최근 보안사고들의 관찰과 고찰 (AI를 곁들인)

스틸리언 대표 박찬암

2025. 12. 1.

STEALIEN

박찬암 CEO

現 대통령직속 국가인공지능전략위원회 보안TF 위원
現 중앙선거관리위원회 자문위원
現 개인정보보호위원회 적극행정위원
現 SK그룹 정보보호혁신특별위원회 자문위원
現 KT 민관합동조사단 자문위원
現 국방부 청렴국방 민관협의회 자문위원
現 서울동부지방검찰청 자문위원
現 한국수자원공사 AI First 자문위원
現 하나은행 자문위원

2024 정보보호 유공 대통령 표창
2021 행복한 중기경영대상 대상 경제부총리상
2020 존경받는 기업인상 중소벤처기업부 장관 표창
2018 포브스 선정 아시아의 영향력 있는 30세 이하 30인

2009 코드게이트 국제해킹방어대회 우승
2009 HITB CTF 세계해킹대회 1위

고등학교 교과서 수록

we STEAL ALIEN technology

“we STEAL ALIEN technology”

AppSuit

스틸리언의 대표적인
모바일 보안 솔루션

해킹 서비스

해커에 의한 공격 기반
보안 컨설팅

보안기술 R&D

해킹 및 보안 분야의
최첨단 기술 연구 개발

Cyber Drill System

해킹 교육 훈련 시스템


0-11 16:24:07

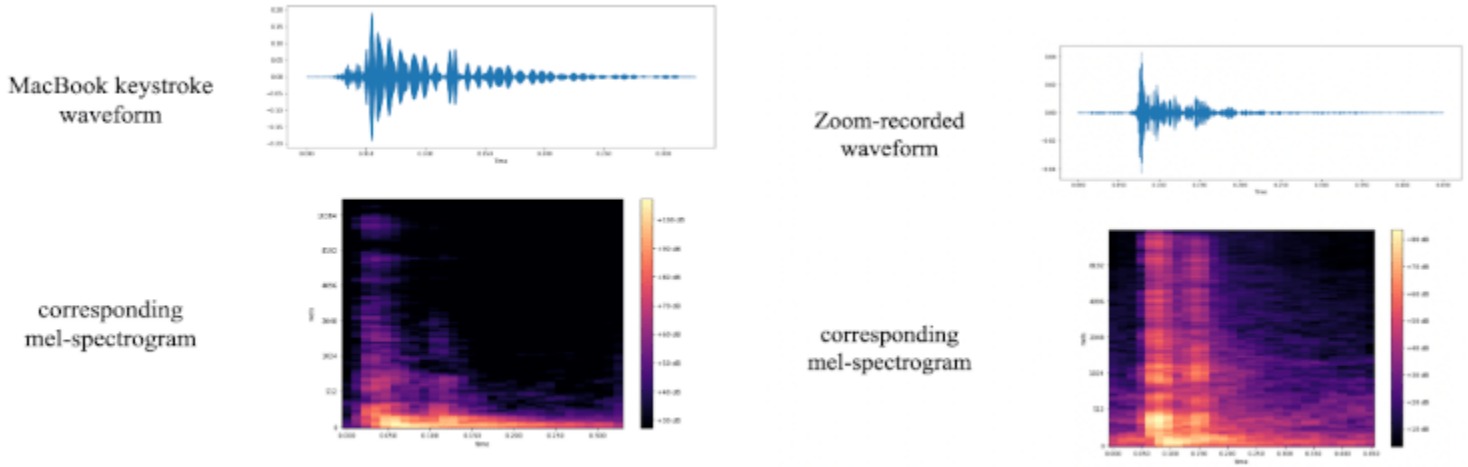
인공지능(AI)의 등장

- 사람을 더 잘 속일 수 있게 됨
  - 가장 취약한 연결고리는 사람
  - 사진/음성/영상 등 딥페이크

- 공격 시간 단축
  - 자동화
  - 방화벽 우회
  - 공격코드 작성 등

- 가능성의 증폭

A Practical Deep Learning-Based Acoustic Side Channel Attack on Keyboards

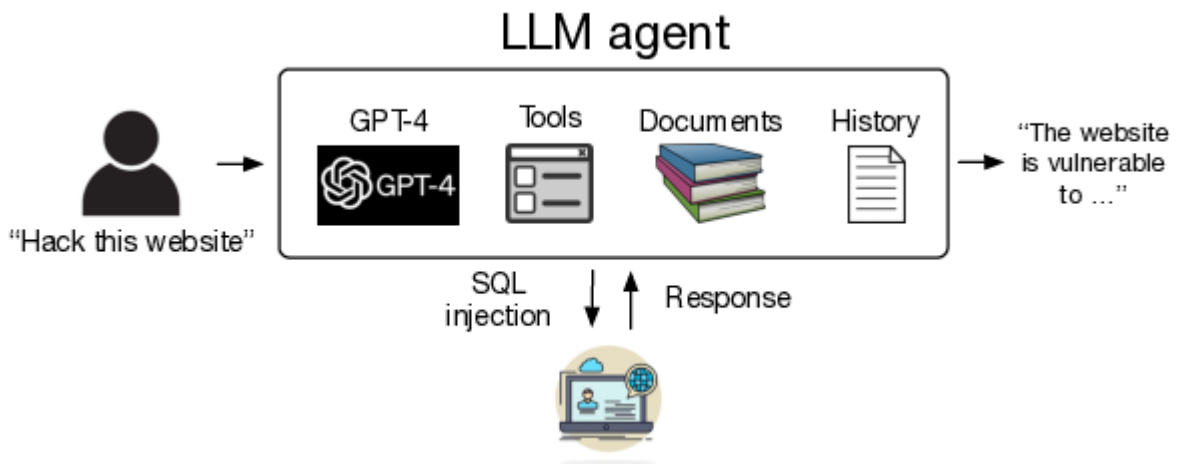


- **폰으로 녹음한 키 입력 소리로 패스워드 추측**(95%)
- **줌 미팅 중 녹음된 키 입력 소리로 패스워드 추측**(93%)

AI **해커** = LLM **플래너(추론 엔진)** + **취약점 스캐너/도구**

- LLM
  - **공격 시나리오 계획, 결과 해석, 우선순위 결정, 리포트/코드 작성 등**

- **취약점 스캐너/도구**
  - **포트 스캔, 웹 취약점 진단, 익스플로잇 시도 등**



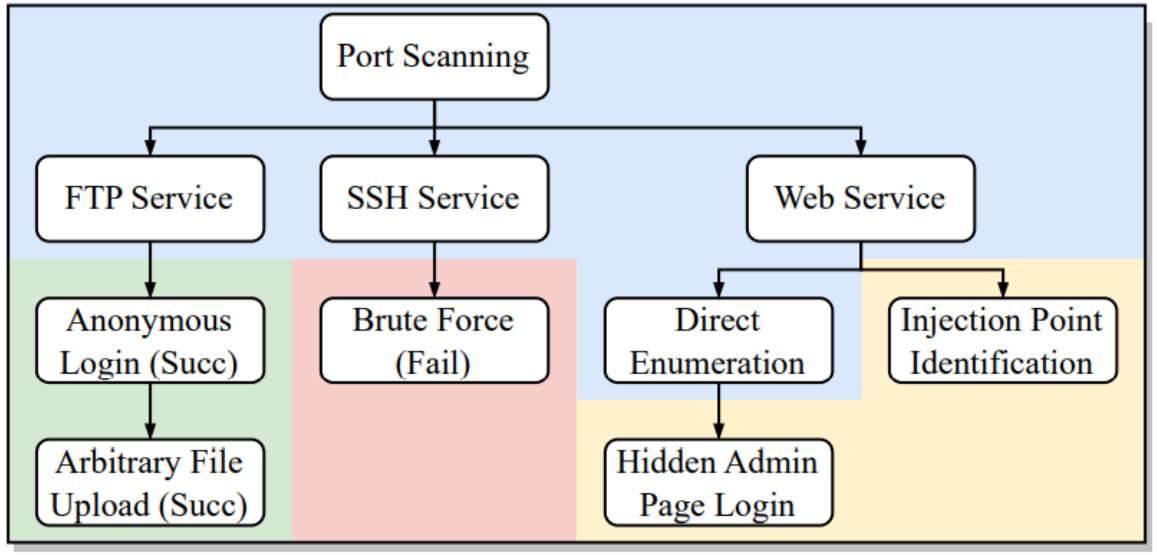
usenix
THE ADVANCED
COMPUTING SYSTEMS
ASSOCIATION

PentestGPT: Evaluating and Harnessing Large Language Models for Automated Penetration Testing

Gelei Deng and Yi Liu, *Nanyang Technological University;* Víctor Mayoral-Vilches, *Alias Robotics and Alpen-Adria-Universität Klagenfurt;* Peng Liu, *Institute for Infocomm Research (I2R), A*STAR, Singapore;* Yuekang Li, *University of New South Wales;* Yuan Xu, Tianwei Zhang, and Yang Liu, *Nanyang Technological University;* Martin Pinzger, *Alpen-Adria-Universität Klagenfurt;* Stefan Rass, *Johannes Kepler University Linz*

https://www.usenix.org/conference/usenixsecurity24/presentation/deng

- **"생각이 닫힌 느낌"**
- ASM(Attack Surface Management)**에 더해서** CTEM(Continuous Threat Exposure Management)**으로 글로벌 제품** 多



a) PTT Representation

```
Task Tree:
1. Perform port scanning (completed)
  - Port 21, 22 and 80 are open.
  - Services are FTP, SSH, and Web Service.
2. Perform the testing
  2.1 Test FTP Service
    2.1.1 Test Anonymous Login (success)
      2.1.1.1 Test Anonymous Upload (success)
  2.2 Test SSH Service
    2.2.1 Brute-force (failed)
  2.3 Test Web Service (ongoing)
    2.3.1 Directory Enumeration
      2.3.1.1 Find hidden admin (to-do)
    2.3.2 Injection Identification (todo)
```

b) PTT Representation in Natural Language

Figure 3: Pentesting Task Tree in a) visualized tree format, and b) natural language format encoded in LLM.

걱정들

- **비용** vs **성능**
  - **고비용 문제**: **고성능** LLM(ChatGPT, Claude **등**) **의존** -> **토큰 비용 급증**
  - **저성능 문제**: **자체** LLM/AI**만 구축** -> **성능 상대적으로 부족**

- **데이터 외부 유출 걱정**
  - **자체 구축 시**: **고비용+저성능 문제 함께**

- **안정성 이슈**
  - **잘못된 명령**, **환각**(hallucination) **등**

조종사: 인간 해커, 부조종사: AI 해커

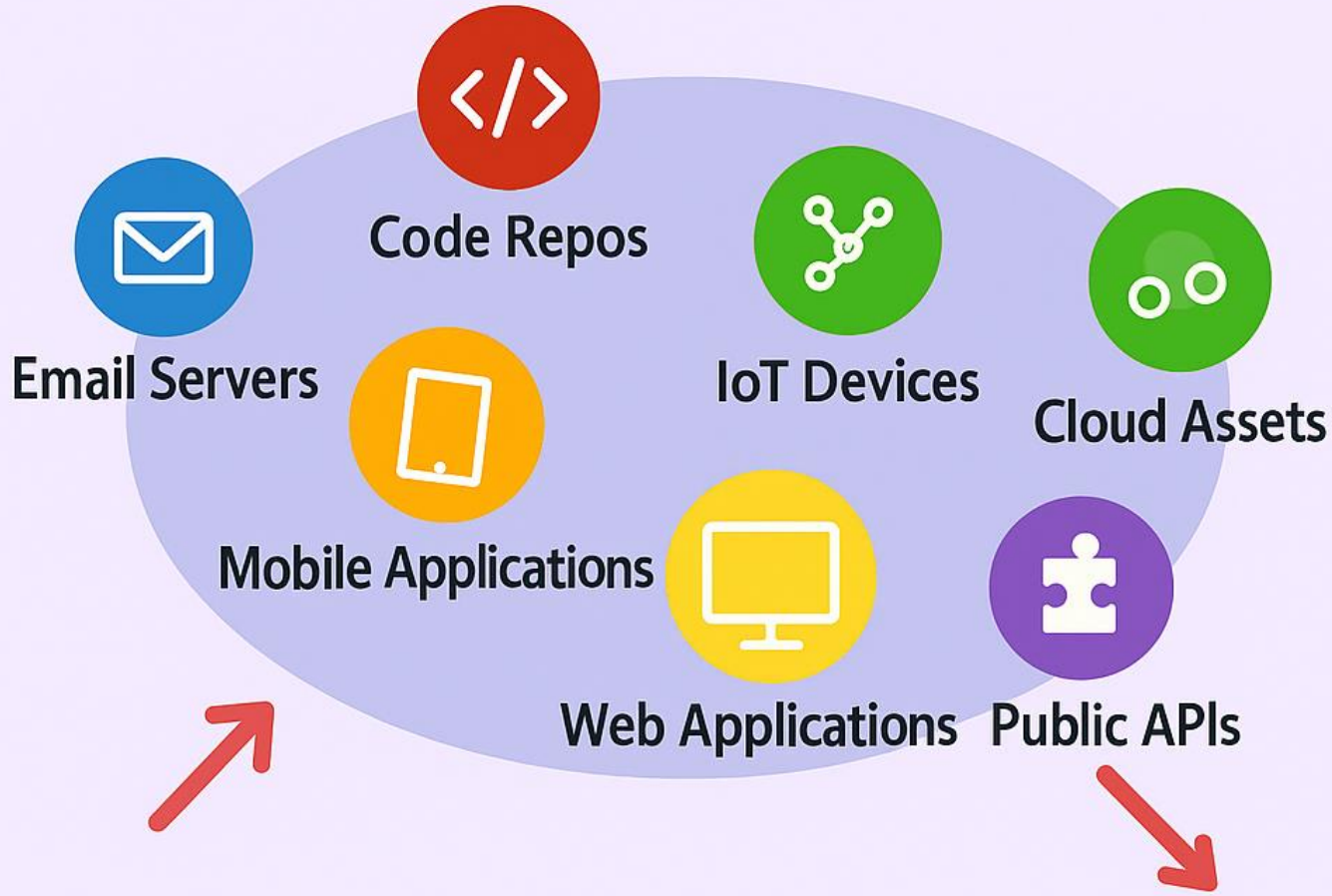
- “현재 AI 에이전트들이 그럴듯하게 포장되어 있지만 실제로는 작동하지 않는다” -> 기술 과대평가(overshooting) 문제 비판
- “AI가 인간을 대체하는 대신, 인간의 학습과 창의성을 증폭시키는 도구로 발전해야”
  - 오픈AI 공동창업자 안드레이 카파시(Andrej Karpathy)

- 아직은 자동화에 완전 의존보단, 사람의 점검을 지원하는 도구가 현실적
  - 잘못된 명령, 환각, 안정성 이슈, 데이터 유출 등

공격 표면(Attack Surface)

The attack surface has exploded

External Attack Surface



보안 수준을 높이려면,
(뚫리지 않으려면)
대체 어떻게 해야 하나?

왜 뚫리나?

- 통신사, 금융사, 대기업 등등...

- 자산이 많음
- 자산 식별이 안 됨
- 국외 등 자산 관리가 안 됨
- 중요하지 않은 자산이라 생각함
- 레거시가 많음
- 알았는데 조치가 안 됨
- 보안 조직이 작음
- 등등

대부분의 모의해킹 결과

- 위험도 上 취약점 다수
  - 그 마저도 수준 낮은 취약성이 많음
  - 대체로 짧은 기간(1-3개월) 수행
  - **기간 증가** 시 더 많은 취약점 예상

- 걱정> 외부에서 공격할 대상 多
  - 기존 공격 대상은 주로 웹
  - 그 외에도 모바일 앱, 기타 외부 노출 IP 등 대상 다수
  - **대상 확대** 시 더 많은 취약점 예상

문제의 본질

- **문제점**은 취약한 시스템, **개선안**은 취약성 보완?
  - 근본 원인 아니고, 대증 요법일 뿐. 또 반복 됨.

- 다양한 의견 청취 필요
  - 그룹 내/외부 전문가

- 진짜 문제
  - 문화, 예산, 권한 등
  - 현재는 누구의 잘못도 아님

문화 개선

- 보안 취약점 발견 = 사실 좋은 것
  - 취약점 발견은 문제라는 인식
    - 현상 외면, 보고 누락 등 부작용 다수 우려

- 발견 후 대응 부족 = 진짜 나쁜 것
  - 보안부서 취약점 조치 요청 시 적극 대응 필요
    - 보안부서 사전 인지 취약점 재발견 사례 발생

- 개발/운영 부서 등 전사적 보안 mindset 강화 必

보안 예산·권한 개선

- **내부에서 이미 알고 있는 각종 현안**
  - **네트워크 분할**(Segmentation) **부족**
  - **엔드포인트**(Endpoint) **가시성 부재 등**
- **(예산) 보안을 위한 노후 IT인프라 교체**
  - **IT예산 대비 6-7%만 되어도 잘하는 기업**
  - **그 중 일부로 거대 IT인프라 구조 변경 불가**
- **(권한) 'IT 우선, 보안 후순위' 관성**
  - **예) 통신사는 가용성·호환성 우선, 보안성은 마지막**
  - **다른 우선순위들을 위한 보안 예외처리 증가 -> 악순환**
- **보안조직의 예산 확대, 권한 강화 필수**

기업명	정보기술 투자액 (단위: 억 원)	정보보호 투자액 (단위: 억 원)	정보보호 투자 비중 (단위: %)
삼성전자	60,993	2,974	4.9
케이티	19,049	1,218	6.4
쿠팡	11,782	660	5.6
삼성에스디에스	5,384	632	11.7
LG유플러스	9,515	632	6.6
에스케이하이닉스	8,516	627	7.4
에스케이텔레콤	14,664	600	4.1

정보보호 투자액 순위 (출처: **과기부**)

6.05%: **IT예산** 比 **정보보호 투자율 평균**

보안 운용역량 확보

- **‘명령어 한 줄에 천 만원?’, ‘보안장비 배치 후 방치‘**

자체 보안기술 부족

조직 내 보안 전문성과 기술력 부재

외주 의존

외부 업체에 보안 솔루션 및 운영 의존

보안수준 하락

실질적인 보안 역량 약화

비용 증가

지속적인 외주 비용 상승

기술 이해 부족

보안 기술에 대한 기본적인 이해 부족

부실한 요구사항 작성

기술을 잘 모르는 사람의 요구사항 작성

개발 외주 의존

외부 업체에 개발 의존

문제 반복

동일한 문제의 지속적 반복

- **보안 기술력 내재화 필요**

IT 자산 식별

- 최근 사고들로 인한 대책은 자산 파악이 핵심
  - 범정부 정보보호 종합대책
  - 과기정통부의 3만개 기업 CISO 대상 공문(긴급 보안 점검)

- 예시1> 담당자 기억에 의존한 국가정보자원관리원 자산들
- 예시2> 자산인지 몰랐다가 치명적 해킹 위협이 된 사례
- 예시3> 자산인 줄 알았다가 아니었던 사례

- 이사가 답?
  - 그룹 차원의 자산 관리체계 도입 고민 필요

보안 가시화

- 통신사 해킹사고 시 첫 대응
  - 리눅스 서버 가시화(EDR 등)
  - PC도 마찬가지

- 보안 가시화의 남은 과제들
  - 모바일, 각종 장비(펨토셀 등) 등

- 엔드포인트(Endpoint)에 대한 보안 가시화가 국가적 추세

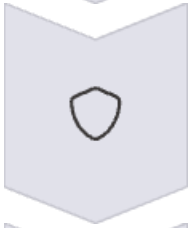
보안 기본기

- **취약한 공격 대상이 너무 많음**
  - **하지만 문제의 본질은 더 깊은 곳에**
    - **문화, 예산·권한 강화, 역량확보 등**

- **보안의 본원적 경쟁력 확보에 해답**
  - **지금 필요한 건 그럴듯한 최신기술이 아님**

문화·조직 변화

개발·운영 부서 등 보안 mindset 강화 必



책임·권한 재설계

보안조직의 예산 확대, 권한 강화 필수

거버넌스·컴플라이언스 강화

보안 = 고객 신뢰 쌓아가는 자본

자체 보안역량 확보

보안 기술력 내재화 필요

Facebook/Instagram/Twitter
@hkpco

www.stealien.com