

Secure Home Gateway – CIRA Labs Innovation At Work

As the Internet of Things (IoT) continues on its upward growth trajectory, security remains a major concern for businesses, governments, consumers, and IoT vendors. Today, the large number of poorly secured IoT devices on the market poses significant risks to consumers. Attackers can steal private data, send spam, and introduce destructive malware into their home networks by exploiting security vulnerabilities in these devices.

These vulnerabilities can have even greater consequences for the Internet at large. Millions of common IoT devices can be weaponized and used to launch crippling distributed denial of service (DDoS) attacks on corporate, media and consumers sites, as was the case with the Mirai attack in 2016.

But it's not only consumers who are vulnerable. IoT vendors who fail to properly secure their products face their own risks, including negative PR, lost sales and declining revenue. On the other hand, IoT vendors who offer strong protection from cyber threats have an opportunity to create differentiation for their products in a fast-growing and increasingly lucrative market.

Recognizing the lack of a standard security framework for home networks, CIRA Labs has developed a new functional prototype to protect consumers—and the Internet—from the rise of IoT-based cyberattacks. Called the Secure Home Gateway project, this prototype is intended to address the numerous security limitations of home gateway products and IoT solutions currently available on the market.