# Hacker builds $1,500 cell-phone tapping device

August 1 2010, By JORDAN ROBERTSON , AP Technology Writer

In this July 30, 2010 photo, hacker Chris Paget sets up a long range RFID reading device at the DefCon hacker conference in Las Vegas. (AP Photo/Isaac Brekken)

(AP) -- A computer security researcher has built a device for just $1,500 that can intercept some kinds of cell phone calls and record everything that's said.

The attack Chris Paget showed Saturday illustrates weaknesses in GSM, one of the world's most widely used cellular communications technologies.

His attack was benign; he showed how he could intercept a few dozen calls made by fellow hackers in the audience for his talk at the DefCon conference here. But it illustrates that criminals could do the same thing

for malicious purposes, and that consumers have few options for protecting themselves.

Paget said he hopes his research helps spur adoption of newer communications standards that are more secure.

"GSM is broken - it's just plain broken," he said.

GSM is considered 2G, or "second generation," cellular technology. Phones that run on the newer 3G and 4G standards aren't vulnerable to his attack.

If you're using an iPhone or other smart phone and the screen shows that your call is going over a 3G network, for example, you are protected. BlackBerry phones apply encryption to calls that foil the attack, Paget pointed out. But if you're using a type of phone that doesn't specify which type of network it uses, those phones are often vulnerable, Paget said.

Paget's device tricks nearby cell phones into believing it is a legitimate cell phone tower and routing their calls through it. Paget uses Internet-based calling technology to complete the calls and log everything that's said.

A caveat is that recipients see numbers on their Caller IDs that are different than the cell numbers of the people calling them. Paget claims it would be easy to upgrade the software to also include the callers' real numbers.

The device he built is called an "IMSI catcher," which refers to the unique International Mobile Subscriber Identity numbers that phones use to identify themselves to cellular networks.

Commercial versions of such devices have existed for decades and have mainly been used by law enforcement. Paget's work shows how cheaply hobbyists can make the devices using equipment found on the Internet.

"That's a significant change for research - it's a major breakthrough for everyone," said Don Bailey, a GSM expert with iSec Partners who wasn't involved in Paget's research.

Another security expert, Nicholas DePetrillo, said such devices haven't been built as cheaply in the past because the hardware makers have closely controlled who they sell to. Only recently has the necessary equipment become available cheaply online.

In the U.S., AT&T Inc. and T-Mobile USA are two cellular operators whose networks include GSM.

There are more than 3 billion GSM users and the technology is used in nearly three quarters of the world's cell phone markets, according to the GSM Association, an industry trade group.

In a statement, the group emphasized the hurdles to launching an attack like Paget's, such as the fact an attacker's base station would need to be physically close to the target and that only outgoing calls can be intercepted. Incoming calls are not vulnerable.

"The overall advice for GSM calls and fixed-line calls is the same: neither has ever offered a guarantee of secure communications," the group said. "The great majority of users will make calls with no reason to fear that anyone might be listening. However, users with especially high security requirements should consider adding extra, end-to-end security features over the top of both their fixed line calls and their mobile calls."

A representatives for AT&T had no comment. T-Mobile didn't immediately respond to e-mails Saturday from The Associated Press.

Paget had been debating dropping the demonstration from his talk, after federal authorities told him it might violate wiretapping laws. He went ahead with it after conferring with lawyers. He said he didn't believe he had broken any laws.