypt 알고리즘 병렬 구현 최적화 연구", 한국정보보호학회 하계학술대회 논문집 Vol.33, p106-110, 2023.


Q&A