Literature Survey

A Survey on Layer-Wise Security Attacks in IoT: Attacks,

Countermeasures, and Open-Issues

Team:030\_

Surveyor: Alfred Augustine

There lie a variety of modern implementations of IOT, from currently implemented household models, to industry standard machining models, highly secure military applications and wide range surveying devices.

The wide range of applications as well as diversity of use cases has led to multiple types of protocol and security methodologies implemented.

This however has led to depreciative returns on proprietary security technologies implemented within them. Most of today’s PC cybersecurity protocols rely on the effort of crowd testing to guarantee safety.

IOT technologies being wide and varied, therefore, leave large loopholes when they choose to implement untested technologies.

*“IoT and WSN pose some inherent properties of conventional wireless communication and have several exclusive features. That means that the security requirements for*

*IoT and WSN circumscribe both traditional wireless network and sensor network requirements.*

” (3.1,P1)

The surveyed paper(P1) tests general IOT networks, especially those prone to security weaknesses, WSN(Wireless Sensor Networks).

Network architecture for IOT devices is implemented in a 5 stack layer, unlike the OSI model, here, each layer comes with a layer of compromise which requires devices to work against the same.

There exist a number of listed, general fall-throughs of IOT network which this paper documents.

Apart from this the generic physical, link, network, transport and application protocols have been summarized along with their use-cases.

Many pre-existing as well as recently discovered weaknesses and flaws with current systems, only manage to stay on with IOT devices, this is well documented by the paper.

The highlighted paper finally gives a comparative analysis it tests on ContikiOS against a variety of test cases.(6,P1)

P1: <https://www.researchgate.net/publication/332269060_A_Survey_on_Layer-Wise_Security_Attacks_in_IoT_Attacks_Countermeasures_and_Open-Issues>