안전한 컴퓨터 접근을 위한 NFC 기반 실시간 사용자 인증 시스템 개발

김시훈, 천유석, 박기윤, 박수빈, 석병진

한성대학교

발표자: 김시훈

목차

연구 배경 및 필요성

■ 비밀번호 인증 문제점

- 여러 곳에서 **비밀번호 재사용**으로 인해 유출, 무차별 대입 공격 취약
- 공용 컴퓨터에서의 **비밀번호 관리 번거로움**


Researcher claims 184 million Facebook, Google, and Microsoft passwords leaked online

It's probably a good time to update your passwords.

By Matt Binder on May 27, 2025

< 비밀번호 유출 사건('25.05) >

■ 기존 시스템

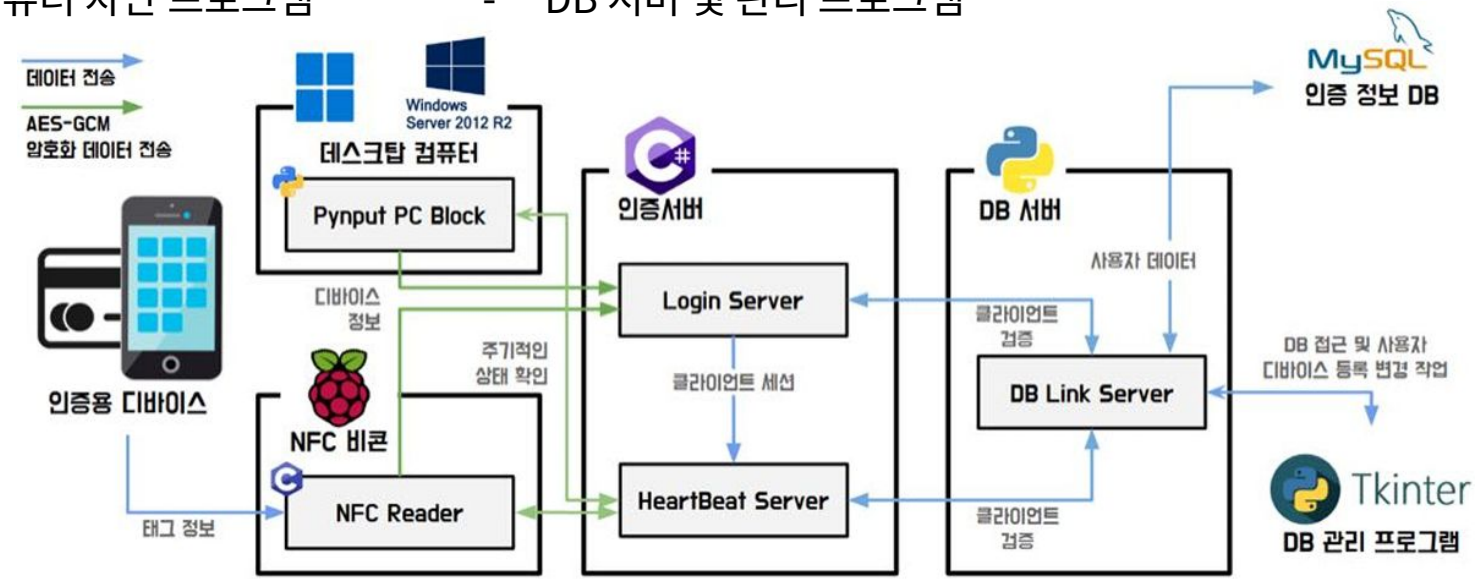
- RSSI 기반 거리 추정 후 자동 잠금 (Windows Dynamic Lock) ⇒ **주변 신호 간섭 등 실시간 인증 한계**
- 전용 수신기 활용 자동 로그인/잠금 솔루션 (GateKeeper) ⇒ **값비싼 전용 하드웨어로 도입 부담**

현실성, 편의성 및 보안성 향상을 위한 실시간 컴퓨터 차단 시스템 제안

제안 시스템 구성 및 기능

■ 시스템 구성

- NFC 비콘 장비
- 컴퓨터 차단 프로그램
- 인증서버
- DB 서버 및 관리 프로그램



< 전체 시스템 구조도 >

제안 시스템 구성 및 기능

■ NFC 비콘 장비

- NFC 사용 가능한 **디바이스의 값 읽기**
- NFC 센서 + 싱글보드 컴퓨터와 연결하여 데이터 수신 구성

■ 컴퓨터 차단 프로그램

- 인증 서버의 명령에 따라 **잠금을 수행**
- Pynput 라이브러리를 활용하여 **입력 인터셉트** 수행
- Windows 레지스트리에서 USBSTOR 차단
- 잠금 활성화 시 **키보드, 마우스, USB 포트 차단**

■ 인증 서버

- NFC 비콘 장비와 컴퓨터 차단 프로그램 **세션 관리** 및 암호화 통신 수행
- 패킷 관리를 위한 중계 및 **인증 서버** 역할

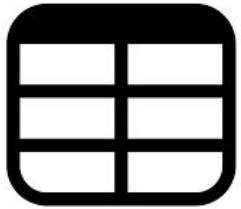
■ DB 서버

- 잠금 해제 정보와 잠금 해제 대상 컴퓨터의 **테이블 관리**

동작 과정

인증용 디바이스로 NFC 태그

Hash(NFC 비콘 장비 MAC, 사용자 태그 정보)



DB 대조하여 인증된 사용자인지 판별

대조 일치된 컴퓨터 MAC

잠금 해제 컴퓨터 정보 확보

Open 명령 패킷

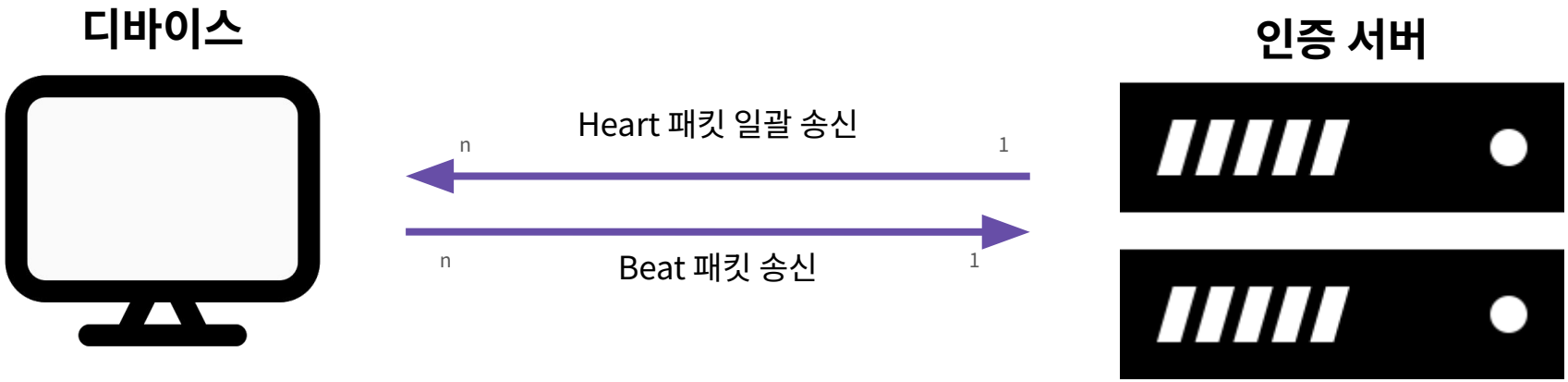
컴퓨터 잠금 해제

동작 과정

Beat 패킷 데이터

- **NFC 비콘 장비**: Hash(NFC 비콘 장비 MAC, 사용자 태그 정보)
- **컴퓨터 차단 프로그램**: 컴퓨터 MAC

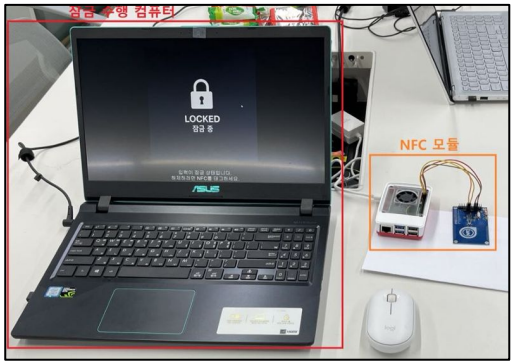
디바이스에서 **Beat 패킷을 전송하지 않을 때** 인증 서버에서 **세션 차단**



실험

■ 테스트 시나리오

1. 잠금 수행 중 USB 연결
2. 인가된 사용자 인증 시도
3. 비인가 사용자 인증 시도
4. 잠금/해제 성능 측정



< 실험 세팅 >

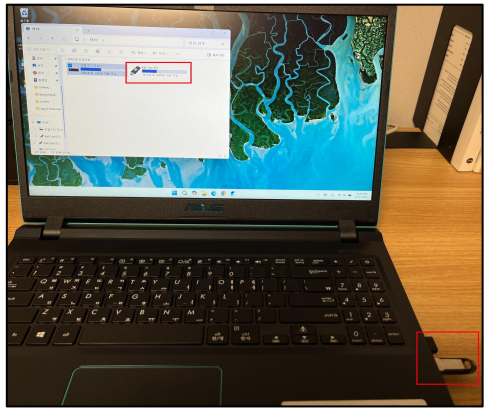
구분	상세 명세		
HW	Raspberry Pi 5	CPU	Quad-core Arm Cortex-A76 @2.4GHz
		Memory	2G
	PN532 (NFC 모듈)	Power	5V
		통신 방법	I2C
	인증 기기	Samsung Galaxy S24 Ultra (SM-S928N), (Android 15)	
SW	운영체제	Raspberry Pi 5	Debian GNU/Linux 12 (bookworm)
		잠금 PC	Windows 10
	개발언어	C, C#, Python	
	라이브러리	cryptography 38.0.4, pyMySQL 1.1.1, libnfc 1.8.0-2, pynput 1.8.1, Pillow 11.2.1	

< 실험에 사용한 장비 >

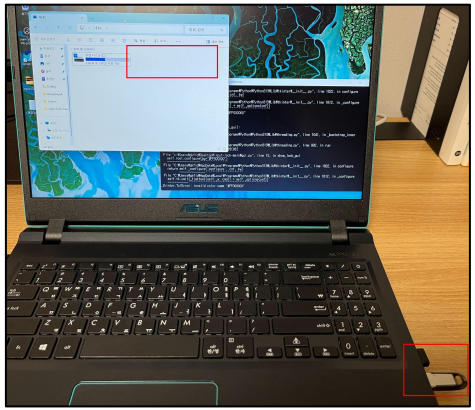
실험

■ 잠금 수행 중 USB 연결

- 잠금이 활성화 될 때 **USB 연결 시 OS에서 이를 인식하지 않음**
- 악성코드를 담은 USB 공격 시나리오에 대응 가능



< 프로그램 실행 전 USB 인식 확인 >



< USB 인식이 되지 않는 상황 >

실험

■ 인가된 사용자 인증 시도

- DB 대조 결과 해당 **컴퓨터 MAC 주소를 반환**
- 해당 컴퓨터에게 **Open 패킷** 전송 후 **잠금 해제**

```
[Heartbeat] Get Response: com/ NIC: 70-85-C2-C1-6D-28
[DB] 해싱 비교 데이터 전송: {"uid_mac_hash":"c23bf751ed782d40907bf5807d2ed98243dfcab7db48ae77b0b1fbfcc86c201b"}
[DB] 사용자 매칭 결과: 70-85-C2-C1-6D-28
접속시도
Connected to DB server.
[송신] 패킷종류: ORDER_TO_CLI
[송신] IV: 0C-00-00-00 | D7-AA-70-21-99-3A-8E-7A-27-B1-8E-23
[송신] Tag: 10-00-00-00 | 0B-F2-F9-0E-62-9A-41-B3-BF-AF-F5-1B-B7-BE-DE-27
[송신] Data: 04-00-00-00 | E8-97-62-AC
```

< 인증 서버에서 Open 패킷 전송 로그 >

```
[Auth] 매칭 완료: c769f3b3634d528efbeab650d218dfb0b5817e1268f7c53905ad670250a7a90b -> b'Non'
[Auth] 매칭 완료: c769f3b3634d528efbeab650d218dfb0b5817e1268f7c53905ad670250a7a90b -> b'Non'
[Auth] 매칭 완료: c769f3b3634d528efbeab650d218dfb0b5817e1268f7c53905ad670250a7a90b -> b'Non'
[Auth] 매칭 완료: c23bf751ed782d40907bf5807d2ed98243dfcab7db48ae77b0b1fbfcc86c201b -> b'70-85-C2-C1-6D-28'
[Auth] 매칭 완료: c23bf751ed782d40907bf5807d2ed98243dfcab7db48ae77b0b1fbfcc86c201b -> b'70-85-C2-C1-6D-28'
[Auth] 매칭 완료: c23bf751ed782d40907bf5807d2ed98243dfcab7db48ae77b0b1fbfcc86c201b -> b'70-85-C2-C1-6D-28'
```

< 인가된 상황에서의 DB 서버 로그 >

실험

■ 비인가 사용자 인증 시도

- DB 검색에 실패해 **‘Non’으로 예외 처리**
- 공격자가 인증되지 않은 디바이스를 NFC 비콘 장비에 태그 시 방어 가능

```
[Auth] 매칭 완료: c769f3b3634d528efbeab650d218dfb0b5817e1268f7c53905ad670250a7a90b -> b'Non'
[Auth] 매칭 완료: c769f3b3634d528efbeab650d218dfb0b5817e1268f7c53905ad670250a7a90b -> b'Non'
[Auth] 매칭 완료: c769f3b3634d528efbeab650d218dfb0b5817e1268f7c53905ad670250a7a90b -> b'Non'
[Auth] 매칭 완료: d9df1bc0f701bb96a884927d73fe835fae31a4a3f8f9618e68054b0a036be96d -> b'Non'
[Auth] 매칭 완료: d9df1bc0f701bb96a884927d73fe835fae31a4a3f8f9618e68054b0a036be96d -> b'Non'
[Auth] 매칭 완료: d9df1bc0f701bb96a884927d73fe835fae31a4a3f8f9618e68054b0a036be96d -> b'Non'
```

< 비인가 상황에서의 DB 서버 로그 >

실험 - 잠금/해제 성능 측정

■ 잠금/해제 성능 측정

- NFC 비콘 장비에 태그 시작, 태그 해제 시 시간 측정
- 태그를 시도하면 빠른 시간 내에 잠금이 해제됨을 확인

시도횟수	열리는 시간 (초)	잠기는 시간 (초)
1	3.29	8.98
2	2.96	8.65
3	2.98	9.13
4	1.65	8.10
5	3.14	8.97

< 잠금/해제 시간 측정 >

결론

■ 본 논문의 의의

- 네트워크를 사용하는 OS에서 여러 **공격 시나리오를 실시간으로 보호**함을 확인
- 타 인증 시스템과 비교해 **저렴한 가격**으로 가용성 높은 **보안 기능을 제공**

■ 향후 계획

- iOS 기반 인증용 디바이스가 보안 문제로 NFC 활성화가 되지 않음. 애플리케이션을 통해 NFC를 활성화하는 방안을 구상 중
- 현재 시스템은 NFC 비콘 장비에 인증용 디바이스를 항상 태그해야 해서 이를 시간 기반 세션 관리를 진행 예정

참고문헌

[1]A. Büttner and N. Gruschka, Device-Bound vs. Synced Credentials: A Comparative Evaluation of Passkey Authentication, I n Proceedings of the 11th International Conference on Information Systems Security and Privacy - Volume 2, 2025, pages 651-659. DOI: 10.5220/0013380600003899

[2]Mashable, Inc., Researcher claims 184 million Facebook, Google, and Microsoft passwords leaked online, https://mashable.com/article/infostealer-malware-184-million-passwords-social-media-database-data-leak

[3]Microsoft, Inc., Sign-in options in Windows, https://support.microsoft.com/en-us/windows/sign-in-options-in-windows-8ae09c04-c5da-41c9-972f-b126a13d18a8

[4]GateKeeper Support, What is GateKeeper Proximity authentication?, https://gatekeeperhelp.zendesk.com/hc/en-us/articles/360015080614-What-is-GateKeeper-Proximity-authentication