ETAS

DRIVING EMBEDDED EXCELLENCE

자동차 사이버보안에서의 침입탐지 및 방지 시스템

이해승 상무
이타스코리아 기술부

인터넷 서핑 중에 아래 문장들을 발견했습니다.

Given enough time all security will fail: Security in today's world is incredibly challenging to get right. You have to be perfect all the time but a hacker only has to succeed once to defeat you.

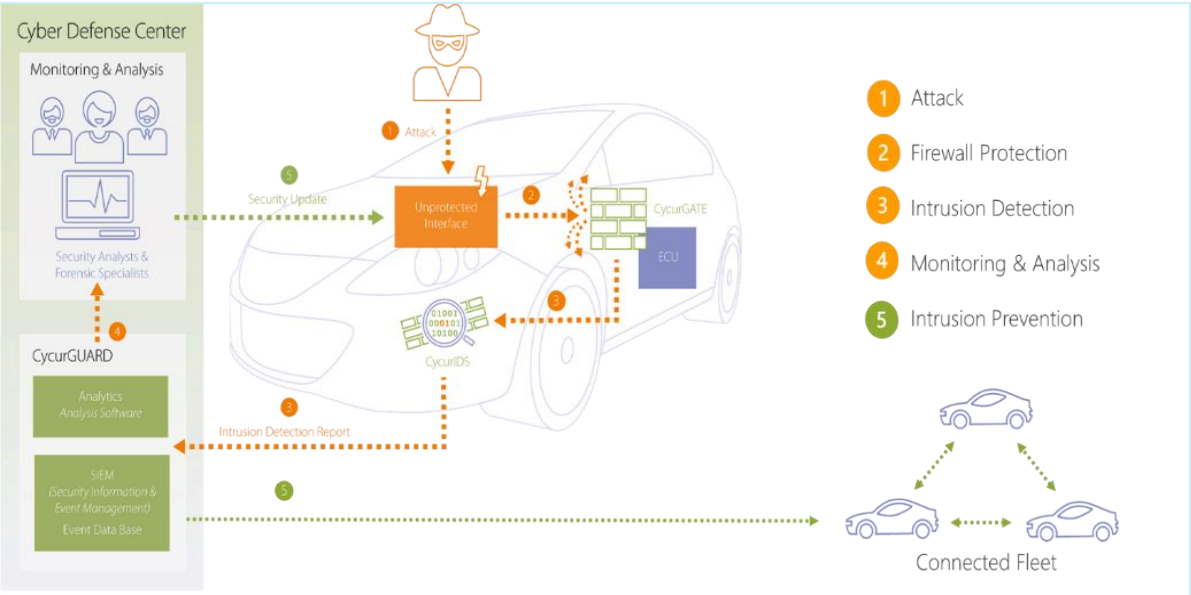
<출처: http://thecodist.com/article/lessons_from_a_lifetime_of_being_a_programmer>

모든 보안책은 결국 시간이 지나면 취약점을 드러낸다는 너무도 당연한 이야기라 메시지의 신선함은 적습니다. 그런데 그 이유를 개발자 관점에서 표현한 것이 설득력이 있습니다. "당신은 늘 완벽해야 하지만, 해커는 한 번만 당신을 이기면 된다." 그래서 "시간이 지나면 취약점을 드러낼 수 밖에 없는 보안 문제에는 어떻게 대처해야 할까?"라는 의문은 왠지 자연스럽게 느껴지기까지 합니다.

저는 이타스라는 회사의 에스크립트 사업 부서에서 일합니다. 이타스는 주로 자동차용 전자제어 시스템의 소프트웨어 개발에 필요한 툴을 전문으로 하는 회사입니다. 에스크립트는 전자제어 시스템의 보안 솔루션을 전문으로 합니다. 이런 연유로 에스크립트는 특히 "자동차용" 전자제어 시스템의 보안에 대해서 많은 연구 개발을 하고 있습니다. 그래서 위 의문을 자동차에 적용하면 이렇게 바꿀 수 있습니다. "시간이 지나면 취약점을 드러낼 수 밖에 없는 자동차 보안 문제에는 어떻게 대처해야 할까?"

에스크립트는 이에 대해 다양한 대비책들을 마련하고 있습니다. 그리고 이런 다양한 대비책들은 서로가 서로를 보완하는 관계에 있기에 동시에 함께 적용되어야 합니다. 그 중에서 IDPS (Intrusion Detection Prevention System, 침입 탐지 및 방지 시스템)에 대한 에스크립트의 솔루션을 소개하고자 합니다.

에스크립트의 IDPS 시스템은 아래 그림과 같이 구성되어 있습니다.



잘 아시는 바와 같이, 자동차의 시스템들은 내부 네트워크를 통해서 직간접적으로 서로 연결되어 있습니다. 그리고 점점 더 많은 차들의 내부 네트워크가 텔리매틱스 시스템을 통해서 외부 인터넷과 연결되고 있습니다. 인터넷에 연결된 모든 장치들은 꾸준히 침입 시도를 받고 있습니다. (지금 제가 개인적으로 갖고 있는 NAS 의 로그를 보니, 지난 18 시간 동안 13 번의 접속 차단이 있었습니다.) 인터넷에 연결된 소위 커넥티드 자동차들도 이런 침입 위험의 예외일 수 없습니다.

해커가 인터넷을 통해서 차량 내부 네트워크에 침입하려고 하는 경우, 일차적으로 방화벽이 침입을 차단합니다. **(그림의 ①②에 해당)** 해커가 방화벽을 뚫고 칩입에 성공하는 것은 시간 문제입니다. 이럴 때를 대비해서 IDS(Intrusion Detection System, 침입 탐지 시스템)가 있습니다. IDS 는 미리 정해진 룰에 따라 침입을 탐지합니다. 룰의 간단한 예를 들자면, 어떤 특정 아이디의 메시지는 10msec 주기로 전송되어야 하는데 그보다 더 자주 전송된다거나, 어떤 메시지는 차가 정지한 상태에서만 전송되어야 하는데 운행 중에 전송이 된다거나 하는 것입니다. 탐지된 침입은 IDS 에 기록으로 남습니다. 이런 침입 기록은 작게는 하루 수 만 개에서 많게는 수 억 개가 될 수 있으며, 소위, 백-엔드로 수집됩니다. **(그림의 ③에 해당)**

백-엔드에 모아진 침입 기록들은 프로그램에 의해서 자동으로 분류되게 됩니다. 그리고 이렇게 분류된 침입들은 보안 전문가들의 점검과 분석을 받게 됩니다. 보안 전문가들은 각 침입에 대해서 대응책이 필요한지를 판단합니다. 그리고 실질적으로 위험이 되는 침입에 대해서는 방화벽을 비롯하여 해당 위협에 노출된 제어기들의 보안 소프트웨어를 개선하게 합니다. IDS 가 지나치게 민감하게 탐지한 침입에 대해서는 불필요한 탐지가 없도록 개선하게 합니다. **(그림의 ⑤에 해당)**

보안 위협에 빠르게 대처하기 위해서, IDS 소프트웨어 개선 및 배포는 자동차가 운행되는 동안 반복적으로 이루어져야 합니다. 또, 보안 미비 기간을 최단으로 하기 위해서, IDS 개선 소프트웨어 개발은 최대한 신속하게 이루어져야 합니다. 에스크립트는 이런 필요에 맞추어 IDS 소프트웨어 개발을 편리하고, 신속하고, 신뢰성있게 할 수 있도록 지원하는 툴인 CycurID 를 개발하여 출시를 앞두고 있습니다.

DRIVING EMBEDDED EXCELLENCE

CycurIDS 는 사용자가 GUI 를 통해서 IDS 룰을 편리하고 신속하게 설계할 수 있게 해주며, 설계된 룰에서 제어기 소프트웨어에 포함될 오브젝트 파일을 자동으로 생성해줍니다. CycurIDS 의 높은 품질로 생성된 오프젝트 파일은 높은 신뢰성을 갖습니다.

에스크립트는 IDS 제어기로 인한 원가 인상을 최소화하는 방안으로, IDS 의 탐지 기능이 네트워크에 연결된 다양한 제어기에 분산 탑재될 것으로 예상하고 있습니다. 각 제어기가 갖고 있는 여분의 메모리와 연산 능력을 활용하면, IDS 의 성능을 유지하면서, IDS 제어기의 사양을 낮게 가져갈 수 있어 원가 인상을 피할 수 있기 때문입니다.

이타스의 앞선 임베디드 소프트웨어 기술과 에스크립트의 앞선 임베디드 보안 기술이 합쳐져서 어떤 기술 발전을, 궁극적으로, 우리 삶에 어떤 혜택을 가져올지 지켜봐 주시고 격려해주시기를 부탁드립니다.

##

[에스크립트 소개]
에스크립트는 이타스의 임베디드 보안 자회사로서 자동차 사이버 보안 시장의 선도기업이며, 보안수준분석부터, 제어기, 네트워크, 시스템 구축, 조직 구성에 이르는 통합적인 보안 솔루션을 제공하고 있습니다. 2017 년 2 월 '트러스트 포인트(TrustPoint Innovation Technologies, Ltd.)'인수를 통해 사업영역을 전체 IoT 보안으로까지 확장하고 있으며, 에스크립트 한국사무소는 ITU-T(International Telecommunication Union Telecommunication Standardization Sector)가 진행하고 있는 커넥티드카의 내장형 보안과 관련된 국제표준 개발 프로젝트에 한국 대표의 일원으로 참여하고 있다.