Hacker Spoofs Cell Phone Tower to Intercept Calls

By Kim Zetter ✉ July 31, 2010 | 7:57 pm | Categories: Cybersecurity, DefCon, Surveillance

A directional antenna is set up for a demonstration by security researcher Chris Paget, center. (Photo: Dave Bullock)

LAS VEGAS — A security researcher created a cell phone base station that tricks cell phones into routing their outbound calls through his device, allowing someone to intercept even encrypted calls in the clear.

The device tricks the phones into disabling encryption and records call details and content before they're routed on their proper way through voice-over-IP.

The low-cost, home-brewed device, developed by researcher Chris Paget, mimics more expensive devices already used by intelligence and law enforcement agencies – called IMSI catchers – that can capture phone ID data and content. The devices essentially spoof a legitimate GSM tower and entice cell phones to send them data by emitting a signal that's stronger than legitimate towers in the area.

“If you have the ability to deliver a reasonably strong signal, then those around are owned,” Paget said.

Paget’s system costs only about $1,500, as opposed to several hundreds of thousands for professional products. Most of the price is for the laptop he used to operate the system.

Doing this kind of interception “used to be a million dollars, now you can do it with a thousand times less cost,” Paget said during a press conference after his attack. “If it’s $1,500, it’s just beyond the range that people can start buying them for themselves and listening in on their neighbors.”

Paget’s device captures only 2G GSM calls, making AT&T and T-Mobile calls, which use GSM, vulnerable to interception. Paget’s aim was to highlight vulnerabilities in the GSM standard that allows a rogue station to capture calls. GSM is a second-generation technology that is not as secure as 3G technology.

Encrypted calls are not protected from interception because the rogue tower can simply turn it off. Although the GSM specifications say that a phone should pop up a warning when it connects to a station that does not have encryption, SIM cards disable that setting so that alerts are not displayed.

“Even though the GSM spec requires it, this is a deliberate choice on the cell phone makers,” Paget said.

The system captures only outbound calls. Inbound calls would go directly to voicemail during the period that someone’s phone is connected to Paget’s tower.

The device could be used by corporate spies, criminals, or private investigators to intercept private calls of targets.

“Any information that goes across a cell phone you can now intercept,” he said, except data. Professional grade IMSI catchers do capture data transfers, but Paget’s system doesn’t currently do this.

His setup included two RF directional antennas about three feet long to amplify his signal in the large conference room, a laptop and open source software. The system emitted only 25 milliwatts, “a hundred times less than your average cell phone,” he said.

Paget received a call from FCC officials on Friday who raised a list of possible regulations his demonstration might violate. To get around legal concerns, he broadcast on a GSM spectrum for HAM radios, 900Mhz, which is the same frequency used by GSM phones and towers in Europe, thus avoiding possible violations of U.S. regulations.

Just turning on the antennas caused two dozen phones in the room to connect to Paget’s tower. He then set it to spoof an AT&T tower to capture calls from customers of that carrier.

“As far as your cell phones are concerned, I am now indistinguishable from AT&T,” he said. “Every AT&T cell phone in the room will gradually start handing over to my network.”

During the demonstration, only about 30 phones were actually connecting to his tower. Paget says it can take time for phones to find the signal and hand off to the tower, but there are methods for speeding up that process.

To address privacy concerns, he set up the system to deliver a recorded message to anyone who tried to make a call from the room while connected to his tower. The message disclosed that their calls were being recorded. All of the data Paget recorded was saved to a USB stick, which he destroyed after the talk.

Customers of carriers that use GSM could try to protect their calls from being intercepted in this manner by switching their phones to 3G mode if it's an option.

But Paget said he could also capture phones using 3G by sending out jamming noise to block 3G. Phones would then switch to 2G and hook up with his rogue tower. Paget had his jammer and an amplifier on stage but declined to turn them on saying they would "probably knock out all Las Vegas cell phone systems."

Photo: Dave Bullock

Tags: Chris Paget, GSM, Surveillance
Post Comment | Permalink

Also on Wired.com

- Russian Convicted of $9 Million RBS WorldPay Hack Avoids Jail
- Jupiter's Moon Helps Peek Below Planet's Belt
- One Million EVs Is Difficult But Doable
- HP Launches WebOS-Powered Tablet, Phones
- Astronomers Suggest Crowdsourcing Letters to Aliens
- One database to hold them all

Related Topics:

- AT&T Inc.,
- Cellular Phones,
- Chris Paget,
- Consumer Electronics,
- Electronics,
- Science and Technology

Add New Comment

Required: Please login below to comment.

Type your comment here.

Post as ...

Showing 23 comments

Sort by Popular now

Subscribe by email Subscribe by RSS

Real-time updating is **paused**. (Resume)

TechW 6 months ago

Of course everyone knows the government can monitor any calls. That would not be of interest to anyone. What is interesting is the method they came up with to monitor the calls and that basically anyone could do it.

Like Reply

joan666 6 months ago

Today's lesson, forget your cellphone and see Rubicon and write your messages in crossword puzzles. Norad and Ivan plan joint terror Air Defense Exercise this month. Northern 911 part 2? I Hope not.

Like Reply

rajbhai 6 months ago

i want to be a member of ur team

Like Reply

pippers 6 months ago

I'm pretty sure everyone knows this sort of thing is possible. I have no doubt certain agencies can tap into anything they want, whenever they want it.

What the guy demonstrating here, and the real concern is, that this can be done by anyone for almost nothing.

Like Reply

jotorious 6 months ago

yawn....

The only thing interesting about this article is how blissfully unaware most people are about the technologies upon which they rely. And how nobody really cares until they are ones being targeted.

Here's a primer..Your cellphone, when powered, transmits a message saying "I'm Here" that all the towers in the area receive. The towers look up your number in a table and verifiy they you have paid for service. The towers than arbitrate which tower your voice/data calls will go through. The tower that your phone is talking to is then put in a table so that when someone calls you, the cell system knows where you are. While your cell phone is on, the cell system knows to the tower level where you are. While the content of your communications..voice,text, et cetera might be private, courts haven't found that the protocols used by the cell system are "yours" or "private" or "privledged". All of which means that the US Government in cahoots with Verizon can monitor your location, without a warrant, without probable cause, without any finding by any judicial authority anywhere. And basically no-one cares to figure out what authority the Government should have...Is your current location private? Should US surveilance laws be changed so that Telecoms have to protect this sort of information? Are We ok with this intrusion, under the guise of "Keeping America Safe?"

Like Reply

kelarius 6 months ago

So how long is it before someone hacks an AT&T Microcell and just sets that up where they want to intercept calls? All it would take it an internet connection after you hacked the device and setting it up in your locale of choice as im sure the Microcell would have stronger signal strength than the ambient network.

Like Reply

yuyutyty 6 months ago

how could he ONLY use the HAM spectrum with a GSM phone? The up- and the downlink need to be separated by 45MHz. This is not covered by this spectrum.

Like Reply

SaintWaldo 6 months ago

@thousandsun - If he has a HAM license and broadcasts on a HAM freq that _also_ is used by 2G (900MHz like the article says), he's probably in the clear, esp when he goes out of his way to show lack of nefarious intent (in the demo...).

Like Reply

ErinsDad 6 months ago

I would have liked to listen in on the response to that call from the FCC... "So Bite Me...", then a lot of giggles and laughter, then a dial tone.

Like Reply

thousandsun 6 months ago

"Paget received a call from FCC officials on Friday who raised a list of possible regulations his demonstration might violate. To get around legal concerns, he broadcast on a GSM spectrum for HAM radios, 900Mhz, which is the same frequency used by GSM phones and towers in Europe, thus avoiding possible violations of U.S. regulations."

As far as I understand FCC rules, using a signal on any frequency which interferes or emulates a pre-existing signal is a major no-no according to FCC regulations. Can anyone more in the know clarify this for me?

Like Reply

tsport100 6 months ago

Most early Cordless phones used 27 Mhz because it was an unlicensed band and anyone with a CB radio could eavesdrop BFD!

Like Reply

Elfish 6 months ago

Better watch the way you hold that thang, else...

Like Reply

honest_cloud 6 months ago

Tapes of a horny "family values" Republican cheating on his wife in 3...2...1

Like Reply

jasonwalls 6 months ago

Chris: I suspect it's suppose to be switch phone to 3G only. Any attack that would force the phone to 2G would fail in that instance.

Like Reply

AtlPatrick 6 months ago

Heck, it the analog days of cell phones, you could tune an old (60's-70's) television to any channel above 69 and listen to cell phone calls: the FCC expanded cell phone coverage by taking away UHF television channels 70-83. And, in the early era of cell phones (late 80's, early 90's), most radio scanners sold that could receive 800Mhz (Radio Shack, Uniden, etc) were locked from receiving cell phone calls but allowed for an easy fix (cutting a diode, usually) to break the lock.

I'm guessing that you can set at least some 3G cell phones to be 3G only, which would protect you from this hack, but would mean you would be less likely to make/receive calls (either because you are in an area without 3G, or because the 3G system is busy and it wants to route you to a 2G system).

Like Reply

Bruckley 6 months ago

Hackers FTW

Like Reply

delahaya 6 months ago

Maybe I'm wrong, but this is not new. What is new is the low cost of the home-brewed device.

Like Reply

Kim Zetter 6 months ago

@Chris9876 Thanks for pointing that out. I've rearranged the paragraphs and tweaked to fix that confusion.

Like Reply

redPill 6 months ago

CDMA has always offered the best security, and AT&T will either move to a new platform or the CDMA platform within the next two years. T-Mobile will probably be out of business in another year anyways.

Overall, this really doesn't mean much. Yeah, you can listen to conversations all you want, but without any context, it's pretty worthless. Besides, the government already has the technology - so big deal.

Back in the day, you could take an analog Motorola phone and turn it into a scanner with a few easy steps. Yeah, you could listen to people talking on their phones, but after a few minutes, it's gets pretty boring - trust me.

Like Reply

Chris9876 6 months ago

"Customers of carriers that use GSM can protect their calls from being intercepted in this manner by switching their phones to 3G mode if it’s an option."

"Paget said he could also capture phones using 3G by sending out jamming noise to block 3G. Phones would then switch to 2G and hook up with his rogue tower."

Does anyone else see a conflict between these two statements?

Like Reply

elf25s 6 months ago

dollars to donuts i bet that after this major providers will either sue him into submision to get the tech and specs from him. or sue him for exposing their big dirty secret. as for fcc they will try to get him on some charge of violating speectrum on the frequencies he was using to show the demonstration.

now dont get me wrong if anyting this man should be praised for showing how we loose any privicy when on any cell phone and how easly our data can be intercepted that we trust the carriers to keep safe. this man should be rewarded millions.

Like Reply

eliatic 6 months ago

Some really old cordless landlines used medium wave frequencies around 1.7MHz to talk to the base. An AM radio could listen to the calls. But landline phones used hardwired datapaths and had no CPUs. Ownage was 'only' available to Telcos and their friends.

This is orders of magnitude more sophisticated, and I have to laud Paget for having the cajones to reveal to everyone that their comms can be owned by anyone, anywhere, anytime.

Like Reply

Transmeta 6 months ago

“Even though the GSM spec requires it, this is a deliberate choice on the cell phone makers,” Paget said.
While that is his comment, it is not entirely true, it is the choice of the provider who programs the SIM to disable those warnings.
This has also been around for years, maybe even going back to cordless landline phones.

Like Reply

Reactions

nimrody 6 months ago

From Hacker News via BackType

It all depends on the operator. A UMTS (3G) network can accept users using a GSM SIM if the operator allows it.Authentication is performed by the network HLR (Home location register) which is independent of the radio technology used. The procedure/algorithms are different for 3G-capable UEs with USIM, but the HLR can accept 2G users as well. Bottom line is that if your 'home carrier' (the one that produced the SIM) allows it, you can use your SIM in any 3G network that is part of the roaming agreement of that carrier.

mctavjb9 6 months ago

From Hacker News via BackType

This demonstration is neither particularly novel nor particularly legal.http://laforge.gnumonks.org/weblog/2010/08/01/#20100801-on_r...

tudorw 6 months ago

From Hacker News via BackType

As I had not seen this mentioned here or in article; You can read more about Chris's work here, http://www.tombom.co.uk/blog/ and I would have posted the 'OpenBTS on Droid' a while back if I'd known it was a 'scoop' :) My thoughts were of some kind of shared cellular access point that could be used in the developing world to give access to a sub-let access point with a 'real' connection.

grogers 6 months ago

From Hacker News via BackType

Most phones do issue a warning if ciphering isn't enabled. On some you may be able to force it to require it. But keep in mind that this is only applied on the radio interface anyways (and GSM encryption is so broken you shouldn't be relying on it anyways). If you want end to end encryption of your calls you will need to use encrypted VOIP over your data connection.

grogers 6 months ago

From Hacker News via BackType

I know there are several conversion functions for a USIM to be able to authenticate on a 2G network, but I didn't think it was possible for a 2G SIM to register on a 3G network. Can you explain this more thoroughly?

friendlyhacker 6 months ago

From Hacker News via BackType

http://webcache.googleusercontent.com/search?q=cache:VArK7Jz...

bnchdrff 6 months ago

From Hacker News via BackType

in WEP's case, your AP would receive an auth response encrypted with the keyphrase... you'd have to get quite a few of these to deduce the password, in general. people find it easier to just sniff traffic and deduce the key from all the traffic generated from someone downloading crap.i don't think this is at all realistic with wpa. you could just set up an open network with an equivalent essid, but that's nothing new is it? :)

lt 6 months ago

From Hacker News via BackType

Can a similar, simpler method be used to steal WEP/WPA passwords?Set up a wireless AP broadcasting an existing SSID. Some existing clients connect to it passing the keyphrase. Verify against the actual AP. Would this work?

Jim Bergman 6 months ago

From Friendfeed via BackType

You can do this type of intercept with unsecured wifi also. I hope cell companies will tighten security for calls. Makes me want to always use a VPN for cell data.

mkramlich 6 months ago

From Hacker News via BackType

> I'm just waiting for the first fully autonomous weapon which combines signals intelligence and killing -- flies around listening for a specific IMSI, then drops down on the target and blows up.The road to Skynet is paved with these kind of desires.

Show more reactions