Subject: The Internet of things was only mentioned briefly in relation to bot nets. I would like to learn more about how the internet of things can be more secure and the techniques people use to form the bot nets.

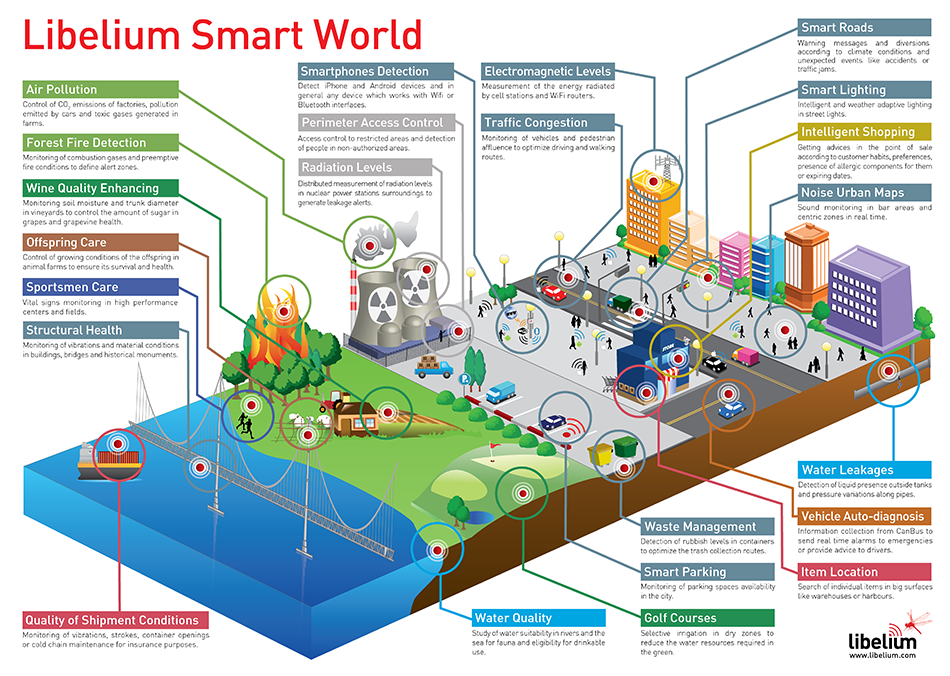
Outline:

1. Summary

This paper will outline and discuss the issues surrounding devices known as the Internet of Things devices. The intent is to discover the definition of these devices, where they are used, why they are used. It will then discuss how they are being misused, what allows misuse, damages that are caused by this misuses. Finally, the paper will discuss some of the remedies or precautions that we can take to still enjoy the benefits of having our world connected.

1. IoT
   1. What is IoT?

Forbes has an article that summarizes what the basics of IoT are or can be: “*Simply put, this is the concept of basically connecting any device with an on and off switch to the Internet (and/or to each other)…. The analyst firm Gartner says that by 2020 there will be over 26 billion connected devices... That's a lot of connections (some even estimate this number to be much higher, over 100 billion). The IoT is a giant network of connected "things" (which also includes people). The relationship will be between people-people, people-things, and things-things.”* [2]

* + 1. [](http://www.libelium.com/libelium-smart-world-infographic-smart-cities-internet-of-things/)What sort of devices are IoT?

[3]

While the list of devices that are included in the realm of “things” is nearly endless, the infographic above provides a graphical idea of the places where we could find “things”. A more complete list is included at <http://www.libelium.com/libelium-smart-world-infographic-smart-cities-internet-of-things/>.

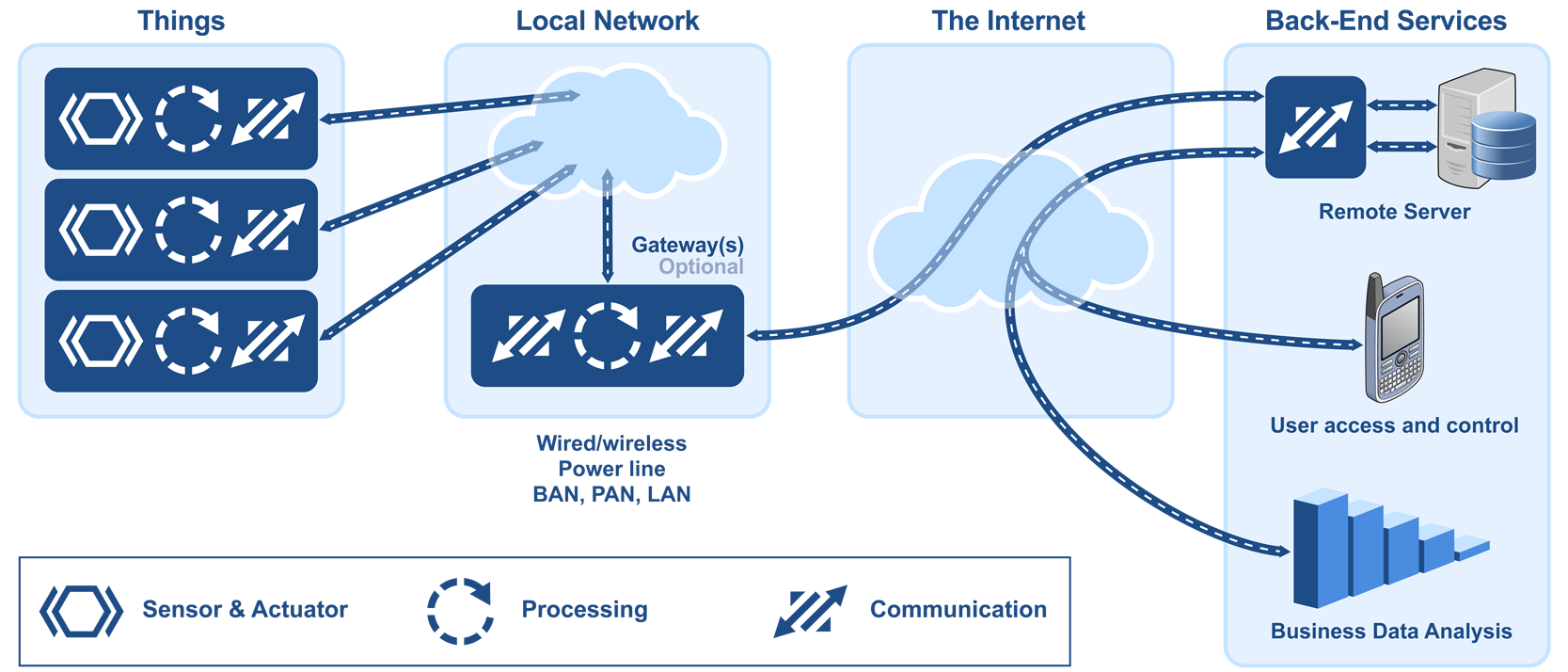
Devices are split in to two distinct groups, residential and commercial.

* + 1. Commercial

These are devices that a business or government entity may use.

* + 1. Residential

These devices are the type that a consumer would buy from a retailer, the devices are typically mass produced. These can include DVRs, home security cameras, smart TVs, and many other items that are in each of our lives.

* + 1. Security

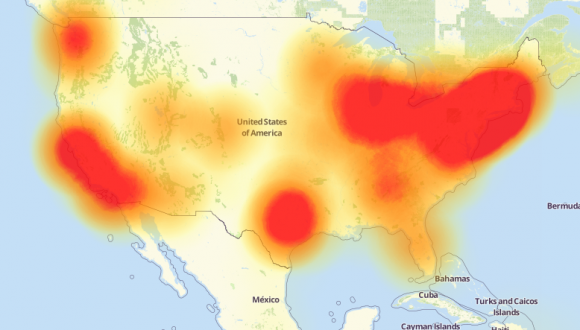
“Devices usually contained a system on a chip (SoC) that executed the actual protocol connection to the internet. Vulnerable devices also had active login passwords that had not been changed from the default settings. Since the chip was integrated into some other product, the user may not have been offered the option to change the login info — perhaps the manufacturer found these default credentials useful in testing the overall device.” [7] “More than just the administrator panel is vulnerable here. Direct services, like Secure Shell (SSH) and Telnet, have shipped with default passwords and no way for users to change the state of the connection. “The password is hardcoded into the firmware, and the tools necessary to disable it are not present,” security researcher Zach Wikholm of Flashpoint told KrebsOnSecurity. “Even worse, the web interface is not aware that these credentials even exist.”” [7]

1. Bots
   1. What are bot nets?

Malwarebytes labs defines Botnets as *“networks of computers infected by a botnet agent that are under hidden control of a third party.” [5]* Kaspersky labs defines them as *“any collection of compromised PCs controlled by an attacker remotely.” [6]* Typically these bot nets are formed from IoT devices.

* 1. What does a bot net need to exist?

A bot net needs two things to exists, first it needs a command and control center, or a device that controls the other device, second it needs devices to control.

* + 1. Miri

One of the better-known botnets was labeled Mirai was able to produce massive attack that led to an outage last year. The picture below is a depiction of what that outage looked like.

Several steps can be taken to avoid compromised devices. Default passwords should always be changed, un-used ports restricted, and understanding what your devices have and use.

[1[] <https://krebsonsecurity.com/2016/10/hacked-cameras-dvrs-powered-todays-massive-internet-outage/>

[2] <http://www.forbes.com/sites/jacobmorgan/2014/05/13/simple-explanation-internet-things-that-anyone-can-understand/#1a67d3b46828>

[3] <http://www.libelium.com/libelium-smart-world-infographic-smart-cities-internet-of-things/>

[4] <http://www.postscapes.com/internet-of-things-protocols/>

[5] <https://blog.malwarebytes.com/threats/botnets/>

[6] <https://blog.kaspersky.com/botnet/1742/>

[7] <https://securityintelligence.com/the-internet-of-trouble-securing-vulnerable-iot-devices/>