

How South Korea Makes White-hat Hackers *# 2013 edition!*

beist (Korea University, GrayHash)

email: beist@grayhash.com

web: <http://grayhash.com>



About me



- ✦ SeungJin “Beist” Lee
- ✦ Ms-Phd course at Korea University (CIST IAS LAB)
- ✦ Member of advisory council for Cyber Command in Korea
- ✦ Principal Security Consultant at GrayHash
 - ✦ Consulting for big companies in Korea
- ✦ Many wins at hacking contests/Run hacking contests/conferences
- ✦ Talk at SYSCAN, CANSECWEST, TROOPERS, SECUINSIDE, etc
- ✦ Hunting bugs is my favorite hobby

Intro

- ✦ This is not a tech talk
 - ✦ Very easy talk, so, relax
- ✦ This talk doesn't say everything about the situation in Korea
 - ✦ But tried to put together as much as i can
- ✦ A bit of security scene history in Korea
- ✦ How we get inspired
- ✦ How we make white-hat hackers
- ✦ This is an extended version of AVTOKYO talk i gave at

When the scene gets activated

- ✦ People say the scene has been started since the end of 90'
- ✦ There were 2 big events at that time
 - ✦ Elite hackers at top universities (Postech and Kaist)
 - ✦ They were hacking each other and some went to jail
 - ✦ This was issued even on the media
 - ✦ Hackerslab (Wargame site)
 - ✦ Most underground hackers started from the site
 - ✦ First well-known infosec IRC in Korea

When the scene gets activated

- ✦ From 2000, there have been underground teams
 - ✦ Hackerschool
 - ✦ BEISTLAB
 - ✦ Wowhacker
 - ✦ Null@root
- ✦ No illegal stuff, they teach and train next generation
- ✦ Many of them are now high-ups and still working in this field
- ✦ They really do for the community

When the scene gets activated

- ✦ Industry around 2000
 - ✦ There were many security products
 - ✦ Mostly, IDS, Firewall and Secure OS
 - ✦ But penetration testing really made infosec guys
 - ✦ As it's "hack"
 - ✦ Pen-testing business was really messed up at that time
 - ✦ Companies stole others' contracts by hacking

Why the scene is motivated?

(What happened?)

- ✦ Motivations to
 - ✦ Government
 - ✦ Industry
 - ✦ The community

Why the scene is motivated?

(What happened?)

- ✦ Government
 - ✦ We have a very special situation
 - ✦ South Korea vs North Korea
 - ✦ The government started to find good hackers
 - ✦ They (secretly) supported the community
 - ✦ But most helpful move by them was pushing industry to spend money for information security

Why the scene is motivated?

(What happened?)

- ✦ Industry

- ✦ We have to say “money” can do a lot of things

- ✦ Some big (like financial) companies realized that cyber attack is real

- ✦ Auction, SK Communications, HyunDae Card and +++

- ✦ The strict law made them to spend money for security

- ✦ (Will cover about this later)

Why the scene is motivated?

(What happened?)

- ✦ Industry
 - ✦ So, they spent a ton of money and hired many infosec guys
 - ✦ Having regular penetration testing is kind of mandatory
 - ✦ Which means security firms are not going to starve
 - ✦ This says everything: we have over 200 security companies in this small country

Why the scene is motivated?

(What happened?)

- ✦ The community
 - ✦ Fortunately, we've got hacking competitions from 1999
 - ✦ Even though there was (still) a language barrier, Korean hackers were really passionate on CTF
 - ✦ Defcon CTF was a fire
 - ✦ Before 2006, Defcon CTF was a dream for Korean hackers
 - ✦ Anyway, they were excited, and made it to finals

Why the scene is motivated?

(What happened?)

- ✦ The community
 - ✦ And the community was inspired by researches from world class hackers
 - ✦ RTL by Solar designer, IIS 0days by Chinese hackers and a lot of cool stuff
 - ✦ They tried to make something themselves

What they are doing

- ✦ We can categorize as
 - ✦ Community
 - ✦ Industry
 - ✦ Academy
 - ✦ Government

Community

- ✦ We have over 10 hacking contests/conferences per year
 - ✦ Majors: Secuinside, Codegate, ISEC, KISA
- ✦ Most of them are involved with the community
 - ✦ Companies pay for run and the community helps

Community



- ✦ <http://hackerschool.org>
 - ✦ This site really does a lot of cool things for the community
 - ✦ Cartoon based lecture
 - ✦ For example) <http://bit.ly/SP0enX>
 - ✦ Hacking camp for elementary students
 - ✦ Hacking contest for women
 - ✦ Article) <http://t.co/uZMWf2rV>

Community



- ✦ KOSEC
 - ✦ Cool local meet-up (like NYSEC in NYC)
 - ✦ Hang out and chill
 - ✦ Sometimes talks included
 - ✦ Every 1 or 2 month
 - ✦ 40~50 people to come (100 was maximum)
 - ✦ Charlie Miller was here!

Community

- ✦ Try hard to do for next generation
 - ✦ The underground teams find young guys
 - ✦ And they train them about security
 - ✦ Also, they emphasize ethics
 - ✦ They think they have to give back to the community
 - ✦ Example) beistlab got \$10,000 and spent back for making a hacking contest (JFF)

Industry

- ✦ As we mentioned, we have over 200 security firms
- ✦ They support conferences and hackers' activity
 - ✦ Example) LAW&TEK supports HARU for hackerspace
- ✦ One good thing is that young guys can work for security companies instead of going to army

Industry

- They try to make something good for the community with hackers
- Example) SECUSIDE by KOSCOM and HARU
 - <http://secuinside.com>
 - KOSCOM is a financial company
 - They spend big money for running the conference/CTF
 - And the community, called HARU, actually runs
 - Win Win (Popularity for KOSCOM and Fun for HARU)

Industry

- ✦ POC Conference (<http://www.powerofcommunity.net/>)
 - ✦ HNS company
 - ✦ It was started by hackers
 - ✦ It seems it wants to be like a Korea Defcon
- ✦ CODEGATE Conference
 - ✦ Softforum company
 - ✦ It is fancy and a big conference
 - ✦ High up guys at the government involved

Academy

- ✦ As information security is getting more and more important, universities start to have infosec related majors
 - ✦ Korea university
 - ✦ Seoul women university
 - ✦ Sejong university
 - ✦ Soonchunhyang university
 - ✦ And more than 10 schools

Academy

- ✦ Korea university is a somewhat special case
 - ✦ They have MOU with Cyber command (Sound scary?)
 - ✦ Only top 1% SAT guys go there
 - ✦ All students of cyber warfare major at Korea university get full scholarship
 - ✦ And they go to Army after graduating (For 5 years)
 - ✦ Which means they'll be specialized at the field
 - ✦ Their curriculum and students are secret

Academy

- Like in Taiwan, if students want to get into good school, they have to get good SAT score
- But from around middle of 2000', we have seen that they can get in if they're really good at Hacking
 - Schools give students advantages if they have awards from hacking contests
- This is a big fire to encourage students (even their parents!) to learn about computer security

Academy

- ✦ At school, over 30 information security clubs in Korea
- ✦ They are extremely activated
- ✦ Making articles and joining/running infosec events
- ✦ Some clubs are famous at the world class CTFs
 - ✦ GoN (KAIST), PLUS (Postech)

Government

- ✦ All governments are eager to hire people
 - ✦ Lack of skilled hackers
- ✦ Usually, it is not easy to get into governments
 - ✦ Like NIS, Cyber command for examples
 - ✦ Good GPA, Good schools required
- ✦ But they are making exceptions for skilled hackers

Government

- ✦ KISA (Korea Internet & Security Agency)
 - ✦ <http://kisa.or.kr>
 - ✦ They do CERT (incident response or something like that)
 - ✦ They encourage and support university school students
 - ✦ They made KUCIS (Korea University Clubs of Information Security) and support university clubs
 - ✦ Awards and money

Government

- ✦ KISA (Korea Internet & Security Agency)
 - ✦ KISA also gives motivations to hackers
 - ✦ They run a bug bounty (since september 2012)
 - ✦ I'm one of judges
 - ✦ Every quarter
 - ✦ Over 100 submits to this program
 - ✦ Even middle/high school students submit bugs

Government

↙ Vulnerability report program

취약점 신고

☰ 상담 및 신고 > 취약점 신고



대검찰청, 경찰청, 인터넷진흥원, 금융기관 등을 사칭하는
보이스피싱, 피싱사이트, 피싱 문자로 인한 금전적 피해가 발생하고 있습니다.
사이트 접속시 바로 **개인정보를 입력하지 말고 사이트 주소를 확인하시고 주의해 주십시오!**

S/W 신규 보안 취약점 신고 포상제

2012년 10월 부터 소프트웨어 신규 보안 취약점 신고 포상제를 실시합니다.

포상금 지급을 위한 평가는 분기별로 실시하며, 분기별 우수 취약점을 선정하여 평가 결과에 따라 최고 500만원의 포상금이 지급됩니다. 신고 포상을 원하는 경우 아래의 신고 양식을 다운로드 받아 작성하여, 관련파일에 첨부하여 주시기 바랍니다.

[신고양식 한글\(hwp\)](#)

[신고양식 워드\(doc\)](#)

[포상제 안내문 보기](#)

[포상제 FAQ 보기](#)

http://www.krcert.or.kr/kor/consult/consult_04.jsp

Government

- ✦ KISA (Korea Internet & Security Agency)
 - ✦ The maximum prize is about \$5,000 per person
 - ✦ Obviously not enough, but at least a good move
 - ✦ And focused on korean software which no one would buy that means reasonable
 - ✦ When they get reports from hackers and let vendors know

Government

- ✦ KISA (Korea Internet & Security Agency)
 - ✦ When hackers report to this program
 - ✦ The credit goes to to them
 - ✦ They can use their bugs as reference
 - ✦ Only korean citizen can participate
 - ✦ But if you team up with korean, yes you can
- ✦ Examination standard
 - ✦ Impact, difficulty, report quality

Government

- ✦ Cyber command
 - ✦ We have Cyber command like in US
 - ✦ They're responsible
 - ✦ Plan cyber wars
 - ✦ Attack and defense in the cyber field
 - ✦ Develop cyber security technique
 - ✦ Bring up cyber warriors
 - ✦ etc

Government

- ✦ Cyber command
 - ✦ In korea, we go to army for 2 years
 - ✦ Spending 2 years at army is not easy for young guys
 - ✦ Cyber command makes a way for them that they can be focused on information security or do cyber security
 - ✦ That is huge welcome for people who do not want to be “real soldiers”

Government

- ✦ Cyber command
 - ✦ Also, they show the community a good move
 - ✦ They try to make good relationship with hackers
 - ✦ Like Jeff Moss named to advisory council for DHS
 - ✦ They get hackers to their advisory council
 - ✦ Thanks! I'm one of them.

Government

- ✦ NCSC (National Cyber Security Center)
 - ✦ It's like Korea NSA (<http://ncsc.go.kr>)
 - ✦ They run a bug bounty as well
 - ✦ But the prize is small
 - ✦ I've not seen anyone got over \$2,000 from the program
- ✦ However, still interesting as the government is doing that
 - ✦ Probably it's a first case around the world

Government



- ✦ BoB (Best of the best)
 - ✦ <http://www.kitribob.kr/>
 - ✦ By ministry of Knowledge Economy and KITRI
 - ✦ Training program for young guys to be security professional
 - ✦ Very well organized program
 - ✦ I'm one of mentors in BoB

Government

- ✦ BoB (Best of the best)
 - ✦ BoB started from since 2012
 - ✦ Last year, we made huge success
 - ✦ Around 300 students applied to be 60
 - ✦ Students made good result
 - ✦ Got media attention
 - ✦ Even CNN

South Korea's 'Best of the Best' tackle cyber crime

By KJ Kwon, CNN

January 14, 2013 -- Updated 0709 GMT (1509 HKT)

Government

- ✦ BoB (Best of the best)
 - ✦ As the success, the government decided to support more for this program
 - ✦ More \$\$\$ and +++
 - ✦ More bigger in 2013
 - ✦ About 500 students applied to be 120

Government

- ✦ BoB (Best of the best)
 - ✦ 8 month course
 - ✦ Survival program
 - ✦ At the beginning: 60 students -> **120**
 - ✦ After 6 month: 30 students
 - ✦ Only 10 students selected at the end

Government

- ✦ BoB (Best of the best)
 - ✦ First 6 months
 - ✦ Learning about information security from professionals
 - ✦ Crypto, network, OS, hacking, ethics and ++
 - ✦ Projects with mentors
 - ✦ And 2 months
 - ✦ Advanced researches with mentors
- ✦ World popular hackers come to korea to teach students
 - ✦ In 2012, Stefan Esser

Government

- BoB (Best of the best)
 - Students get paid monthly (For only learning!)
 - And free laptops
 - The 10 students will get around \$17,000 each
 - Also supported overseas study

Collaboration



- ✦ Junior CTF
 - ✦ It's a hacking competition dedicated only for middle and high school students
 - ✦ It's a joint event by the government (ETRI), industry (Softforum), and the community (GrayHash)
 - ✦ I and Mongii make challenges and run this competition

Collaboration

- Junior CTF
 - This is a nice chance for young students
 - As if they won, the prize can be good reference when they get into colleges
 - We're planning to make this one more bigger and bigger

Things to mention



- Cyber Law
 - The cyber law in Korea is extremely strict
 - If companies got hacked and it turned out that it was companies' fault, they have to pay customers for damage
 - Sounds a bit weird but true (victims pay?)
 - Especially, personal information privacy law is strict too

Things to mention

- Cyber law
 - Cyber law is cruel for companies
 - But we have to admit that because of the law, the information security field is growing very quickly
 - As they have to spend money

Things to mention

- ✦ Black-market
 - ✦ Of course, we have script kiddies
 - ✦ But, we don't have any black-market or serious cyber criminal crew
 - ✦ Don't know why, but, I think the strict law is one of reasons
 - ✦ Even reversing was illegal a few years ago

Dark side

- ✦ Even though, information security field is very activated, this industry doesn't give dream to everyone
- ✦ There are roughly 5 positions for engineers
 - ✦ Monitoring
 - ✦ Penetration testing
 - ✦ Reversing or analyzing malware
 - ✦ Hunting bugs
 - ✦ Consulting

Dark side

- ✦ Only skilled reverser and bug hunters get paid good
- ✦ Other positions, they work unbelievably hard
 - ✦ 9 to 10 or longer
 - ✦ But, payment is no good
- ✦ High-up guys still don't understand security
- ✦ It's hard to persuade them to know it

Dark side

- Some people say it's because there are too many infosec guys
- Also, monitoring job is easy and penetration testing (depends on) is not hard
- So, people just dive into the positions

Where hackers want to work?

- I gave questions to over my 50 infosec friends
 - Working outside of korea (but language barrier)
 - Financial companies
 - Governments (like NIS or Cyber command)
 - Big companies (like SamSung)
 - Known security firms (like Ahnlab)
 - Small security firms



Off topic

- ✦ I did a quick survey
 - ✦ I gave some questions to young hackers in Korea
 - ✦ What is your main interests in information security?
 - ✦ If you like offensive research, what do you dig into?
 - ✦ Is it easy to find people or community to get help?
 - ✦ What do you want support from the government?

Off topic

- ✦ What is your main interests in information security?
 - ✦ Most people say
 - ✦ Finding vulnerabilities
 - ✦ Hardware hacking
 - ✦ Exploiting technique
 - ✦ Reverse engineering

Off topic

- If you like offensive research, what do you dig into?
 - Most people say
 - Hunting bugs in popular software
 - Web browsers, telecommunication protocols, web servers, ftp servers, etc

Off topic

- ✦ Is it easy to find people or community to get help?
 - ✦ Most people say 'yes'
 - ✦ Even though there is a language barrier, there is a ton of translated documentations
 - ✦ Local hackers also make good materials
 - ✦ Remember, hackerschool.org even has manga-lectures
 - ✦ And local meet-up like KOSEC is good to get help

Off topic

- What do you want support from the government?
 - They say the government support is getting better
 - But they wish there was a program like CFT (Cyber Fast Track by DARPA)
 - They want to get supported from their own research

Conclusion

- ✦ Korea is probably most activated infosec country in East Asia
- ✦ But the language barrier is a huge problem
 - ✦ How many korean hackers do you know?
- ✦ We need more skilled people and do some real world researches (Not just CTFs!)
- ✦ However, It's going to be much better as the community, industry, academy and government are helping and collaborating each other
- ✦ Contact me if you have questions!

Thanks!

- ✦ Big thanks to HITCON Crew
 - ✦ Dan dai and taiwanese l33ts
- ✦ Greetz to
 - ✦ HARU, hackerschool, korea university
- ✦ Give me questions
 - ✦ beist@grayhash.com