

IoT 디바이스 보안의 신기술 동향





내용

- IoT 디바이스의 보안 위협
- IoT 디바이스의 보안기술
 - HW 기반의 시큐어부트
 - HW TRNG



시큐어부트



IoT 디바이스의 보안위협

- ❑ BlackHat USA 2015: remote exploitation of an unaltered passenger vehicle



Step 1: hacking wifi & taking control over head unit



Step 2: hacking cellular network with help of femtocell from eBay

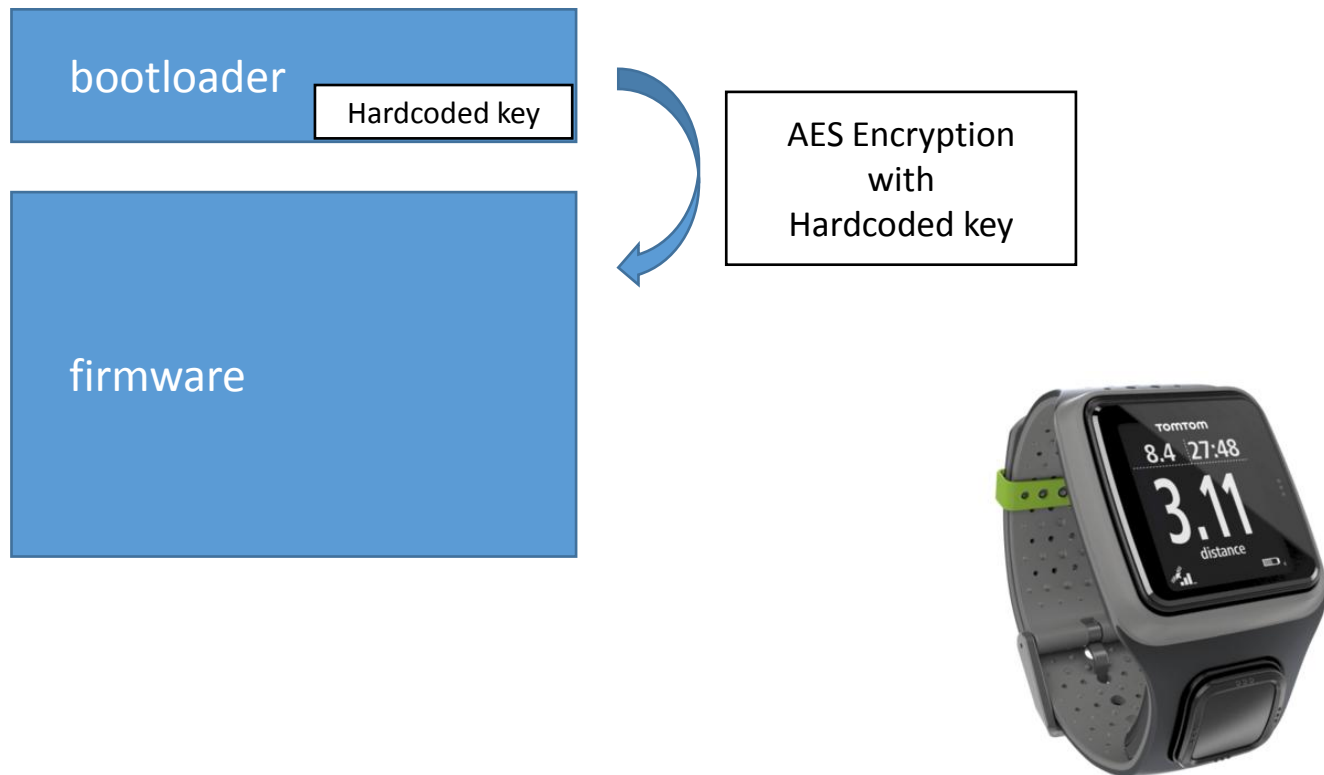


Step 3: hacking CAN bus. Changing firmware of CAN bus controller via head unit's multimedia system controller



Hacking smartwatch: tomtom runner

- 부트 관련 구조





Hacking smartwatch: tomtom runner

4. **AES key brute-force approach:** Our first naive approach to recover the AES key by scraping the bootloader binary.
6. **Final hurdles and MD5 verifications:** After recovering the AES key we must be able to unpack and pack the firmware file. Some hurdles had to be overcome, and MD5 checksums were found and computed.

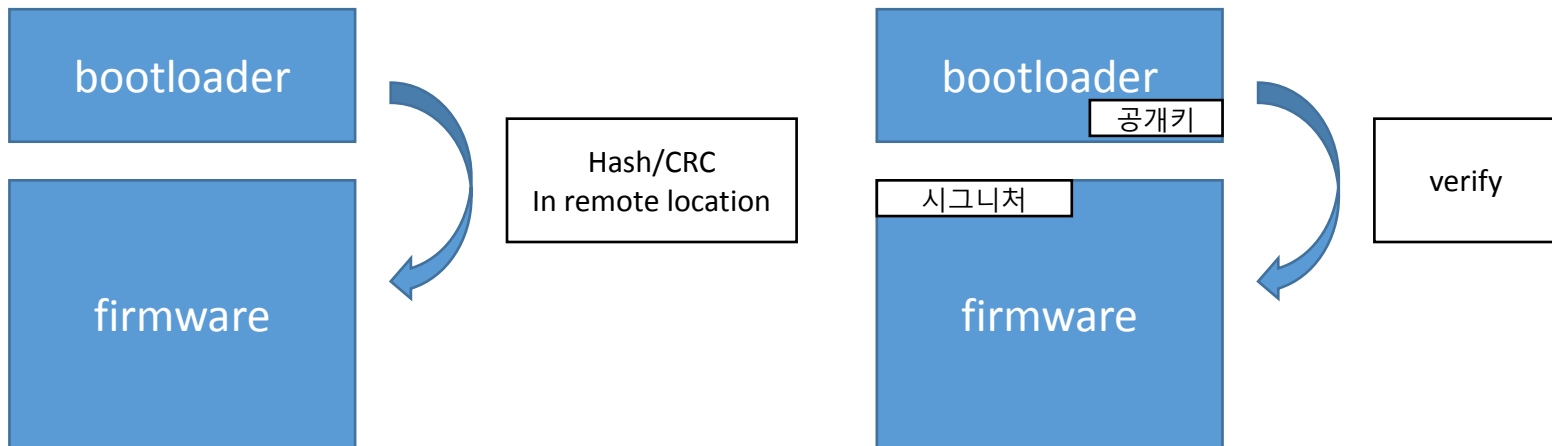




□ KDFS 2015 디지털 포렌식 챌린지 – 변조된 공유기 펌웨어 분석

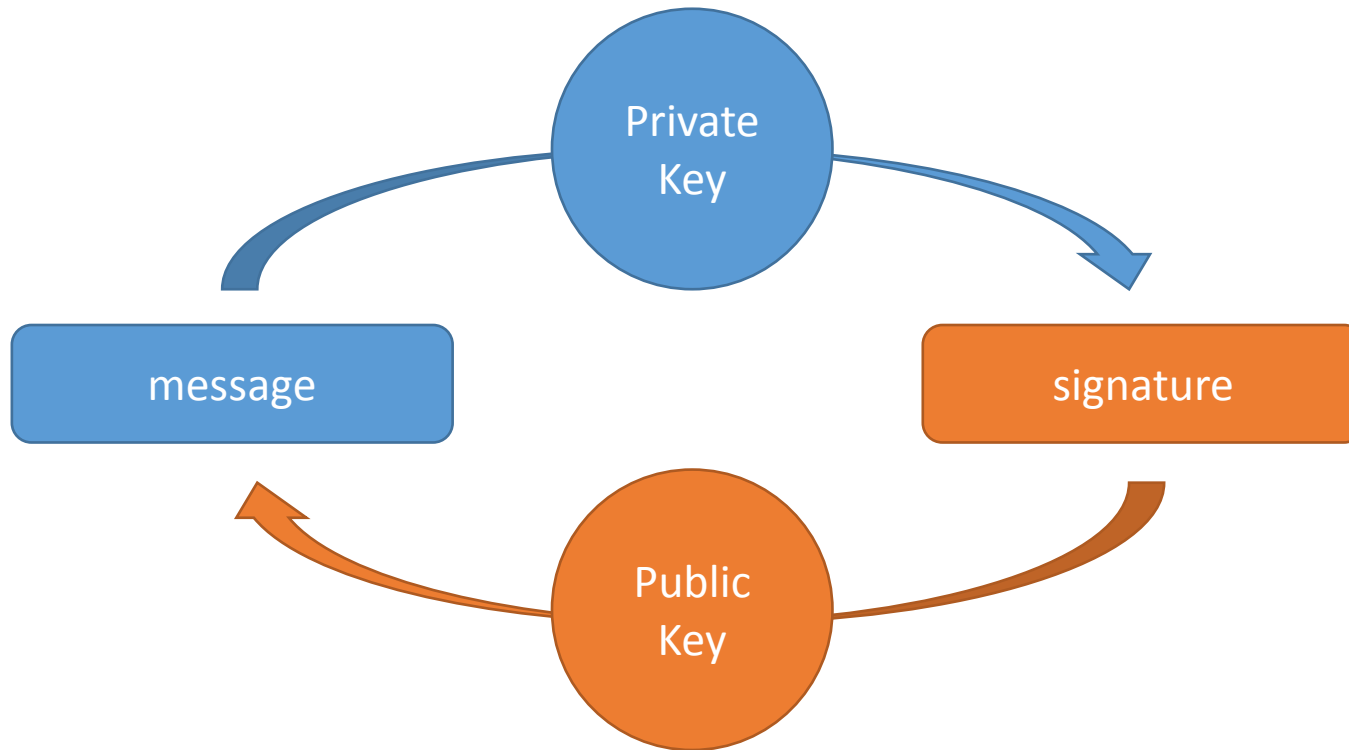
○ → CRC의 원격 보관, 공개키 사용 등을 권장하지만 한계를 인정

<http://kdfs.or.kr/images/5.pdf>



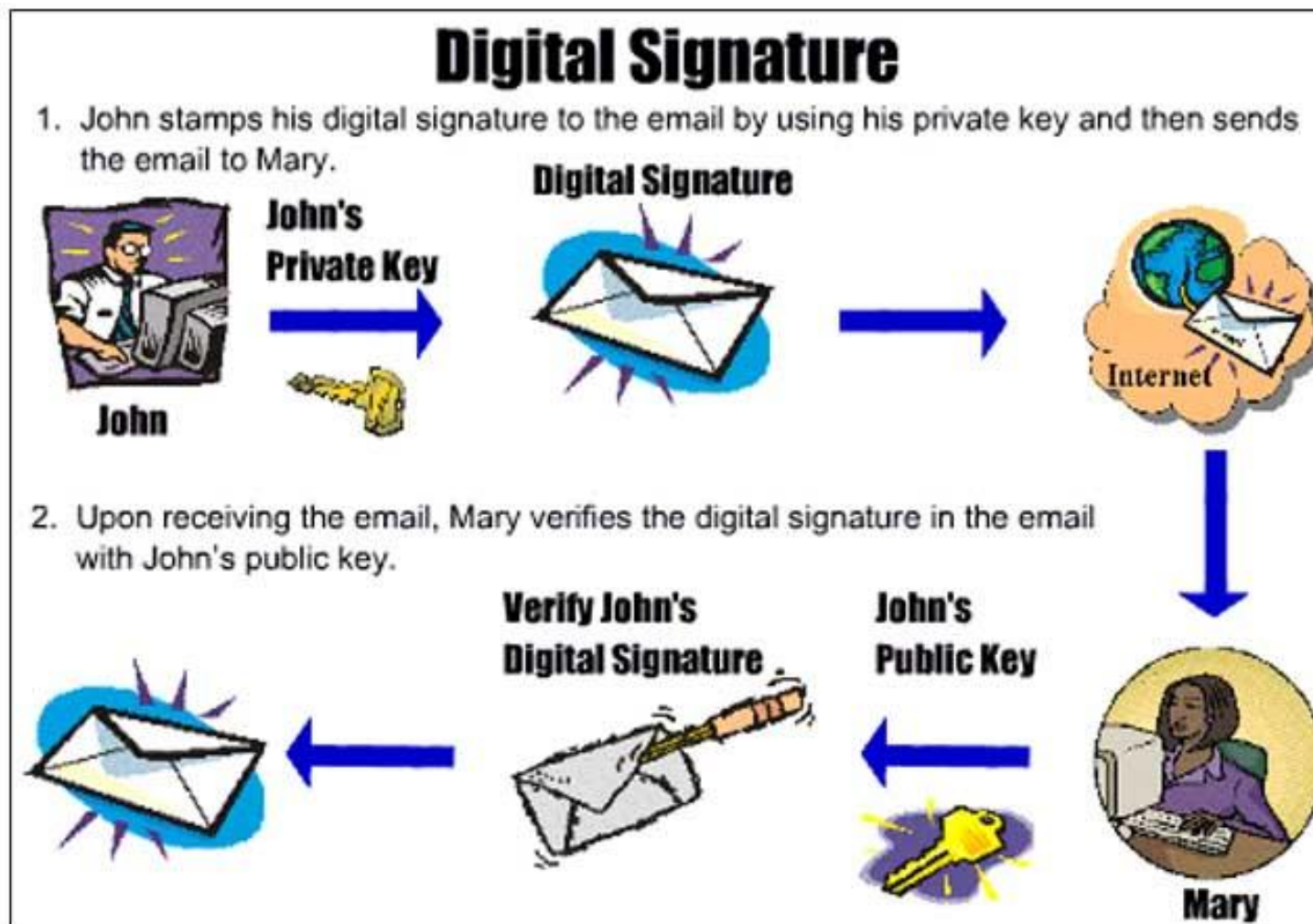


여기서 잠깐: 디지털 시그니처





디지털 시그니처






IoT 디바이스의 보안기술

security
platform
시큐리티 플랫폼

□ 시큐어부트



Google 시큐어부트

전체 이미지 동영상 뉴스 지도 더보기 검색 도구

검색결과 약 62,100,000개 (0.23초)

관련검색: 시큐어 부트 해제 시큐어 부팅 secure boot 란 secure boot 설정 secure boot

Magical Memories i ... 윈도우8과 ...
mmemories.tistory.com ...
2013. 10. 26. - 1. 컴퓨터 ... 같은 스크린을 경험한 ... 바랍시다.
증상1 윈도우즈 7과 8 ... 윈도우즈7 사용중 바이오스 ...

컴퓨터PC USB부팅을 위해 UEFI 부트 시큐어부 ...
rdsong.com/1427 ...
2015. 2. 23. - 컴퓨터PC USB부팅을 위해 UEFI 부트 시큐어 ... 서 바이오스(legacy Bios) 로 변경하다,IT리뷰.

윈도우 10 시큐어 부트, "리눅스 설 ... - ITWorld ...
www.itworld.co.kr/news/92524 ...
2015. 3. 24. - PC 업체들이 시큐어 부트(Secure Boot) ... 기능을 윈도우 10 제품에 포함하
지 않을 가능성이 제기되고 있다. 이 경우 사 ... 에 다른 ...

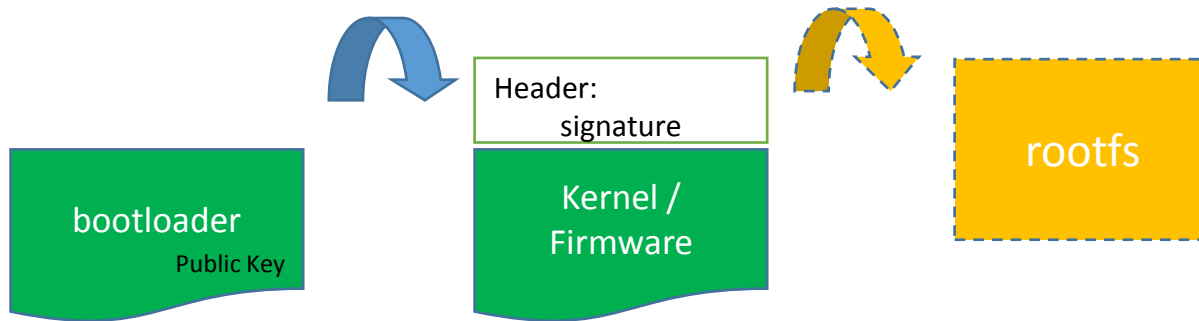
여유 그리고 즐거움 :: Secure Boot 사용하기
acoolwind.tistory.com/entry/Secure-Boot-사용하기 ...
2014. 5. 2. - Win 8 부터 보안기능을 강화하 ... 능이 추가되었습니다. 그 중 보안부
팅 (Secure Boot) 기능 사용에 대해 간략히 ...

UEFI - 나무위키
https://namu.wiki/w/UEFI ...
2016. 3. 15. - 리눅스의 경우는 부트로더가 GRUB 2.0 이상이면 거의 다 지원을 한다고 ... 또
한 Secure Boot는 UEFI Bios 제조자와 미리 서명인증협약이 되어있는 ...

새해 PC에 리눅스 사용 '어려우니 포기해' - 지디넷코리아
www.zdnet.co.kr/news/news_view.asp?article_id=20130102103357 ...
2013. 1. 2. - 시큐어부트가 유해소프트웨어 실행을 막는 원리는 간단하다. 컴퓨터가 부팅될 동
안 승인되지 않은 바이너리프로그램 호출을 차단하는 것이다.

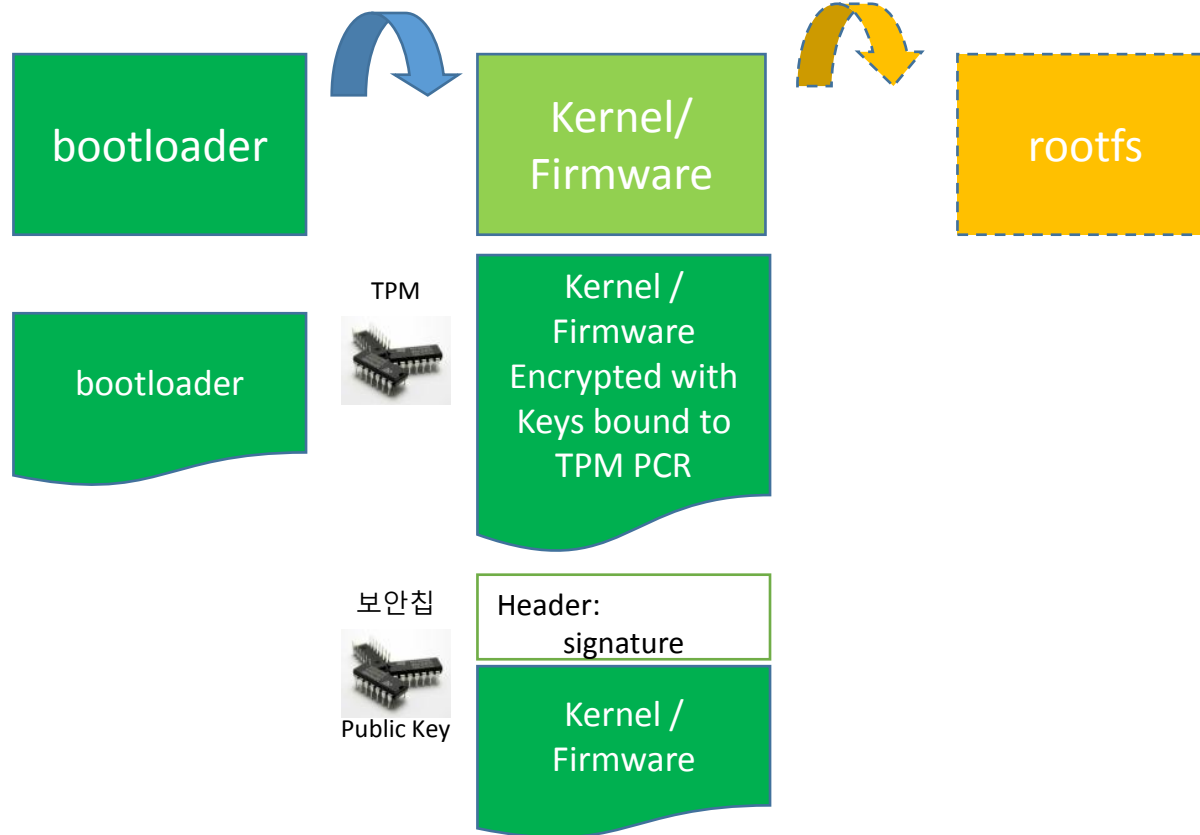


시큐어부트



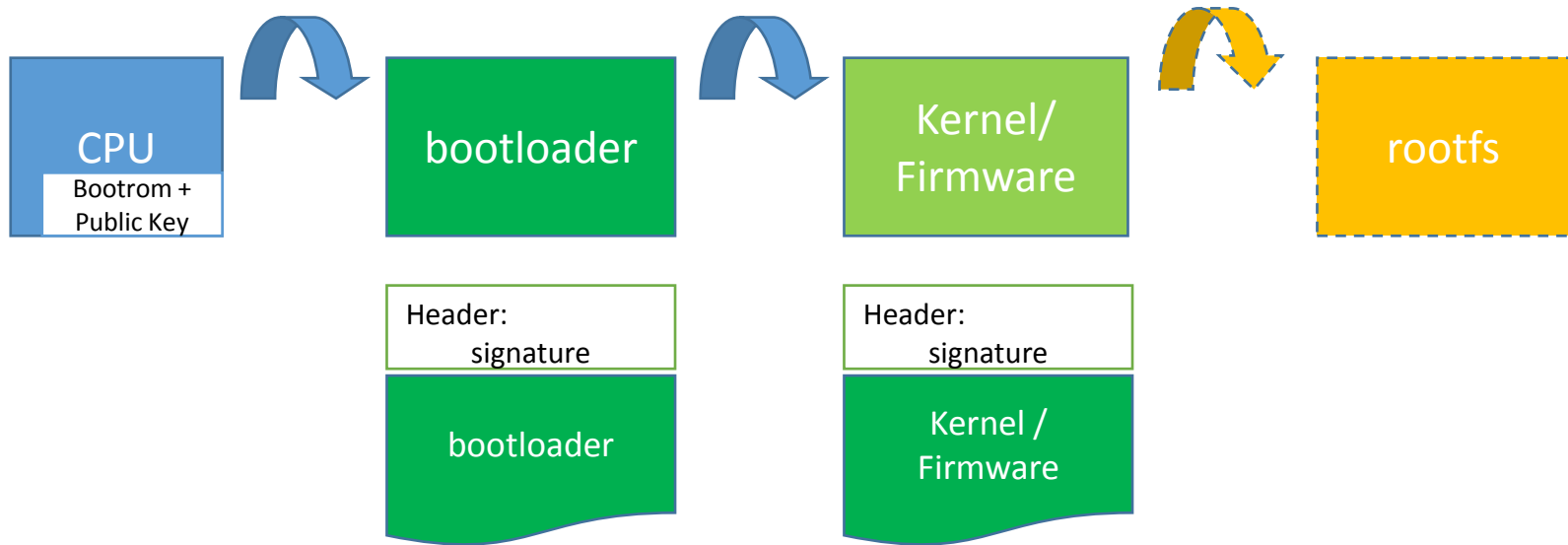


HW 지원 시큐어부트





CPU 지원 시큐어부트





국내회사의 시큐어부트 지원 현황

32-bit ARM® Cortex™-M3 CPU

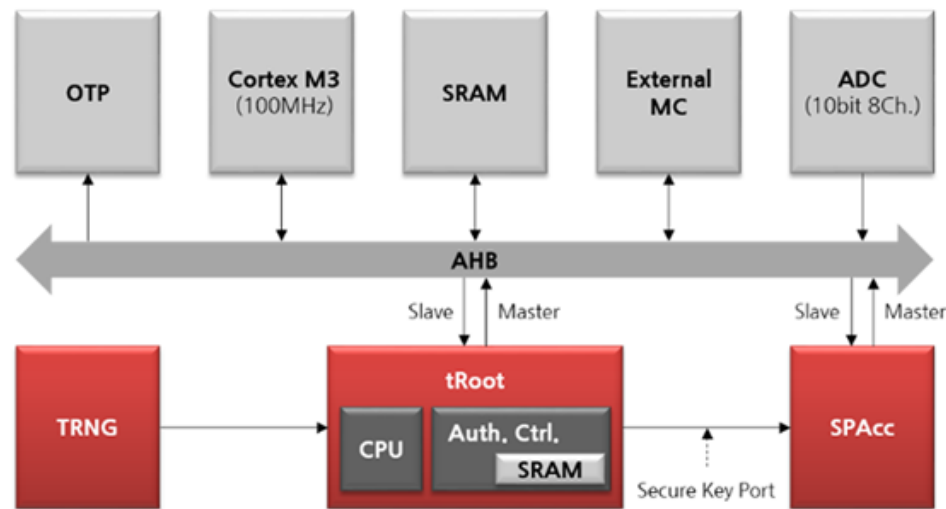
– tRoot (Secure Hardware Root of Trust)

- Secure Boot

- Primary security capability of tRoot which is used to bring up a device into a secure state and ensure that it runs only trusted firmware

Functional Diagram

This diagram shows the superset of features for the MS1000 microcontroller.





난수발생기



IoT 디바이스의 보안위협

- ❑ BlackHat USA 2015: remote exploitation of an unaltered passenger vehicle



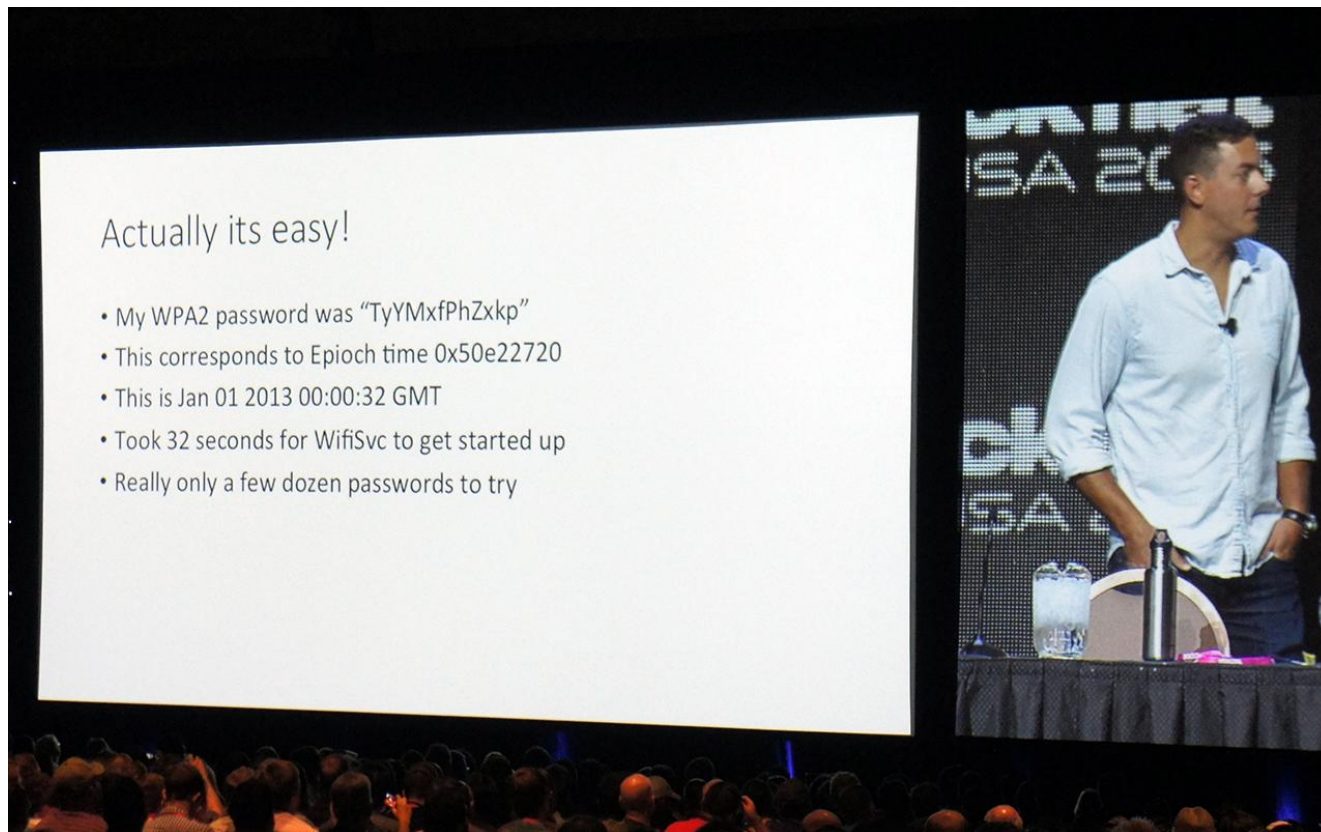
Step 1: hacking wifi & taking control over head unit





IoT 디바이스의 보안위협

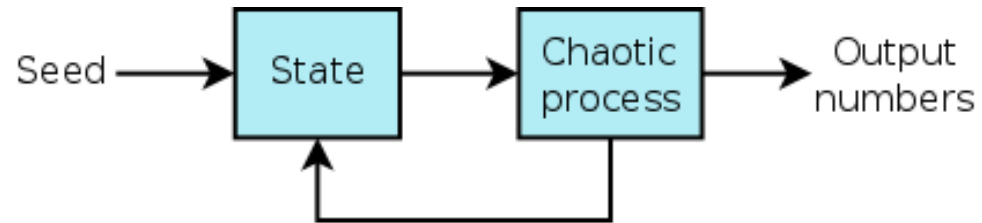
☐ Hacking car's wifi



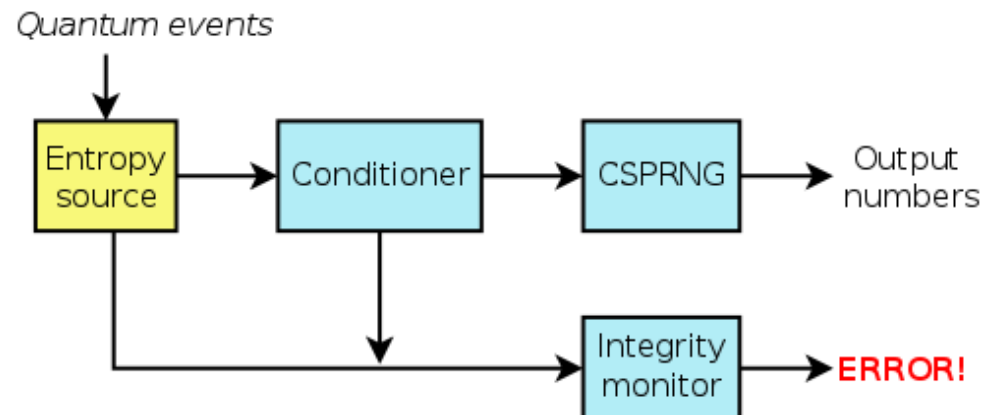


난수발생기

Pseudo RNG



True RNG



CSPRNG: cryptographically secure pseudo-random number generator

Conditioner: the "obvious" non-randomness is eliminated

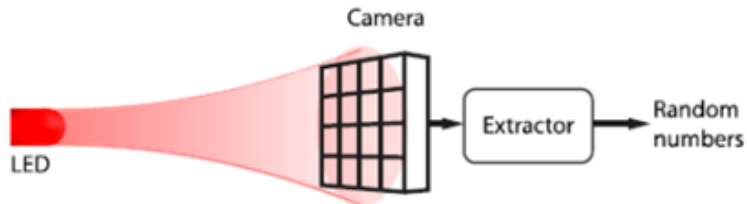
<https://lwn.net/Articles/525459/>



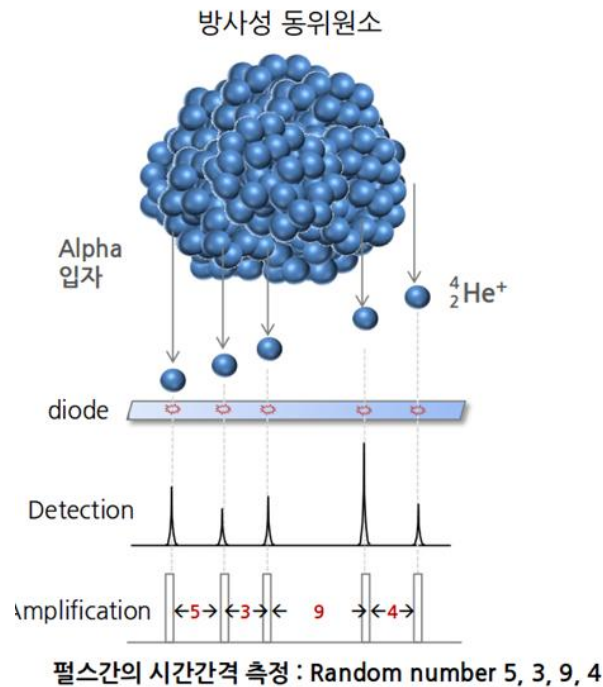
- 장치 고유의, 임의의 패스워드를 생성하는 방법?
 - 외부의 난수발생장치
 - 내부의 난수발생장치



국내회사의 TRNG

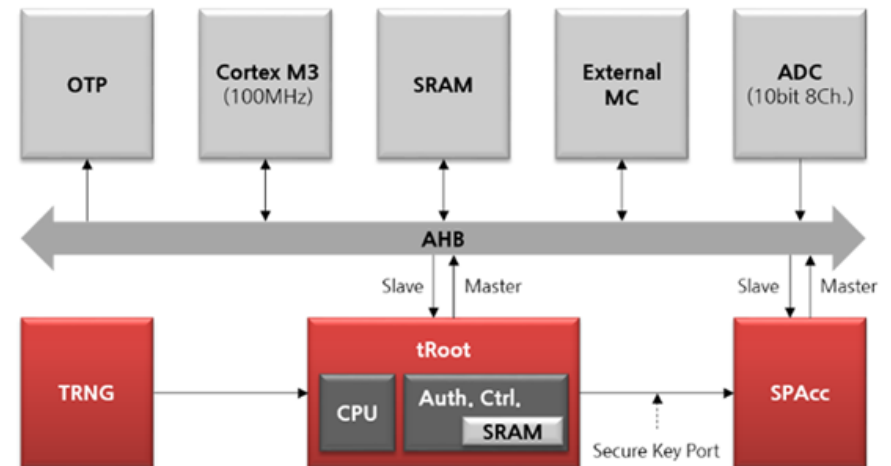


● : photon



Functional Diagram

This diagram shows the superset of features for the MS1000 microcontroller.





정리

☐ 시큐어부트

☐ HW TRNG



보안은 문화다!