딥러닝 기반 패스워드 생성 기술 동향

https://youtu.be/L5PVI29dRxA

Contents

CryptoCraft LAB

01. 패스워드의 보안 취약점

1) 패스워드는 **구현이 간단하여 가장 많이 사용**되고 있지만, 사람의 기억에 의존하는 특성이 있어 많은 사용자들이 **'!iloveY0u'**나 **생년월일 및 가족 이름과 같은 개인정보가 포함된** 기억하기 쉬운 패스워드를 사용

2) 일반적으로 사용자 한 명당 20개 이상의 계정을 가지고 있으며 40%가 패스워드를 **재사용**함

→사용자들의 패스워드 간 **규칙성**이 생기며 취약점으로 이어져 패스워드 크래킹 도구에 의해 해킹될 수 있음

→ John the Ripper, HashCat

- 패스워드 크래킹 도구는 패스워드의 구조 및 조합에 대한 **사전 지식과 전문적 지식이 요구**됨
- 딥러닝을 이용하여 패스워드를 생성하는 경우에는 패스워드 데이터셋으로부터 **모델이 스스로 패턴을 추출하고 학습함**

02. 관련 연구

패스워드 생성에서의 표적 공격 / 비표적 공격

- 개인정보가 포함된 패스워드는 공격 대상이 존재하는 표적 공격에 해당
- 개인정보에 관계없이 수행되는 공격은 비표적 공격에 해당
  (딥러닝을 활용한 패스워드 생성 기술은 **비표적 공격에 초점을 맞춰** 수행되고 있음)

패스워드 공격을 위한 3가지 접근 방식 (규칙 기반, 확률 기반, 딥러닝 기반)

- 규칙 기반 방식 - John the Ripper, HashCat
  - ✓ 패스워드 유출로 데이터의 패턴을 수집할 수 있으며 이를 통해 후보 패스워드를 생성할 수 있음 (생성 속도가 가장 빠름)
  - ✓ 규칙 생성을 위한 전문 지식이 요구됨 + 규칙 정의가 잘못된 경우 공격 성공확률이 크게 떨어짐
- 확률 기반 방식 - Markov 모델, PCFG (Probabilistic Context-Free Grammar)
  - ✓ 기존의 패스워드 생성 모델은 확률 기반 방식을 따름
  - ✓ Markov 모델 : 중요한 모든 패스워드의 특징이 n-gram으로 구체화될 수 있다는 가정으로 구축된 모델
  - ✓ PCFG : 공개된 패스워드에 포함된 문법 구조 (특수 문자, 숫자 및 영문자의 조합)를 검사하고 분포 확률을 생성하여 패스워드 후보군을 생성
- 딥러닝 기반 방식
  - ✓ 패스워드로부터 모델이 스스로 패턴을 추출하고 학습 (전문적 지식 요구X)
  - ✓ 패스워드의 생성 가능한 범위가 제한되지 않음 → 규칙 기반, 확률 기반 방식을 뛰어넘어 **더욱 광범위한 패스워드 생성 가능**

03. 딥러닝 기반 패스워드 생성 기술 동향

- **FLA** [Fast, lean, and accurate: Modeling password guessability using neural networks]
  - 패스워드 생성에 딥러닝을 적용한 **최초의 연구**
  - RNN 모델 (3개의 LSTM layer과 2개의 Fully Connected layer)을 사용하여 패스워드의 특징 추출
  - Markov 모델과 유사하게 패스워드의 선행 문자가 주어지면 다음 문자를 생성하도록 학습
    - ✓ 유사성으로 인해 FLA도 n-gram 범위에 포함되지 않는 특징은 인코딩에서 생략될 수 있음
    - ✓ **딥러닝 모델을 GPU 상에서 효율적으로 구현할 수 있다**는 점에서 Markov 모델보다 이점이 있음
  - 제안 모델은 **패스워드 예측 횟수가 많거나, 복잡하고 긴 패스워드를 대상으로 할 때** 더 높은 성능을 보임

03. 딥러닝 기반 패스워드 생성 기술 동향

- **GENPass** [GENPass: A general deep learning model for password guessing with PCFG rules and adversarial generation]
  - **다양한 데이터셋**에서 훈련되고 테스트되더라도 높은 성능을 가지는 하이브리드 모델 제안
  - 패스워드 일치율을 높이기 위해 **PCFG를 전처리에 사용**
  - 패스워드를 일련의 단위로 인코딩하여 PCFG 기반의 태그를 부여해 사전에 처리 → LSTM을 통해 패스워드 생성
  - 패스워드의 가능성이 높은 단어 목록을 정하기 위해 CNN 분류기를 구축
  - **동일 데이터셋의 하위 집합에서** LSTM만 사용한 모델보다 **약 1/10개의 패스워드만 생성하여 50%의 일치율 달성**
  - **다양한 데이터셋의 경우** LSTM만 사용한 모델보다 **패스워드 일치율을 16~30% 향상**시킴

03. 딥러닝 기반 패스워드 생성 기술 동향

- **Language Model** [Password guessing via neural language modeling]
  - Attention 기법
    - ✓ 텍스트가 입력으로 들어오면 단어, 문자 및 구문과 같은 특정 토큰에 **우선순위 부여**
      → 모델이 문법, 의미, 단어의 구조 등을 **학습하는데 도움을 주어** 텍스트 분류, **생성** 및 해석 가능성을 **향상**시킴
  - 5개의 LSTM layer와 Output layer로 구성된 모델 제안
  - **BERT** (Bidirectional Encoder Representation from Transformers) 모델을 사용하여 제안한 모델을 **지도하고 개선**
  - BERT의 학습 과정이 모델의 성능을 크게 향상시킬 수 있음을 보임
  - 데이터셋의 범위와 관계없이 PCFG 및 Markov 모델의 성능을 능가함

03. 딥러닝 기반 패스워드 생성 기술 동향

- **PassGAN** [Passgan: A deep learning approach for password guessing]
  - 패스워드 생성에 **GAN을 적용한 최초의 연구** (IWGAN 적용)
  - 패스워드 데이터셋을 사용하여 판별자 훈련 → 생성자가 실제 패스워드의 분포에 가깝게 생성하도록 학습
  - 충분한 패스워드를 생성했을 때, 규칙 기반 기법들과 FLA를 능가함
  - **HashCat과 결합**하여 사용할 경우, 단독으로 사용하는 경우보다 **패스워드 일치율이 크게 증가함**
  - 생성기에서 마지막 softmax 활성화 함수로 인해 **고유한 훈련 불안정성**이 있어 **추측 정확도가 낮아질 수 있다**는 단점 존재

04. 결론

- 딥러닝을 사용하여 패스워드를 생성하면 전문적인 지식 없이도 데이터로부터 **자동으로** 패턴을 추출하고 학습할 수 있음
- RNN, Attention 기반 모델, GAN과 같은 다양한 딥러닝 모델을 기반으로 한 패스워드 생성 기술의 연구동향을 살펴봄
- 텍스트 기반의 최신 딥러닝 기법들이 등장함에 따라 **기존 모델들과 최신 기술을 결합하여 패스워드 일치율을 향상시키는 방향으로 연구가 수행**되고 있음
- 패스워드 생성 기술은 **패스워드 보안 강도 평가**와 같은 분야에 응용될 수 있으므로 더욱 활발한 연구가 필요

05. 앞으로 할 일

- 동향 논문은 급하게 쓴거라 패스워드 생성 관련 최신 논문을 조금 더 찾아볼 생각입니다...
- 데이터셋 확보 (여러 논문에서 사용한 데이터셋 + 한글 자판 패스워드 데이터셋 등)
- GAN 모델 실습 및 BERT와 같은 최신 딥러닝 기술 실습
- 구현 논문들 코드 찾아서 분석
- 교수님께서 지난번에 제안해주신 예시 방향성으로 진행
  - ✓ 한국어 모델 특성에 맞는 학습 기법 (중국어 음절 기반 패스워드 생성 논문이 있음. 참고할 예정)
  - ✓ 패스워드 구성에 따른 기법 (특수문자, 소문자, 대문자, 숫자 등)
  - ✓ 패스워드 길이에 따른 기법
  - ✓ 최신 GAN 기술을 통해 네트워크 수정 (→ 생성 데이터셋의 다양성을 보장하는 BigGAN 기술 적용해보기)
  - ✓ 네트워크 하이퍼파라미터 수정

Q & A