Samsung S6 calls open to man-in-the-middle base station snooping

By Darren Pauli

Published: 2015-11-12 · Archived: 2026-04-05 14:51:57 UTC

PacSec Modern Samsung devices including the S6, S6 Edge and Note 4 can have phone calls intercepted using malicious base stations, according to initial research findings from two researchers.

Daniel Komaromy and Nico Golde demonstrated the attacks on Samsung's 'Shannon' line of baseband chips today at the Mobile Pwn2Own competition at PacSec, Toyko.

Full exploitation details of their research has not been publicly detailed, but it has been disclosed to Samsung.

Their cheap man-in-the-middle attack requires an OpenBTS base station to be established and located near target handsets.

Handsets will automatically connect to the bogus station.

The malicious base station then pushes firmware to the phone's baseband processor (the chip that handles voice calls, and which isn't directly accessible to end users).

The firmware patch pushes phone calls through the bogus base station, which redirects them to a proxy that records them and passes them on to the intended recipient.

Komaromy says the full impact of the attack along with any mitigating factors will be known once seasoned researchers examine their work.

"Our example of modifying the baseband to hijack calls is just an example," Komaromy told *Vulture South*.

"The idea with hijacking would be that you can redirect calls to a proxy (like a SIP proxy) and that way you can man-in-the-middle the call.

"So that means the caller sees her original call connected - but it can be recorded in the proxy [which is how] it's like a wiretap implant."

Nico Golde (l) and Daniel Komaromy at Pwn2Own today. 📷 Drago Ruiu

The attack was tested on a new Samsung Galaxy S6 Edge which PacSec organiser Dragos Ruiu took out of its box and updated before handing it over.

"I turned it on next to their radio and then dialled myself," Ruiu says of the demonstration held deep below the Tokyo conference to avoid pwning delegate phones. "And instead of ringing on my phone it rang on theirs."

The hacker duo now own the phone as a prize and will in March travel to Canada for CanSecWest on a ski trip along with their spouses. They will present further technical detail of the attack at that lauded conference.

It comes as Chinese researcher Guang Gong popped the latest version of Google Chrome at the contest.

As *El Reg* reported, the attack likely affects all Android phones and allows the devices to be completely compromised through a single exploit that requires no interaction beyond visiting a crafted web site.

Ruiu is offering ski trips and vendors may cough up bug bounties in exchange for the winning hacks. Last year hackers hosed popular phones for shares in $425,000 in cash rewards, but security sponsors Google, Apple, Microsoft and Hewlett Packard's Zero Day Initiative pulled out. ®
