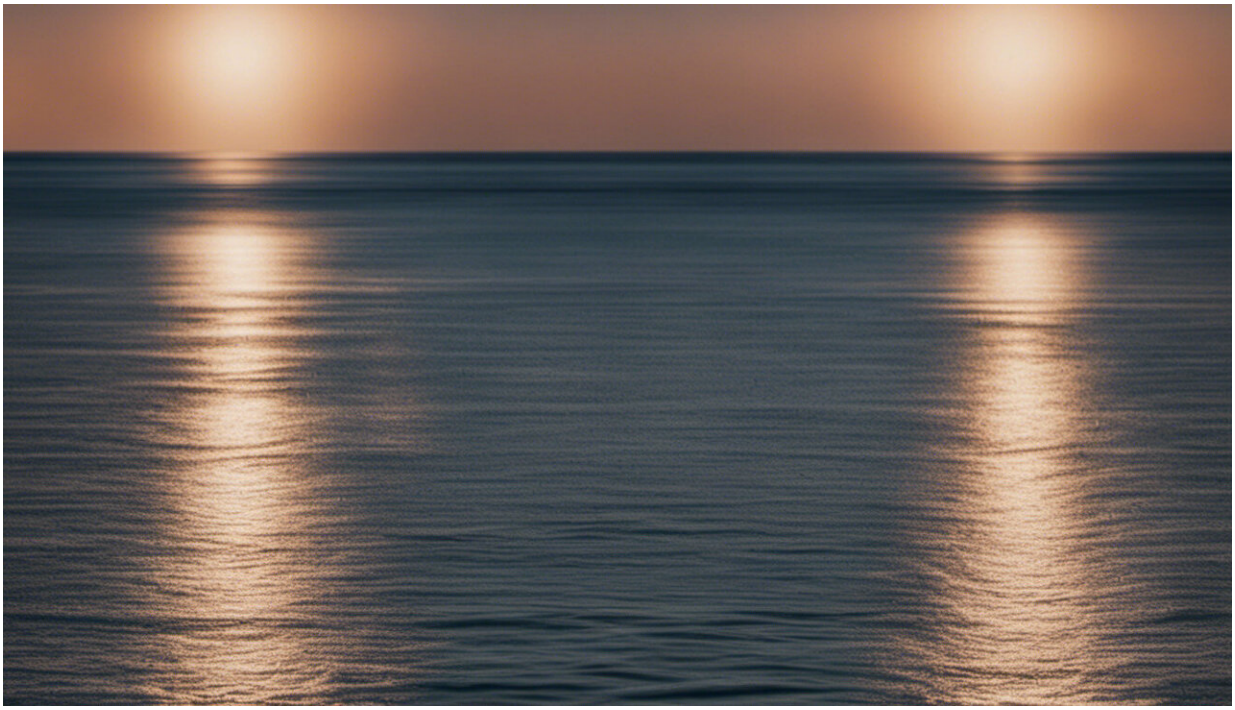
Security and the Internet of Things

November 18 2014, by Temitope Oluwafemi



Credit: AI-generated image (disclaimer)

An ever-increasing number of our consumer electronics is internet-connected. We're living at the dawn of the age of the Internet of Things. Appliances ranging from light switches and door locks, to cars and medical devices boast connectivity in addition to basic functionality.

The convenience can't be beat. But what are the security and privacy implications? Is a patient implanted with a remotely-controllable

pacemaker at risk for security compromise? Vice President Dick Cheney's doctors worried enough about an assassination attempt via implant that they disabled his defibrillator's wireless capability. Should we expect capital crimes via hacked internet-enabled devices? Could hackers mount large-scale terrorist attacks? Our research suggests these scenarios are within reason.

Your car, out of your control

Modern cars are one of the most connected products consumers interact with today. Many of a vehicle's fundamental building blocks – including the engine and brake control modules – are now electronically controlled. Newer cars also support long-range wireless connections via cellular network and Wi-Fi. But hi-tech definitely doesn't mean highly secure.

Our group of security researchers at the University of Washington was able to remotely compromise and control a highly-computerized vehicle. They invaded the privacy of vehicle occupants by listening in on their conversations. Even more worrisome, they remotely disabled brake and lighting systems and brought the car to a complete stop on a simulated major highway. By exploiting vulnerabilities in critical modules, including the brake systems and engine control, along with in radio and telematics components, our group completely overrode the driver's control of the vehicle. The safety implications are obvious.

This attack raises important questions about how much manufacturers and consumers are willing to sacrifice security and privacy for increased functionality and convenience. Car companies are starting to take these threats seriously, appointing cybersecurity executives. But for the most part, automakers appear to be playing catchup, dealing with security as an afterthought of the design process.

Home insecurity

An increasing number of devices around the home are automated and connected to the internet. Many rely on a proprietary wireless communications protocol called Z-Wave.

Two UK researchers exploited security loopholes in Z-Wave's cryptographic libraries - that's the software toolkit that authenticates any device being connected to the home network, among other functions, while providing communication security over the internet. The researchers were able to compromise home automation controllers and remotely-controlled appliances including door locks and alarm systems. Z-Wave's security relied solely on keeping the algorithm a secret from the public, but the researchers were able to reverse engineer the protocol to find weak spots.

Our group was able to compromise Z-Wave controllers via another vulnerability: their web interfaces. Via the web, we could control all home appliances connected to the Z-Wave controller, showing that a hacker could, for instance, turn off the heat in wintertime or watch inhabitants via webcam feeds. We also demonstrated an inherent danger in connecting compact fluorescent lamps (CFL) to a Z-Wave dimmer. These bulbs were not designed with remote manipulations over the internet in mind. We found an attacker could send unique signals to CFLs that would burn them out, emitting sparks that could potentially result in house fires.

Our group also pondered the possibility of a large-scale terrorist attack. The threat model assumes that home automation becomes so ubiquitous that it's a standard feature installed in homes by developers. An attacker could exploit a vulnerability in the automation controllers to turn on power-hungry devices - like HVAC systems - in an entire neighborhood at the same time. With the A/C roaring in every single house, shared

power transformers would be overloaded and whole neighborhoods could be knocked off the power grid.

Harnessing hackers' knowledge

One of the best practices of designing elegant security solutions is to enlist the help of the security community to find and report weak spots otherwise undetected by the manufacturer. If the internal cryptographic libraries these devices use to obfuscate and recover data, amongst other tasks, are open-source, they can be vetted by the security community. Once issues are found, updates can be pushed to resolve them. Crypto libraries implemented from scratch may be riddled with bugs that the security community would likely find and fix – hopefully before the bad guys find and exploit. Unfortunately, this sound principle has not been strictly adhered to in the world of the Internet of Things.

Third party vendors designed the web interfaces and home appliances with Z-Wave support that our group exploited. We found that, even if a manufacturer has done a very good job and released a secure product, retailers who repackage it with added functionality - like third party software - could introduce vulnerabilities. The end-user can also compromise security by failing to operate the product properly. That's why robust multi-layered security solutions are vital – so a breach can be limited to just a single component, rather than a successful hack into one component compromising the whole system.

Level of risk

There is one Internet of Things security loophole that law enforcement has taken notice of: thieves' use of scanner boxes that mimic the signals sent out by remote key fobs to break into cars. The other attacks I've described are feasible, but haven't made any headlines yet. Risks today

remain low for a variety of reasons. Home automation system attacks at this point appear to be very targeted in nature. Perpetrating them on a neighborhood-wide scale could be a very expensive task for the hacker, thereby decreasing the likelihood of it occurring.

There needs to be a concerted effort to improve security of future devices. Researchers, manufacturers and end users need to be aware that privacy, health and safety can be compromised by increased connectivity. Benefits in convenience must be balanced with security and privacy costs as the Internet of Things continues to infiltrate our personal spaces.

This story is published courtesy of The Conversation *(under Creative Commons-Attribution/No derivatives).*

Source: The Conversation