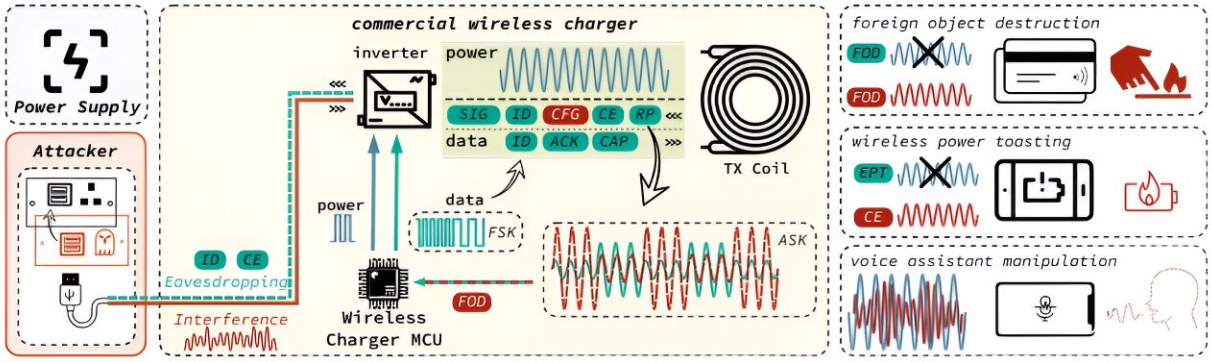
A type of cyberattack that could set your smartphone on fire using its wireless charger

February 23 2024, by Bob Yirka



Attack overview: A victim uses Commercial-Off-The-Shelf Qi-compatible wireless chargers and power receivers. An intermediary-connected attacking device on the power adapter manipulates the output voltage and current to: 1) manipulate the magnetic field to interfere with the charged device. 2) interactively communicate with the charger and control the charging process. This setup enables foreign object destruction, wireless power toasting, and voice assistant manipulation attacks. Credit: *arXiv* (2024). DOI: 10.48550/arxiv.2402.11423

A team of security experts at the University of Florida working with security audit company CertiK has found that a certain class of cyberattacks could cause a smartphone to catch fire via its wireless charger. The team has posted a paper describing their research and results on the *arXiv* preprint server.

Inductive chargers are devices that can be used to charge a smartphone or other device without the need for plugging in a cable. Such devices work by making use of electromagnetic fields to transfer energy from one device to another through induction. In order for a smartphone to be charged properly on such a device, it must communicate with the charger through a Qi communication-based feedback control system. And in order for a wireless charger to work, it must be connected to an AC outlet.

But the charger, like a phone, cannot plug directly into the wall; it plugs instead into an adapter. And this, the researchers suggest, is where the system's vulnerabilities lie. They have found through testing that by attaching an intermediary device to the adapter, disruptions can be made to the Qi communication-based feedback control system, resulting in signals that can override controls that stop overcharging, which can lead to overheating, and in some cases a fire. They call such an attack a "VoltSchemer."

The research team has come up with three types of attacks that can occur with a VoltSchemer. According to the researchers, "A charger can be manipulated to control voice assistants via inaudible voice commands, damage devices being charged through overcharging or overheating, and bypass Qi-standard specified foreign-object-detection mechanism to damage valuable items exposed to intense magnetic fields."

The researchers tested multiple types of wireless chargers and phones and found they were all vulnerable. They have notified manufacturers and expect that changes will be made to overcome these vulnerabilities to protect consumers from VoltSchemer attacks.

More information: Zihao Zhan et al, VoltSchemer: Use Voltage Noise to Manipulate Your Wireless Charger, *arXiv* (2024). DOI: 10.48550/arxiv.2402.11423