

**EMERGING CONSENSUS ON ICS CYBERSECURITY**  
 Experts agree: protecting safety & reliability is key for ICS

[Download whitepaper](#)

- Featured news**
- Endpoint breach prevention by reducing attack surfaces
  - Telecom services: Patient zero for email-based attacks?
  - Busting the security myth: Should I use WordPress for my website?
  - New infosec products of the week: August 17, 2018
  - AT&T sued for enabling SIM swap fraud
  - Google offers rewards for techniques that bypass their abuse, fraud, and spam systems
  - 2.6 billion records exposed in 2,300 disclosed breaches so far this year
  - Cloud computing remains top emerging business risk
  - eBook: Windows PowerShell Scripting Tutorial
  - Networking vendors patch against new cryptographic attack
  - Chaos and confusion reign with existing firewall infrastructure
  - August 2018 Patch Tuesday: Microsoft fixes two actively exploited zero-days

 **Zeljka Zorz**, Managing Editor  
 July 29, 2014

Share this article [f](#) [t](#) [in](#) [e](#)

# Researchers successfully attack Android through device's speaker

Achieve more in your IT career with these 9 tips. [Get the eBook >](#)

A group of researchers from the Chinese University of Hong Kong have demonstrated that even applications with zero permissions can be used to launch attacks that allow attackers to forge text and email messages, access private information, receive sensitive data, and even gain remote control of the targeted device.



Tested on a Samsung Galaxy S3, a Meizu MX2 and a Motorola A953, their "GVS-Attack" was successful independently on whether the device was running the vendor's official Android version or CyanogenMod OS.

"GVS-Attack utilizes an Android system built-in voice assistant module – Google Voice Search," they explain in a [paper](#), and invokes the device's speaker.

"Through Android Intent mechanism, VoicEmployer (their prototype attack app) triggers Google Voice Search to the foreground, and then plays prepared audio files (like "call number 1234 5678") in the background. Google Voice Search can recognize this voice command and execute corresponding operations."

The researchers have also discovered a vulnerability of status checking in Google Search app, which can be exploited by the GVS-Attack to make the device call arbitrary malicious numbers. This can be executed even when the device is locked and secured with a password, ideally in the early hours of the morning, when the device owner is more likely to be asleep.

In order to execute the attack, a malicious app – in this case their own VoicEmployer – has to be installed on the target's phone and run.

Users who don't lock their phones are even in more danger, as the data contained on their device can be transmitted to the attacker, and he (or she) can gain control of the victim's Android phone remotely.

The malicious app is able to do all this by bypassing a number of Android permissions (Read Contacts, Write SMS, Send SMS, Internet, Set Alarm, Get Accounts, and so on).

"GVS-Attack can dial a malicious number through playing "call ...", when this call is answered by an auto audio record machine, actually the data transmission channel has been built. Any audio type of data can be transferred through this channel instead of commonly used Internet connection," they explained.

It's also interesting to note that a number of popular mobile apps weren't able to detect VoicEmployer as malicious.

"Through experiments, the feasibility of our attack schemes has been demonstrated in the real world," they concluded, adding that they hope that their research will "inspire application developers and researchers rethink that zero permission doesn't mean safety and the speaker can be treated as a new attack surface."

More about [Android](#) [vulnerability](#)

Share this article [f](#) [t](#) [in](#) [e](#)

**Endpoint breach prevention by reducing attack surfaces**

2.6 billion records exposed in 2,300 disclosed breaches so far this year

August 2018 Patch Tuesday: Microsoft fixes two actively exploited zero-days

DDoS attackers increasingly strike outside of normal business hours







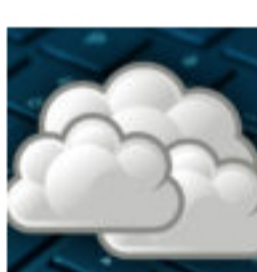

Microsoft ADFS flaw allows attackers to bypass MFA safeguards

**Spot light eBook: Windows PowerShell Scripting Tutorial**

**SmartNA PortPlus™**  
 Your Speed | Your Scale | Your Network

[REQUEST DATA SHEET](#)

## + What's New

-  **Telecom services: Patient zero for email-based attacks?**
-  **New infosec products of the week: August 17, 2018**
-  **Busting the security myth: Should I use WordPress for my website?**
-  **Endpoint breach prevention by reducing attack surfaces**
-  **Google offers rewards for techniques that bypass their abuse, fraud, and spam systems**
-  **AT&T sued for enabling SIM swap fraud**
-  **Cloud computing remains top emerging business risk**
-  **eBook: Windows PowerShell Scripting Tutorial**






**SSCP** Systems Security Certified Practitioner  
 An (ISC)² Certification

**THE FUTURE BELONGS TO THOSE WHO PREPARE FOR IT TODAY.**

Achieve more in your IT career with these 9 tips. [>](#)

- [Android Fake ID bug allows malware to impersonate trusted apps](#)
- [Researchers successfully attack Android through device's speaker](#)
- [Continuous monitoring for enterprise incident response](#)

**+ Don't miss**

-  Endpoint breach prevention by reducing attack surfaces
-  Telecom services: Patient zero for email-based attacks?
-  Busting the security myth: Should I use WordPress for my website?
-  New infosec products of the week: August 17, 2018
-  eBook: Windows PowerShell Scripting Tutorial

**SUBSCRIBE TO (IN)SECURE MAGAZINE**

**Newsletters**

Subscribe to get regular updates from Help Net Security. The weekly newsletter contains a selection of the best stories, while the daily newsletter highlights all the latest headlines!

Your email address

Weekly newsletter  Daily newsletter [subscribe](#)