난수화 토큰인증 기술
Randomized Token Authentication

2017. 9.

중부대학교 정보보호학과
이병천 교수

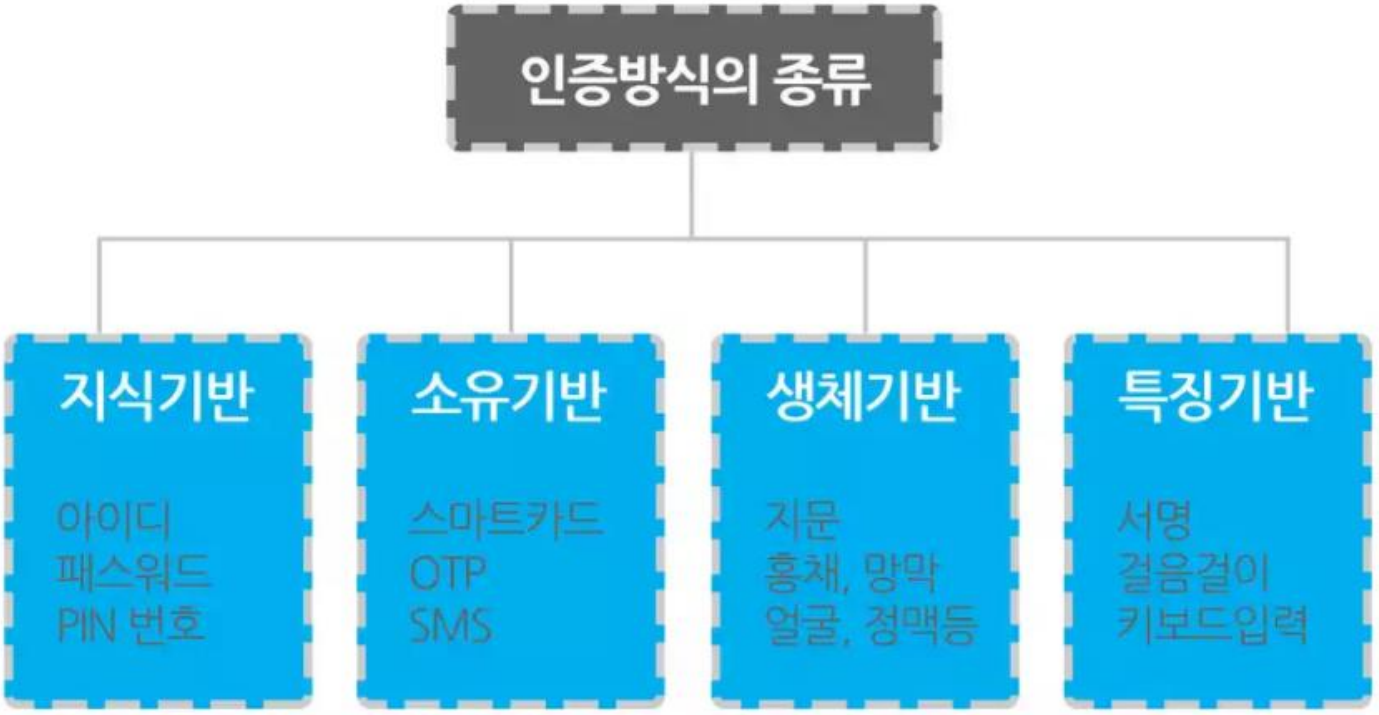
sultan@joongbu.ac.kr

목차

인증기술의 중요성

안전한 인증기술은 모든 보안의 출발점

상대방의 신분을 확인한 후 다양한 보안기술을 추가 적용 가능



초기인증기술 vs. 인증유지기술

처음 접속시의 사용자 신분 인증
ID/pass, 인증서, 고유주소, Biometrics, 멀티팩터 인증 등
엄밀한 인증 절차 필요
서버측에서는 사용자 계정 DB 확인 필요

초기인증기술

인증유지기술

초기 인증 완료된 사용자의 인증상태를 유지하는 기술
쿠키, 세션, 토큰 등
사용자 계정 DB 확인이 필요 없는 무상태 서비스(stateless service) 요구
많은 사용자를 위한 확장성, 효율성이 있는 기술 필요
OAuth, JSON Web Token 기술

인증유지기술의 현재

한번 로그인 하면 인증정보를 더이상 요구하지 않고 로그인 상태를 오랜 기간 유지. 사용자 편의성 향상.

자주 이용하는 SNS등의 로그인 정보를 이용하여 로그인 가능. 사이트별 계정등록의 불편함 개선.

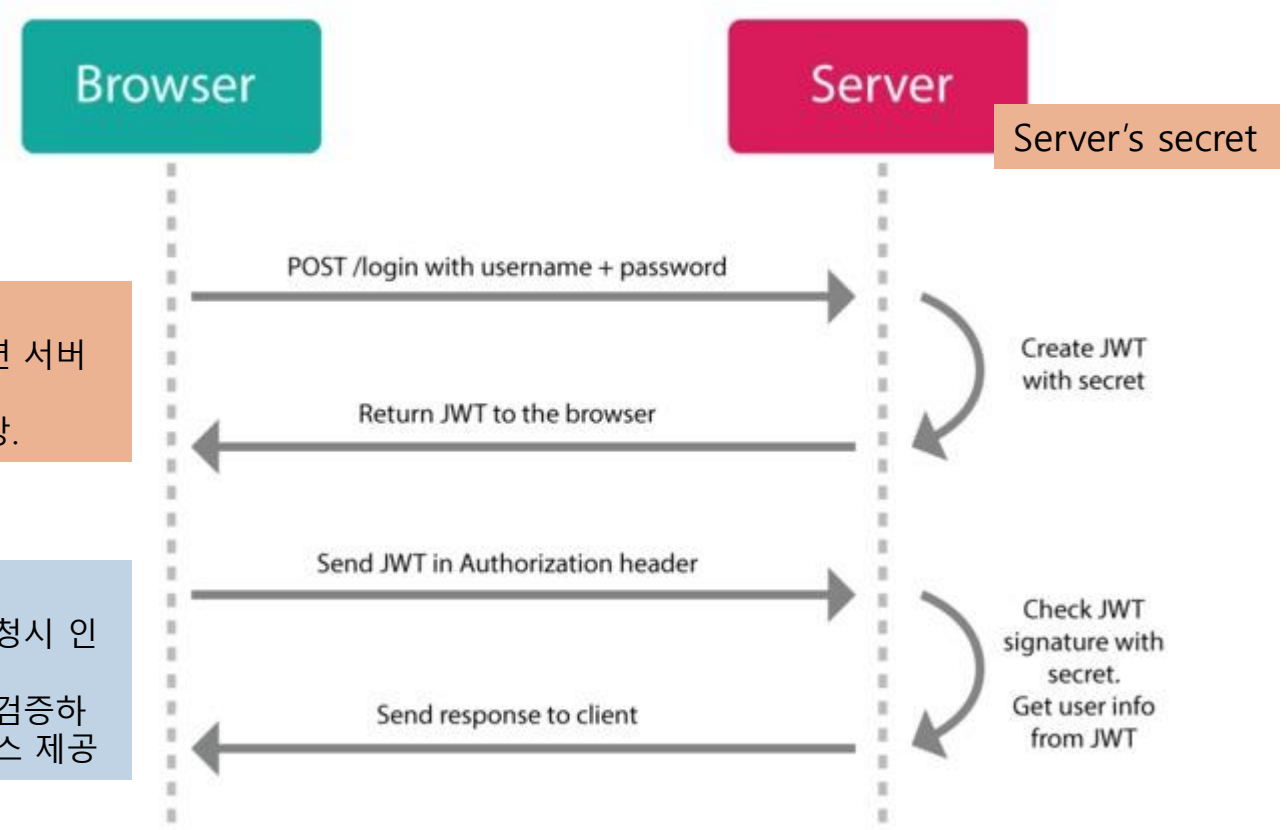
현재 사용되는 표준기술 - OAuth, JWT(JSON Web Token)

JSON Web Token 기술

https://jwt.io/

초기인증
패스워드 인증에 성공하면 서버가 인증토큰을 발급해줌.
브라우저에 인증토큰 저장.

인증유지
초기인증 이후 서비스 요청시 인증토큰을 첨부하여 요청.
서버는 토큰의 유효성을 검증하여 인증을 유지하고 서비스 제공



JSON Web Token의 구조

- 토큰 디코딩 및 사용자 정보 획득 가능
- 서명은 서버 비밀값을 이용한 HMAC 계산으로 서버만 계산 및 검증 가능. 제3자의 위조 불가.

JWT 토큰인증의 장단점

- 장점
  - 브라우저에서 전송해온 토큰에 사용자 정보가 포함되어 있어서 서버는 계정DB 접근이 필요 없이 인증 가능
  - 토큰은 서버가 서명한 값으로 남이 위조할 수 없음

- 취약점
  - 고정된 인증토큰이 오랜 시간(유효기간)동안 반복 전송됨
  - 공격자가 도청으로 타인의 인증토큰을 획득하면 타인 신분으로 로그인 가능 (재전송 공격)

- HTTPS 보안통신 적용 필수. 비용 발생.
  - 보안통신세션의 설정/유지/통신에 시간, 비용 소요
  - 서버측은 접속된 사용자의 보안세션 정보를 유지해야 함. 무상태 서비스 어려움.
  - 클라이언트측은 서버의 신분(인증서) 확인 필요. 중간자 도청공격 방지.

난수화 토큰인증 기술

- JWT 토큰인증의 문제점을 해결할 수 있는 난수화 토큰 인증(Randomized Token Authentication) 기술 개발
  - 논문 발표: 2017. 4.
  - 특허 출원: 2017. 7.
  - 데모 서비스 개발: 2017. 8.

- 데모 서비스
  - http://isweb.joongbu.ac.kr:3000/ (한글)
  - http://isweb.joongbu.ac.kr:3001/ (영문)

난수화 토큰인증 기술의 목표

1. 서버의 DB접근이 필요 없는 무상태 토큰인증
   - 토큰을 이용한 자동 로그인, 인증 유지
2. 고정된 bearer token 사용의 취약점 개선
   - 난수화된 인증정보 계산에 시간 기반 난수화 적용.
3. 보안통신채널이 불필요한 토큰인증
   - 시간 기반 난수화 적용으로 인증정보를 도청해도 재사용 불가
4. 널리 확산된 JWT의 기본 메커니즘을 활용
   - JWT 인증과 함께 시간 기반 난수화를 부가 인증으로 사용
5. Https 적용하지 않고도 필요시 보안통신채널 제공
   - 시간 기반 난수화 인증정보를 공유된 비밀키로 사용하여 메시지 암호화, 메시지 인증 기능 제공

방법론

- 서버는 로그인된 사용자에게 두개의 토큰을 발급
  - 공개토큰: 공개 가능, 개인정보 전달용
  - 비밀토큰: 공개 불가, 인증정보 계산용
- 요구사항
  - 토큰은 서버만이 계산할 수 있어야 함 (서버의 비밀정보 K 이용)
  - 서버는 공개토큰으로부터 비밀토큰을 언제든지 계산 가능함
- 토큰 계산 방법

공개토큰 $t_P = HMAC(\text{사용자정보}, K)$

공개토큰은 사용자정보에 대한 서버의 서명값

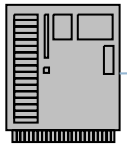
비밀토큰 $t_S = HMAC(t_P, K)$

비밀토큰은 사용자 공개토큰에 대한 서버의 서명값

난수화 토큰인증 구성도

클라이언트

서버



DB

ID, hpass 저장

암호화 채널

초기인증

ID/Pass 입력

$< ID, pass >$

DB 검색, 사용자 인증

인증된 사용자에게 토큰 발급

토큰 발급

공개토큰, 비밀토큰 저장

평문 채널

인증유지

비밀토큰, 현재시간을 이용하여
난수화 인증정보 계산

현재시간
난수화 인증정보

공개토큰에서 사용자정보 확인
공개토큰 이용하여 비밀토큰 계산
난수화 인증정보 검증
시간정보 검증

기술개발 내용

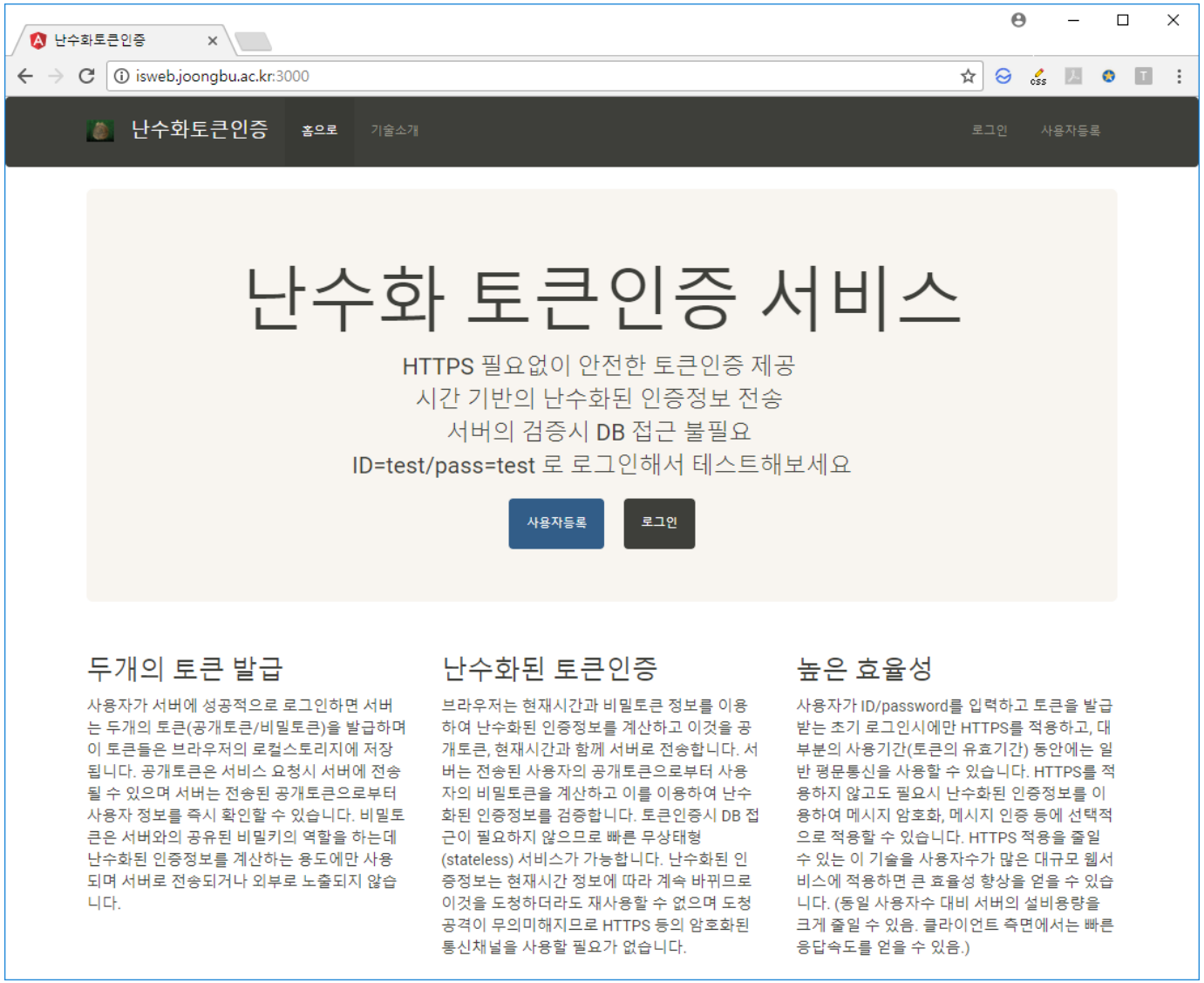
1. 난수화 토큰인증
   - https 통신보안 필요없는 안전한 인증유지기술
   - https 통신보안은 초기인증시에만 적용. 오랜기간 사용하게 되는 인증유지시에는 https 미적용 가능

2. 선택적 메시지 암호화
   - https 사용하지 않고도 필요시 선택된 메시지에 대한 암호화 적용 가능

3. 선택적 메시지 인증
   - https 사용하지 않고도 필요시 선택된 메시지에 대한 메시지 인증 적용 가능

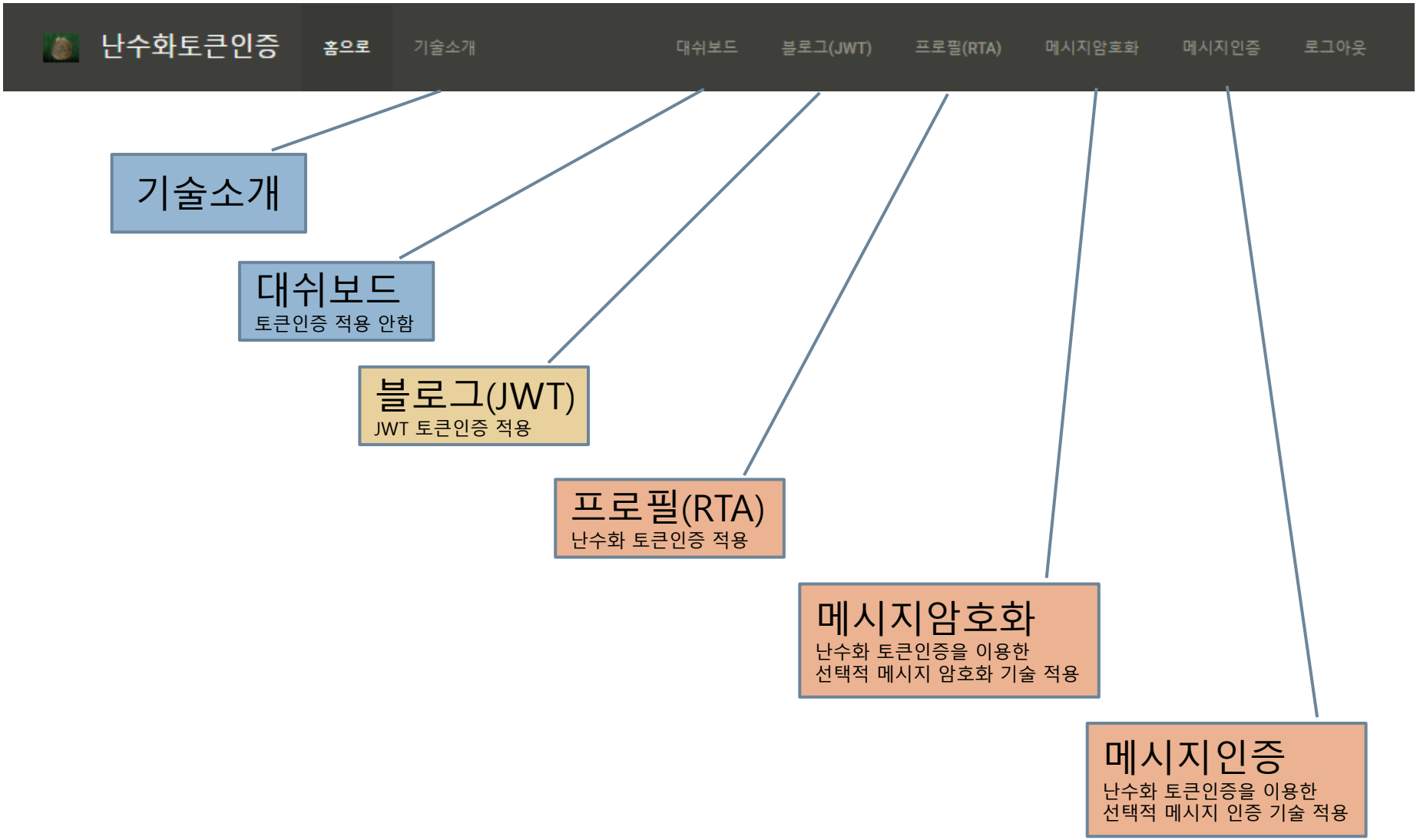
데모 서비스

http://isweb.joongbu.ac.kr:3000/



데모 서비스

http://isweb.joongbu.ac.kr:3000/



난수화된 토큰인증의 효과

- 서버 측면
  - 서버의 계정DB 검색 필요 없는 무상태(stateless) 인증유지
    - 대규모 분산서비스 등 서버의 확장성에 효과
  - https 통신보안은 초기 로그인시에만 적용하고 대부분의 인증유지 단계에서는 https를 사용할 필요가 없음
    - https 세션정보 관리 불필요. 서버의 운영비용 감소.
    - 동일 사용자수 대비 서버 설비용량을 절반 이하로 절감 가능
- 클라이언트 측면
  - https 세션을 이용할 필요가 없음. 빠른 응답속도.
  - 성능이 제약되는 IoT 디바이스에도 적합
- 공격자 측면
  - 도청 정보 재사용 불가, 통신 도청이 쓸모 없음

적용 가능 분야

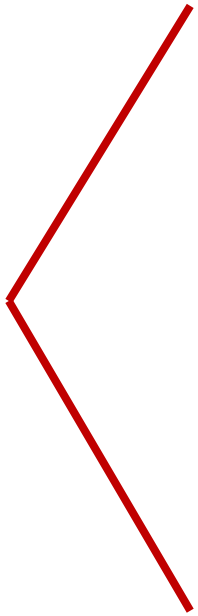
- 대규모 웹서비스에서의 인증
  - https 보안통신은 초기인증시에만 적용하고 대부분의 사용기간 동안 https를 적용하지 않음
  - 서버운영비용 감소 (동일 동시 접속자수 대비 서버용량 절반 이하로 절감)
  - https 보안통신과 함께 적용시 도청공격에 강한 이중보안 제공
- 모바일 앱에서의 인증
  - 패스워드 입력이 불편한 모바일 앱에서 토큰인증은 필수
  - https 미적용시 서버운영비용 감소
- IoT 디바이스 인증
  - 성능이 제약되는 IoT 디바이스에서 https 보안통신 적용은 부담
  - 사람의 개입 없이 이벤트 기반의 간헐적 통신으로 자동 동작하는 사물인터넷 환경에서의 https/DTLS 보안통신 부담 해제

효율성 분석

- https 보안통신을 적게 사용함으로 인해 대규모 웹서비스의 서버 설비용량을 절반 이하로 감축 가능

초기 인증시

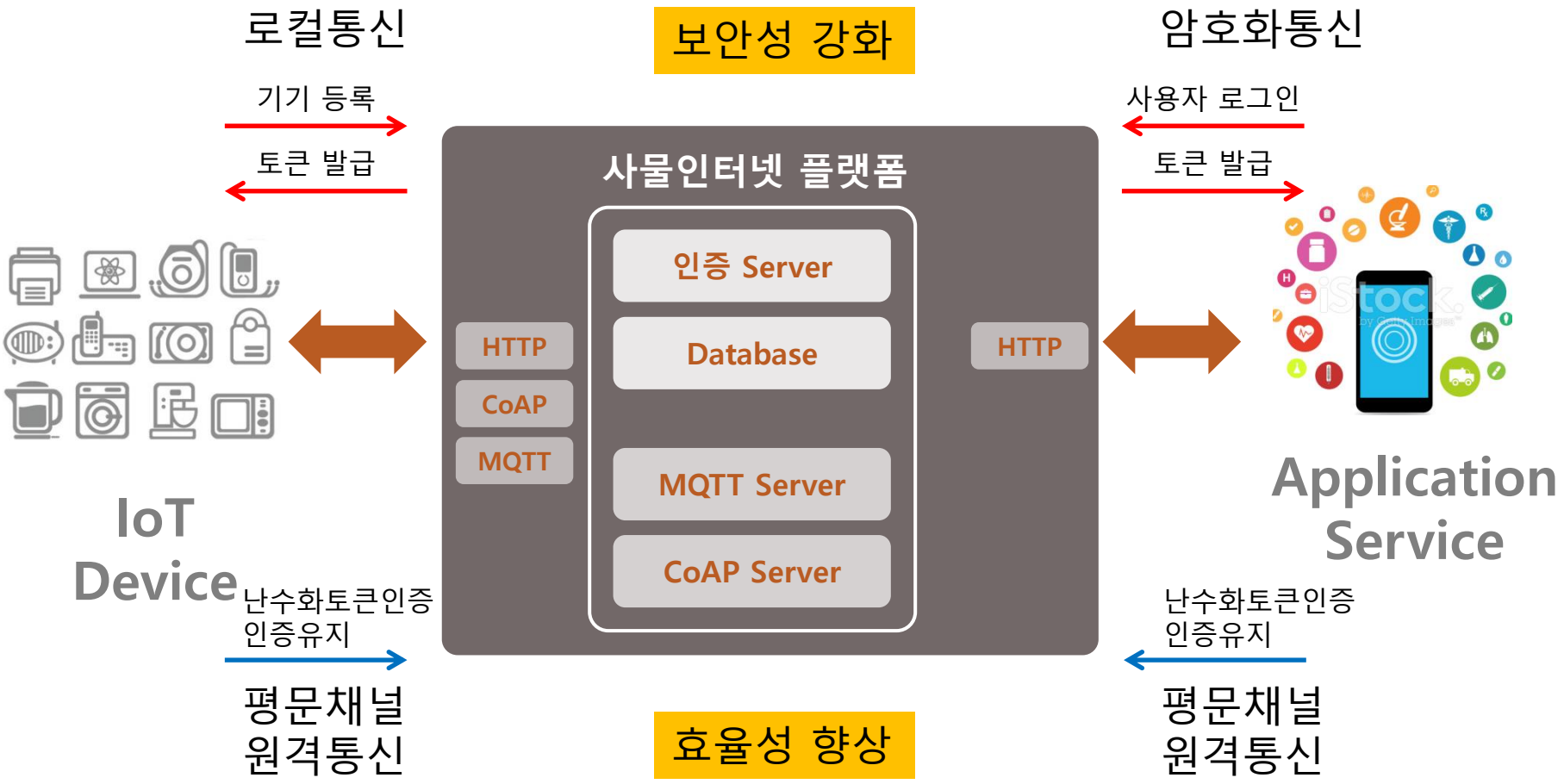
(간헐적 이용)



인증 유지시

(오랜기간 지속적 이용)

IoT 인증 시나리오


로컬통신
보안성 강화
암호화통신
기기 등록
토큰 발급
사용자 로그인
토큰 발급
사물인터넷 플랫폼
인증 Server
Database
HTTP
CoAP
MQTT
MQTT Server
CoAP Server
HTTP
IoT Device
Application Service
난수화토큰인증
인증유지
난수화토큰인증
인증유지
평문채널 원격통신
효율성 향상
평문채널 원격통신

난수화 토큰인증은 미래사회의 필수 인증기술

sultan@joongbu.ac.kr