보안성 강화를 위해 필요한
Bugbounty 제도의 개선 방향

안양대학교 정준영

1.1 버그바운티의 포상과 관련되어서 개선해야할 사항들

국내의 버그바운티 프로그램들을 보면, 네이버, 삼성전자와 같은 기업은 자체 운영 버그바운티 방식이며, 많은 기업들은 KISA에서 운영하는 신고포상제 프로그램을 통해서 버그바운티를 진행하고 있습니다.

FIND THE GAP → 추가로 국내의 버그바운티 플랫폼으로는 파인더갭, zerowhale, BugCamp, PatchDay가 있습니다.

구분	시행사	프로그램	대상	보상	시행시기
국내	NCSC	국가 사이버안전 위협정보 신고제	모든 S/W, 서비스	~1,000만원	'07
	KISA	S/W 신규 취약점 신고포상제	모든 S/W	5만원~1,000만원	'12.10
	삼성전자	스마트TV 보상 프로그램	스마트TV	$1,000+α/명예의 전당	'12
	네이버	네이버 보상 프로그램	네이버 서비스, S/W	$1,000+α	'19. 3분기
	리디북스	리디북스 보상 프로그램	모바일 앱, 서비스	200만원 이상	'19
국외	구글	구글 취약점 포상 프로그램	웹 서비스	$100~$20,000/명예의 전당	'10.11
		크롬 보상 프로그램	크롬 브라우저, 운영체제	$500~$15,000/명예의 전당	'10.1
		패치 보상 프로그램	오픈소스 S/W 일부	$500~$10,000	13.10
	페이스북	페이스북 버그바운티 프로그램	웹 서비스	$500~/명예의전당	'11.7
	마이크로소프트	보안기법 우회	윈도우 플랫폼	~$100,000/명예의 전당	'13.6
		블루햇 보너스 포 디펜스	윈도우 플랫폼	~$200,000	'13.6
		온라인 서비스 버그바운티	온라인 서비스	$500~$1,500/명예의 전당	'14.9
		스파르탄 프로젝트 버그바운티	최신 브라우저	~$15,000/명예의 전당	'15.4~6
		.NET Core, ASP.NET 버그바운티	웹 개발 툴	~$15,000	'15.10~'16.1
	ZDI	제로데이 이니셔티브	모든 S/W	자체 평가 포상금 / 마일리지 제도	'05.8
	라인	라인 버그바운티	라인 메신저	$500~$20,000/명예의 전당	'15.8~9

<국내와 해외의 버그바운티 보상 금액>

해외의 대표적인 버그바운티 플랫폼은 Hackerone이 있습니다.

WACON
정 준 영
안양대학교 대학생

1.2 포상에 대한 불만으로 일어날 수 있는 문제점

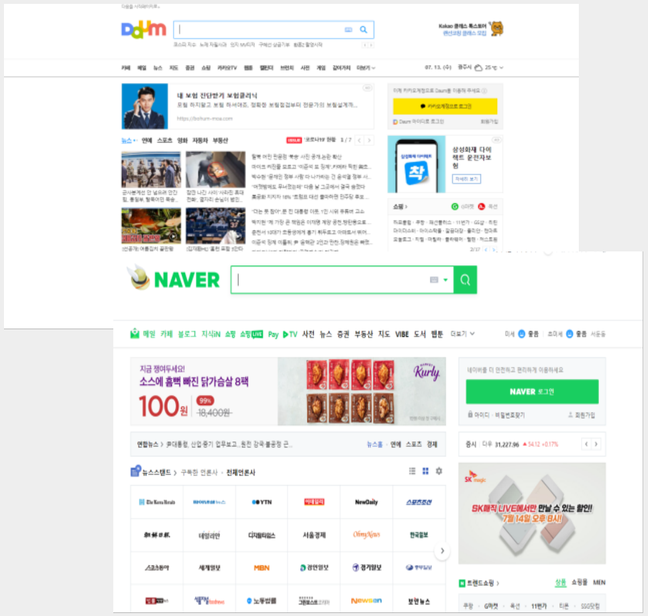
> 해외의 버그바운티 포상 금액에 비해서 국내의 포상 금액이 적다면, 버그 바운티 참여자들이 국내의 버그 바운티 프로그램이 아닌 해외의 다른 버그바운티 프로그램에 참여하게 될 문제점이 존재합니다.

> 국내의 버그바운티 참여자 수가 적어지게 된다면, 그에 따라서 버그바운티 제보 횟수도 줄어들기 때문에 다양한 보안 위협을 가지고 올 가능성이 존재합니다.

> 또한, 발견한 취약점을 제보가 아닌 블랙마켓과 같은 곳에 판매할 가능성이 상승할 확률이 높아질 수 있습니다.

- 따라서, 해외의 버그바운티 사례를 참고하거나 포상 체계를 확대하는 방안이 필수적으로 필요하다고 할 수 있습니다.

2.1 기업 내부에서만 사용하는 프로그램 및 운영 중인 서비스에 대한 취약점 점검의 문제



> 기업 내부에서만 사용하거나 웹 포털 사이트처럼 24시간 운영되는 서비스의 경우에는 취약점 점검이 어렵거나 자체적인 취약점 점검의 형태로 끝날 가능성도 존재합니다.

> 이를 공개적 버그바운티와 같은 방안으로 추진을 하기에는 정보통신망법과 같은 정보보호 법률, 또는 서비스 장애라는 심각한 문제를 불러올 수도 있는 상황 때문에 도입하는 것이 어렵다고 할 수 있습니다.

> 그러나, 이를 비공개적으로 진행한다면 더욱 개선할 가능성이 있다고 생각하였고, 비공개적으로 진행하는 버그바운티 방법이 실행 중에 있다는 것을 확인할 수 있었습니다.

*정보통신망 이용촉진 및 정보보호 등에 관한 법률 제 71조 제 10호 제 48조 3항 : 누구든지 정보통신망의 안정적 운영을 방해할 목적으로 대량의 신호 또는 데이터를 보내거나 부정한 명령을 처리하도록 하는 등의 방법으로 정보통신망에 장애가 발생하게 하여서는 아니 된다.

WACON
정준영
안양대학교 대학생

3.1 다양한 분야에서의 버그바운티 도입 필요성

보안 취약점이 발생할 수 있는 분야는 매우 다양합니다.

> 그 중 대표적인 예시로 자동차를 예로 들겠습니다.

> 과거 자동차는 단순한 하드웨어 즉, 기계로만 이루어진 존재라고 할 수 있었습니다. 이러한 기기가 시대의 흐름에 따라서 소프트웨어가 도입되고, 하드웨어의 성능이 증가하다보니 현대에 와서는 자율주행(FSD), 커넥티드 카, 스마트키 등 다양한 기술이 새로 등장하고 있습니다.

> 이렇게 자동차라는 기기 또한 시대에 맞춰서 발전하였고, 이제는 소프트웨어로 자동차를 조작할 수도 있는데, 이와 관련된 취약점을 해커가 악의적으로 이용할 경우 생명과 연관되는 아주 위험한 일이 발생할 수 있습니다.

과거

현재

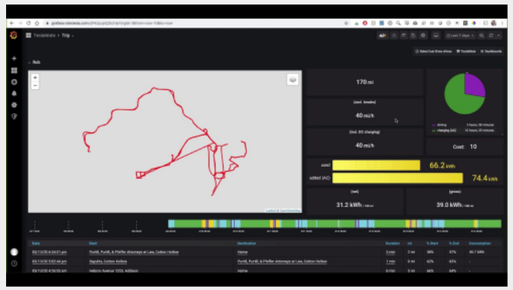
WACON
정준영
안양대학교 대학생

3.2 자동차에서 발견되었던 보안 취약점

테슬라 모델 3의 취약점 CVE-2020-10558

> CVE-2020-10558 취약점은 DRIVING INTERFACE 권한 상승 취약점으로 해당 취약점을 이용하면, 부적절한 프로세스 분리로 인해 서비스 거부가 발생하여 공격자가 속도계, 웹 브라우저, 실내 온도 조절 장치, 방향 지시등 시각 및 소리, 내비게이션, 자동 조종 장치를 비활성화할 수 있습니다.

TeslaMate관련 취약점 CVE-2022-23126



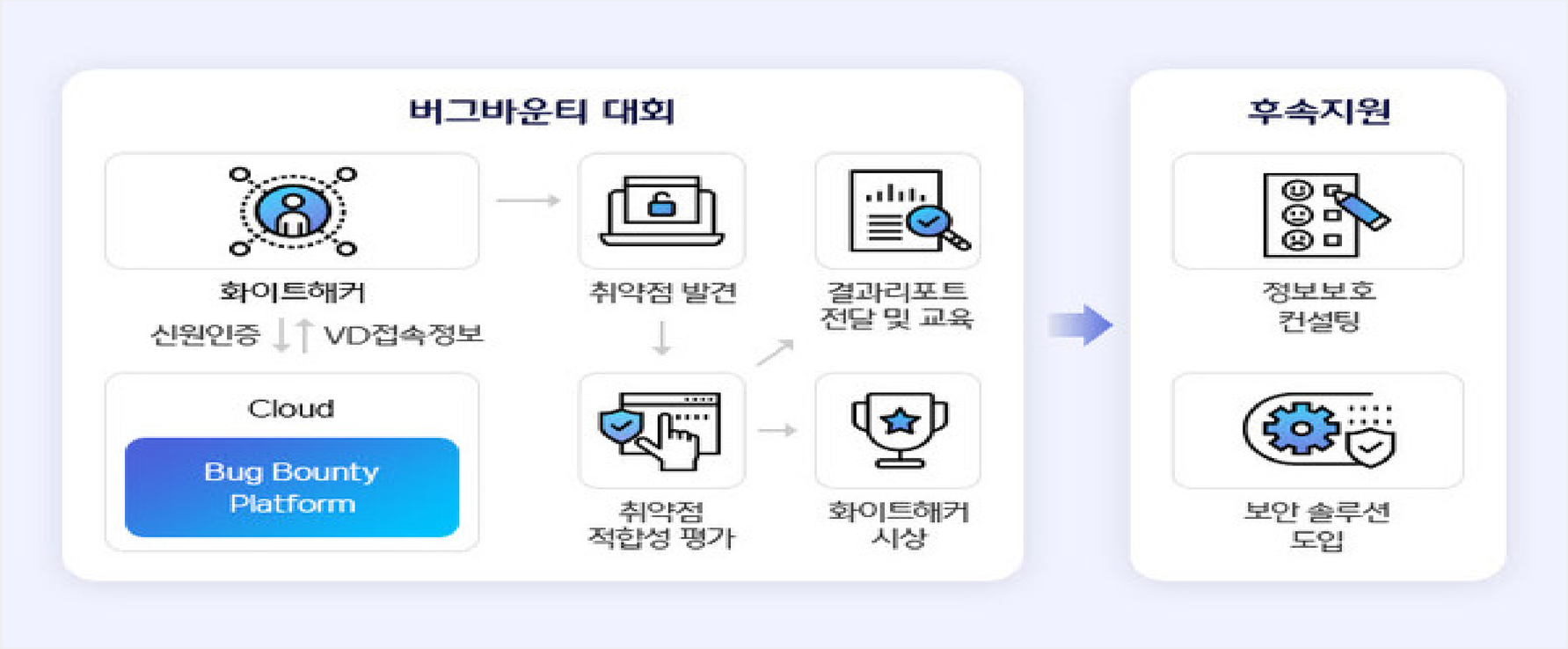
> TeslaMate는 테슬라의 데이터베이스 프로그램이라고 할 수 있으며, 충전, 운전 기록, 효율, 전비, 위치, 마일리지, 배터리 열화도, 팬텀드레인, 방문지, 펌웨어 업데이트 기록과 같은 테슬라를 운행하였던 모든 데이터를 제공하는 프로그램입니다.

해당 취약점을 이용하면, 공격자가 Tesla 차량의 문을 열고 Keyless Driving을 시작하고 도중에 차량 작동을 방해할 수 있습니다.

정 준 영 안양대학교 대학생

4.1 버그바운티 대회를 활용하는 방안

국내의 대표적인 버그바운티 대회 : KISA의 Hack the Challenge, 파인더갭의 화이트햇 투게더



4.2 버그 바운티 대회를 통해서 얻을 수 있는 효과

> 화이트 해커의 신원을 조금이라도 정확하게 확인할 수 있기 때문에 좀 더 안전한 버그 헌팅이 가능하다고 할 수 있습니다.

> 대기업과의 연결이 아닌 중소기업과의 연결을 통한 대회 주최로 인해서 중소기업의 보안 취약점을 점검할 수 있는 기회를 제공할 수 있습니다.

> 비공개 버그바운티 대회를 통해서 기업에서 운영하는 비공식적인 서비스에 대해서도 취약점 점검을 진행할 수 있다는 장점을 가져올 수 있습니다.

즉, 기존 버그바운티 제도를 조금이라도 더 개선하여 실행할 수 있다는 장점을 가지고 있다고 생각할 수 있습니다.

WACON
정 준 영
안양대학교 대학생

5.1 보안성 강화를 위해서 중소기업 및 개인 기업이 노력해야 하는 점

> 현재 중소 기업과 개인 기업의 보안성은 안 좋거나 보안에 대한 운영이 어렵다고 할 수 있습니다.

> 하나의 결과물이 좋더라도 나머지 기업의 결과가 나쁘다면 아직은 올바르지 않다고 생각할 수 있습니다.

> 이러한 보안성이 아직 강화되지 않은 중소기업 및 개인 기업의 보안성 향상을 위해서는 중소기업을 대상으로 하는 버그바운티 대회를 운영하거나, 중소 기업 및 개인 기업에게 보안성 강화를 위한 메뉴얼 가이드 같은 것을 제공하는 방식 또한 고민해봐야 하는 사항인 것 같습니다.

내용을 정리하자면, 보안은 하나의 기업만 우수하다고 되는 것이 아니라 모든 기업들이 공통적으로 관리 해야할 사항이므로 보안성 강화를 위한 방안과 노력이 필요하다고 할 수 있습니다.

이상으로 발표를 마치도록 하겠습니다.

들어주셔서 감사합니다.

WACON
정준영
안양대학교 대학생