ceocfointerviews.com

Issue: March 30, 2015
The Most Powerful Name in Corporate News

Mobile App Security Solutions

Mary Min
VP Global Business

CEOCFO: ***Ms. Min, what is the concept behind SEworks?***
Ms. Min: Our company was founded by a group of white hat security specialists with many years of background in doing security research and creating security software. Originally, we started working at creating our own apps. When we started researching different security solutions to protect our own applications against hackers, we realized there really was not anything out there that was easy to use, powerful and secure. That's when we decided to make our own solution, which is AppSecu.re.

CEOCFO: ***What is the approach at SEworks? What do you understand fundamentally about security that has allowed you to come up with a better product?***
Ms. Min: I would say that in regards to security on mobile, we do not claim to be the answer to every problem that you will have on mobile. We like to say "security should live on every single layer across the board". With mobile, there are different places where you can have security. The device needs to be secure, communication needs to be secure, the data needs to be secure and there are a lot of startups working on those problems. We found that there weren't many startups that were tackling the problem of making apps secure. It is interesting because your mobile app is usually the gateway and the first line of defense, and the first thing that hackers will analyze and attack when they are trying to compromise your app, device and/or service. I come from a non hacker background; more specifically, I developed mobile gaming apps before joining SEWORKS. Many of the solutions that I had reviewed when I was developing mobile apps were just really hard to use and required a great deal of learning and integration time, something most developers cannot afford in this age of time-to-market. And they were not as powerful as we wanted them to be. We've been able to apply our collective experiences to create an approach that makes this process as easy and painless as possible for everyone. We do a binary level injection, post compile, which means you do not have to write a line of code. When you are using our solution for Android, you maintain your existing development process and build the application as you would like. Then before you submit it to Google Play or whatever application store you are targeting, you simply upload the file to our server, select whatever options you want, press click and then we do all the magic on the back end to make it secure before we hand the file back to you. That's it.

CEOCFO: ***Are there different levels of security? What would the app developer be choosing?***
Ms. Min: You are choosing from different options that may or may not apply to you, depending on the way that you write your application. For the Android platform, which is an incredibly flexible environment, you can code in a numerous variety of languages. There are different options that you can employ, and we support all of them. We also offer a very game specific feature called memory hacking protection, which does not apply to most other non-gaming applications. In mobile games, you will have levels you try to achieve, coins that you try to earn or buy, and items that you purchase or earn. With memory hacking, you can access that application's memory and change certain values that allow you to bypass the normal method to level up or get to a certain stage in a game or earn the coins, allowing you to change those values as you see fit. We prevent this from happening.

CEOCFO: ***Are developers becoming increasingly aware they should be working on security or is there still a lot of education?***
Ms. Min: I think there is a great deal of education that still needs to happen, in raising the general awareness of the need for security, and the different types of security in the mobile landscape. Developers need to understand that there are

multiple layers to mobile: the app, the data, the communications, the device, the servers, etc. and that security measures should be in place across all of them. For example, the first fundamental step should be to ensure your app was developed in a secure manner, which can be tested by scanners such as AppSecu.re SCAN and penetration testing. Then there is the second step of ensuring the app stays secure, which is where AppSecu.re's core features come into play. Our comprehensive approach tackles the app security issue from multiple angles. If you write and keep the app secure, chances of your app being compromised greatly decrease. This sounds like a simple concept, but when we talk with potential clients or developers, you would be surprised how many developers are not aware the problem exists. Worse, other responses that we get are that they know security is important but they do not have time or energy to address the problem right now.

CEOCFO: ***How are you reaching out to prospective customers and the industry?***
Ms. Min: We are going live next week, so we have not really started reaching out to many prospective clients. We have a few trusted clients that are helping us test our product before we officially open it to the public. Once we're live, we will be starting our marketing efforts and developer outreach through a combination of direct sales, partnerships, and self-served diagnostics. That last piece ties into AppSecu.re SCAN, which is the first component of the AppSecu.re solution.

"Your mobile app is usually the first thing that hackers will analyze and attack when they are trying to compromise your [business]...We always try to stay a few steps ahead."- Mary Min

There are three parts to AppSecu.re. The first part is called SCAN, and will scan your app to do a vulnerability analysis. You upload your application and we run diagnostics on the application to see whether the application is secure or not. We conduct a check to see if we were able to decompile your app and identify security concerns. That way you can actually see for yourself whether you are actually vulnerable and whether you need someone like us. This is a completely free service that we offer. The second part is called PROTECT, and that is the app protection part. We do our magic; we take care of the encryption and protection for your app, and hand it back to you. We support all Android apps, and for apps built on the Unity 3D engine, Android and iOS. Native iOS support is offered in limited scopes, due to Apple platform policies. With our third part, which is called AppSecu.re TRACK, we monitor and track each individual install of your application. Let's say you are a mobile developer and your app has four million downloads. That's fantastic, but if I were to ask you "has your app been hacked? How many times?" it's hard to know for sure. Until now, it's been a reactive versus a proactive approach: you rely on Google searches or scour forums to see if someone has posted a crack or claimed to, then test to see if their claims are true or not. That wastes valuable engineering time that could otherwise be used towards actual development. No one has provided a handy tool to trace every single one of those four million installs and says, "This one is ok and that one is ok. I think somebody is trying to mess with this particular install on this one device." That is what we do. We track every single one of those installs. We show you a nice real-time analytic dashboard that shows the number of installs that you have, the number of good installs that have not been hacked, and which ones had a hack attempt. Then you can view the list of the ones that we deem to have been compromised and decide on an action. We do something called a device-level targeted kill switch, which means that if I don't want my app to run on your phone, for example, I can choose to not have that app run.

CEOCFO: ***Was the ability to know about the hacking part of the original plan or did that develop as you were creating the product?***
Ms. Min: Our core engineering team has always done security software. Originally at SEWORKS, we started developing our own app, and consequently looking for a security solution to protect our app. That's when we discovered that no simple solution existed that met our needs, and we ended up developing something for our own use. That evolved into an encryption and obfuscation solution that is the core of AppSecur.e PROTECT. We originally thought of just doing the protection piece, but as we started interviewing many prospective clients and talking to many more app developers, we realized that many of them were not even aware that they need security measures or that their security measures are not sufficient enough. In short, people were not aware that the problem existed. We created a SCAN portion for people to be able to diagnose their applications. And we went out and talked to folks, they said "That's really cool and nice, but we want to know if our application is safe once it is released into the wild." That prompted us to create the TRACK piece.

CECOFO: ***What is the plan for the next six months to a year?***
Ms. Min: We are going to be focusing on increasing the level of security that we can offer and seeing what we can do to make the iOS side as safe as we do on Android. We are always in a race. As soon as you put out a solution, hackers are going to try to compromise it. We always try to stay a few steps ahead of hackers to figure out the newest hacking trends and the newest security threats that we need to be aware of, so we can apply immediately to our own solution.

CEOCFO: ***Are you funded for the steps you would like to take and will you be seeking investments or partnerships?***
Ms. Min: We received our seed round in 2013. That has luckily brought us this far. We are going to be starting our Series-A fund raising process soon after we launch this product.

CEOCFO: ***Why pay attention to SEworks today?***
Ms. Min: Today 70-80% of hacking efforts are still in the PC space, indicating that most hackers are still primarily focused there. However, the tide is shifting and more hackers are turning their eyes to mobile. It's inevitable that the hacking trends we saw in the PC space will carry over to mobile – a mobile phone is really a portable computer with wireless phone capabilities. According to Gartner, 75% of mobile breaches will be due to mobile app vulnerabilities by 2017. And that's why you need our solution –app security is something that you do need to address now, and we are a very easy to use, secure and comprehensive solution. We help you prepare for threats that are emerging now.

CEOCFO: ***Final thoughts?***
Ms. Min: Security is something that you should be thinking about from the beginning, and very early on before your app release. Security expenses grow by at least 4 fold if you try to apply measures after a breach, as opposed to implementing solutions before you launch an app. We have many application developers who will release their applications, and then they are hacked and come to us for help. Sometimes we see instances where the damage is irreparable and developers are forced to shut down the app. If your application has already been compromised and there is a pirated version floating out there for example, there is going to brand identity confusion. People might be driven away. Users might be fragmented. They might be confused. Sometimes someone might package malware into that copy of the application and then you have an image or a perception from consumers that you are a malware company. People can manipulate values inside an app to give themselves gold or items that they didn't pay for. There are many things that can happen, so you should be thinking about security early on and not later.

Interview conducted by: Lynn Fosse, Senior Editor, CEOCFO Magazine

Seworks

For more information visit:
www.seworks.co.kr

Contact:
Jeff Yu
650-656-7495
jeff@seworks.co