순환 신경망을 사용한 텍스트 기반 패스워드 예측 연구 동향

임세진[1], 김현지[1], 강예준[1], 김원웅[1], 오유진[1], 서화정[1]
[1]한성대학교 IT융합공학과
dlatpwls834@gmail.com, khj1594012@gmail.com, etus1211@gmail.com,
dnjsdndeee@gmail.com, oyj0922@gmail.com, hwajeong84@gmail.com

Text-based Password Guessing Research Trend using Recurrent Neural Networks

Se-Jin Lim[1], Hyun-Ji Kim[1], Yea-Jun Kang[1], Won-Woong Kim[1], Yu-Jin Oh[1], Hwa-Jeong Seo[1]
[1]Dept. of IT Convergence Engineering, Han-Sung University

요 약

텍스트를 기반으로 하는 패스워드는 다방면에서 가장 많이 사용되고 있는 인증 수단이다. 하지만 이러한 패스워드는 사용자의 기억에 의존하기 때문에 사람들은 일반적으로 기억하기 쉽게 '!iloveY0u'와 같은 암호를 사용한다. 이로 인해 사용자들의 패스워드 간에 규칙성이 생기게 되어 HashCat과 같은 크래킹 도구에 의해 해킹될 수 있다. 딥러닝을 통한 패스워드 예측의 경우, 일반적인 패스워드 크래킹 도구와 달리 패스워드 구조 및 속성에 대한 사전 지식 및 전문적 지식 없이도 패턴을 추출하고 학습할 수 있어 활발히 연구되고 있다. 본 논문에서는 딥러닝 모델 중에서도 순환 신경망을 사용하여 텍스트 기반의 패스워드를 예측하는 연구의 동향에 대해 알아본다.

1. 서론

텍스트를 기반으로 하는 패스워드는 다방면에서 가장 많이 사용되고 있는 인증 수단이다. 장비를 필요로하는 지문인식, 홍채인식 등과 같은 생체인증과는 달리 구현이 간단하여 널리 사용되고 있다. 하지만 이러한 패스워드는 사용자의 기억에 의존하기 때문에 사람들은 일반적으로 기억하기 쉽게 '!iloveY0u'와 같은 암호를 사용한다. 또한 일반적으로 한명의 사용자 당 20개 이상의 계정을 가지고 있어 40% 이상이 패스워드를 재사용한다[1]. 이러한 행위는 사용자들의 패스워드 간에 규칙성 및 취약점을 발생시키며 HashCat과 같은 크래킹 도구에 의해 패스워드가 해킹될 수 있다. 딥러닝을 통한 패스워드 예측의 경우, 일반적인 패스워드 크래킹 도구와 달리 패스워드 구조 및 속성에 대한 사전 지식 및 전문적 지식 없이도 패턴을 추출하고 학습할 수 있어 활발히 연구되고 있다. 본 논문에서는 딥러닝 모델 중에서도 순환 신경망을 사용하여 텍스트 기반의 패스워드를 예측하는 연구의 동향에 대해 알아본다.

2. 관련 연구

2.1 패스워드 크래킹

패스워드 크래킹은 가능한 모든 암호를 예측하는 무차별 대입 공격과 일반적인 단어 사전을 사용하여 사용자의 패스워드를 알아내는 사전 공격으로 나눌 수 있다. 대표적인 패스워드 크래킹 도구에는 John the Ripper[2]와 HashCat[3]이 있다. 이 도구들은 일련의 문자에 대한 해시 값을 계산하여 공격 대상 패스워드의 해시 값과 비교하여 패스워드를 크래킹하게 된다.

2.2 확률 기반 패스워드 예측

대부분의 패스워드 예측 모델은 확률 기반 모델이다.

확률 기반 모델에서 많이 사용되는 접근 방식은 Markov 모델[4]과 PCFG(Probabilistic Context-Free Grammar)[5]이다. Markov 모델은 모든 중요한 패스워드의 특징이 n-gram으로 구체화될 수 있다는 가정으로 구축된 모델이다. PCFG는 공개된 패스워드에 포함된 특수 문자, 숫자 및 영문자의 조합과 같은 문법 구조를 검사하고 분포 확률을 생성하여 이를 통해 패스워드 후보군을 생성하는 접근 방식이다.

3. 순환 신경망을 사용한 텍스트 기반 패스워드 예측 연구 동향

3.1 [6]

[6]에서는 처음으로 RNN을 사용하여 패스워드의 특징을 추출하였다. 3개의 LSTM 계층과 2개의 연결

된 계층으로 구성된 모델을 제안하였다. 제안하는 모델은 Fast, Lean, Accurate을 의미하는 FLA로 명명하였다. 해당 연구에서는 패스워드 예측 횟수가 많거나 복잡하거나 긴 패스워드를 대상으로 학습할 때 더 높은 성능을 보임을 알아냈다.

3.2 [7]

[7]에서는 구조적인 분할과 양방향 LSTM을 기반으로 하는 하이브리드 패스워드 예측 모델인 SPRNN을 제안했다. PCFG는 사용자의 패스워드 구성 습관을 학습하고 확률에 따라 정렬된 기본 구조 및 문자열 사전 모음을 생성하는 역할을 한다. 즉 패스워드 데이터셋을 구조화하는 구조 분할에 사용된다. PCFG에서 생성한 문자열 사전을 사용하여 양방향 LSTM을 훈련시키게 된다. 성능 평가를 위해 다양한 데이터셋에서 훈련되고 테스트한 모델의 경우와 동일한 데이터셋의 하위 집합에서 훈련되고 테스트한 모델의 경우의 시나리오로 나누었다. 두 시나리오 모두 확률 기반 접근 방식인 Markov 모델과 PCFG보다 우수한 성능을 보였으며 동일한 데이터셋을 사용한 모델이 다양한 데이터셋을 사용한 모델보다 높은 성능을 보였다.

3.3 [8]

[8]에서는 다양한 데이터셋에서 훈련되고 테스트되더라도 높은 성능을 가지는 하이브리드 모델인 GENPass를 제안했다. 이 모델은 패스워드를 일련의 단위로 인코딩하여 PCFG를 기반으로 한 태그를 부여하여 사전에 처리한다. 그 다음에 LSTM을 사용하여 패스워드를 생성하게 된다. 또한 패스워드의 가능성이 높은 단어들의 목록을 정하기 위해 CNN 분류기를 구축하였다. 결과적으로 GENPass는 동일한 데이터셋의 하위 집합에서는 LSTM 모델과 동일한 수준의 보안 레벨을 달성하면서 상당히 낮은 순위의 암호를 생성하였다. 하지만 다양한 데이터셋의 경우 LSTM보다 패스워드 일치율을 16~30% 향상시켰다.

4. 결론

본 논문에서는 순환 신경망을 사용하여 텍스트 기반의 패스워드를 예측하는 연구 동향에 대해 살펴보았다. 모델을 LSTM 계층과 다양한 방식을 하이브리드로 구현하는 방식으로 연구들이 진행되고 있음을 알 수 있다. 딥러닝을 사용하여 패스워드를 예측하게 되면 패드워드에 대한 사전 지식 및 전문적인 지식이 없어도 패턴을 추출하고 학습할 수 있으므로 이러한 예측 모델에 대항할 수 있는 방법에 대한 연구가 필요할 것으로 보인다.

5. Acknowledgement

This work was supported by Institute for Information & communications Technology Promotion(IITP) grant funded by the Korea government(MSIT) (No.2018-0-00264, Research on Blockchain Security Technology for IoT Services).

참고문헌

[1] Pearman, Sarah, et al. “Let's go in for a closer look: Observing passwords in their natural habitat,” Proceedings of the 2017 ACM SIGSAC Conference on Computer and Communications Security. 2017.

[2] John the Ripper. 2017. http://www.openwall.com/john/.

[3] HashCat. 2017. https://hashcat.net.

[4] Narayanan, Arvind, and Vitaly Shmatikov. “Fast dictionary attacks on passwords using time-space tradeoff,” Proceedings of the 12th ACM conference on Computer and communications security. 2005.

[5] Weir, Matt, et al. “Password cracking using probabilistic context-free grammars,” 2009 30th IEEE Symposium on Security and Privacy. IEEE, 2009.

[6] Melicher, William, et al. “Fast, lean, and accurate: Modeling password guessability using neural networks,” 25th USENIX Security Symposium (USENIX Security 16). 2016.

[7] Zhang, Mengli, et al. “A password cracking method based on structure partition and BiLSTM recurrent neural network,” Proceedings of the 8th International Conference on Communication and Network Security. 2018.

[8] Liu, Yunyu, et al. “GENPass: A general deep learning model for password guessing with PCFG rules and adversarial generation,” 2018 IEEE International Conference on Communications (ICC). IEEE, 2018.