스마트 자동차 보안 기술 동향

차영태 (고려대학교 융합소프트웨어전문대학원)

목차

1. 개 요

그동안 자동차는 단순한 운송 수단으로써 기계 장치로 여겨졌으나 최근에는 인포테인먼트, 자율 주행, 커넥티드 카 등의 용어에서 보듯이 전장화의 추세가 매우 급속히 이루어지고 있다.우선 자동차 내부에서는 100개 가까이 되는 ECU (Electronic Control Unit)가 존재하여 자동차의 각종 기능을 전자적으로 제어하고 있으며 외부적으로는 텔레매틱스 도구를 이용한 서비스가 확장되고 있는 추세이다. 비록 아직 V2X(Vehicle to Everything)와 같이 그간 제시되었던 모든 꿈같은 서비스가 시행되는 데는 아직 다소 시간이 필요하지만 이러한 발전 방향에 대한 공감대는 충분히 형성되어 있다고 본다.

이러한 자동차의 전장화 및 정보화에 따라 많이 우려되는 문제가 보안의 문제이며 본 논문의 주제이다. 본 논문에서는 이중에서도 특히 외부의 사이버 공격에 대해 안전을 확보하기 위한 보안 기술에 대해 주로 다루고자 한다.

그동안 보안 문제는 정보시스템에서 많은 기술이 축적되어 왔으며 여러 보안 시스템을 중복하여 여러 계층으로 사용하는 다계층 보안 구조가 일반적인 개념이다. 하지만 오랜 보안 기술의 축적 및 여러 보안 시스템을 사용함에도 불구하고 정보 시스템에서 조차 아직 공격 기술을 따라 가지 못하고 있는 실정이다

자동차라는 임베디드 시스템에서 보안 문제는 안전성에 관련되므로 매우 중요하나 기술적으로는 실시간 및 자원 제약 문제로 말미암아 적용할 수 있는 기술 범위가 오히려 좁은 면이 있다. 예를 들면 바이러스 백신이나 패치 관리 시스템 등을 자동차 같은 임베디드 시스템에 사용하는 것은 적당하지 않다고 여겨지고 있는 것이다. 하지만 이와 반대로 자동차 내부 네트워크는 그 구조 및 트래픽의 종류가 정보 시스템보다는 매우 단

순하고 또 한번 자동차가 출시되면 변하지 않는 구조를 가지고 있으므로 보안에는 쉬운 특성이 될 수도 있다고 본다.

본 논문에서는 그동안 제시되었던 자동차에 대한 사이버 공격 및 이에 대응하는 유망한 자동차 보안 기술을 살펴 보며 또한 근본적으로 사이버 공격에 대응할 수 있는 기술을 살펴 봄으로써 향후 기술 발전에 도움이 되고자 한다.

2. 사이버 공격 기술 동향

본 절에서는 자동차에 대한 사이버 공격에 대해서 기술적으로 중요한 시도에 대해서 살펴본다. 자동차에 대한 사이버 공격에 대한 우려는 이전에도 제시되었지만 2010년 워싱턴 대학교와 샌디에고 대학교의[1] 일단의 과학자들은 자동차의 내부 네트워크에 접근한 상태에서 엔진, 브레이크등 safety critical한 기능을 포함하여 거의 모든 기능을 악의적으로 제어할 수 있음을 보였으며, CARShark이라는 도구를 만들어 CAN 버스를 분석하고 임의로 만들어진 패킷을 주입할 수 있음을 보였다. 이에 대하여 물리적으로 자동차 내부 네트워크에 접근한 상태에서 사이버 공격을 하는 것보다 그냥 브레이크 라인을 끊는 것이 보다 현실적이라는 비판이 있기도 하였지만 이들의 시도는 이후 자동차에 대한 사이버 공격에 대한 다양한 연구의 시발점이 되었다.

이듬해인 2011년 위의 과학자들은 다시 자동차의 내부 네트워크에 접근할 수 있는 다양한 외부 공격 경로를 제시하는 연구 결과를 발표하였다[2]. 이후 이들은 공격 경로로 물리적인 접근이 필요한 자동차 OBD-II 진단 포트와 오디오 기기 뿐만이 아니라 근접한 거리에서 떨어져서 접근 가능한 블루투스 및 원격에서 접근 가능한 무선 셀룰라 통신을 공격하는 방법을 제시하였다. 이로써 자동차에 대한 사이버 공격이 더 이상 물리적으로 자동차에 접근하지 않은 상태에서도 가능하게 되었다.

이제까지의 사이버 공격이 그래도 학술적인 성격이 많았다면 보다 실제적인 성격의 사이버 공격이 Miller와 Valasek에 의해 시작된다[3]. 2013년에 이들은 포드사의 Escape와 토요타의 PRIUS에 대해서 정상적인 패킷과 진단 패킷을 이용해 공격할 수 있는 부분을 발표하였으며 CAN 버스에 접속하여 펌웨어를 수정하는 방법까지 발표하였다. 더욱이 이들은 이러한 공격을 위해 제작된 EcomCat이라는 CAN 버스에 어떤 정보를 읽고 쓰는 도구를 모두 공개하였다. 사이버 해킹세계에서 항상 그렇듯이 해킹하는 도구를 가지면 수많은 사람들이 이것을 사용해 봄으로써 향후 공격의 빈도가 높아지듯이 이 도구의 공개는 자동차라는 새로운 공격 대상을 제시하게 되었다고 볼 수 있을 것이다.

계속하여 이들은 이듬해인 2014년에 전 세계에서 생산된 20종의 자동차에 대하여 브레이크를 작동하거나 가속을 시키는 등의 실제로 의미 있는 수준의 공격이 가능한 가를 살펴보았으며 또한 이러한 safety critical한 기능을 얼마나 방어할 수 있게 제작되었는가를 조사했다[4]. 즉 자동차를 외부에서 조종하여 이상 동작을 일으키는 시나리오에 따라 조사를 수행한 바, 첫째, 외부와 통신하는 기능이 있는 ECU에 대한 접근 권한을 획득하고, 둘째로 권한을 획득한 ECU에서 원하는 safety critical한 기능을 담당하는 ECU에 대해 접근하는 방법을 획득하고, 마지막으로 원하는 safety critical한 기능을 담당하는 타깃 ECU가 원하는 이상 동작을 하도록 조작할 수 있는가를 조사했다.

첫째 단계를 위해서는 외부와 통신하는 모든 부분(remote attack surface)을 조사했으며 단순한

통신 기능 예를 들면 열쇠를 꽂지 않고 문을 여는 등의 단순 통신 기능으로는 이러한 시나리오를 성공시키기에 다소 부적합하며 텔레매틱스나 자동차에서 제공하는 인터넷 접속 기능을 공격하면 충분하다는 것을 알고 이 기능들의 제공 여부를 기준으로 삼았다. 둘째 단계로는 자동차 내부 네트워크의 구조인데 접근하기 쉬운 ECU와 타깃 ECU가 얼마나 떨어져 있는가를 기준으로 삼았다. 마지막으로 타깃 ECU가 원하는 동작을 하도록 조작할 수 있는 가의 여부는 대상 자동차가 보유하고 있는 기능이 있으면 조작이 용이해지므로 이미 사이버 물리 기능을 가지고 있는가의 여부를 기준으로 삼았다. 아래의 그림 [1]은 분석한 결과를 보여 준다. +는 공격이 쉬움을 나타내고 ++는 아주 쉬움을 -, --는 이와 반대를 나타낸다.

Car	Attack Surface	Network Architecture	Cyber Physical
2014 Audi A8	++	--	+
2014 Honda Accord LX	-	+	+
2014 Infiniti Q50	++	+	+
2010 Infiniti G37	-	++	+
2014 Jeep Cherokee	++	++	++
2014 Dodge Ram 3500	++	++	--
2014 Chrysler 300	++	-	++
2014 Dodge Viper	++	-	--
2015 Cadillac Escalade	++	+	+
2006 Ford Fusion	--	--	--
2014 Ford Fusion	++	-	++
2014 BMW 3 series	++	--	+
2014 BMW X3	++	--	++
2014 BMW i12	++	--	+
2014 Range Rover Evoque	++	-	++
2010 Range Rover Sport	-	--	-
2006 Range Rover Sport	-	--	-
2014 Toyota Prius	+	+	++
2010 Toyota Prius	+	+	++
2006 Toyota Prius	-	--	--

(그림 1) 여러 가지 자동차의 취약점 분석

3. 기존 보안 기술 동향

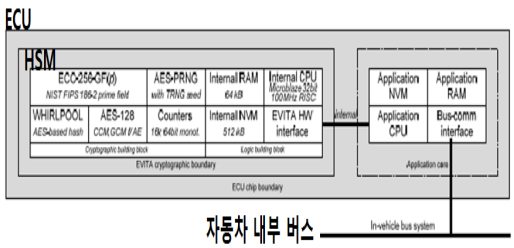
본 절에서는 사이버 공격에 대응하기 위한 보안 기술을 소개한다. 사실 보안 기술은 정보시스템에서 오랫동안 발전해왔으며 그 종류도 매우 다양하다.

하지만 자동차라는 임베디드 시스템에 적용하기 위해서는 대표적으로 자원의 제약 문제 및 실시간성의 문제를 극복하여야 할 것이므로 앞으로 많은 변모를 거치게 될 것으로 보이며 여기서는 대표적으로 유망한 기술을 보이도록 한다.

3.1 암호기술을 이용한 방어 기술

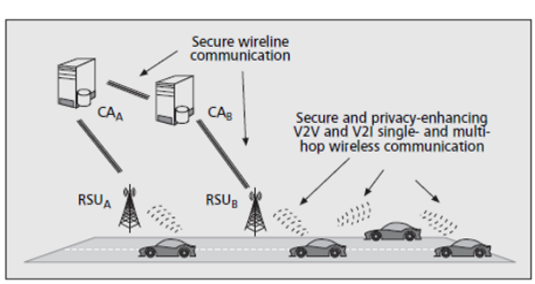
EU에서 2000년 중반부터 수행한 EVITA와 SEVECOM 프로젝트는 자동차가 외부와 연결될 때 필요한 보안 기술을 개발하였다. 우선 EVITA 프로젝트는 ECU 내부의 보안 플랫폼을 제공하기 위하여 모든 신뢰의 바탕이 되는 그림 [2]의 HSM(Hardware Security Module)을 제안하였다[5]. 이 HSM은 ECU 칩 내부에서 보조 프로세서 형태로 존재하고 모든 암호키의 저장 및 암호 계산을 담당함으로써 상위 계층에서 필요한 보안 기능을 담당한다. 여기서 필요한 보안 기능이라 함은 상위 계층에서 안전한 통신을 하기 위한 암호 계산은 물론이고 필요한 정보를 안전하게 저장하는 장소를 제공함으로써 ECU의 소프트웨어 및 안전이 필요한 정보의 위변조를 방지할 수 있는 플랫폼을 제공하는 것이다. 또한 CAN 통신에서는 전혀 보안 기능을 제공하지 않는 문제의 보완을 위하여 ECU와 ECU 사이의 통신 보안 기술도 제안하였다. 즉 CAN 버스의 통신 규격이 8 바이트임을 감안하여 비밀키 방식을 이용한 다소 간략한 암호 프로토콜을 제안한 것이다. 현재 프리스케일과 인피니언등 칩 벤더에서 HSM을 제공하고 있으며 이를 바탕으로 자동차 관련 기관에서 여러 가지 보안 기능이 계속 개발되고 있다.

SEVECOM 프로젝트에서는 자동차의 외부 통



(그림 2) EVITA 프로젝트의 HSM 구조

신을 안전하게 함과 동시에 프라이버시를 보장하기 위한 전체 통신 구조를 제안하였다[6]. 이 프로젝트에서 주로 다룬 문제는 외부로부터의 정보를 안전하게 받고자 하는 것이다. 예를 들어 악의적인 공격자가 주변 도로의 상황을 왜곡되게 전달할 경우 이 정보에 기초하여 판단하는 것은 오히려 해가 된다는 것이다. 또한 프라이버시 문제로는 자동차가 이동한 흔적을 남겨 이를 추적할 수 있게 되면 운전자의 동선이 그대로 노출된다는 것이다. 이러한 문제의 해결을 위해서 그림 [3]의 공개키 기반 구조를 응용한 보안 구조를 이용하여 정보의 안전성을 보장하고 또 이때 사용하는 인증서는 장시간 사용하는 인증서와 단기간 사용하는 인증서를 구분함과 동시에 여기에 사용하는 아이디는 여러 개의 pseudonym을 이용하여 인증서의 아이디를 바꿈으로써 프라이버시를 지키는 방법을 제안하였다.

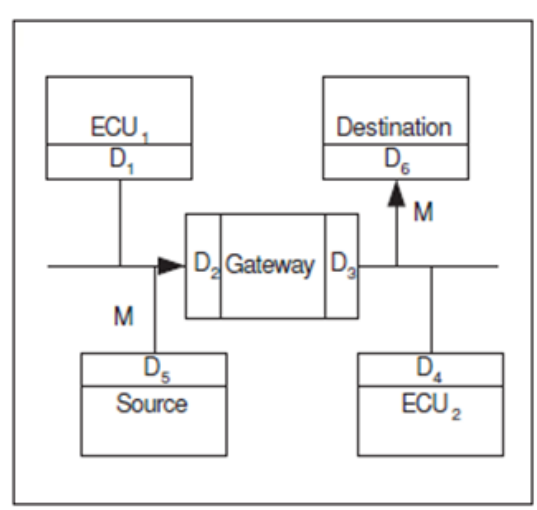


(그림 3) SEVECOM 프로젝트의 보안 구조

3.2 침입탐지기술

불법적으로 어떤 시스템에 침입했는지 여부를 탐지하기 위한 침입탐지기술은 자동차의 보안에서 매우 유용하게 되리라 보이며 그동안 있었던 대표적인 연구 결과 및 향후 전망을 살펴본다.

U. E. Larson등은 CAN 프로토콜 및 CAN을 사용하기 위한 응용 프로토콜인 CANopen을 분석하여 침입을 탐지하고자 하였다[7]. 이들은 CAN 특성상 메시지가 CAN 네트워크에 있으면 메시지의 출발지와 목적지에 대한 정보가 부족하므로 이를 극복하기 위하여 모든 ECU에 침입탐지 모듈이 있는 호스트 기반의 방식을 제안한다. 그림 [4]의 차량 내부 네트워크의 간략한 개념도에서 어떤 메시지가 출발지에서 목적지로 간다면 이 메시지의 경로와 관련된 ECU에서는 메시지를 쓰고 읽는 동작 중 필요한 동작만 하여야 할 것이며 또한 관련되지 않은 ECU에서는 불필요한 동작을 하지 않아야 할 것이다. 불필요한 동작의 존재 여부를 모든 ECU에 있는 호스트 기반 침입탐지 모듈에서 감시하게 되며 존재시 침입이 있는 것으로 간주할 수 있다는 것이 이들의 연구 결과



(그림 4) 차량 내부 네트워크의 간략한 개념도

Nr	Sensor	Description
S-1	Formality	Correct message size, header and field size, field delimiters, checksum, etc.
S-2	Location	Message is allowed with respect to dedicated bus system
S-3	Range	Compliance of payload in terms of data range
S-4	Frequency	Timing behavior of messages is approved
S-5	Correlation	Correlation of messages on different bus systems adheres to specification
S-6	Protocol	Correct order, start-time, etc. of internal challenge-response protocols
S-7	Plausibility	Content of message payload is plausible, no infeasible correlation with previous values
S-8	Consistency	Data from redundant sources is consistent

(그림 5) 침입탐지를 위한 8개의 센서

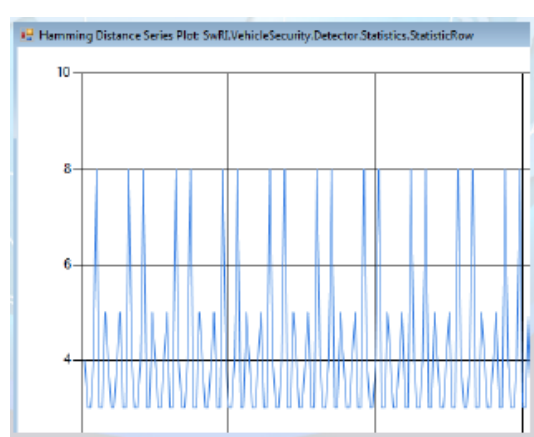
이다. 그림 [4]의 게이트웨이는 모든 메시지의 중계를 담당하므로 그 역할이 매우 중요하며 침입자에게 게이트웨이가 점령이 되면 모든 공격 행위가 가능하게 될 수 있다. 그러므로 게이트웨이의 침입 탐지 모듈의 역할이 특별히 중요하며 이 부분의 계산량이 매우 복잡해질 수 있는 약점이 있다.

M. Muter등은 비정상 패킷을 감지하기 위하여 그림 [5]와 같은 오탐이 전혀 없는 8개의 센서를 제안하였다[8]. 그림에서 보듯이 이들 센서는 패킷에 관련된 상세한 정보를 가져 오는 것을 의미한다. 또한 이들 센서로 오탐없이 침입을 탐지할 수 있다는 장점은 침입탐지의 또 다른 중요한 점인 탐지하지 못하는 공격이 있을 수 있다. 실제로 공격자가 CAN 규격에 맞는 제대로 된 메시지를 주입하면 전혀 탐지가 불가능하다는 약점이 있다.

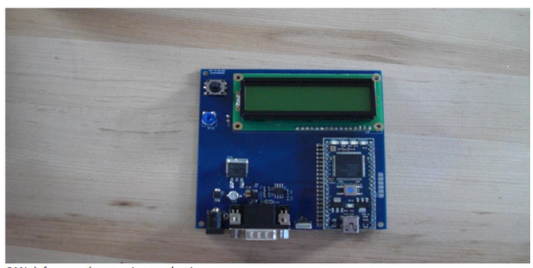
앞의 두 방법이 프로토콜 혹은 메시지의 규격을 지키지 않아서 생기는 이상 현상을 탐지하는데 주력했다면 M. Brooks는 메시지의 트래픽 특성을 분석하여 침입을 탐지하고자 하였다[9]. 즉 차량 네트워크상의 메시지의 트래픽 특성을 보면 완전히 주기적인 메시지, 이벤트가 있는 주기적인 메시지이나 가끔 이벤트가 포함되는 메시지, 이벤트에 의해서만 생성되는 메시지의 세 가지가 있다. 여기서 완전히 주기적인 메시지는 메시지와 메시지 사이의 시간 간격이 거의 일정한 메시지를 말하며 이벤트라 함은 사용자가 어떤 버튼을 눌렀을 때 생성되는 메시지를 가리킨다. 이들 특성을 보면 그림 [6]과 같이 차량 내부의 메시지는 대부분 주기적인 특성을 가지며 이를 이용해서 이상 현상을 감시할 수 있다는 것이다.

저자는 실험을 통하여 탐지의 정확도를 살펴보았는데 실제 정상 트래픽에 각종 공격 트래픽을 실험적으로 보내어 탐지를 시도하였다. 그 결과 완전히 주기적인 경우의 탐지율은 매우 높았으나 이벤트가 있는 경우는 다소 낮아서 이를 개선하는 하는 연구를 계속 진행할 예정임을 밝혔다.

침입 탐지 기술에서 마지막으로 한 가지는 앞의 공격자들에 의해 제안되었다[4]. 앞에서 말한대로 이들은 실제로 의미 있는 공격을 시도하면서 얻어진 아이디어를 바탕으로 침입탐지 방법을 제안하였다. 즉 어떤 점령된 ECU에서 타깃 ECU로



(그림 6) 차량 내부 네트워크의 트래픽 특성



(그림 7) 트래픽 양을 바탕으로 한 공격 탐지 장치

공격용 패킷을 만들어 보내면 최소한 정상 패킷과 공격 패킷이 보내져 트래픽 양이 늘어나게 된다. 따라서 실제로 공격이 일어나게 되는 경우에는 최소한 2배, 보통은 20-100 배의 트래픽 양이 지나게 되어 공격을 감지할 수 있게 되며 이를 이용하여 그림 [7]의 탐지 장치를 구현하여 제시하였다.

지금까지 여러 가지 침입탐지 기법에 대해서 살펴보았으나 또 한 가지 문제는 탐지 후 알람에 대한 처리 문제이다. 즉 침입이 탐지된 후 대응을 어떻게 하는가 하는 문제인데, 탐지된 이벤트의 심각도에 따라 여러 가지 방법 즉 시각적, 음향적, 햅틱적인 방법으로 사용자에 정보를 제공할 수 있을 것이다. 여기서 한 발 더 나아가 능동적으로 침입에 대응하는 시스템도(Intrusion Prevention System) 기술적으로는 가능하나 자동차라는 safety-critical한 시스템에서 법적인 문제까지 연결되어 쉽지 않을 것이라 전망된다.

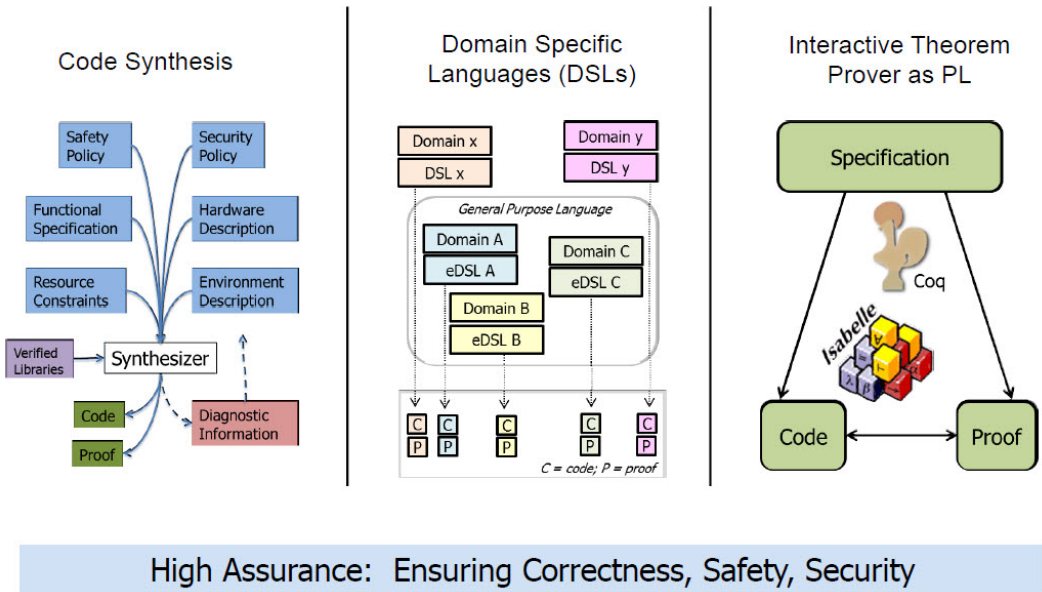
4. HACMS

현재 자동차 보안 기술은 정보시스템에 사용되던 기술을 자동차 분야에 맞게 변형한 것이나 자원이 부족하고 실시간성이 강한 임베디드 시스템 특성으로 말미암아 사용하기 적합지 않은 면이 있다. 또한 정보 시스템에서도 그동안 많이 지적되어 왔지만 공격 능력에 비해 충분한 대비가 되지 않는다는 것이다. 즉 알려진 어떤 문제에 대해서는 다소 방어가 되지만 알려지지 않은 공격에 대해서는 방어가 어려운 면이 있다. 이에 DARPA에서는 HACMS(High Assurance Cyber Military System)라는 프로젝트를 통해 근본적으로 다른 접근 방법을 선보인바 이를 간략히 살펴보기로 한다[10].

우선 HACMS 프로젝트의 목적은 지상 팀과 항공 팀의 두 팀이 각각 해킹 공격에 안전한 무인 자동차와 드론을 만드는 것이며, 이 프로젝트에 흐르는 가장 기본적인 생각은 소프트웨어가 사양에 명시된 대로 작동한다면 아주 적은 부분만 공격에 취약하게 되고 이 부분만 방어하면 된다는 것이다. 따라서 설계된 기능 명세를 만족함과 동시에 안전 및 보안 정책(safety and security policy)을 만족하도록 정형 기법을 사용하여 엄밀히 개발 및 검증함으로써 오류 및 해킹에 최대한 안전한 시스템을 만들고자 하였으며 그림 [8]에 전체적인 개발 방법에 대한 개념이 제시되어 있다.

이 두 팀의 프로젝트는 모두 학계 및 산업계를 선도하고 있는 여러 기관이 협력해서 수행한 대규모 프로젝트로 내용을 간단히 기술하기 어려우나 항공 팀의 프로젝트를 대략 살펴봄으로써 향후 기술의 방향 설정에 참고해 보고자 한다.

항공 팀 프로젝트의 중요한 핵심 기술은 seL4라는 세계 최초로 정형기법으로 검증된 OS 마이크로커널이다[11]. 이 마이크로커널은 기능적으로 오작동이 없고 보안성면에서 무결성과 비밀성이 보장됨이 theorem proving이라는 정형기법으로 증명이 되어 있어서 이 커널을 사용하면 모든 시스템 콜은 반드시 끝이 나며, 예외 경우, 널 포인터 역참조, 메모리 누수, 연산 오류 등의 기능적인 모든 오류가 전혀 없으며 보안 문제의 원인이 되는 버퍼 오버플로우 및 코드 인젝션 등이 원천



(그림 8) HACMS의 개발 방법 개념도

적으로 불가능하다[12].

이 마이크로커널이 제공하는 정형기법으로 증명이 된 신뢰할 수 있는 기능을 기본 바탕으로 하고, 또한 상위 계층의 소프트웨어도 역시 컴포넌트 기반 플랫폼[13] 및 DSL[14]을 이용하여 신뢰할 수 있는 시스템을 지향하여 개발하였다. 결과적으로 소스코드까지 포함된 개발 결과물을 별도의 사이버 공격 팀에 의뢰하여 취약점을 찾고자 시도하였으나 6주간 아무런 취약점이 발견되지 않은 좋은 결과를 얻게 되었다.

5. 결 론

본 논문에서는 자동차에 대한 사이버 공격 및 이에 대한 방어 기술에 대해 기술하였다. 최근 자동차 공격에 사용된 기술이 공개화 됨에 따라 관련 기술이 일반화되어 실제 문제화되는 빈도가 빠르게 늘어나리라 생각한다. 또한 학자 층에서도 자동차 보안 기술을 단순히 실험실 수준이 아닌 실제 생산된 전 세계의 여러 가지 자동차를 검증하는 수준까지 시도하고 있어 향후 각 자동차 회사의 평판에도 많은 영향을 미치리라 짐작된다.

보안 기술로는 기존 정보시스템에도 사용되던 기술 중 임베디드 시스템에 적합하리라 생각되는 암호 기술을 이용한 방어 기술과 침입탐지기술에 대해 살펴보았다. 아직 이러한 기술이 본격적으로 자동차에 적용되지는 않지만 향후 필요성이 높으리라 생각된다. 또한 보안 문제를 근본적으로 해결하기 위해 정형기법을 사용하여 신뢰 가능한 시스템을 구축하려는 프로젝트를 소개하였는바 향후 자동차 보안 기술의 발전 방향에 많은 시사점을 제시하길 기대한다.

참 고 문 헌

[1] K. Koscher et. al., “Experimental Security Analysis of a Modern Automobile”, IEEE Symposium on Security and Privacy, 2010.

[2] S. Checkoway et. al., “Comprehensive Experimental Analyses of Automotive Attack Surfaces”, 20th USENIX conf. on Security, 2011.

[3] C. Miller and C. Valasek, “Adventures in Automotive Networks and Control Units”, Defcon conf., 2013.

[4] C. Miller and C. Valasek, “A Survey of Remote Attack Surfaces”, Defcon conf., 2014.

[5] H. Seudie, “Vehicular On-board Security: EVITA Project”, C2C-CC Security Workshop, 2009.

[6] P. Papadimitratos et. al., “Secure Vehicular Communication Systems: Design and Architecture”, IEEE Communication Magazine, 2008.

[7] U. E. Larson et. al., “An Approach to Specification-based Attack Detection for In-Vehicle Networks”, Proc. of the IEEE Intelligent Vehicles Symposium, 2008.

[8] M. Muter et. al., “A Structured Approach to Anomaly Detection for In-Vehicle Networks”, International Conf. on Information Assurance and Security, 2010.

[9] M. Brooks, “Anomaly Detection on Vehicle Networks”, Escar Conference USA, 2013.

[10] K. Fisher, “High Assurance Cyber Military System: Making sure you are in control of your vehicle”, Escar Conference USA, 2013.

[11] G. Klein et. al., “Comprehensive Formal Verification of an OS Microkernel”, ACM Trans. on Computer Systems, Feb. 2014.

[12] D. Elkaduwe et. al., “Verified Protection Model of the seL4 Microkernel”, Proc. of the 2nd International Conference on Verified Software: Theories, Tools, Experiments. 2008.

[13] G. Heiser et. al., “Towards Trustworthy Computing Systems: Taking Microkernels to the Next Level”, ACM SIGOPS Operating Systems Review Vol 41 Issue 4. Jul. 2007.

[14] P. C. Hickey et. al., “Building Embedded Systems with Embedded DSLs”, ICFP Sep. 2014.

저 자 약 력

차 영 태

이메일: ytcha77@korea.ac.kr

- 2013년~현재 고려대학교 융합소프트웨어전문대학원
- 2011년~2013년 산업자원부 지식정보보안 PD
- 2000년~2010년 시큐아이 연구소장
- 1994년~2000년 삼성종합기술원 수석연구원
- 관심분야 : 네트워크 보안, 시스템 보안, 자동차 보안