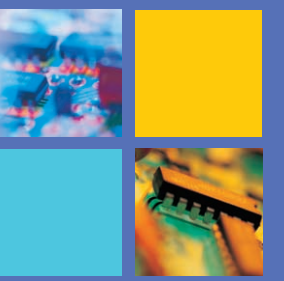


Design Methodology 1:

시스템 보안칩 솔루션 소개

남상준
(주)코아리버 연구소장
(victornam@coreriver.com)

1. 개요

더욱더 복잡해지는 정보사회에서 많은 전자 시스템 업체들은 콘텐츠 보호, 데이터 보호 등 자사 제품 시스템 무단 복제방지에 골머리를 앓고 있다. 첨단 기술이 발전함에 따라 자사 제품의 기술적 가치가 점점 높아지고 있는 가운데 자사 기술이 무단으로 도용되어 시장에 뿌려질 경우, 수년간 투자한 자금과 노력을 고스란히 남의 손에 넘겨주는 일이 비일비재하게 발생하고 있다. 이러한 현실은 비단 어제, 오늘만의 일이 아니며 전자 산업에만 국한되지 않고 산업체 전반적으로 일어나고 있다. 이를 방지하기 위한 관련 법제도가 제정되기도 하지만 이것만으로 무단 복제가 자취를 감출 수 있는 일은 아니다. 개발업체들 스스로 자사의 지적 재산권을 보호하고자 여러 가지 방안을 강구해야 하는 실정이다.

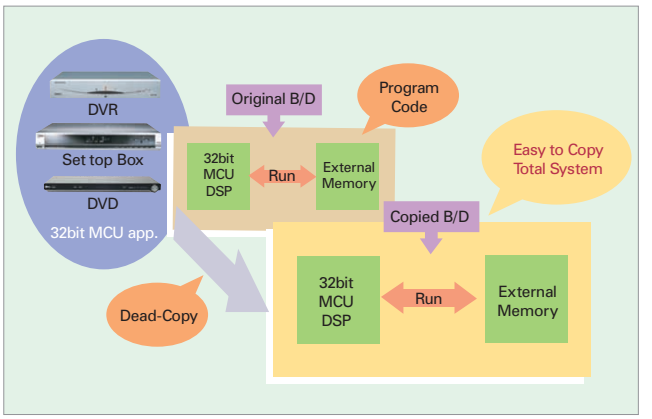
특히 값싼 노동시장을 갖춘 해외 현지에서 조립 생산되는 셋톱박스, 모바일 폰, MP3플레이어, PMP, DVD, DVR 등의 시스템에서의 시스템 무단 복제는 매우 심각한 상태이다. 본 지면에서는 ㈜코아리버에서 공급하는 MCU를 이용한 보안칩 솔루션인 SecurityCore와 UniChip에 대해 설명하고자 한다.

2. SecurityCore : 무단 복제 방지 IC

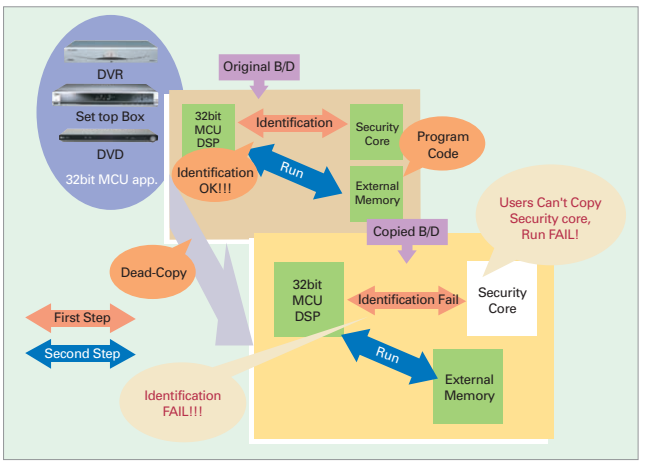
32bit 기반의 ARM9이나, MIPS 구조의 베이스밴드 마이크로컨트롤러를 사용하게 되면 코드영역을 플래쉬 메모리에 저장하여 시스템이 실행하게 된다. 그러나 이 플래쉬 메모리의 읽기 방법이 공개되어 있으므로, 그 내용을 읽어들이는 것은 그다지 어려운 일이 아니다. 따라서 〈그림 1〉과 같이 플래쉬 메모리 내용을 읽어냄으로써 쉽게 전체 시스템을 dead copy할 수 있다.

그러나 〈그림 2〉와 같은 SecurityCore와 같은 보안칩을 사용하는 경우, 시스템의 dead copy가 근본적으로 불가능하게 된다. 보안칩이 탑재된 시스템에서는 맨처음 베이스밴드 마이크로컨트롤러와 보안칩간에 인증절차가 완료되어야만 보드의 다른 기능이 동작할 수 있게 되어 있다. 그러나 원본 보드에 탑재된 보안칩을 해킹업체에서 구입할 수조차 없고, 또한 입수하더라도 프로토콜, 암호 알고리즘 등의 보안 장치를 알 수 없기 때문에 복제가 원천적으로 방지되는 것이다.

코아리버의 SecurityCore는 고객 요청에 따라 베이스밴드 마이크로컨트롤러와의 인터페이스를 자유롭게 변경할 수 있으며 손쉽게 다른 부가 기능을 추가할 수도 있다. 또한 동작 중에 내부적으로 부분적인 코드영역을 변경하는 IAP (In-Application Programming) 기능으로 알고리즘 자체를 변경 가능하다. 따라서 해킹의 위험이 인지되는 시점에서 알고리즘을 변경하여 무단 복제를 원천적으로 막을 수가 있다.

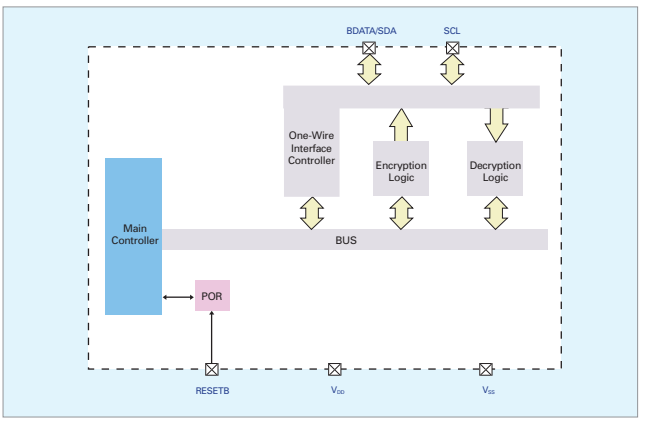


〈그림 1〉 보안칩이 탑재되지 않은 시스템에서의 Dead Copy



〈그림 2〉 보안칩이 탑재된 시스템에서의 Dead Copy 불가

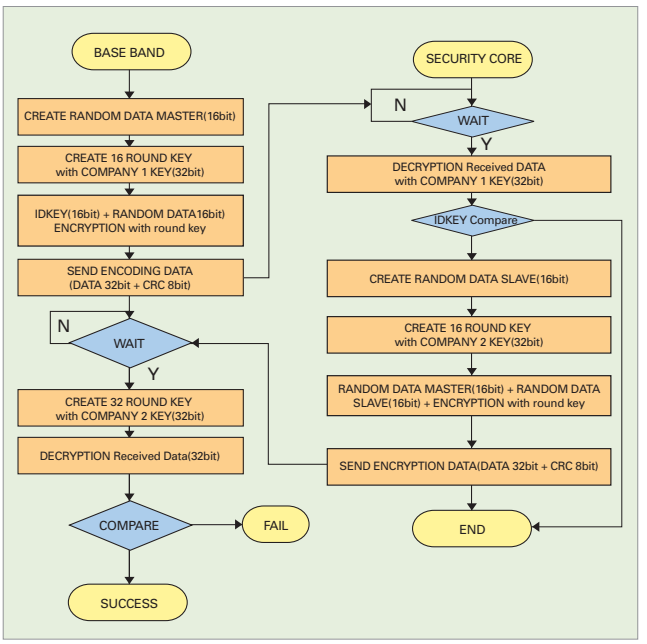
〈그림 3〉은 SecurityCore의 구조로 고유 알고리즘 암호화, 복호화 블록을 내장하고, 온-칩 오실레이터, 파워온리셋(POR), 그리고, 코아리버에서 자체 개발한 마이크로프로세서(MCU)코어를 내장하고 있다. 또한, SecurityCore가 다양한 시스템에서 적용될 수 있도록 폭넓은 동작전압 (1.8V ~ 5.5V)에서 동작되며, 전류 소모량도 500uA로 현저히 낮아, Security-Core추가시 시스템의 부담을 최소화하였다. 내부에 EEPROM 영역이 있기 때문에 사용자 데이터를 임시 저장하는 용도로도 사용할 수 있다. 한편 각 회사마다 고유의 ID를 부여함으로써 타사에서 다른 유통경로로 SecurityCore를 입수하였다 하더라도, ID가 다르기 때문에 정상 동작하지 않는다. 그리고 각 시스템 업체마다 상이한 보안 알고리즘을 채택하기 때문에 각 회



〈그림 3〉 SecurityCore의 구조

사별로 공급한 반도체가 서로 호환되지 않는다. SecurityCore는 이와 같이 여러 단계의 보안 레벨을 지니고 있는 것이 특징이다. 이러한 장점을 지닌 SecurityCore는 다른 용도로 사용 가능하다. 시스템의 복잡도가 높아짐에 따라 S/W 개발 업체들의 솔루션의 위상이 높아지고 있고, 개발 기간도 상당히 소요되고 있다. 이러한 소프트웨어 솔루션을 로열티를 받는 방식으로 하드웨어 제조업체에 공급 시 소프트웨어는 무형의 자산이라 실제로 얼마나 양산되고 있는지 확인하기 어려운 실정이다. 이러한 비즈니스 모델에서 SecurityCore를 사용하면 양산수량 파악이 손쉽게 이루어진다. 즉 소프트웨어 솔루션 내에 Security Core에서 인증 받는 기능을 부여하면 SecurityCore의 납품 개수만큼 소프트웨어 솔루션이 양산되는 것이므로, 정확한 수량이 파악하여 통제가 가능하게 된다.

〈그림 4〉는 SecurityCore와 베이스밴드 마이크로프로세서 간의 알고리즘의 간략한 흐름도이다.



〈그림 4〉 SecurityCore의 알고리즘 흐름도

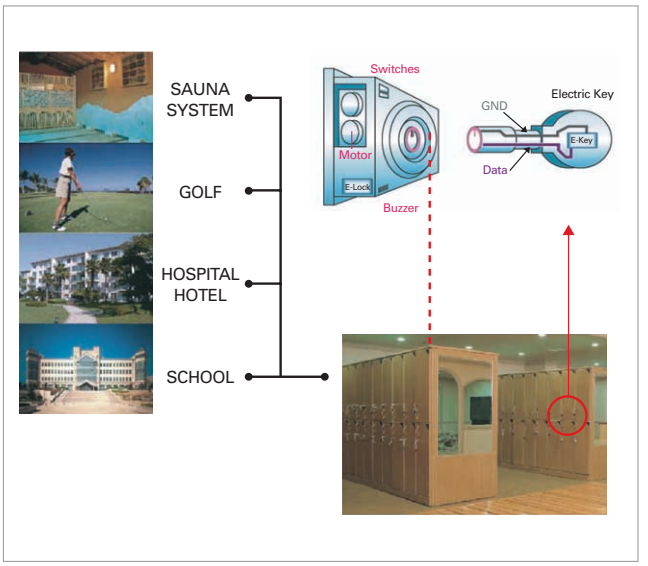
현재 SecurityCore는 셋톱박스를 중심으로 급격하게 양산 물량이 늘어가는 상태이다.

3. UniChip : 전자키

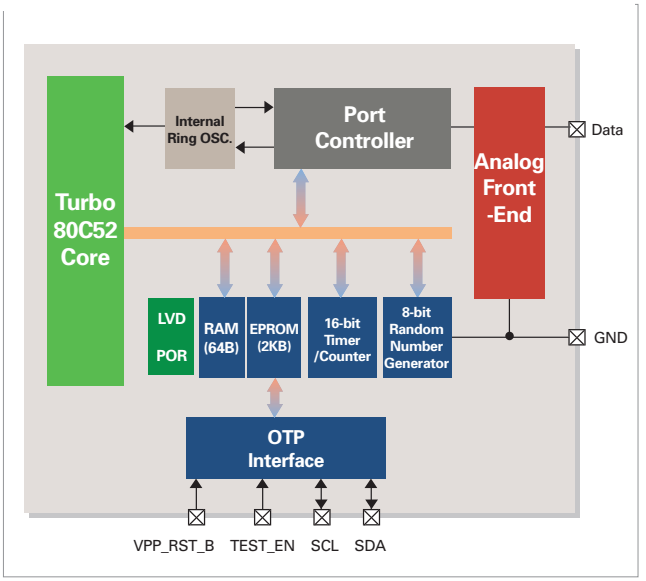
요즘에서는 보통의 기계식 열쇠 대신에 전자키가 주머니 한자리를 차지하고 있다. 전자키는 가정의 디지털 도어락에서 뿐만 아니라 일상생활의 다양한 장소에서 접할 수 있다. 즉, 찜질방, 사우나, 스포츠센터, 학교 등에서도 쉽게 접할 수 있다. 조그마한 전자키 하나로 단순한 입장 및 퇴장 관리 뿐만 아니라 후불정산관리, 회원관리 등의 종합적인 통합관리 시스템을 구축할 수 있게 되었다 〈그림 5〉. 그러나 손쉽게 복제가 가능한 기계식 열쇠라면 이러한 통합관리는 상상도 할 수 없는 일일 것이다. 코아리버의 UniChip과 같은 전자키를 이용하면 이러한 시스템 구축이 복제 위험 없이 가능하게 된다.

각각 다른 일련번호로 ID를 부여하는 보안 알고리즘이 EPROM에 내장된 UniChip을 사용하기 때문에, 일반 기계식 열쇠와 같이 중복 키 제작이 불가능하며, ID가 지워지는 것을 방지할 수 있다. 여분의 키를 새롭게 등록하면 되기 때문에 새로운 잠금장치 교환이 불필요하게 되어 비용을 절감할 수 있는 효과가 있다. 또한 마스터 키를 사용하면 사용자 키가 자동으로 삭제되어 사용할 수 없게 되므로, 사용자 키로 열리지 않으면 마스터 키가 사용되었다는 증거가 돼서 도난 사실 확인이 가능하다. 도난 사고 발생시 또는 키의 사용 내역을 확인하고자 할 때는 전용 단말기를 통해서 키의 사용 기록을 확인 및 조회할 수도 있다. 키 하나로 다양한 종류의 잠금장치에 사용할 수 있으므로 잠금장치별로 여러 개의 키 소지가 불필요하여 사용자의 편의성이 높아진다. 즉 전자키 하나로 가정의 현관 열쇠, 안방 열쇠, 사무실 열쇠 등으로 한꺼번에 사용이 가능한 것이다.

하지만 무엇보다도 기술적으로 흥미로운 부분은 UniChip이 ID와 알고리즘 쓰기를 위해 제작 당시 사용하는 4핀 이외에 동작 중에는 단지 2핀만(Data, GND)이 사용된다는 점이다. 칩이라면 전원(VDD, GND) 2핀 이외에 다른 핀을 갖는 것이 일반적으로 알려져 있다. 그러나 UniChip에서는 Data 핀을 이용해서 전반부에는 전원을 공급받고 이 전원을 칩 내부의 capacitor에 저장하며, 후반부에는 capacitor에 저장된 에너지를 칩 내부 전원으로 사용하면서 Data 핀으로 다시 잠금장치와의 송수신 통신을 통해 인증절차를 거치게 된다. 이와 같이 Data 핀 하나로 전원과 데이터 통신을 동시에 행할 수 있는



〈그림 5〉 UniChip의 적용 예



〈그림 6〉 UniChip의 구조

특수한 Analog Front End 블록이 내장되어 있는 것이 UniChip의 가장 큰 특징이다 〈그림 6〉.

한편 내장된 8-bit 난수발생기(random number generator)를 통해 잠금장치와의 송수신 통신의 seed로 사용하게 되며, 이 난수발생기를 통해 보다 높은 보안단계를 제공할 수 있게 된다.

4. 결론

코아리버는 범용 MCU 제품인 MiDAS 시리즈를 주력으로 본 지면에 소개한 SecurityCore와 UniChip 이외에 자동차 산업의 주요부품의 떠오르는 RF 방식의 TPMS(Tire Pressure Monitoring System)를 지원하는 MCU 제품군, 리모콘용 4비트 MCU 제품군인 ATOM 시리즈를 단계적으로 선보일 예정이다. 특히, 코아리버에서는 2003년 상반기에 기존의 인텔 80C52 제품보다 약 3배가 빠른 Turbo80C52 코아를 개발하였고, Turbo80C52 코아와 다양한 아날로그 및 디지털 IP (Intellectual Property)를 내장한 MiDAS 시리즈를 성공적으로 개발하였다.

또한 칩 뿐만 아니라 이를 제품에 대한 응용 시스템 MDS(Micro-processor Development System)와 C 컴파일러를 포함한 개발환경을 모두 구축하였다. 이 환경을 이용하여 범용 MCU 뿐만 아니라 고객의 요구사항에 따른 MCU 제품인 AS-MCU (Application-Specific MCU)제품을 전개하고 있다.

더불어 32bit ARM9 코어를 이용한 TiTAN 시리즈로 무선통신, 멀티미디어 관련 제품 개발로 영역 확대와 안정적인 제품 포트폴리오의 구성을 꾀하고 있다. 또한 코어의 개발도 기존 80C52 터보 코어 외에 ARM9 시리즈 성능의 Open RISC 및 모바일 RISC DSP 코어까지 확대될 전망이다.

코아리버는 '토종 MCU의 자부심'을 바탕으로 한 끊임없는 기술 개발과 마케팅을 통해 세계 유수 메이저 업체와 경쟁하면서 단계적 성장을 거듭하고 있다. 주력 사업분야에서 업계 1위를 차지할 수 있을 만큼 역량을 높이는 한편, 기업의 발전을 뒷받침할 수 있는 기업의 문화를 창출, 발전 시키고자 오늘도 임직원 모두 뜻을 모아 끊임없는 노력을 다하고 있다.

【 참고 문헌 】

[1] 유영준, "디지털 암호화 기술 현황", 전자부품연구원 전자정보센터

[2] 이현노, "IPTV 산업동향", IT SoC Magazine

[3] 코아리버, www.coreriver.com