Security in IOT

Concerns have been raised that the Internet of things is being developed rapidly without appropriate consideration of the profound security challenges involved and the regulatory changes that might be necessary.

Most of the technical security issues are similar to those of conventional servers, workstations and smartphones, but the firewall, security update and anti-malware systems used for those are generally unsuitable for the much smaller, less capable, IoT devices.

According to the Business Insider Intelligence Survey conducted in the last quarter of 2014, 39% of the respondents said that security is the biggest concern in adopting Internet of things technology.

In particular, as the Internet of things spreads widely, cyber attacks are likely to become an increasingly physical (rather than simply virtual) threat.

In a January 2014 article in *Forbes*, cyber-security columnist Joseph Steinberg listed many Internet-connected appliances that can already "spy on people in their own homes" including televisions, kitchen appliances, cameras, and thermostats.

Computer-controlled devices in automobiles such as brakes, engine, locks, hood and trunk releases, horn, heat, and dashboard have been shown to be vulnerable to attackers who have access to the on-board network.

In some cases, vehicle computer systems are Internet-connected, allowing them to be exploited remotely. By 2008 security researchers had shown the ability to remotely control pacemakers without authority.

Later hackers demonstrated remote control of insulin pumps and implantable cardioverter defibrillators.

David Pogue wrote that some recently published reports about hackers remotely controlling certain functions of automobiles were not as serious as one might otherwise guess because of various mitigating circumstances; such as the bug that allowed the hack having been fixed before the report was published, or that the hack required security researchers having physical access to the car prior to the hack to prepare for it.

The U.S. National Intelligence Council in an unclassified report maintains that it would be hard to deny "access to networks of sensors and remotely-controlled objects by enemies of the United States, criminals, and mischief makers...

An open market for aggregated sensor data could serve the interests of commerce and security no less than it helps criminals and spies identify vulnerable targets.

Thus, massively parallel sensor fusion may undermine social cohesion, if it proves to be fundamentally incompatible with Fourth-Amendment guarantees against unreasonable search.

In general, the intelligence community views the Internet of things as a rich source of data

As a response to increasing concerns over security, the Internet of Things Security Foundation (IoTSF) was launched on 23 September 2015.

IoTSF has a mission to secure the Internet of things by promoting knowledge and best practice.

Its founding board is made from technology providers and telecommunications companies including BT, Vodafone, Imagination Technologies and Pen Test Partners.

In addition, large IT companies are continuously developing innovative solutions to ensure the security for IoT devices.

As per the estimates from KBV Research, the overall IoT security market would grow at 27.9% rate during 2016–2022 as a result of growing infrastructural concerns and diversified usage of Internet of things.

In 2016, a distributed denial of service attack powered by Internet of things devices running the Mirai malware took down a DNS provider and major web sites. In May 2017, Junade Ali, a Computer Scientist at Cloudflare noted that native DDoS vulnerabilities exist in IoT devices due to a poor implementation of the Publish–subscribe pattern.

While security is a concern there are many things being done to protect devices.

Device data is following cryptographic standards and encryption is being used in end-to-end scenarios.

To help with this scenario x.509 certificates are also being used to verify device identity.

Security experts view Internet of things as a threat to the traditional Internet.

Some argue that market incentive to secure IoT devices is insufficient and increased governmental regulation is necessary to make the Internet of things secure.

The overall understanding of IoT is essential for basic user security. Keeping up with current anti virus software and patching updates will help mitigate cyber attacks.