Final Year Project Plan

**Full Unit – Project Plan**

Testing and Analysing IP Camera to detect vulnerabilities

Nurfatin Abdulhani

A report submitted in part fulfilment of the degree of

**BSc (Hons) in Computer Science**

**Supervisor:** Danielle Sgandurra



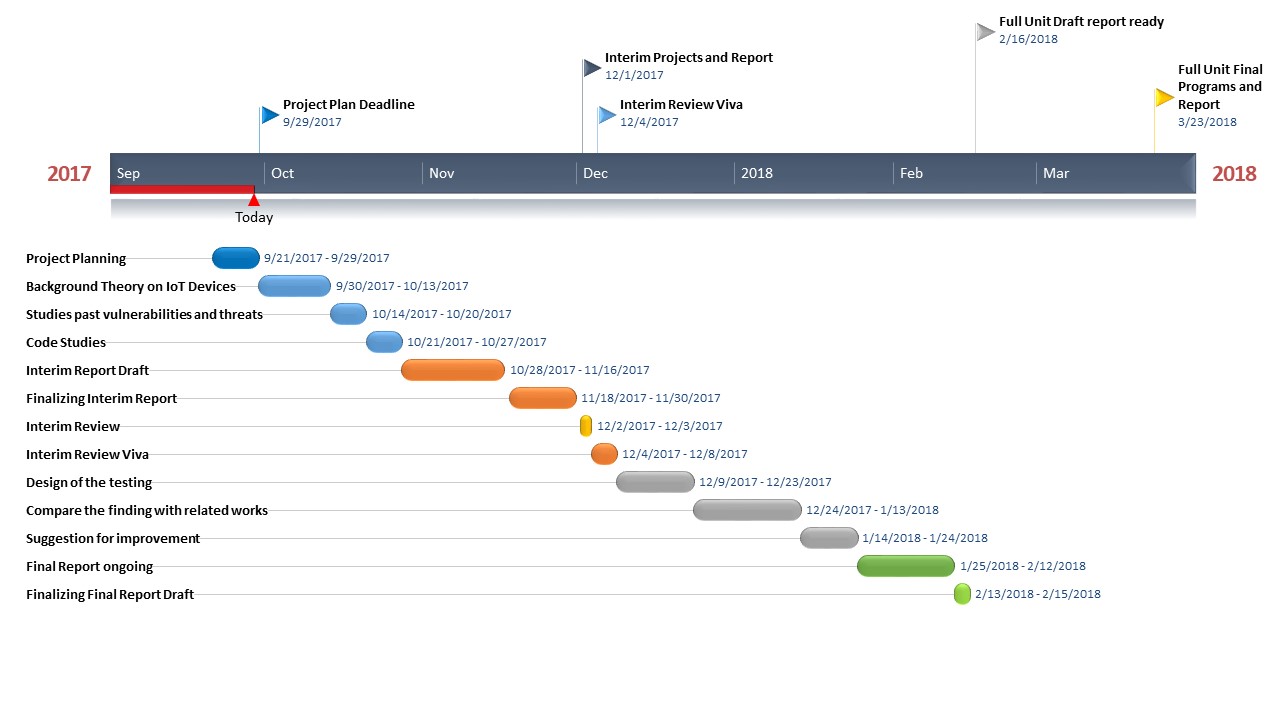
Department of Computer Science Royal Holloway, University of London

September 29, 2017

Abstract

Smart home applications is part of the evolution of technology which has been around since the 1970s, with those applications people tend to feel safer, energy usage and cost efficiency with security and automatic settings available in their household. The most common applications of smart home applications are Smart Lock, Lighting Control, HVAC (Heating, Ventilation and Air conditioning), Thermostat and much more. But how sure we are that we could 100% relay our security and safety with this technology? With this engaging world we are living in, it sure have been growing rapidly. With a product that have been release few weeks ago, there will be a better version of the same product release today. Everyday security researches discover new (critical) vulnerabilities on Internet of Things devices). As for example of vulnerabilities that have been exploit, where the customer information are exploit who have the IP camera where because of “isolated a small piece of code” that creates the vulnerability of hackers could easy get in through the backdoor. Basically it allows unauthorized admin access the internet and gained the information; this attack happens to a company where engineers with Dahua Technology USA began creating firmware updates to prevent the backdoor open. This project presents the inner depth of security analysis of the famous smart home programming platform. We analyzed IP Camera, which send and receive data via a computer network and the internet. The goals of this analysis is to dive in deep on vulnerabilities of IP Camera even though many programmers have solved the problem yet there’s always a blind spot which attacker could enter and hacked the system.

Timeline



Bibliography

Mohamed Abomhara, Geir M.Koien, **Cyber Security and the Internet of Things: Vulnerabilities, Threats, Intruders and Attack**, Journal of Cyber Security, Vol 4, 65-88

In this article, it give more information and the basic knowledge to start the project and which is leads to. It’s quite a read and it somehow gave me a glimpse of the end result of my project report.

Yin Minn Pa Pa, Shogo Suzuki, Katsunari Yoshioka, Tsutomu Matsumoto, Takahiro Kasama, Chritian Rossow, **IoTPOT: Analyzing the Rise of IoT Compromises**, USENIX Woot, 2015 August 15

They point out there’s a huge increase of attacks on IoT devices and they gave information about a novel honeypot called IoTPOT, which the attacks mimics the devices and captures telnet-based intrusions.

Grant Ho, Derek Leung, Pratyush Mishra, Askhan Hosseini, Dawn Song, David Wagner, **Smart Locks: Lesson for securing Commodity Internet of Things Devices**, 2016 Mar

This focuses on smart lock devices which they have found that the attacks are caused by the weakness in their system design compare to the implementation bugs and sort of all current systems use insecure mechanisms.

Alison E.Berman, Jason Dorrier, **Technology Feels like It’s Accelerating – Because it actually Is**, SingularityHub, 2016 Mar 22

I read the article to find out the fast pacing of our technology which it says that our technology is part of the evolution. This article is useful for me to double check on the new technology produce every single day which is better than the other yet still have a weakness.

Andy O’Donnel, **How to Secure Your IP Security Cameras**, Lifewire, 2017 July 12

This article just to show that a solution which I can’t use for my project threats solutions, which mostly I found is an update to the camera’s firmware which previous article I’ve read gave the same solution.

Pierre Kim, **IT Security Research By Pierre**, Pierrekim, 2017 March 8

On this article, he had found a pre-authorize RCE as root against 1250 camera models which the cloud have a clear information UDP tunnels between the attacker and the cameras just by using the serial number of the camera. It happens because of the code reusing.

Chris Brook, **Dahua Patching Backdoor in DVRS**, IP Cameras, 2017 March 7

In this article, it explains how the engineers of the dahua technology usa secure back the IP cameras by pushing firmware update for the issue of “a small piece of code” which create backdoor for hackers to easily exploit the information.

Risk Assessment

The risk assessment that I’m actually in a middle of deciding whether IP camera is a good device to be my main topic for my project. I don’t have much experience knowing IP camera as much as others, but reading the article shared by my supervisor and on the internet do helps but it’s still risky of me to decide on whether this decision would giving me a flying colors mark for my final year project. I have everything as planned for the milestone which states the process I’ll be doing and the date that have been decide. Things could go wrong during the project process even though I have everything planned in the milestone, I think my scope could be changing during term time. The biggest risk that I’ve been thinking a lot is on the coding part and testing. I’m not a good programmer but I’m a learner which that’s the only thing that positive that I could think about.