Author: Andy Greenberg. Andy Greenberg Security

Date of Publication: 07.29.15. 07.29.15 Time of Publication: 7:00 am. 7:00 am

Hackers Can Disable a Sniper Rifle—Or Change Its Target

Put a computer on a sniper rifle, and it can turn the most amateur shooter into a world-class marksman. But add a wireless connection to that computer-aided weapon, and you may find that your smart gun suddenly seems to have a mind of its own—and a very different idea of the target.



Click to Open Overlay GallerySecurity researchers Runa Sandvik, left, and husband Michael Auger have figured out how to hack into a Tracking Point TP750 rifle to disable it or control the trajectory of its bullets. Greg Kahn for WIRED

At the Black Hat hacker conference in two weeks, security researchers Runa Sandvik and Michael Auger plan to present the results of a year of work hacking a pair of $13,000 TrackingPoint self-aiming rifles. The married hacker couple have developed a set of techniques that could allow an attacker to compromise the rifle via its Wi-Fi connection and exploit vulnerabilities in its software. Their tricks can change variables in the scope's calculations that make the rifle inexplicably miss its target, permanently disable the scope's computer, or even prevent the gun from firing. In a demonstration for WIRED (shown in the video above), the researchers were able to dial in their changes to the scope's targeting system so precisely that they could cause a bullet to hit a bullseye of the hacker's choosing rather than the one chosen by the shooter.

"You can make it lie constantly to the user so they'll always miss their shot," says Sandvik, a former developer for the anonymity software Tor. Or the attacker can just as easily lock out the user or erase the gun's entire file system. "If the scope is bricked, you have a six to seven thousand dollar computer you can't use on top of a rifle that you still have to aim yourself."



Click to Open Overlay GallerySandvik and Auger got their hands on two of the $13,000 TP750 rifles, and dissected this one to access its circuit board and reverse engineer its software. Greg Kahn for WIRED

Since TrackingPoint launched in 2011, the company has sold more than a thousand of its high-end, Linux-power rifles with a self-aiming system. The scope allows you to designate a target and dial in variables like wind, temperature, and the weight of the ammunition being fired. Then, after the trigger is pulled, the computerized rifle itself chooses the exact moment to fire, activating its firing pin only when its barrel is perfectly oriented to hit the target. The result is a weapon that can allow even a gun novice to reliably hit targets from as far as a mile away.

But Sandvik and Auger found that they could use a chain of vulnerabilities in the rifle's software to take control of those self-aiming functions. The first of these has to do with the Wi-Fi, which is off by default, but can be enabled so you can do things like stream a video of your shot to a laptop or iPad. When the Wi-Fi is on, the gun's network has a default password that allows anyone within Wi-Fi range to connect to it. From there, a hacker can treat the gun as a server and access APIs to alter key variables in its targeting application. (The hacker pair were only able to find those changeable variables by dissecting one of the two rifles they worked with, using an eMMC reader to copy data from the computer's flash storage with wires they clipped onto its circuit board pins.)



Click to Open Overlay GalleryThough the rifle's scope seemed to be pointed at the target on the right, the researchers were able to make it hit the bullseye on the left instead. Greg Kahn for WIRED

In the video demonstration for WIRED at a West Virginia firing range, Auger first took a shot with the unaltered rifle and, using the TrackingPoint rifle's aiming mechanism, hit a bullseye on his first attempt. Then, with a laptop connected to the rifle via Wi-Fi, Sandvik invisibly altered the variable in the rifle's ballistic calculations that accounted for the ammunition's weight, changing it from around .4 ounces to a ludicrous 72 pounds. "You can set it to whatever crazy value you want and it will happily accept it," says Sandvik.

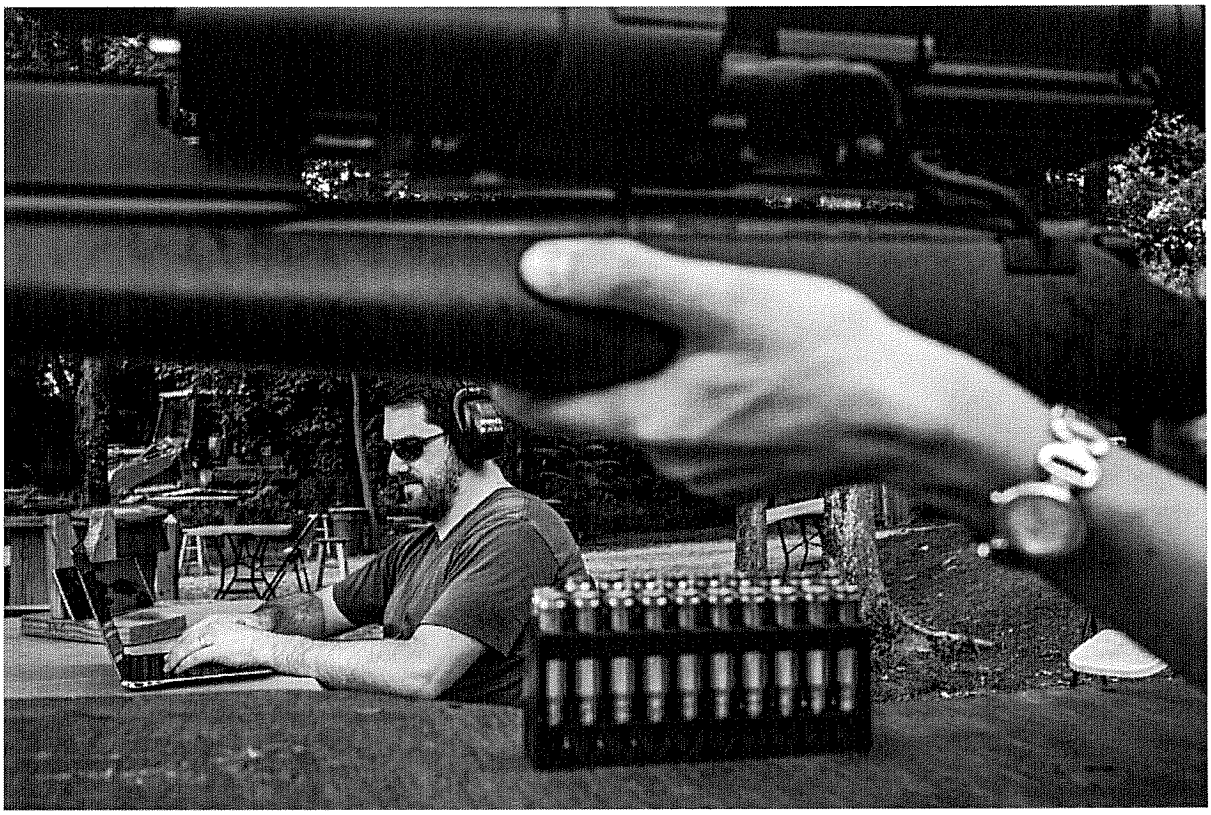
Sandvik and Auger haven't figured out why, but they've observed that higher ammunition weights aim a shot to the left, while lower or negative values aim it to the right. So on Auger's next shot, Sandvik's change of that single number in the rifle's software made the bullet fly 2.5-feet to the left, bullseyeing an entirely different target.

The only alert a shooter might have to that hack would be a sudden jump in the scope's view as it shifts position. But that change in view is almost indistinguishable from jostling the rifle. "Depending on how good a shooter you are, you might chalk that up to 'I bumped it,'" says Sandvik.

The two hackers' wireless control of the rifle doesn't end there. Sandvik and Auger found that through the Wi-Fi connection, an attacker could also add themselves as a "root" user on the device, taking full control of its software, making permanent changes to its targeting variables, or deleting files to render the scope inoperable. If a user has set a PIN to limit other users' access to the gun, that root attack can nonetheless gain full access and lock out the gun's owner with a new PIN. The attacker can even disable the firing pin, a computer controlled solenoid, to prevent the gun from firing.

One thing their attack can't do, the two researchers point out, is cause the gun to fire unexpectedly. Thankfully TrackingPoint rifles are designed not to fire unless the trigger is manually pulled.

In a phone call with WIRED, TrackingPoint founder John McHale said that he appreciates Sandvik and Auger's research, and that the company will work with them to develop a software update to patch the rifle's hackable flaws as quickly as possible. When it's ready, that update will be mailed out to customers as a USB drive, he said. But he argued that the software vulnerabilities don't fundamentally change the gun's safety. "The shooter's got to pull the rifle's trigger, and the shooter is responsible for making sure it's pointed in a safe direction. It's my responsibility to make sure my scope is pointed where my gun is pointing," McHale says. "The fundamentals of shooting don't change even if the gun is hacked."



Click to Open Overlay GalleryRuna Sandvik fires a round from a Tracking Point TP750 rifle at a target 50 yards away as husband and fellow security researcher Michael Auger uses a laptop to hack into the rifle's Wi-Fi, changing the angle of its shot. Greg Kahn for WIRED

He also pointed out that the Wi-Fi range of the hack would limit its real-world use. "It's highly unlikely when a hunter is on a ranch in Texas, or on the plains of the Serengeti in Africa, that there's a Wi-Fi internet connection," he says. "The probability of someone hiding nearby in the bush in Tanzania are very low."

But Auger and Sandvik counter that with their attack, a hacker could alter the rifle in a way that would persist long after that Wi-Fi connection is broken. It's even possible (although likely difficult), they suggest, to implant the gun with malware that would only take effect at a certain time or location based on querying a user's connected phone.

In fact, Auger and Sandvik have been attempting to contact TrackingPoint to help the company patch its rifles' security flaws for months, emailing the company without response. The company's silence until WIRED's inquiry may be due to its financial problems: Over the last year, TrackingPoint has laid off the majority of its staff, switched CEOs and even ceased to take new orders for rifles. McHale insists that the company hasn't gone out of business, though it's "working through an internal restructuring."



Click to Open Overlay GalleryA view through the scope of the Tracking Point TP750. Greg Kahn for WIRED

Given TrackingPoint's financial straits, Sandvik and Auger say they won't release the full code for their exploit for fear that the company won't have the manpower to fix its software. And with only a thousand vulnerable rifles in consumers' hands and the hack's limited range, it may be unlikely that anyone will actually be victimized by the attack.

But the rifles' flaws signal a future where objects of all kinds are increasingly connected to the Internet and are vulnerable to hackers—including lethal weapons. "There are so many things with the Internet attached to them: cars, fridges, coffee machines, and now guns," says Sandvik. "There's a message here for TrackingPoint and other companies...when you put technology on items that haven't had it before, you run into security challenges you haven't thought about before."