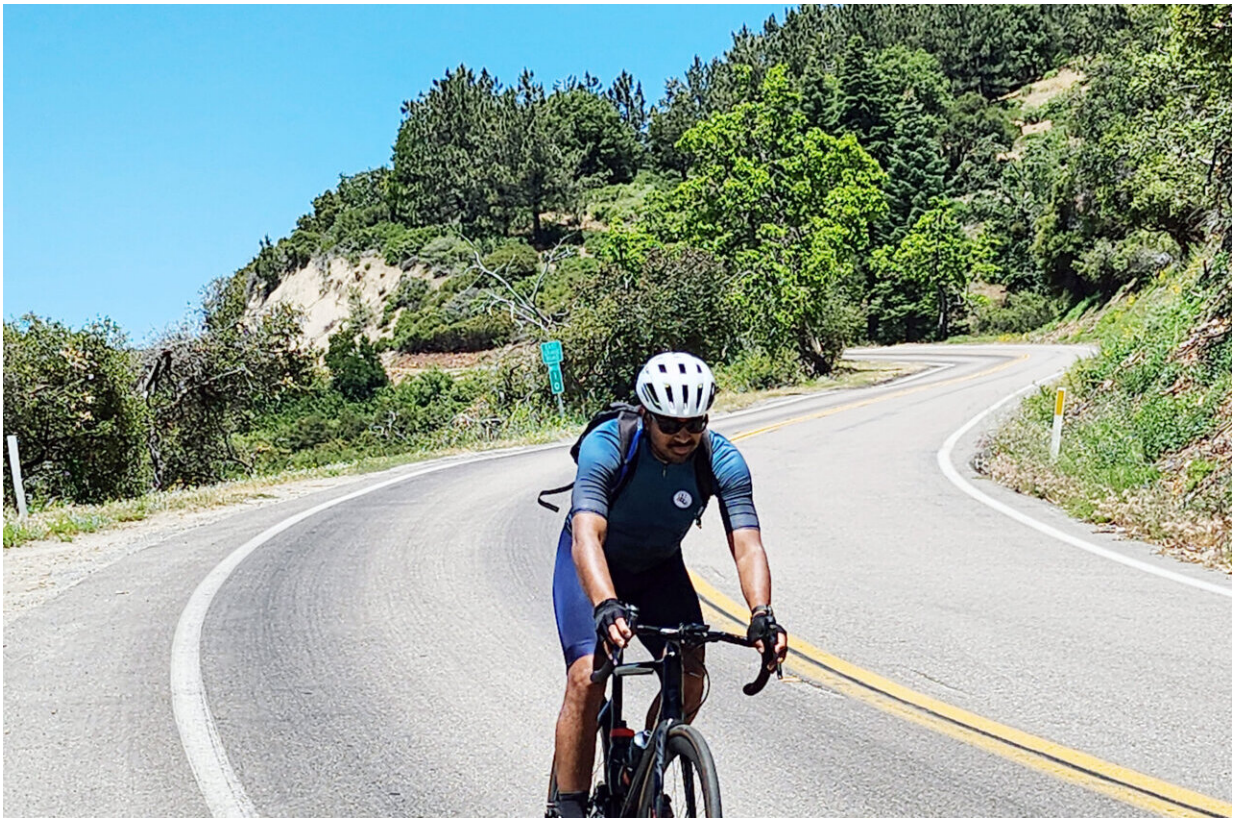
Cybersecurity flaws could derail high-profile cycling races

August 14 2024



Earlence Fernandes, one of the paper's lead co-authors and a computer scientist at the University of Califonria San Diego, is a biking enthusiast. He is pictured here during a recent trip to Catalina Island. Credit: Earlence Fernandes/University of California San Diego

High-end bicycles used for high-profile road races such as the Tour de

France are vulnerable to cybersecurity attacks targeting the bike's wireless gear shifting system.

In recent years, bicycle manufacturers have adopted wireless gear-shifting technology, which gives riders better control over changing gears. The technology is not vulnerable to the physical issues that plague mechanical systems. However, the way the wireless systems were built created critical cybersecurity vulnerabilities, which a team of computer scientists from the University of California San Diego and Northeastern University have uncovered.

"Security vulnerabilities in wireless gear-shifting systems can critically impact rider safety and performance, particularly in professional bike races," the researchers write. "In these races, attackers could exploit these weaknesses to gain an unfair advantage, potentially causing crashes or injuries by manipulating gear shifts or jamming the shifting operation."

The researchers are now working with Shimano, one of the leading bicycle component manufacturers, to patch the vulnerabilities. They focused on Shimano because the company has the largest market share for wireless gear shifters. Researchers will present their work at the 18th USENIX WOOT Conference, which will be held on August 12 and 13 in Philadelphia.

The gear shifting system works by deploying wireless links between the gear shifters controlled by the riders and the device that moves chains between gears on the bike, called a derailleur.

The team uncovered three key vulnerabilities within this wireless system:

1. Attackers can record and retransmit gear-shifting commands, allowing them to control gear-shifting on the bike without the

need for authentication via cryptographic keys. The research team successfully conducted record and replay attacks from a distance of up to 10 meters (roughly 10 yards) using off the shelf devices known as software-defined radios, without needing an amplifier to boost signal strength. Recorded data could be reused anytime, provided the bike components remain paired.

2. Attackers can also easily disable and jam gear shifting on a specific bike without affecting nearby systems, creating significant risks for riders.
3. The wireless system used a communication protocol, ANT+, which leaks information, allowing attackers to monitor what their target is doing in real-time.

"The history of professional cycling's struggles with illegal performance-enhancing drugs underscores the appeal of such undetectable attacks, which could similarly compromise the sport's integrity. Given these risks, it is essential to adopt an adversary's viewpoint and ensure that this technology can withstand motivated attackers in the highly competitive environment of professional cycling," researchers add.

Researchers developed several countermeasures to prevent replay attacks, mitigate targeted jamming, and prevent information leakage. Shimano has already implemented some of these measures and a new update will make them widely available soon.

More information: Motallebighomi et al. MakeShift: Security Analysis of Shimano Di2 Wireless Gear Shifting in Bicycles (2024). www.usenix.org/conference/woot … ation/motallebighomi

Provided by University of California - San Diego