VASCO Security Response

Mitigating Transaction Manipulation Attacks against App-based Authentication Schemes

Response ID: vasco-sr-20161019-transman

Revision number: 1.0

Date and time of release: October 19 2016 12:00 UTC

Date and time of last update: October 19 2016 12:00 UTC

Introduction

In October 2016, researchers Vincent Haupert and Tilo Müller from the University of Erlangen – Nuremberg published an article [1] outlining a transaction manipulation attack against the app-based authentication schemes of several German banks. The researchers intend to show that app-based authentication schemes, whereby a mobile banking app and an authentication app are run on the same mobile device, can technically speaking not be considered secure. This Security Response describes the transaction manipulation attack, provides a risk assessment of the attack, and describes ways to mitigate the risk.

Description of the attack

The transaction manipulation attack targets app-based authentication schemes, whereby a mobile banking app is used to initiate a financial transaction and a separate authentication app is used to confirm the transaction. Both apps, which interact via app-to-app communication, reside on the same mobile device of the victim. The attack is based on manipulation of the transaction data that is entered by the victim into the mobile banking app as well as the transaction data that is shown to the victim by the authentication app.

The attack consists of the following steps:

1) The victim launches the mobile banking app, enters transaction data (e.g. beneficiary account number, amount of money), and submits the transaction to the banking server.
2) The adversary intercepts and manipulates the transaction. For instance, he might change the beneficiary's account number and amount of money. The adversary sends the manipulated transaction to the banking server.
3) The mobile banking app prompts the victim to verify and confirm the transaction in the authentication app. The latter app, which is under the control of the adversary, shows the original transaction data to the victim. Since the victim believes the transaction is correct, he confirms it. However, in reality the authentication app generates a signature or TAN over the manipulated transaction data, and returns it to the mobile banking app.
4) In the mobile banking app, the victim confirms that the signature (TAN) can be sent to the banking server.
5) The banking server receives the signature, verifies whether it corresponds to the manipulated transaction, and executes the manipulated transaction.

The attack is implemented using malware that exploits a privilege escalation vulnerability on the mobile device in order to obtain root access to the device.

The root cause for the attack is that app-based authentication schemes with app-to-app communication are implemented entirely on the same mobile device. Mobile devices are open, multi-purpose devices with a complex security architecture. The attack does not exploit a vulnerability in VASCO's CRONTO products for mobile devices.

Repackaging detection by RASP

One of the authentication apps described in the article by Haupert and Müller is protected using Runtime Application Self-Protection (RASP) technology from VASCO. RASP provides a large number of security services to mobile apps, such as root detection, repackaging detection, code injection detection and debugger protection.

The researchers point out that they managed to circumvent the repackaging detection of RASP. VASCO confirms that the researchers exploited a weakness in its RASP technology. However, exploiting this weakness requires a highly tailored attack that is difficult to execute. VASCO assigns a low probability of occurrence to this attack for the reasons outlined below. Furthermore VASCO will release a patch in the week of October 17th to resolve the weakness.

Risk assessment for the attack

VASCO assigns a low probability of occurrence to the transaction manipulation attack because of several reasons:

- The functionality of the malware used in order to perform the attack is very advanced, and certainly much more advanced than the functionality of malware that VASCO observes “in the wild” today. The level of sophistication of malware used by the researchers is currently only observed in research labs. The attack only works in a controlled environment.
- The researchers assume that targeted mobile devices are subject to a privilege escalation vulnerability that allows malware to root the device without the user noticing. Although such vulnerabilities exist, they typically require different exploitation techniques on different types of devices and operating systems. This makes it difficult to launch the attack against a large number of users.
- The researchers assume that the malware can obtain root access on the device. While rooting a single type of mobile device can be performed relatively easily in the controlled environment of a lab, obtaining root access to a large number of devices is significantly harder.
- In order to successfully carry out this attack, the attacker needs a way to make the user install targeted malware on the victim's device. This requires a form of social engineering, targeted at individual users.
- Many mobile banking apps impose a limit on the amount of money that can be transferred. The possible economic return for the adversary is therefore relatively low compared to the required effort.

Mitigating the attack

VASCO recommends to mitigate the transaction manipulation attack as follows:

1) VASCO recommends using Runtime Application Self-Protection (RASP) technology to protect mobile apps. RASP ensures that the amount of effort and level of expertise required to conduct the transaction manipulation attack increases significantly. This is also pointed out by the researchers themselves.
2) In order to completely mitigate the transaction manipulation attack, VASCO recommends using a separate hardware device to authenticate financial transactions. As pointed out by the researchers, the usage of a dedicated hardware device to authenticate financial transactions provides excellent protection against this type of attack.

References

[1] Vincent Haupert and Tilo Müller, On App-based Matrix Code Authentication in Online Banking, https://www1.cs.fau.de/content/app-based-matrix-code-authentication-online-banking

Legal disclaimer