**Annotated Bibliography**

Klaus, Schwab, “The Fourth Industrial Revolution: what it means, how to respond” (14/1/2016) [Online] Available at:<https://www.weforum.org/agenda/2016/01/the-fourth-industrial-revolution-what-it-means-and-how-to-respond/>

[Accessed October 2016].

* Background on subject of IOT
* Outlines fourth industrial revolution
* Recognises need for security
* Documents new opportunity possible with IOT

Oxford Dictionary, “Internet of Things” [Online] Available at:

<https://en.oxforddictionaries.com/definition/internet\_of\_things>

[Accessed September 2016].

* IOT definition

Greenough, John, “The 'Internet of Things' Will Be the World's Most Massive Device Market and Save Companies Billions of Dollars” (18/11/2014) [Online] Available at:

<http://uk.businessinsider.com/how-the-internet-of-things-market-will-grow-2014-10?r=US&IR=T>

[Accessed October 2016].

* Business and marketing statistics on IOT
* Growth rate of devices predictions
* Financial statistics of growth
* Business sector information and predictions

Gartner Inc., “Gartner Says 4.9 Billion Connected “Things” Will Be in Use in 2015” (11/11/2014) [Online] Available at:

<https://www.gartner.com/newsroom/id/2905717>

[Accessed September 2016].

* Main reference for device predictions
* 2020 statistics
* Categorised statistics of business sectors
* Industry perspective
* Consumer perspective
* Mainly introduction/ background

SpiceWorks IT, “2016 IoT Tends: The Devices have Landed, How IT and IoT are learning to peacefully coexist” (2016) [Online] Available at:

<https://www.spiceworks.com/marketing/reports/iot-trends/#section-0>

[Accessed October 2016].

* Marketing information
* Privacy concerns
* Wearable technologies statistics
* Survey of security concerns

Munford, Monty, BBC News – “Could your ‘smart’ home be a weapon of destruction?” (28/10/2016) [Online] Available at:

<http://www.bbc.co.uk/news/business-37776964>

[Accessed November 2016].

* Smart home context
* Consumer context
* Media context

Albrechtx Katherine, McIntyre Liz, “Privacy Nightmare: When Baby Monitors Go Bad” (16/9/2016) [Online] Available at:

<http://ieeexplore.ieee.org/document/7270426/?arnumber=7270426>

[Accessed November 2016].

* Baby monitor – **case study**
* Relatable to security camera
* Weak paswords

Lee, Dave, BBC News – “'Smart' home devices used as weapons in website attack” (22/10/2016) [Online] Available at:

<http://www.bbc.co.uk/news/technology-37738823>

[Accessed October 2016].

* Smart home context
* Media context
* Consumer context
* Example of large scale attack using compromised IOT devices.
* Highlights consumer need for security as well as industry

Hewlett-Packard (29/7/2014) [Online] Available at:

<http://www8.hp.com/us/en/hp-news/press-release.html?id=1744676#.WB\_RU-GLThM>

[Accessed September 2016].

* IOT device security statistics
* **Case study of techniques**
  + Password security
  + Encryption
  + Granular access permissions
  + Cloud components
  + Mobile components
  + Web interfaces
  + Software protection
* Revenue statistics

Stanford University – “Secure Internet of Things Project” Available at:

<http://iot.stanford.edu/people.html>

[Accessed November 2016].

* Professional option
* Background

Gubbi, J., Buyya, R., Marusic, S. and Palaniswami, M. ‘Internet of things (IoT): A vision, architectural elements, and future directions’(24/2/2013) [Online] Available at:

<http://www.sciencedirect.com/science/article/pii/S0167739X13000241>

[Accessed October 2016].

* Future directions of IOT
* Security considerations
* Architectural elements

Bradley, Tony, “Study: 7 in 10 concerned about security of Internet-of-Things” (23/6/2014) [Online] Available at:

<http://www.pcworld.com/article/2366165/7-in-10-concerned-about-security-of-internet-of-things.html>

[Accessed November 2016].

* Opionin poll of security concern
* “professional opinion” arguments
* Statistics
* Relation to china products

OWASP Internet Of Thing Project Top Ten (10/9/2016) [Online], Available at:

<https://www.owasp.org/index.php/OWASP\_Internet\_of\_Things\_Top\_Ten\_Project>

[Accessed September 2016].

* Main methodology source
* Standardised source amongst professionals
* Top vulnerability statistics
* Statistics of attack vectors

Denis, M., Zena, C. and Hayajneh, T. (2016). IEEE Xplore Document - Penetration testing: Concepts, attack methods, and defense strategies. [Online] Available at: <http://ieeexplore.ieee.org/abstract/document/7494156/>

[Accessed November 2016].

* **Main practical case study !!**
  + Pen testing
  + Attacking tools
  + Attack methodologies
  + Defense strategies
  + Bluetooth attacks
  + Traffic sniffing
  + Protected WPA wifi attacks
  + **Man in the middle attacks**
  + Other privacy files, eg. Laptop microphone recording and spying

Morgner, P., Mattejat, S. and Benenson, Z. (12/8/2016). All Your Bulbs Are Belong to Us: Investigating the Current State of Security in Connected Lighting Systems. [Online] Available at:

https://arxiv.org/pdf/1608.03732v1.pdf

[Accessed November2016].

* Specific reference for lighting systems
* Can this be performed on the lightbulbs in question?