Researchers unveil new way to counter mobile phone 'account takeover' attacks

January 22 2024

Credit: CC0 Public Domain

Computer science researchers have developed a new way to identify security weaknesses that leave people vulnerable to account takeover attacks, where a hacker gains unauthorized access to online accounts.

Most mobiles are now home to a complex ecosystem of interconnected operating software and Apps, and as the connections between online services have increased, so have the possibilities for hackers to exploit the security weaknesses, often with disastrous consequences for their owner.

Dr. Luca Arnaboldi, from the University of Birmingham's School of Computer Science, explains, "The ruse of looking over someone's shoulder to find out their PIN is well known. However, the end game for the attacker is to gain access to the Apps, which store a wealth of personal information and can provide access to accounts such as Amazon, Google, X, Apple Pay, and even bank accounts."

To understand and prevent these attacks, researchers had to get into the mind of the hacker, who can build a complex attack by combining smaller tactical steps.

Dr. Luca Arnaboldi worked with Professor David Aspinall from the University of Edinburgh, Dr. Christina Kolb from the University of Twente, and Dr. Sasa Radomirovic from the University of Surrey to define a way of cataloging security vulnerabilities and modeling account takeover attacks, by reducing them their constituent building blocks.

Until now, security vulnerabilities have been studied using "account access graphs," which show the phone, the SIM card, the Apps, and the security features that limit each stage of access.

However, account access graphs do not model account takeovers, where an attacker disconnects a device, or an App, from the account ecosystem by, for instance, by taking out the SIM card and putting it into a second phone. As SMS messages will be visible on the second phone, the attacker can then use SMS-driven password recovery methods.

The researchers overcame this obstacle by developing a new way to model how account access changes as devices, SIM cards, or Apps are disconnected from the account ecosystem.

Their method, which is based on the formal logic used by mathematicians and philosophers, captures the choices faced by a hacker who has access to the mobile phone and the PIN.

The researchers expect this approach to be adopted by device manufacturers and App developers who wish to catalog vulnerabilities, and further their understanding of complex hacking attacks. The study is published in *Computer Security—ESORICS 2023*.

The published account also details how the researchers tested their approach against claims made in a report by Wall Street Journal, which speculated that an attack strategy used to access data and bank accounts on an iPhone could be replicated on Android, even though no such attacks were reported.

Apps for Android are installed from the Play Store, and installation requires a Google account, and the researchers found that this connection provides some protection against attacks. Their work also suggested a security fix for iPhone.

Dr. Arnaboldi says, "The results of our simulations showed the attack strategies used by iPhone hackers to access Apple Pay could not be used to access Android Pay on Android, due to security features on the Google account. The simulations also suggested a security fix for iPhone—requiring the use of a previous password as well as a pin, a simple choice that most users would welcome."

Apple has now implemented a fix for this, providing a new layer of protection for iPhone users.

The researchers repeated this exercise across other devices (Motorola G10 Android 11, Lenovo YT-X705F Android 10, Xiaomi Redmi Note Pro 10 Android 11, and Samsung Galaxy Tab S6 Lite Android). Here they found that the devices that had their own manufacturer accounts (Samsung and Xiaomi) had the same vulnerability as Apple—although the Google account remained safe, the bespoke accounts were compromised.

The researchers also used their method to test the security on their own mobile devices, with an unexpected result. One of them found that giving his wife access to a shared iCloud account had compromised his security—while his security measures were as secure as they could be, her chain of connections was not secure.

More information: Luca Arnaboldi et al, Tactics for Account Access Graphs, *Computer Security—ESORICS 2023* (2024). DOI: 10.1007/978-3-031-51479-1_23

Provided by University of Birmingham