FINISHED FILE

ASIA PACIFIC INTERNET GOVERNANCE FORUM
MACAO 2015
EVOLUTION OF INTERNET GOVERNANCE:
EMPOWERING SUSTAINABLE DEVELOPMENT
01 JULY 2015
16:00
INFORMATION SECURITY AND PRIVACY IN THE IOT ERA
SESSION 46

Services provided by:
Caption First, Inc.
P.O. Box 3066
Monument, CO 80132
1-877-825-5234
+001-719-481-9835
Www.captionfirst.com

***

***

Live captioning at APrIGF Macao 2015 is brought to you by Internet Society

>> KI SHIK PARK: I'm waiting for one speaker.

Okay. He is coming in. So good after noon ladies and gentlemen. My name is Ki Shik Park and I'm very pleased to be here to moderate this important session this afternoon. "Information security and privacy in the IoT era."

I'm currently working for ETRI in Korea. Some of you may know ETRI stands for Electronics and Telecommunications Research Institute in Korea. It's one of the biggest institutes in the Governmental area in ICT, in Korea, and it led to today's Korea ICT development fundamentally.

I've been very much involved in the issue of Internet Governance directly and indirectly. Mostly, in relation to my standardization related activities, such as long time ITU Chairmanship and also some advisory work and some board memberships for IEEE or W3C and also some chairmanship for some global cooperation conferences.

I believe the topic of this session, information security and privacy in the IoT era, includes many, many important issues for the future Internet Society. Especially, the Internet today

is an indispensable tool for our daily lives. So I believe it's very important for us to make the Internet more human centric or human oriented matters, tours. Considering various issues, including security and privacy relating matters.

However, I don't think IoT is really a new concept. However, I believe it is a very useful concept for us to remind that we are now entering into a new Internet age. A new revolutionary Internet age, I believe. So in this context this afternoon, we are going to talk and discuss about how to minimize the negative effect of the Internet as well as how to maximize its benefit for human beings.

For this session, we will have four speakers, mainly, and ten to fifteen minutes' time will be given to each speaker. So taking this opportunity, let me ask kindly our speakers to keep their presentation time sharply. I don't like to lose some chances for the floor to ask questions and also we will provide answers for our presentations.

So having said that, now let me invite our first speaker, Mr. Adli Wahid from APNIC. Mr. Adli Wahid is the security specialist of APNIC, and please welcome him to the podium with a big hand.

(Applause)

>> ADLI WAHID: Thank you. Good afternoon, everyone. My name is Adli Wahid, from APNIC.

First off, I'd like to thank Ki Shik for inviting me to be part of this panel on the Internet of Things, specifically on the security challenges on the Internet of Things.

Now before I begin, and I know that we have other speakers -- So before I begin, and I know that we have other speakers on the list, my background is -- so at APNIC I do a lot of security outreach activity, working with different types of outreach organisations, some of that is in the area of promoting security best practices, improving security. I also work a lot with CSIRTS and CERTS in the regions as well as law enforcement agencies when it comes to doing some Internet online investigation. Because of this, my approach to this topic today will look at how we will deal with IoTs, given the fact that, you know, we have a lot of security problems today. And looking to some of the challenges on how we handle security these day, particularly with regards to cybercrime, cyberattacks, and try to relate it to the IoTs and try to get all of us to think how we will deal with some of these issues.

As you are aware, we have four people on the panel, so people will talk about different issues. And my talking points for today is to highlight some of the security concerns from the cybersecurity community, people who are doing security response on the IoT. If you listened to the opening remarks by Dr. Park, a lot of things that we look the are not new. The IoT is not a

new concept, but it is providing some new challenges for how we manage and deal with security in the long run.

So in my talk today, I will cover three things. One is to just give some perspective on the IoTs. Looking into also the security risk, whether they are -- there are new things that we have to be worried about and if they are, what are those things. And last but not least, the security considerations. Perhaps I can share with you some of the thoughts that are happening within the community with regards to how we should tackle the issue of security when the Internet of Things comes into our space or our domain.

Now, as the first speaker, I have the opportunity to also define a few things. So if you look at many of the literature out there, when people talk about the Internet of Things, they are talking about things that can communicate, connect and compute. That sounds really familiar with what we have on a day-to-day basis. But the main thing about the Internet of Things are the things that people tend to highlight when talking about the Internet of Things, we are talking more than just computers. We are not just talking about mobile devices anymore. They are things that we use, we wear, sensors that we put in place, and they can communicate. They connect to the Internet, which means they have Internet visibility and they can compute and therefore produce a lot of data. And this data can later on be processed in one way or the other, for the benefit of humankind.

In the last six months alone I've been attending many conferences that talks about the IoTs, and every time the Internet of Things or the IoTs are discussed from different angles. So there is a lot of discussion about the Internet of Things which means that people are really excited about this whole new possibilities of communicating, processing data, and improving quality of life when we make all of these things available.

In the morning we heard the IoT being discussed from the perspective of IPv6. There is a lot of discussion on innovation, on how people are producing new things for people, and how this will improve, you know, quality of human life. There is a lot of discussion on big data. On -- that we are producing so much data and this will allow us to automate a lot of things in our lives. There is also a lot of discussion on security, and this is basically what we will be talking about today. A lot of things on privacy. With all of the data that we are produce, how are we protecting this information from being abused by whoever is taking care of this information. And lots of things about entrepreneurship and so on and so forth. So IoT is a big thing and it's something that we hear from time to time these days.

The other things about the IoTs is about the numbers, about how big this will be. If you read different reports, different publication, people say by a certain date there will be 20 billion IoTs. Some people say 50 billion. Others say 100 billion. So this means something. This means that we are looking at something really, really big. And from the security perspective, this also means that, you know, there are a lot more things to take care of. Right? And the main question will be, and I'll highlight this again towards the end, is how are we going to manage the security of these devices if it's going to be really, really large? And we should be able to basically think about it and look into how security is being implemented or managed. And if something goes wrong, how are we going to handle them?

The thing about the big number is also about the expiring. So there is a lot of discussion about the Internet of Things, it's something that people buy and use and they will be there for a long, long time, which means that they will always be connected to the Internet. And as a result, they may contain vulnerabilities that can last a long time. And this is a big issue when it comes to security, as I will highlight later on.

So what is the expiring date for the IoTs? So maybe the things, if you are wearing something that connects to the Internet, you may replace them once in a while. But what about things that people have produced that probably have very, very long shelf life? Maybe things that you install and forget. Things that you buy and you run and that's it. It's running.

So there are a lot of these things that exist today and it becomes a security problem if, number one, they are continually exposed to the Internet and people don't really think about them anymore.

When it comes to security risk, the traditional way of looking at security is to discuss security from the perspective of first of all exposure. So once you have something exposed on the Internet, then you have a lot of risk that comes to it. So typically people talk about the CIA, not the agency, but confidentiality of information, integrity of data, and the availability of services on the devices that we use on a day-to-day basis.

Lately privacy has come into the discussion. Because we have a lot of stuff that we share with card providers, for instance, and third parties, and how this information is being protected from being abused and so on.

Now when it comes to security risk, also, discussions about CIAs -- confidentiality, integrity and availability -- tend to be theoretical at times. Most importantly, when we look at security risk, what is the impact of a security breech, for instance? Is it loss of income? So, for example, if today we

have a website that is being attacked by someone in terms of DDOS or defacement, we talk about loss of potential income. You cannot make money. And this is closely related to a lot of activities in the cybercrime world, where the bad guys or the actors are finding ways to monetize vulnerabilities or weaknesses on the Internet to make money. They sell data, provide infrastructure for other actors to spam, to send spam on the Internet, or to infect more machines and so on and so forth. But when it comes to the Internet of Things, perhaps we are also looking at the possibility of critical systems or critical devices being connected to the Internet. And once they are breeched, could potentially cause the loss of life. So do we have IoTs that could affect lives of people if they are being exposed or breeched? Or if there is a sabotage, that sort of thing.

Of course today we look at many systems that are connected to the Internet, like scaler systems or initial control systems or others that could have this affect if they are being compromised or attacked. But with more and more devices connected to the Internet or exposed to security risk, could this be one of the results or one of the potential risks of the Internet of Things?

If you look at a lot of the security breeches today, they tend to evolve around these few things. And if you look at it, they are really, really business basic stuff. Many reports being produced by many of the security vendors, even many security teams. If you cake earlier, the Macao CERT talks about some of the security breeches that happen here. You realize a lot of the things are related to the four things I mentioned here. A lot of it are related to the basic way in how we protect systems. Passwords. Authentication is broken. And if you look at the IoTs, you are wondering whether or not they have really proper authentication and how is authentication being done. If it's just password, just like what we have today, then it's probably not a good way to move forward.

A lot of the attacks happen because of social engineering, which means that people are tricked into doing something that an attacker wants the people to do or the victim to do.

So this this is also one thing that we have to look at. If we have a lot of devices on the Internet, how easy is it for the attackers to run mass social engineering attacks? And this is related to security awareness. So in the current PC or mobile device world, many of the security awareness programs that we see out there tend to evolve around don't click on this link, don't click on that link. This is how you secure your devices, you have to install antivirus software, you have to do this or that. But many of that if you look today are related to computers, related to devices that people have. Will the IoTs,

as soon as we have them, and we have them in a mass way, will it change how we do security awareness for the users of people who are using these devices?

So how do we teach them about security? Will security be improved or be hard? Will the devices or IoTs be secured by default? So that's one of the things we should think about and look at.

And of course you cannot run away from the issues of vulnerabilities. Because we use software and hardware that continually have vulnerabilities. Either people discover them or people manage to figure out ways to bypass security features of the software or hardware that is being used.

And this brings up the issue of patch management and vulnerability management. A lot of the compromises or the attacks that we see today are as a result of people not fixing things on time. So they remain open for a long time, and as a result bad guys gain access to these devices.

And a lot of the security breeches, if you look at it from the point of View Of an enterprise, where they have capabilities, like people in the organisation doing patch management, you know, doing security updates on the devices, even so, you know, we have a lot of vulnerabilities in place where bad guys still manage to get in. So imagine with the Internet of Things if the owners of these things, let's say if they are home users, will they have the capabilities and capacity to perform the patches if we assume that patch management will be done using the same way, for instance.

Now I'll bring you to another perspective. People who deal with security problems on a day-to-day basis. A lot of the vulnerabilities that we look at today, there are things that you probably read on a day-to-day basis about attacks and vulnerabilities. There is a group of people that normally work to manage these vulnerabilities from being further exploited by the bad guys. Those are the CSIRTS or forensics teams. So they basically read about some major vulnerabilities, they take this information, they coordinate it and share it with other users in their localities or in their country, for instance. And they focus more on, you know, sending the information so that people know what to do in terms of how to fix it, how to apply the firewall rules, how to clean the infected computers and so on. So this is a typical way of doing this.

We are basically still struggling. So I just want to give you one example with the very critical vulnerability last year called heartbleed. So this particular vulnerability affected the open SSL software, which was being used by more than 600,000 computers. And after two months, right, despite the media hype, the massive coordination that people were doing to spread the word so that people fixed this vulnerability, only half of that

were patched. And so you're looking at 600,000 systems, two months later, 300,000 are still open to attack or vulnerable to this risk or particular attack.

If you remember about how many billion computers, IoTs that we will have out there, if these systems are exposed to the Internet and they have a major vulnerability and people are not fixing them on time, then there are more attacks for the bad guys to exploit.

How do you manage this? Many of the vulnerable machines affected by heartbleed are in organisations and enterprises, where normally there is a way for me to reach out to them, saying hey, there is a critical vulnerability, please patch your systems. Despite that, people are not fixing things on time or timely.

I'll give you another example with customer premise equipments. So this is the things that we normally have at home, the WiFis at home, and they are vulnerable on various accounts. One, because of default passwords. So these are being shipped with default passwords and people of course normally don't change them. So as a result there are a lot of tools that scan for the things and do brute force and gain access to them. And, also, a lot of devices are turned on by default on them. Such as the DNS, for instance.

And this has been abused by attackers and they tend to use these devices to launch massive reflective service attacks. So I'm not -- I don't want to talk about the DNS DDOS attacks, but to talk about the assumptions that people have when they sell things to the end users or to the customers that people will apply security best practices on the devices. So the expectation of users will change the password, that just doesn't happen. And also disabling the device, it could be very difficult for these people.

To show you very quickly how many open DNS resolvers as a result of the open CPEs, in our region alone there is more than 2 million computers ready to be used for DDOS attacks.

And so those are typical systems that we have. Think about in the future when we have things like this. How do we get people to fix it if they have such vulnerability? How do I give the instruction and how do I ensure that users are actually applying the patches on time so they are not being exploited?

The last slide, I know Doctor Park is becoming uneasy. So the question is, when it comes to the IoT, things that we have to think about, will security be the same? Will the assumptions be the same? And therefore, you know, there are four things that we have to think about:

How do we limit the exposure of the IoTs? And this is probably, you know, how do we look at default security? What is the mindset of people who are, you know, developing these IoTs,

when they roll out the device, how are they going to make sure that security can be easily managed? That we maybe harden the systems by default. And what are the roles and responsibilities of various parties when it comes to managing security vulnerabilities.

And also I'm talk about the roles and responsibilities of people doing research and how we could simplify security, and also at the same time make sure that we don't encounter the same problems that we have today with the nonIoT things.

So with that I'd like to end this presentation, and I think we can take up some questions in the end.

Thank you very much.

(Applause)

>> KI SHIK PARK: Thank you. Please, stay there. We will have some discussion sessions after all four presentations.

But, however, if you have any questions for clarification on his presentation, please... okay.

Your presentation was perfect. Thank you.

>> ADLI WAHID: Thanks.

>> KI SHIK PARK: The next speaker will be Dr. Peng Hwa Ang from Nanyang University, Singapore. And he is going to speak on privacy and the Internet of Things. Mainly he will speak on some current IoT, privacy issues, and also the way how we should respond and prepare the IoT services in the future.

So... Professor, are you ready?

>> PENG HWA ANG: I'll move straight to the presentation on privacy.

Quickly to talk about what the IoT is about. Adli talked something about communication and connection. This is one other view about what IoT is. To have sensors connected to machines or people.

I did a Google as to understand what IoT is, and I think there is some misunderstanding. This one looks at IoT -- it looks like Internet in things. And it's not. It's Internet of Things. So it looks like the image is Internet in the car. So you're able to access the Internet, you know, I guess WiFi in the car. And this is not what the Internet of Things is. It's not Internet while on the move.

So IoT means that you have sensors that are embedded into devices. Some are immovable. I think on the left you have your smoke sensor. Then the baby monitors, using WiFi. Bottom left, you have this fitness tracker which I also have. And the nice thing about this, this fitness tracker, is it's connected to my phone. So it's (inaudible.) When I reach on my phone, this tracker will unlock my phone. Most of the time your phone, you have to unlock physically. This one, when I bring it to the phone, the phone unlocks. Nice. I'm very happy with it. And it's only Singapore 19 dollars or US 17, 16 or 15 dollars

elsewhere. Great bargain.

So why is IoT now happening? And one factor is of coures how the prices have dropped. My device, I mentioned, here is $15. It's becoming a commodity. And you can see the price drop. Of course, if you cross the border to just China, you can see there is manufacturing going on with these devices.

I brought up also this issue of looking at fitness trackers, and to give you a sense of kind of the spread, the plethora of IoT and why it's possible to have this whole range of estimates from 20 million to 20 billion to 100 billion. So some are harder to move. Like weight machines. I have a weight machine that measures my fat. I have some fat in me, yes. Fat, muscle, potential muscle, and so forth. But, unfortunately, it's not using IoT. If you have IoT what it means is that your measurements will be connected to your device and you can connect and monitor it on your phone. So you see progress and exercise, how much fat you gained, how much muscle you gained over time.

Blood pressure sensors, and I mention that you can e-mail information to your physician. So think about it, you wake up, lo and behold, the information goes to your physician. You don't have to do anything about it. It's automatically done for you. IoT. So that is sort of nonremovable, nonremovable.

So wearable sensors, I show you my arm, it's sensors, contact, patch, you monitor, for example, the heartbeat.

The ingestible sensors. You can swallow that. You have some of these current procedures where they look at you using cameras, and you must be sedated. So your colonoscopy you have to be sedated. Otherwise you can just swallow a pill and the camera pictures are taken of your innards and then the physician can see what you have inside of you.

Of course implantable.

So you see a whole plethora of ways of using this IoT. Very imaginative. Potentially very useful. Money saving, as well as convenient. Think of your ingestible sensors where you swallow this pill, instead of having to go to the hospital to get sedated and having this monitoring done.

But, of course, the issues we are talking about here instead are privacy. And I want to, in this point, I want to draw a very important distinction between privacy and personal data and secrets. I'm working in this area of personal data protection, because in Singapore we just passed a law and the law says that if you have good policies, good personal data policies, you are immune.

So the first thing to note is that privacy is the umbrella term and you have different kinds of privacy. You have your space privacy. You don't want too much people around you, covering you. You have your communication privacy. You want

your information to be secret. You have your territory privacy. Your home is private to you. So different kinds of privacy and it's really an umbrella term.

But your personal data is part of the privacy. And by personal data what is meant is personally identifiable information. This is a standard term used in personal data protection globally. Meaning from the EU to Asia. The EU has tough personal protection data laws in force for sometime now, since '96, almost 20 years. In Asia it's just been happening. The rules were just implemented in Asia in the last year. Singapore laws are just one year old. Malaysia also about one year old. Philippines passed a law. Indonesia passed a law. Hong Kong passed a law. Korea also has. All these laws protect personal data, meaning your personally identifiable information. Information that identifies you.

So personal data can include your name and passport number. But it can also include, for example, your address. Although at your address you may have a few people living in there, but when they combine this information, they can identify you. Your mobile number doesn't identify you, because you can pass the phone to somebody else. But when you combine your mobile phone number with other detail, they can identify you. So all of this comes under the rubric of personal data. So the key to know is personally identifiable data.

But there is a third category of secrets. Things that you don't want people to know. What I call skeletons in your cupboard. Relative secrets. Things that we don't want people to know.

It could be that you -- I didn't do so well in Chinese. Although I'm Chinese, I didn't do so well in the study of Chinese. I had an F. And when I went to claim the results, I was surprised. What happened? The subject disappeared from the table. The subjects I took disappeared. And the reason is that if it disappears from the transcript, it doesn't appear. So now it looks like I passed all the subjects, but the subject that I failed very badly disappeared. So now I don't want people to know. But it could come back. But you don't want people to know. It's a secret.

So let me tell you what happened. It's kind of interesting. There were two focus groups I was involved with. One of high school students, this is in Singapore, and one of retirees. And we were discussing the issue of privacy using the smartphones. And both groups said they are concerned about privacy. But the young people are concerned about privacy of their content details. They didn't want people to harass them. The mobile numbers, the e-mail addresses. The older group were okay. But the younger group didn't worry about posting information about where they have been, what they ate. The older group was

opposite. They didn't mind people knowing their phone numbers, e-mail information, because they knew how to handle harassment. But the older group didn't want people to know their secrets. So the older group were surprised that the younger people posting all this information online, what they ate, where they had been, and so forth. The older group didn't want that.

So this is where you have your so-called secrets. Secrets are not personal data. Meaning that by themselves, the secrets are not your personal data. The phone number can be your personal data, but I feel it's objective. The phone number is one unique number. The phone number is not personally identifiable to me. So this is an important distinction. And I'll show you what is important here, especially later.

The thing is that secrets cannot be protected under personal data protection laws. Meaning that right now, our laws can protect personal data, data that identifies you, data that young people are concerned about. But our laws cannot protect secrets, things that older people are concerned about.

So now the question is, what data did IoT collect? Did it collect location based data? I put yes, no, maybe. Yes, no, maybe, sometimes yes. Some of them no. Some of them maybe, right? If you look at the monitor that I showed you, this tracker that I have, by itself doesn't track the location. I know Fitbit, because I used to have a Fitbit. It can link to the GPS and tells you where you've been. This one doesn't have that. So location based, yes or no, maybe.

Does it collect personally identifiable data? Meaning if I look at data from the IoT, cannot identify you. If I look at this, if somebody takes my data from this tracker be, can you say it's something from Singapore? Okay. So again, yes, no, or maybe.

So if you look at this tracker, you cannot tell that I've been to Macao. It only tells you how many steps I took. How well I slept. That's it. But some of the trackers can tell you it may be you, but you have metrics from other data. Maybe there are some other data at this point.

Can it reveal -- now, this is our real concern. The reason is that presently, it can be stopped by law. Secrets. Can IoT data reveal secrets, information that they don't want people to know?

Okay.

I have a CME phone, which I'm very happy about. But when a CME phone first came out in Singapore, the company actually emailed the data of the individuals back to China. And it was discovered because the Singapore owner suddenly was receiving spam from China. So he complained and there was action taken against it.

So this is where it's possible that this device it collects

such information, may collect secrets. But this is illegal. So I bought a phone and I'm confident if they do it again they will be prosecuted. And I'll do it myself. But can other IoT devices do this, get secrets from you?

So I feel that you need small data to link IoT. So here is one example. This is from Dilbert. It says: "Wear this biosensor so the management can monitor your health during the day." And he says: "Oh, I didn't know you cared so much about my health. Oh, I do." And then it says: "Employee number 479 doesn't have shallow breathing. You can give that one some more work."

So you have a way of finding more information about you, and then getting the result of this IoT. The key is this. This is my thesis right now. I'm still looking at this. You need small data and IoT to get secrets identifiable with you. Without small data, big data alone, it would be difficult to pinpoint you. Not impossible, but a lot of work. So small data right away, quite easily. Small data.

So okay. Some concerns about IoT. Would it create new forms of discrimination based on willingness or ability to provide personal data? If you don't want to give information, does it mean that you have some health problem? Does it mean that there is something you want to hide? And if you do give this information, can I use this information against you? So this is one example of health tracker.

Secondly, I think that some personal data you've got to make anonymous. Meaning some of it will leak out and people will know. If they mention enough of the data, they might be able to track you.

Privacy, right now, we don't have a rule about this IoT consent, because all the personal data protection laws require consent. But IoT doesn't look at

Consent. There is no provision about delete. So I don't know if they take my information and keep track, I don't know.

Policies are not spelled out. So this is not clear. My guess is that if companies want to do work in the future, they have to address these concerns. But this can be worked out. Me talking about it, maybe something will work out.

So my final point, how concerned are we about privacy and IoT? My sense is that you need to address the issue of your PI, personal identifiable information, personal data, and there must be rules to say that it cannot be used to discriminate against you, for instance, by the medical industry. But there is a point and this will happen. And on this point, there are some secrets that cannot be regulated. Secrets can be regulated only up to a point, but some secrets need to go out.

So I'll end on this note.

(Applause)

Thank you.

>> KI SHIK PARK: The same as before, do you have any questions for clarification on his presentation, at this moment?

Okay.

Also, you were successful.

Okay. Then let me invite the next speaker. The next speaker is Dr. Seon-phil Jeong. He is a professor at the United International College, and he is going to speak on security issues on IoT in China.

>> SEON-PHIL JEONG: Good afternoon. I'm not from Macao. I come from BNU-HKBU UIC, which is located in Zhuhai.

And today I'll introduce four parts. First, I will introduce the China Government supporting policy, quickly. And then I'll introduce the current status of IoT in China. And third I will -- I collected some interesting cases and happening and riots about IoT and Internet security, so I will present some cases to you. And, finally, I will tell you some interesting happenings which happened to me yesterday and today.

MIIT is the major Department of PRC that is in charge of the development of information technology. And if you are interested in China's policy or plan, probably you already know that PRC has five years' plan. And now, 2010 to 2015, plans have. And actually I'm not Chinese, but I think I have to praise the Chinese Government and industries. They are doing -- they are doing quite a good job. And according to this plan, from 2010 to 2015, they are going to pull in 200 billion US dollars for IoT industry. And I think they are doing a good job right now.

Let me introduce the current status of the Chinese case for IoT. By now, China, has established a solid Foundation for the IoT industry. And HUWEI and ZTE, I think they produced a good technology product and the marketshare is getting better and better.

And in the R&D and standardizations they have made certain breakthroughs in the sectors. And as you know, China has become a key leader of the WSN-WG7 of ISO.

And now, the China Government and the IoT industry has deployed many of the IoT and smart devices in the real world. IoT has applied in many areas of safety and security, logistics and healthcare, et cetera. And also started to use environmental monitoring for -- unfortunately, China is notorious for pollutions. But now they start to use IoT technology to control and monitor the kind of program and issues. And I think they are going to present some remarkable results from this kind of project pretty soon.

Now I'd like to introduce some security cases. Actually, we have some security specialists, such as Adli and probably some of you may be security specialists. Actually, I'm not a

hacker, but luckily one of my students is kind of a hacker, and I met him a month ago to prepare this presentation. And recently he left the community to pursue his master program in the USA.

Anyway, I got some information from the hacker. Before introducing the Chinese case, many of you already read this article, the Internet census 2012. According to this report, we can see many vulnerable areas, vulnerable points, not only of IoT but also the traditional area, as a lot of points, of actions. And this is the website of zoom eye, which is supported by the Chinese white hacker. And in this website you can trace many of the devices, such as a camera, and router problem as Adli introduced. At this point, I have a point in case, but due to my limited time I will introduce only a few of them.

I'd like to introduce the printers vulnerability. From that zoom eye, I could check printer server in Hong Kong that I can access from here to the printer server. And I can see the status of that printer. And a few days ago, the yellow ink was more than half. But as we can see, it's almost the bottom. So I assume that they are using yellow color very much, for some reason. And I also can check the -- that IP -- the printer's IP address, I can check the physical address from IP find -- IPaddressfind.Com. And it's somewhere here, so I can reach physically the place. And there are many -- there are many other issues, but let me jump to -- there is something that --

(Lost audio for the webcast)

And can you guess which one is the phishing or original website? Yesterday, I got a -- okay.

Okay. It's very difficult to put on the screen. We can tell. Yesterday I got e-mail from my research partner: Hey, Sonnie, your paper was offset by a journal, and she said the URL, but I feel something strange. So I Googled and I ultimately found out that it's a fake website. And I made an International call to cancel her payment, and I think it worked.

Anyhow, this is not IoT case, but let me explain why I brought you this case. IoT is a relatively new technology, new mechanisms. But the traditional Internet still has this kind of problem. We haven't solved this problem. And we are going to face bigger and more problems with IoTs mechanisms in the IoT environment.

So to solve this problem, I think we need to have more discussions. We need to have more cooperations. That is my conclusions.

(Applause)

>> KI SHIK PARK: Thank you very much, Dr. Jeong, for your presentation.

And as before, do we have any quick questions for

clarifications for his presentation? Okay. Then you will have some Q and A questions after all four presentations.

Now let me invite last but not least the speaker today for this session. It's Mr. Samuel Park. He will speak on the human centric Internet for the future. Samuel. Are you ready? Please.

>> SAMUEL PARK: Good afternoon. I'm Samuel Park from the Korea Internet Security Agency. First of all, thank you Dr. Park and Adli and Dr. Ang and also Professor Jeong. Thank you very much for your wonderful presentations. Of course, thank you all for attending this workshop.

This is my first time at APrIGF and also presenting in a workshop. So this all really means a lot for me, and also for Ki Shik I guess.

And let me start with the Internet issues of what is going on around the world and how KISA is doing things to respond to the issues. And the challenges that KISA is facing and the limits. And I'd like to end my presentation with a suggestion.

Recent issues. Working under the Korean Internet Security Agency I've been experiencing a lot of Internet issues as I go around the world right now. So I just want to share them with you right now. It started with the Internet browsers, browsers helping people for easy access to the Internet. So people started to look to the Internet for information. And they started listening to music, watch videos, movies for YouTube, and they started to communicate with each other using the e-mail.

Then they started to pay for extra services, like eBay, Amazon. I guess you already know all the times. And they started using mobile banking for their needs. So at this stage, the Internet was just the method or tool. The people found it when they need to do something.

And then the new SNS services started to come along. Twitter, Facebook. People started sharing their lives with their friends through the Internet. And so the Internet has taken a little portion, bigger and bigger in our lives. And now it's in our glasses, it's in our watches, it's in our TVs and all the thinges in our homes. So I'm trying to say the Internet is getting more and more into our lives. First it started with just a simple tool or method to help the people. Now, it's a very big part of our life.

As you all know, when there is a bright side, this is also a dark site. As Mr. Adli explained, we have technical things, hackings, phishing, farmings, and also I'm not sure if you heard about it, but like webcam hacking, a hacker will hack your laptop and see your private lives through the laptop's cameras. And as Professor Ang addressed, there are lots of privacy leakages, althouth it's difficult to define the privacy and the

security, separate the secrets from our lives. But still, our privacies are leaking.

The good things about SNS is sharing. But the bad thing about SNS is I'm not sure who am I sharing with?

Also, cultural defects, like mental illnesses, like IAD, Internet Addiction Disorder, or web-aholism. And like sites, like gathering people to commit suicide, like leading to copy cat crimes or motivating other people to take their lives. This is getting much more serious.

And also, new cloud services. You know who she is and you know what I'm talking about. And also, like hacking into the very important national facilities, like nuclear power station, you know, hacking those infrastructure will bring not just killing several people and end human or very big disaster.

So what I'm trying to say is that the Internet is taking a very big part of our life and its effects are getting too big. So we cannot chase them anymore. We are trying to handle them and respond to them, but we are on our limits.

To respond to those limits, KISA is doing several things. First of all, in the area of security, we are trying to monitor 2.6 domestic websites. And also 158 ISPs, traffics coming and going. See if there is any abnormal activities or malwares.

Also, we have the policies for assessments, so that very important enterprises like telecommunication companies and critical information infrastructure, like the eGovernment services, have to reach a certain level of security to ensure the level of the security.

And, also, we also have the outreach programs for security for like SMEs, small and media sized enterprises. If they cannot afford to have facilities like data shelters or Web inspection, then KISA is doing that with the Government budget, helping them to build their security levels.

Also, in the area of privacy, in Korea, there is a 13-digit number called the social resident number, which can directly identify who you are. So it's very critical information. So if you have your name and just the social number, they can identify you through the Internet. So those informations are very critical. So to monitor whether those informations are posted up or exposed anywhere, we monitor 2.6 million websites and also have the cooperation with like China and neighboring countries. So whether they are like Chinese websites, whether they post our Korean social numbers, then we go ask them to delete them.

Also, we have policy development, like new IoT services device are coming along, and the policies have to be developed to follow up and catch up, like recently we had guidelines for big data, for personal data protection. Also, the right to be forgotten seminars.

Also, we have education and promotions. Like to share the

best practices and encourage the enterprisers who are very aware of the privacy issues. And also education for CEOs and CPOs on the management level of the enterprises, so that they will be aware of how important this privacy issue is.

And last, but not the least, Internet ethics area. We try to promote things for the TV commercials and hand out leaflets and posters. Also, campaigns for Internet ethics, like we held lots of festivals and campaigns and encourage people to, you know, have more idea of the Internet ethics.

Also, Experience Centre for like children so they can get experience from the experience centre about the new IoT devices or other SNS services so they can be aware of what they are doing for the Internet.

Lastly, education and promotion for teachers. You know, teachers should be aware of their children's -- about cyberabuse activities or any normal activities. And also for education for children and youth education, so that they can be taught what is Internet ethics and how should they behave. And also counseling programs to deal with like cyber abuse and addiction programs.

However, all things are just done in Korea. And the Internet is used by every country, the whole world. So we need more cooperations to, you know, overcome the limits.

You can see cyberattacks come from all over the world. Recently there was a smashing. This malware, once it was installed in the smartphone, it copied all the critical data to a Chinese account, called 126.Com. You may be aware of it. But since Korean CERT cannot authorize the Chinese e-mail account, even though it was very alert and happening in real time, the deletion of the exposed critical information cannot be deleted in real time. So more concrete relationship between other countries is needed.

Also, for privacy, many of IoT services like the big data, cloud services, are coming out from the global firms. But are we ready? Is our policy and regulations all ready to accept that? I'm not sure.

And also, Internet ethics, more like online games, very stimulating contents, illegal contents are posted everywhere from the world, but we cannot handle to manage our children not to see this, not to see that. It's out of our limits.

Okay. So this is basically what we are trying to do. This is the basic idea of CAMP, Cybersecurity Alliance for Mutual Progress. We are trying to cooperate with national organisations and global firms and learn or share current issues with them. Also, projects with neighboring countries and outreach programs for some countries who might need help. So by sharing all the -- by learning from one side and also teaching to the other side, we can share all of the important information so that our security level can go up.

And this is not just for technical areas. What we are trying to do right now is trying to imagine what the ideal figure will be 30 years after today. And compare that figure to the Internet right now. So there must be 30 years of a gap. So comparing -- so figuring this gap, we might have some homework to do to catch up and be an ideal figure after 30 years later. So we are starting -- we made like six agendas, like innovation, ethics, equality, sharing, freedom, responsibility. So that when we reach 30 years after doing all this homework, maybe we can be an ideal figure of the Internet where we imagine it right now.

As we all know, technology development is a matter of time these days. If somebody imagines an idea, an engineer will bring it in and very soon. So it is a matter of time.

However, these very critical issues are not the -- the time is not on our side. I believe it's against us. If you do not -- if we do not do the things we should do, then the time will be against us. More and more technologies will come up. But we will be having a very hard time to catch up and manage all of those problems.

Looking at all the issues all the presenters presented today are very complicated issues. And they will get more complicated as our Internet develops more technically. And maybe there is no answer to it, to fit for all questions.

However, if we share all the efforts with all countries, we might be able to learn from each other. Not the exact answer we are looking for, but maybe learn from other countries' mistakes or learn from other countries' fault, and maybe find a correct answer for each country.

It doesn't matter anymore, but it will matter what what direction our Internet is evolving. Maybe next year I can bring more specific results of the studies of the six agendas above, and maybe if someone can bring their country's, it will definitely be a fruitful and very meaningful sharing.

At the beginning of my presentation I first told you that the Internet first started as a method or a tool, and people needed them. They started to use them as a convenient tool or method. And now they -- this is part of lives not for the human but against the human. So if we gather our thoughts in the direction of a basic idea of human centric so that the Internet should be for the human, not against us, I believe there is a safe, secure and much better future waiting for us.

Thank you.

(Applause)

>> KI SHIK PARK: Thank you, Samuel, for your presentation.

And do you have any questions for clarification only? Please. Here is the microphone.

>> AUDIENCE: Apart from KISA and the issues of privacy and

the Internet, apart from KISA are there any other cooperations that are working together with you on these issues?

>> SAMUEL PARK: Yes. We are trying to evolve in issue, and lots of organisations are working together with us to cover our issues.

>> AUDIENCE: Yet KISA stands for Korea Internet Security Agency --

(Audio difficulties)

>> SAMUEL PARK: KISA is playing a critical and major role in Korea under all the government agencies.

(Audio was disconnected)

>> AUDIENCE: Thank you so much. I'm from --

(Lost audio)

-- as you told, your experience and your study, and if other countries as you told want to apply in their country, it would be a big chance. I would like to -- actually, I would like to take your advice and your study and guidelines.

One more issue I would like to address here. I mean, what is the Governments' attitude? Are the Governments -- how they --

(Audio faded out)

>> SAMUEL PARK: KISA is run by the Government. We are working with the Government. Our budget comes from the Government. All the issues and all the roles KISA is doing, they are all supported by the Government. You can just say that we are on one side. So we are working together. And since -- yes, those critical issues. I think Government ministries will be the policymakers, decision makers, and the actual examiner or action doers are us. So I think you can say that we are all one part.

>> AUDIENCE: Thank you so much.

>> MODERATOR: Thank you for your question, Madam. And here's some Government representatives of Korea, so you can discuss some more details with the ladies from the Government later on.

Okay. And having said that, I was advised to invite all the good looking speakers to the podium again for the Q and A session. So please, have a seat. Professor Ang and Adli and Professor Jeong and also you.

And before I limited questions but now the floor is open. So any question, not only questions for clarification, but also for any other discussions or other views on all those presentations and also regarding the issue we raised in this session.

So now the floor is open to you. Any questions?

Please. Professor Chung.

>> AUDIENCE: My question goes to the professor from Singapore. And you mentioned about small data and big data.

Could you clarify it more? It seems to me you're saying small data is more concern while big data is rather than secure.

And that contradicts my previous understanding. So I'm wondering about the conceptual distinction between small and big data is widely used in your area of expertise.

>> PENG HWA ANG: So for big data, we are talking about, I guess, nowadays we are talking about the millions of data points. But even if you reduce that to a few hundred thousand, the question is whether you can identify you or not. Because when you talk about privacy, what you are concerned about is ourselves. Can this information about whatever it is be traced back to me, to say it is me or not. So from big data it is possible, but it's a lot of work to trace it to the individual. It's possible, but it's a lot of work.

But if you have small data, meaning data about you, then it's far easier to track from the huge mass of information, even millions of data points, if I have some data about you then it will be far easier to determine that this, this is you, and a lot of more information about you from this big data set.

So I'm trying to draw a distinction between sort of what is out there in this big mass of information, and a little bit of information about you.

The law can protect -- a little bit of information about you. Meaning personally identifiable data. Your name and the Social Security number, some identifying number, Singapore also. But even a mobile phone number, that can be a critical number. Which is why, as I said, they are protecting such details now. So little bits of data about you, a little bit. Not a lot, that's why they call it small data. But a bit of data about you, if it's leaked out, it's potentially possible to trace a lot of information out there to you. So this is the concern. This is how you track.

Big data, it's difficult to find out information about you. But big data with a little bit of small data. It's easy to track you.

>> KI SHIK PARK: Please. Yes. And you speakers, also, can raise any questions for others, if time permits. But I'll give the priority to the floor first. Okay? Okay. Please.

>> AUDIENCE: Good evening, everybody. First of all, thank you individually for these beautiful presentations. And I mean, it's kind of a ton of information. I'm Moorehead from the Internet Society UA chapter.

So my question is, I just wanted to take your opinion or advice on how we can address these challenges, what it is. Because what you said was that there is a technology solution and technology collaboration which is required amongst organizations and amongst countries. But what do you think is a bigger challenge? For me, the bigger challenge is working

between the Governments. Because technology still is manageable, and we also think together in APrIGF is one of the good examples that technology people, policy people, can work together very well.

But we are living in an age where people are funding cybersecurity. So there is a statement about cybersecurity attack, which is happening. So what is your solution to this particular lack of will and how can that be addressed between countries?

>> KI SHIK PARK: Okay. Please.

>> When we first started thinking about this human centric Internet for the future and the idea that we should cooperate and share information throughout the world, so that we need to discuss these issues, the first thing was that we -- first, the first clear thing in my mind is that there is no clear answer to fit for all. Because as you mentioned, there are lots of Government, lots of countries, and within that country there will be lots of multistakeholders with very different opinions. So every Government will speak for -- will seek for a very different answer. Although we might be in one place to share all of those issues.

But what I was trying to say was that if we gather all their practices, not the best practices, but all the practices, and present it all within the very organised agendas, then some countries' faults or mistakes can be the best answer for another countries. Some country's maybe best practice may be the other countries have to avoid that to fill their needs.

So obviously I don't have a pure answer, but I do want to have a very meaning that sharing is very important. And we need to, you know, step up and start it right away, because we might be already too late for it. Because all the technologies are developing day after day. So I just wanted to focus on the sharing. So by sharing, all the Governments might find their answers.

>> KI SHIK PARK: Okay. Working together. Hand in hand.

Okay, other questions? Okay. Please.

>> AUDIENCE: Thank you. Please. Very enlightening in many ways. There is a term I'm missing from the debate, and that's the term "Education." Maybe this is because I'm from a university and I'm teaching for a good part of the year. But one of the things that has sort of irked me for quite quite a few years, is when you go to the places, you know, to the people who built the componentry for the Internet, and you look at their curricula, security, there is no emphasis on this. Not at all.

Right? You go around, probably, you know, the top 500 universities on this planet and you go to their computer science departments. And you have a look at what they are churning out.

And do you have a course on computer security? Yes, you can take that at a graduate level if you like, and it's an elective. Undergraduate level, it really sort of sticks to the point of you shall all have your own individual passwords and please don't tell anyone else about it.

So my question is, could you envisage, you know, possibly something like a community driven scheme that says okay, we will do something like an ongoing certification of software developers, maybe through some sort of online courses or something like that, where we basically say okay, these are people that have been made aware of how to, for example, develop a secure Web application. You go back maybe a couple of months, there was a major -- I'm pretty sure some of you may be aware of this -- there was a problem with a very popular content management system, Word Press. And a larger number of sites were upgraded. I'm familiar with a case where someone hosted 30 sites on their server. And one of them had an old version sitting in a subdirectory, which the hackers also scanned for. All of the 30 had been upgraded. The old version wasn't upgraded. They got in there and they wiped out thousands of scripts on that server.

So looking at cases like that, could you imagine that maybe we as a community can go and develop something that gets people to, you know, voluntarily want to advertise saying I'm a certified security software developer. I've been made aware of things and I'm keeping myself abreast by basically saying okay, here is my certificate. You can look it up. I've taken an upgrade course within the last 12 months. Maybe this is something that the community can drive rather than the community changing their curricula, which is difficult.

>> KI SHIK PARK: Professor Jeong ... yes, Adli.

>> ADLI WAHID: I don't have a specific answer for that, but I tend to agree that awareness is not just for people using the system, but people who are developing the system and the tools, and people who are running the systems as well. And I think many of our interactions with network operators has been in the area of how do we manage this thing securely? Because in most cases people got the job and somehow, you know, they don't have the proper security training, however you want to define that.

Many of the universities, and I used to work at universities before, and they don't have this hands-on operational type of security classes. And because of various issues.

There have been some attempts to provide this type of work, and I think there have been hits and misses as well. One is that how do you scale this? For instance, you know, to come up with the curriculum is the number one thing. But also to get

people to actually do it.

So to do it and to do it after the fact. Because in a lot of cases, yes I think we can focus at people who are still in the University and teach them something, and we hope by the time they graduate technology hasn't changed too much. So keeping up with the technology is one of the one of the challenges if you want to introduce this at the University level.

Second of all, there have been some attempts for continuous professional development. So groups like OS is specifically focused on Web security. So you can -- they don't have any certification, but they try to build some knowledge base around the topic of Web security itself. Which is, you know, securing the Web server application, securing the Web application itself. How to write the application securely and how to manage databases and so forth. But that's a huge field of knowledge. It's very niche and only a few people can contribute to it. So some of the things that we expect from people when they do security, they have a lot of knowledge about everything, but to gain that knowledge will take a lot of time.

And I'm not sure how, also, the professional security development program exists from IC squared or others are addressing this. But maybe they are looking at this from more of the security management issues. Organizations like Sands provide very specific technical hands-on security experiences, like how to do forensics and incident responses and so on and so forth.

So there are probably a lot of things out there, but they are not integrated. And as an individual who is work, so let's say I'm a security person in this organisation, I have to actually probably go to different places to learn about different things.

>> KI SHIK PARK: Please be brief. because there are many participants who are breaking for a chance to speak.

Okay. Then please, what is the question from remote?

>> YANNIS LI: We have a promote question from Firdausi from the University in Indonesia, Bandu, and the question is for Mr. Peng Hwa Ang. So she is asking how the standard of privacy in each country can be seen at the same level, given different culture might make a certain concept about privacy which can be different with others.

>> PENG HWI ANG: This is a question I ask myself. Because even in a Chinese culture, privacy is an invented word. There is no concept of privacy. There is just no idea at all. So when I came back from the USA, I was at ATM and there was a guy behind me breathing down my neck, he was that close. And I said can I have some privacy? And he just chuckled. He was like what is privacy? You know, he knows that I have money, so what. And I asked my students, you know, if your privacy is invaded,

what have you lost? And so far no one has said I've lost the right to be left alone. That's kind of the answer I'm looking for. They have no idea what is privacy. So in a sense, privacy is cultural.

For the law, however, the way they define it is, as I mentioned, personally identifiable information. So this is why I mention this, it's important to draw the distinction between your secrets and your personal data and personally identifiable information.

So the law, I would say, I don't say universally, but across the globe, okay, you can have a law that will protect your personally identifiable information. Name, your passport number, your identifying number, your drivers license, your ID car number, home address to a point, bank account number. Your car plate number to a point. So there are a lot of details that identify you. This is privacy in a sense. But the larger aspect of privacy, various cultures, the questioner is right. There is a big cultural element that right now you can't really enforce that.

The closest I would say is the right to be forgotten. That is the closest. But there are a lot other issues. And Asia we are not getting there. So Europe, it's interesting to see how in Europe they are looking at that. The right to be forgotten is that we want our secrets to be forgotten. That stuff to be forgotten. So in a way that is sort of privacy as well.

>> KI SHIK PARK: Thank you. And now we are running out of time. But anyway, let me invite two more very quick questions. If you have, please.

>> AUDIENCE: This is Chester from ISOC Hong Kong. Just actually, because of time, I would like to clarify some things. And for -- it was a speech I think, personal identifiable information or PII, is mainly a US scoped definition of personal data under the law.

Now, for the new data protection directive or including actually several data protection laws in Asia, the PDPA of Singapore, Taiwan, military restrictions, it actually includes more than just your ID number, your address, your phone number. It includes also your religious beliefs, your political affiliations, and, you know, even medical records. Those are not really exactly your personal data or defined as personal data in other areas.

And also, the other thing is for Hong Kong's data protection law, actually concept is not required. That means for collecting of your personal information or personal data, it does not require consent.

Now, the issue of course is still you are required to comply with the use of the personal data, the protection of the data itself. So I just wanted to clarify.

>> KI SHIK PARK: Thank you. And please -- respond, please.

>> PENG HWA ANG: You are right in that personally identifiable information includes bits of information. They can identify you when collected as a group. So looking at religious belief by itself cannot identify you. But if you mention it as part of a small group, it's possible.

So at my seminars a trick question I give is: Can I identify you from occupation? And most of the time people say no. But then I say Prime Minister, and the people say oh, there is only one Prime Minister. So then you identify the person based on the occupation. So various things can identify people.

Of course, there is some variation in terms of what can be done under the personal data laws. But the key part we are all concerned about is actual use of the information. So maybe in Hong Kong consent is not needed. But in Singapore it is. You need that to even collect. But the concern is if this information is used, and basically used against us?

So it's collection and then something beyond that. That is a major concern when it comes to invasion of privacy.

>> KI SHIK PARK: Thank you, Professor Peng Hwa Ang. And the last question we will get is from Dr. Kuo-Wei Wu, ICANN Board of Directors.

>> AUDIENCE: First of all, I totally agree with what Peng Hwa said. Actually, the privacy or the data protection is really based on the cultures. I think in the Asian culture, in general, we really are not -- we don't understand what is privacy or something like that in our regional cultural research. That is a very important thing.

Let me take one simple example. I think in the Asian countries, I think most of the family, you know that. When I was a kid, any data sent to me, my parents always can look at. They always get used to opening your envelope and then you read later. And although you complain, but it doesn't work.

And so I think this is a couple of the very interesting issues. For example, the data protection laws that just passed in Taiwan about one or two years already. But to be honest, I think it's still now, even now, two years -- more than two years after, I think the people are still arguing about how you apply this law in the real behavior in the daily life.

For example, usually when a professor, once the exam finished, the professor always posted the grade for every student on the door of his office. And then after the data protection laws passed, the Professor cannot post that. And then how the student know what is the grade? Or the Professor needs to, personally, need to inform the student what is the grade you have?

And so this is still a lot of learning. I remember in

Japan about the same thing. I don't know how many of you read Japanese personal data information law, too. But originally, Japanese PII is they have very interesting item. Say if the number of the personal data is less than five thousand is not -- it's inclusive of the data protection law, the original idea is thinking about, they tried to minimize the personal data protection law to impact the individual or the SMB, the small medium company, as minimal as possible. But you know the companies are getting smarter. They cut up data everyone in less than five thousand. So if they have 20,000, they cut in four pieces, so the law cannot apply on them. So this is -- and of course, as I know, I think this year the Japanese already amended, you know.

And one more thing I think is important particularly in Asia, the data protection is not only applied to the person but also the company, actually the Government, too. And sometimes I think the people, they thought a couple should be good, because some of the data that is actually leaking is from Governments. And I think this is -- I think we really need education from the very beginning to really understand what is data protection and privacy for the later for the future. Before that, I think it's early to talk about how the privacy really happens in Asia.

Thank you.

>> KI SHIK PARK: Thank you very much, Dr. Wu.

And I don't think you need to respond to his comment.

Anyway, as a Moderator for this session, I want to express my thanks to all of you in this meeting room for your kind attention and active participation. And also my special thanks should go to the speakers for giving us really inspiring presentations. So thank you very much.

This session is adjourned.

Thank you.

(Applause)

>> YANNIS LI: Everyone, so the outgoing outcomes document discussions will be immediately after this session.

Right now, tonight, the shuttle schedule return is scheduled to be at 6:40 p.m. after this outcomes document session. So please stay and join us and provide your input on that.

And also, for the schedule bus schedules it's also revised. So please refer to the event website for the latest schedule for tomorrow and the day after.

Thank you.

(end of session 5:30)

****

order to facilitate communication accessibility and may not be a totally verbatim record of the proceedings.

***