

2022 KAIST Tech Fair KAIST 기술이전 설명회

네트워크 시스템 보안을 위한 프로토콜 다이얼렉트

전산학부 정보보호대학원 강병훈 교수

KAIST

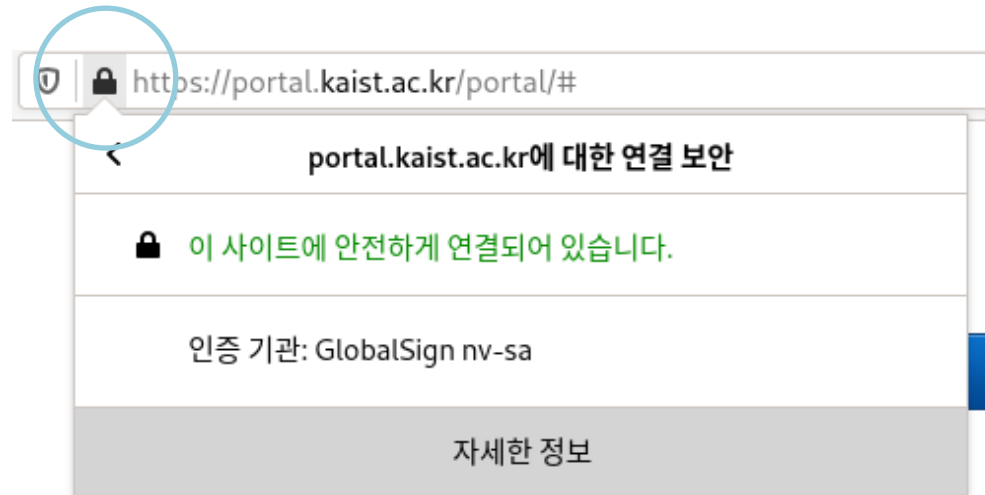


Contents

- 01 연구개발 배경
- 02 기술/아이템 개요
- 03 기술의 특징 및 적용 방식
- 04 기술의 효과
- 05 산업분야 및 시장 규모
- 06 사업화 방안

01. 연구개발 배경

- ◆ 현존 서버-클라이언트 간 모든 통신은 암호화(기밀성/무결성) 되어 **개인정보를 안전하게 보호함**
 - 예) KAIST 웹 사이트 접속시 표시되는 자물쇠 아이콘 (HTTPS)은 암호화된 HTTP 통신을 뜻함



- ◆ 그러나, 이러한 암호화된 통신을 제공하기 위한 프로토콜 소프트웨어 구현에도 **취약점/결함**이 존재함
 - 취약점/결함을 악용하여 개인정보, 금융정보 등의 민감한 정보가 공격자에게 노출될 수 있음
 - 또한, 네트워크에 연결된 모든 서버, 컴퓨터, 모바일, IoT 기기 등의 심각한 안전성 피해로 확대될 수 있음
- ◆ 이는, 안전한 네트워크 세상의 근간을 위협하는 중대한 문제임

◆ 암호화된 통신을 제공하기 위한 프로토콜 소프트웨어 구현에도 결함이 존재

- 2014년 전세계적으로 발생한 **HeartBleed 해킹** 사태
 - 전세계적으로 널리 쓰이고 있는 암호화 통신 (OpenSSL) 을 완벽히 무력화
 - 통신 프로토콜 소프트웨어 구현의 버그를 악용 비밀키 (Secret key) 탈취
 - 암호학자 Bruce Schneier가 "HeartBleed는 보안 문제 등급 1 ~ 10단계 중 11단계"라고 언급, 매우 심각한 전세계적인 문제



2014년 HeartBleed Attack
(취약점 번호 CVE-2014-0160)

- 2021년 전세계적으로 발생한 **PulseSecure VPN 해킹** 사태

- 인증 우회 가능: 공격자가 따로 인증 과정을 거치지 않아도 됨
- 랜섬웨어 공격자들도 해당 취약점을 이용해 시스템에 침투 시도

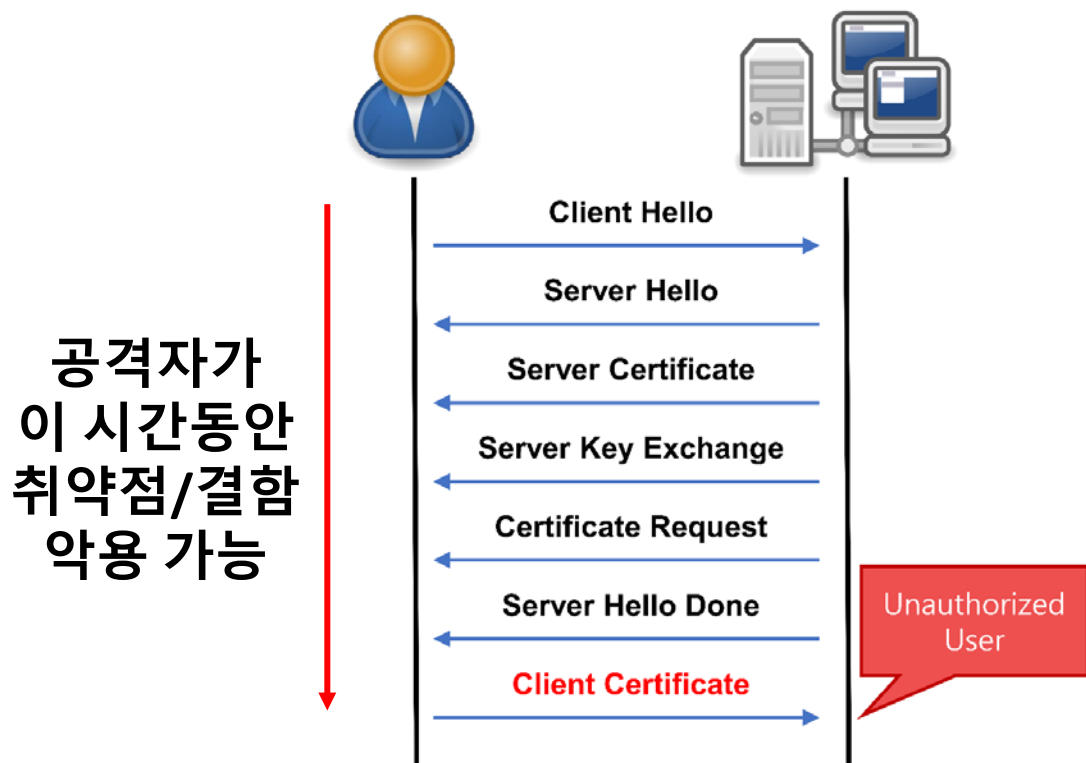


2020-1년 PulseSecure VPN Hacking
(취약점 번호 CVE-2021-22893 외 다수)

◆ 근본적인 선제적 방어 대책 기술이 절실히 요구됨

- 프로토콜 구현의 잠재적인 취약점/버그는 항상 존재함 (다만, 아직 알려지지 않았을 뿐임)
- SSL/TLS의 소프트웨어 구현(OpenSSL, PulseSecure VPN)뿐만 아니라 다른 모든 암호 통신 프로토콜(예, IKE 등)의 소프트웨어 구현의 취약점/결함도 최소화할 수 있는 기술 필요

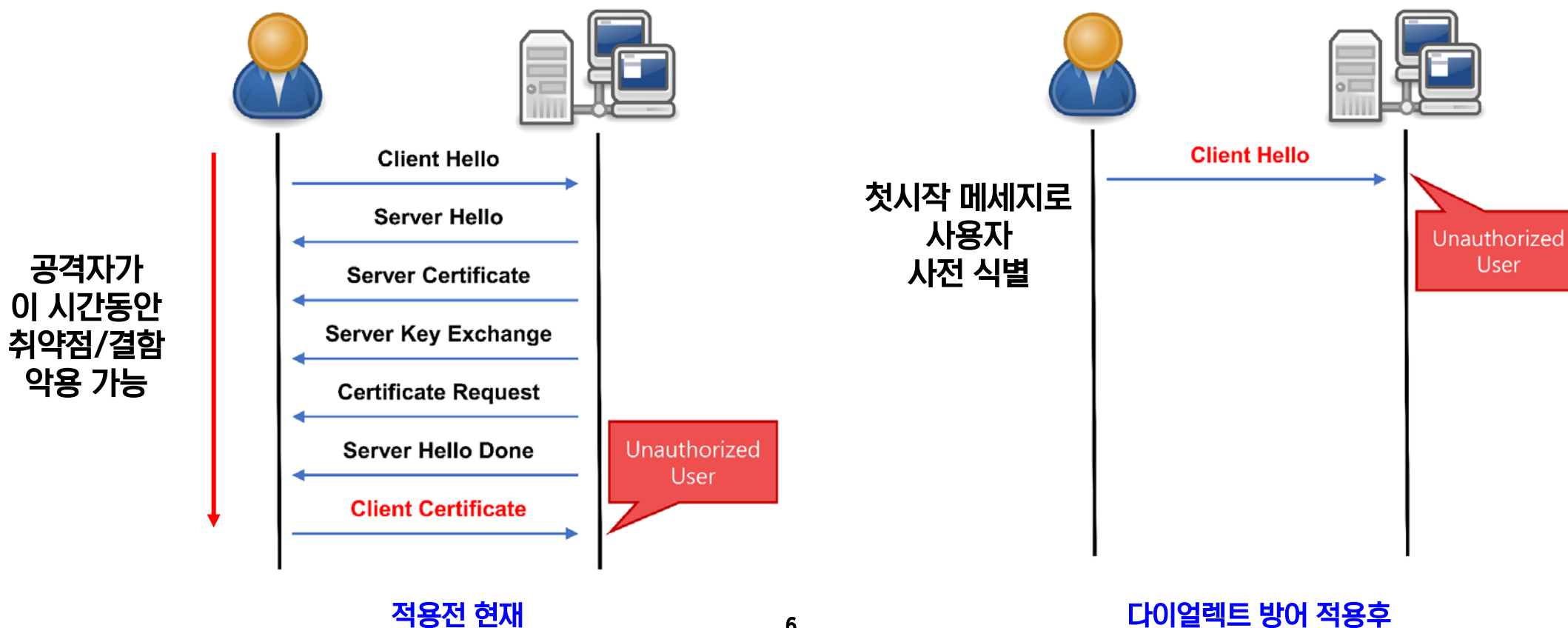
02. 기술/아이템 개요 (요약 소개)



- ◆ 현존하는 암호화된 통신을 제공하기 위한 프로토콜 대부분은 **사용자의 식별(인증, Authentication)**을 가장 먼저 할 수 없는 한계를 가짐
 - 인증 시점 이전까지 공격자가 취약점을 악용할 대상/범위/시간이 충분히 주어짐
 - 사용자 인증 시점은 암호화 HTTP의 기반인 전송 계층 보안 프로토콜 (Transport Layer Security) 은 통신 시작 후 3번째 메시지를 받는 시점에서 사용자를 식별함
 - 3번째 메시지 도착 전에는 인가된 사용자와 공격자를 분간할 방법이 없음
- ◆ 모든 방문자들에 대해서 **집안 문을 항상 먼저 열고 방문자의 신분증을 보며 확인** 해야 하는 것과 같은 위험성을 내포함

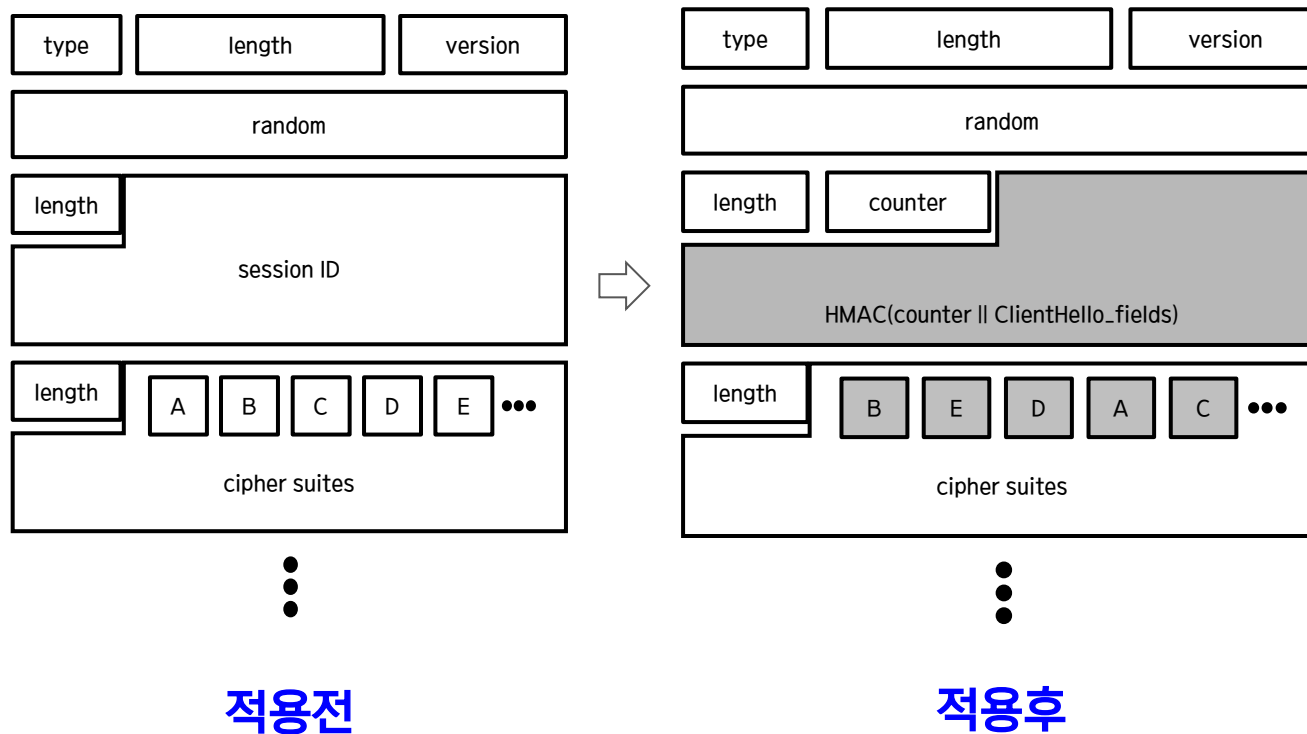
02. 기술/아이템 개요 (요약 소개)

- ◆ 새로운 다이얼렉트(Dialect) 기술로 사용자의 사전 식별을 가장 첫번째 메시지로 이동
 - 사용자의 사전 식별을 위해 첫번째 메시지를 변경하는 **신규 프로토콜의 제시 및 배포**는 현존하는 전세계의 통신 프로토콜을 모두 다 바꾸어야 하기에 거의 불가능함 (**기존 프로토콜 호환성을 100% 보장**해야 함)

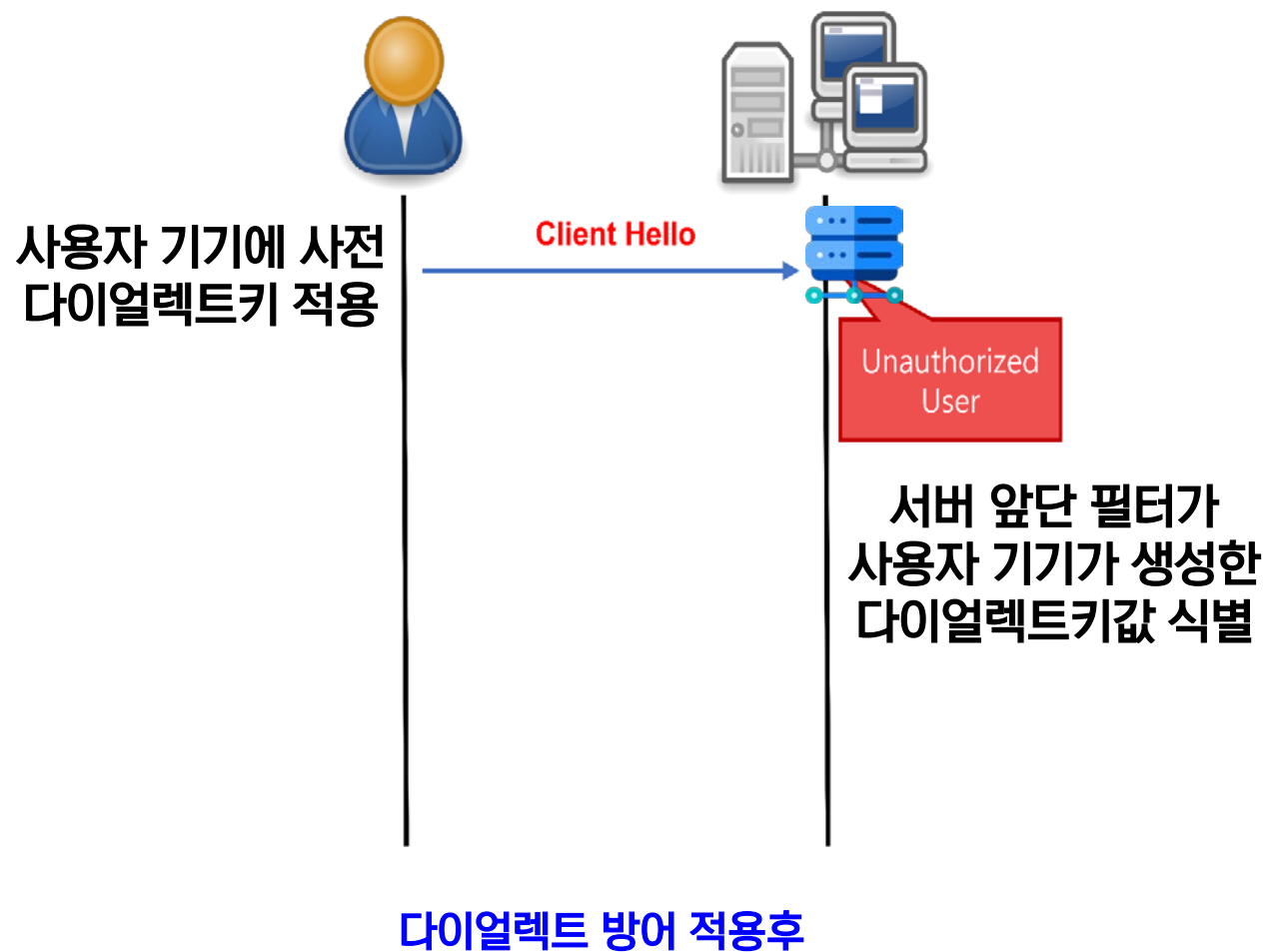
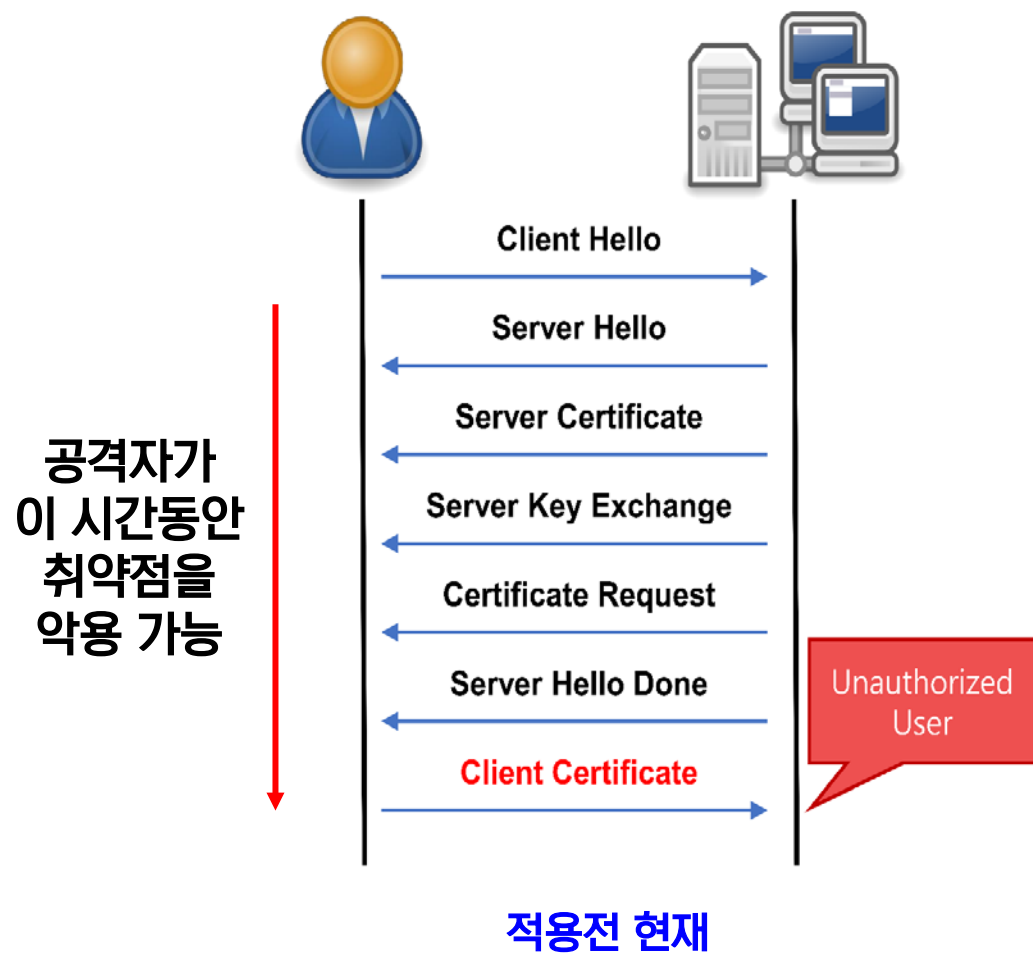


03. 기술의 특징 및 적용 방식

- ◆ 통신 첫번째 메시지에 인가된 사용자 기기만 생성 가능한 암호값과 헤더필드 셔플링 값을 포함시킴
 - 따라서, 비인가된 사용자 (공격자 포함)는 통신 시작 시점부터 사전 식별됨 (Early Filtering)
- ◆ 해당 암호값과 필드 셔플링 값은 **기존 프로토콜과의 호환성**을 전혀 해치지 않는 방식으로 적용됨



03. 기술의 특징 및 적용 방식



04. 기술의 효과

- ◆ 매년 다양한 통신 프로토콜 소프트웨어에서 수많은 **취약점/결함**이 계속 발견되고 있음
 - 해당 취약점/결함을 전세계적 규모의 해커 그룹이 악용하는 경우 종종 발생

2010 ~ 2020년간 발견된 다양한 TLS / IPSec 취약점

CVE	Type	Severity	Description
CVE-2016-6309	RCE	critical	A dangling pointer in the OpenSSL library can be used to cause a denial of service via a crafted RSASSA-PSS signature.
CVE-2016-6304	DoS	high	A maliciously crafted TLS record can cause a denial of service via a crafted RSASSA-PSS signature.
CVE-2016-6307	DoS	medium	An attacker could force up to 21Mb to be allocated to serve a TLS record.
CVE-2016-6306	DoS	medium	Some missing message length checks can result in OOB reads.
CVE-2015-3194	DoS	high	The signature verification routines will crash with a NULL pointer dereference.
CVE-2015-1789	DoS	high	X509 cmp time does not properly check the length of the signature.
CVE-2015-1788	DoS	medium	When processing an ECParameters structure OpenSSL will crash with an invalid read.
CVE-2015-0286	DoS	medium	The function ASN1_TYPE_cmp will crash with an invalid read.
CVE-2015-0208	DoS	medium	The signature verification routines will crash with a NULL pointer dereference.
CVE-2015-0205	other	medium	An OpenSSL server will allow a malicious client to bypass authentication.
CVE-2014-3569	DoS	medium	The ssl method would be used to bypass authentication.
CVE-2014-3512	DoS	high	A malicious client or server can cause a denial of service via a crafted RSA signature.
CVE-2014-0160	info leak	high	A missing bounds check in the GMP plugin allows remote attackers to bypass authentication.
CVE-2011-4619	DoS	medium	The Server Gated Cryptography (SGC) extension allows remote attackers to bypass authentication.
CVE-2011-4577	DoS	medium	Allows remote attackers to bypass authentication.
CVE-2011-4109	other	high	Double free vulnerability in the GMP plugin allows remote attackers to bypass authentication.
CVE-2011-3210	DoS	medium	The IKE daemon does not properly check the return values of snprintf, which can cause a denial of service via an invalid signature.
CVE-2011-0014	DoS	medium	The ASN.1 parser allows remote attackers to cause a denial of service via an invalid IKE SA INIT request.
CVE-2018-6459	DoS	medium	Allows remote attackers to cause a denial of service via a crafted RSASSA-PSS signature.
CVE-2018-17540	BOF	high	The gmp plugin in strongSwan before 5.7.1 has a Buffer Overflow.
CVE-2018-16152	other	high	A remote attacker can forge signatures when small public exponents are being used.
CVE-2018-16151	other	high	A remote attacker can forge signatures when small public exponents are being used.
CVE-2017-9023	DoS	high	The ASN.1 parser improperly handles CHOICE types.
CVE-2017-9022	DoS	high	The gmp plugin does not properly validate RSA public keys.
CVE-2017-11185	DoS	high	NULL pointer dereference and daemon crash via a crafted RSA signature.
CVE-2015-8023	other	medium	Allows remote attackers to bypass authentication via an empty Success message.
CVE-2014-2338	other	medium	Allows remote attackers to bypass authentication.
CVE-2013-2944	other	medium	Allows remote attackers to authenticate as other users via an invalid signature.
CVE-2012-2388	other	high	The GMP Plugin allows remote attackers to bypass authentication.
CVE-2010-2628	RCE	high	The IKE daemon does not properly check the return values of snprintf, which can cause a denial of service via an invalid signature.
CVE-2006-2940	DoS	medium	The ASN.1 parser allows remote attackers to cause a denial of service via an invalid IKE SA INIT request.



2014년 HeartBleed 사태

보안뉴스

‘사이버 폭격’ 맞고 있는 펄스 시큐어 VPN, 중국과 러시아가 배후?

국가 지원을 받는 사이버 공격자들이 펄스 시큐어(Pulse Secure) VPN에서 발견된 취약점들을 활발히 악용

2021년 4월 발견된 PulseSecure VPN 취약점을 악용하는 해커 그룹

안 업체 파이어아이(FireEye) 및 CISA와 함께 사건에 대응하는 중”이라고 밝혔다.



2020-1년 VPN Hacking 사태

- ◆ 본 기술은 이러한 취약점/결함의 악용을 **사전에** 효과적으로 방어 가능
- ◆ 이를 통해, 보안 사고 발생에 따른 사회경제적 비용을 최소화 할 수 있음
- ◆ 안전한 네트워크 세상의 근간을 위협하는 중대한 문제 해결에 기여

- ◆ 향후 더 많은 분야에서 네트워크에 연결된 시스템의 수는 지속적으로 증가 예상
 - IoT(Internet-of-Things), 원격 근무, 원격 의료, 클라우드 기반 서비스, ...
- ◆ 또한, 암호화 통신의 비중도 증가 추세
 - Google은 자사 웹 브라우저인 Chrome에서 점차 비 암호화 통신을 차단하는 정책을 시행 중 ("구글, 크롬에서 HTTPS 아닌 다운로드 점진적으로 차단한다", [2020년 2월 10일 보안뉴스](#))
 - 화상회의 플랫폼인 Zoom 또한 암호화 통신을 적용 중 ("보안 문제로 시끄럽던 '줌', 마침내 종단간 암호화 적용한다", [2020년 10월 15일 보안뉴스](#))
- ◆ 다양한 현존 통신 프로토콜의 소프트웨어 구현에 잠재된 취약점/결함 까지 사전 방지
 - 본 기술의 프로토콜 다이얼렉트는 앞의 예시인 TLS/SSL뿐만 아니라 다양한 프로토콜(IKE 등의 암호화 통신 프로토콜, 평문 HTTP와 같은 비암호화 프로토콜 등)에 적용 가능
 - 이를 통해 본 기술은 TLS/SSL의 소프트웨어 구현(OpenSSL)뿐만 아니라 다양한 프로토콜 소프트웨어 구현에 적용하여 잠재적인 취약점/결함을 사전 방지할 수 있음
 - 다양한 분야의 네트워크 연결 지속 증가 추세와 더불어 본 기술의 확장성(다양한 프로토콜에 적용 가능)을 고려했을 때 활용도 및 발전 가능성이 증가할 것으로 예상됨

◆ 본 기술은 다양한 형태로 적용 가능함

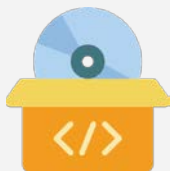
기업 / 시스템 / 통신 인프라



네트워크 장비
제조사



클라우드 서비스
프로바이더



응용소프트웨어
개발사



시스템소프트웨어
개발사

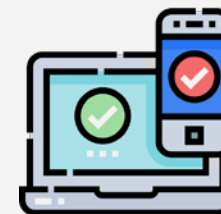
응용 분야



네트워크 기능
가상화



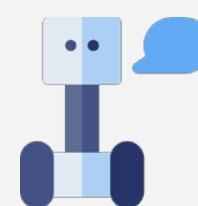
네트워크
접근 제어



디바이스
접근 제어



원격근무



원격현장참여



원격의료