Publication: Eurek Alert Online
Date: 5 March 2021
Headline: A new and non-intrusive method for preventing cyber attacks on Android devices

A new and non-intrusive method for preventing cyber attacks on Android devices

SMU Office of Research and Tech Transfer - Cyber attacks on mobile devices are on the rise, with over 100 million attacks reported per year since 2018.

Despite this, recent security research shows that most companies have unprotected data and poor cybersecurity practices in place, thus making them vulnerable to data breaches and data losses.

"This is a top concern for every company because nearly all workers are routinely accessing corporate data from their smartphones and tablets," SMU Associate Professor of Information Systems Gao Debin told the Office of Research and Tech Transfer. The cost of a corporate data breach is huge. It is estimated at a whopping S$6.8 million (US$3.86 million).

He added; "With work-from-home and workers bringing their own devices (BYOD) to work becoming a norm in today's work environment, I expect the number of cyber attacks to increase significantly in these few years. The security of home networks pales in comparison to corporate networks and BYOD are less secure and riskier as workers may unwittingly expose sensitive data or create vulnerabilities to malware."

Cyber attacks are also becoming increasingly sophisticated as hackers employ techniques that are hard to spot and detect. Hence, to solve this persistent problem, Professor Gao believes that a dynamic yet intelligent method of monitoring and detection is required to give IT staff end-to-end visibility of the IT network including the BYOD that are attached to it.

At a market share of 85 percent across the world, it is of no surprise that Android is the most heavily targeted mobile operating system by malware. Given the severity of the problem, Professor Gao and his team of collaborators - Associate Professor David Lo and Professor Robert Deng, decided to focus their research on malware detection on Android apps. Their vision of a non-intrusive and dynamic solution for malware detection on the Android platform is shared by Acronis Asia R&D Pte Ltd, one of the leading cyber protection service providers that worked with the team in this 30-month research project.

However, designing a malware monitoring and detection system for Android has its challenges. Given that Android is an open source operating system, there are security and privacy mechanisms that prevent another program or app to gain sensitive information on third party apps even if it is to detect malware. Such an operation would also be considered intrusive as it violates the Android security and privacy framework.

Side-channel monitoring solution

This is the reason why the team of researchers decided to leverage a side-channel for detecting sensitive and uncharacteristic behaviours on the mobile apps. A side-channel is an unintended channel emitting information from an electronic device. To illustrate, the presence or absence of executable codes in the Central Processing Unit (CPU) of a mobile device is a side-channel for detecting the running application and behaviour of that particular device.

Using emissions from a side-channel to detect sensitive and uncharacteristic behaviour of the app is non-intrusive. It also does not require rooting or gaining privilege control from the Android users, thus no inconvenience is caused.

Publication: Eurek Alert Online
Date: 5 March 2021
Headline: A new and non-intrusive method for preventing cyber attacks on Android devices

Furthermore, this method of detection is unaffected by Android operating system upgrades and it does not breach the Personal Data Protection Act 2012 as no personal data is extracted in the process.

To design such a side-channel monitoring system, the research team took input from side-channel readings and leveraged artificial intelligence and deep machine learning to train a deep neural network model to determine whether or not a sensitive or uncharacteristic behaviour has occurred on the mobile apps. This method of monitoring and detection provides a way for the researchers to dynamically monitor the behaviour of the apps rather than statically analysing the codes from each app. And this method can detect stealthy attacks, which are attacks that can generate and load new malicious codes quickly and effectively.

Before commencing their research in the real world, the team conducted several rounds of simulations in the lab. The results from the lab were positive - up to 98.5 percent accuracy in sensitive behaviour detection was achieved.

In extending their research to the real world, the researchers selected 30 users and collected the CPU cache based side-channel information of their Android smartphones to determine the accuracy of the side-channel monitoring system. Professor Gao was beaming when he told me that "we achieved over 90 percent accuracy".

While these early results from side-channel monitoring are promising, Professor Gao wants to further this body of research to detect more sophisticated cyber attacks such as code-reuse attacks. This form of cyber attack has been gaining a lot of traction as they bypass even the modern operating system protection mechanisms.

Preventing cyber attacks

Even though various preventive measures have been put in place, no one or no company is immune to cyber attacks. The wide use of smartphones and tablets make it "ripe for the picking" by the hackers as the security on mobile devices lack the detailed privacy controls of personal computers.

Professor Gao acknowledged, "While we have shown great results from our research, there's still so much to do especially when cyber attacks are becoming harder to detect and more sophisticated". That said, he is confident that this research will enhance the security of Android devices and possibly avert large attacks on these devices in the future.

###

By Jovina Ang