

You can now unlock fingerprint protected phones with a printer - blueAPACHE

Canonical:

<https://www.blueapache.com/blog/you-can-now-unlock-fingerprint-protected-phones-with-an-inkjet-printer>

Details:

We explore the security implications of research into bypassing fingerprint protection with printed images.

March 9, 2016

Two researchers at Michigan State University have come up with a new method of hacking devices that use fingerprint biometrics to protect and lock the user's data. Kai Cao and Anil K. Jain from the Department of Computer Science and Engineering have proven you can spoof fingerprints using a regular inkjet printer, three AgIC silver conductive ink cartridges, a normal black ink cartridge, and AgIC paper.

The equipment required costs less than \$500 – making it very accessible. Coupled with how easy it is to do, fingerprint hacking is now a dangerous reality.

You can obtain a fingerprint – even from the stolen phone itself – scan it at 300 dpi and then print it on AgIC paper. Simply placing the printed fingerprint over the phone's scanning sensor unlocks the phone and grants full access to the device and data. This process has been successfully tested on Samsung Galaxy S6 and a Huawei Honor 7. The Samsung was easy to crack, the Huawei phone needed more tries. The video below highlights how simple it is.

The time required? Less than 15 minutes – about the same as it takes to head around the corner and grab a coffee, or the time it takes to realise you left your phone at the coffee shop.

Fingerprints and biometrics are growing in popularity for everything from phones to home security. The research highlights how unsafe this authentication method is, and why organisations need to be investing in other control methods.

If a device is misplaced or stolen (or does not have privileges correctly rescinded upon separation), the data and network access from the device pose a serious risk when fingerprint spoofing is so simple.

But not all is gloom and doom – Mobile Device Management (MDM) software is readily available and easily deployed. MDM solutions like Citrix XenMobile and VMware AirWatch allow organisations to silo and encrypt content on devices, and remotely nuke the content should the device fall into the wrong hands or be misplaced.

There are also file sharing and distribution tools like Citrix ShareFile that extends on traditional sharing by adding encryption and file expiration – enabling confidential or high value documents to be distributed securely. ShareFile (and all files) can also be remotely deleted should the need arise.

If you're not using MDM to remotely control and protect devices, new fingerprint spoofing methods like this should be concerning. All it takes is a single employee to be targeted, fifteen minutes and less than \$500 of equipment.

Mobile Phone Fingerprint Spoof Attacks - YouTube

Tap to unmute

Mobile Phone Fingerprint Spoof Attacks Michigan State University

Michigan State University24.4K subscribers

For more information on the new spoofing technique, you can directly access the research paper (PDF document) [here](#) .

For information on better securing devices through Citrix XenMobile, VMware AirWatch and Citrix ShareFile, contact the our account team .

Who discovered the method for spoofing fingerprints to unlock phones using a printer?

Two researchers at Michigan State University, Kai Cao and Anil K. Jain from the Department of Computer Science and Engineering, discovered this method.

What equipment is needed to spoof a fingerprint according to this research?

The method requires a regular inkjet printer, three AgIC silver conductive ink cartridges, a normal black ink cartridge, and AgIC paper.

How much does the equipment for fingerprint spoofing cost?

The equipment required costs less than \$500, making it very accessible.

How does the fingerprint spoofing process work?

You obtain a fingerprint—even from the stolen phone itself—scan it at 300 dpi, and print it on AgIC paper. Placing the printed fingerprint over the phone's scanning sensor unlocks the phone and grants full access to the device and data.

Which phones were successfully tested with this fingerprint spoofing method?

The process was successfully tested on a Samsung Galaxy S6 and a Huawei Honor 7. The Samsung was easy to crack, while the Huawei phone needed more tries.

How long does the fingerprint spoofing attack take?

The attack takes less than 15 minutes to complete.

What solutions do you recommend to protect against this type of fingerprint spoofing risk?

We recommend Mobile Device Management (MDM) software like Citrix XenMobile and VMware AirWatch, which allow organisations to silo and encrypt content on devices and remotely wipe content if a device is lost or stolen. It also recommends file sharing tools like Citrix ShareFile, which adds encryption and file expiration for secure distribution of confidential documents and allows remote deletion of files.