Project Plan

Abstract:
True randomness of a random number can be important for an organisation to secure their intellectual property. It can also be important for the end-user of a product to verify that the Random Number Generator (RNG) is in fact as secure as the manufacturer labels it as or not tampered with by a third-party after being sent out of the factory. Hard-coded seeds for generating a random number may be used by some parties, and can be a vital security threat. I am therefore willing to see how these RNGs are implemented by different organisations, and how these distinctive implementations affects my statistical tests and the results. For example looking at the difference between test results I get with a hardware-based RNG against a software-based RNG. The tests carried out will primary be lightweight statistical tests to ensure true randomness.

In the end of the project I hope to be able to see how and why different lightweight statistical tests of randomness fails to identify supply chain threats, and how this can be avoided. Through my research I also hope to get a better understanding of the supply chain itself, and how it is built up.

Background:
I have found during my research this summer that the FIPS 140-2 certification standard for cryptographic modules (such as Random Number Generators) and how the certification process for this standard works seems very interesting. One field I found especially interesting and which I will pursue to learn more about are Pseudorandom Number Generators (PRNGS). These are deterministic random numbers as they are not in fact truly random as they need an initial external seed value/input to produce a ‘random’ output. This external value is often predictable as PRNGs are usually software generated.

I am excited to see if my tests in this project will prove that PRNGs are deterministic and will fail the simple and lightweight statistical tests of randomness I will be doing. Also excited to see if True Random Number Generators (TRNG) - which will most likely be hardware implemented - can pass the test suites I will be conducting them through.

I do find information security highly interesting. With this project I hope to be able to prove myself to the industry and later hopefully get employed at a organisation focusing on information security.

I am looking forward to pursue this project over the next months, and looking forward to collaborate with my supervisor during my writing.

Deliverables:

During the first term I aim to write a couple of different reports to lay the basis of my knowledge used in the final project report.

I will be writing my first report on hardware Random Number Generators (RNG), where I will in depth try to explore FIPS testing using tools and test suits. I have looked at NIPS SP800-22 as a possible test suite to have a closer look at, as well as the Dieharder batteries of tests. I am not too familiar with the Dieharder tests yet, but having a well documented Linux man page I am sure I can use these tests in my final report by showing off some tests done with Dieharder.

Also, I will be writing a report about recent supply chain attacks against critical security infrastructure and what damage such attacks can cause to an organisation in their networks. Here I will dig into what effect a third-party partner of the organisation can have on this regarding access levels to the network. Having a look at how these supply chain attacks is built up, I think I can better understand why standards such as FIPS 140-2 and test suites such as NIPS SP800-22 are essential to keep the potential attack surface to a minimum in larger corporations, but also smaller projects where RNGs or other vulnerable technologies might be used.

Then, a deliverable of the interim review. This deliverable will be containing a combined document that I will write about my findings in the two earlier reports. This report for the interim review will also be a preliminary literature review.

Finally, next term the final project submission will be due.

Timeline:

Term 1:

Hardware Random Number Generators - ***20th of October 2020***

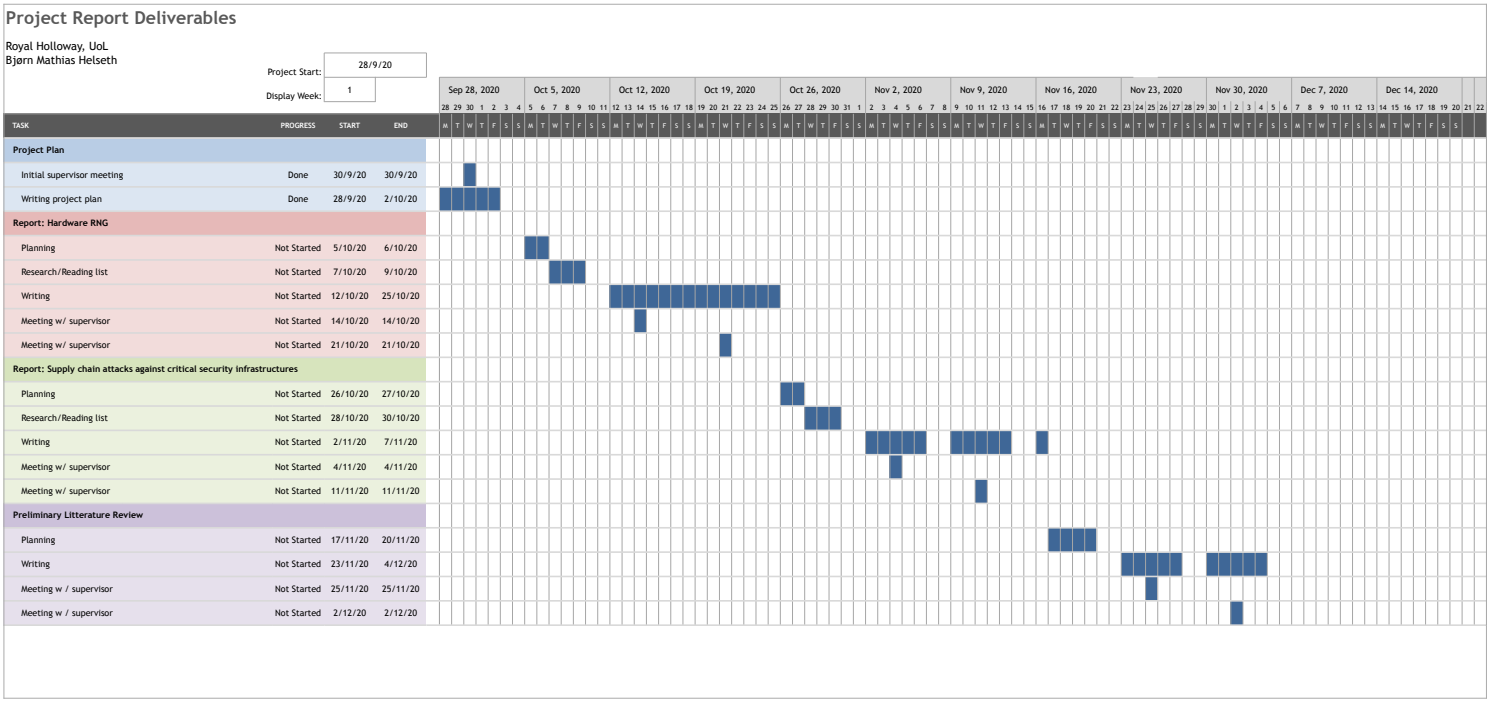
Recent Supply Chain Attacks against critical security infrastructures - ***15th of November 2020***

Interim review - ***4th of December***

Term 2:

Final Project submission - ***Next Year***

Gantt chart of deliverables



Key risks associated with the project:

Each risk denoted below is sorted from top to bottom by importance. They are also colour-coded for likelihood based on a risk assessment (The assessment is based off the "How to avoid" section). Green colour means not that likely, yellow colour means more likely and red colour means likely.

Risk	Affects	Result	How to avoid
Catching Covid-19	My ability to continue my work on the report while staying home or at a hospital with symptoms.	Time lost working on the report. No ability to focus on the report at all. Demotivation.	Taking precautions, following government guidance and informing my supervisor immediately if this unfortunately ends up happening. Currently many reported cases.
Getting mental health issues (For example from lockdown or from stress)	My ability to focus on the project.	Frustration regarding work on the project. No motivation. Depression. Anxiety.	Socialize with friends (Safely, following covid restrictions). Take healthy breaks from university (weekends).

Risk	Affects	Result	How to avoid
Not backing up all data	The final report and also progress that might have been done during research if something gets lost due to unforeseen circumstances.	Lost progress that could end up not being included because I forget the material. Less marks.	Backing up all data into SVN daily and whenever new considerably larger amounts of data has been added.
Losing motivation to work on or finish project	My ability to finish the report or even writing it.	Unfinished report. Zero marks. Less marks. Depression.	Keeping myself in the university loop by following lectures, engaging with the modules and informing my supervisor about progressions. Also taking breaks from working with the project, and keeping myself generally interested.
Not understanding the material	Outcome of the project report, my motivation and interest in learning about the topics.	Might resort into leaving important parts out of my reading list, project or report. Take shortcuts.	Try to spend some time of one topic or technology I do not fully understand, and then coming back to it at a later stage to avoid frustration and getting no work done. Asking my supervisor or fellow students.
Leaving out reading that might be important	The final project report by unknowingly not including information from sources that could have left me with different outcomes.	A report that could have had more information regarding certain topics that could be of high importance. Less marks.	Recording all relevant reading into a reading list.
Looking into too broad topics	My ability to focus on the key points of working on my report. And will lead to time spent doing research on topics that may not be relevant or useful.	unnecessarily time-consuming. Might lose marks by including too much unrelated material in the final report or in early deliverables.	Creating reading lists that are sorted in terms of relevancy. Broader topics can be left out for extra reading.

Bibliography:

"On the unbearable lightness of FIPS 140-2 randomness tests" - Darren Hurley-Smith, Constantinos Patsakis, Julio Hernandez-Castro

https://ieeexplore.ieee.org/abstract/document/9069949/

This publication is a good reference to my project as it is based off from the findings in my supervisors (and Constantinos Patsakis & Julio Hernandez-Castro) research mentioned in this

report. Not only does this report cover most aspects of the red thread that I will be undertaking in my report - How can statistical tests of randomness fail to identify supply chain threats.

"3 ways to prevent supply chain attacks" - Bill Phelps
https://www.boozallen.com/c/insight/blog/3-ways-to-prevent-supply-chain-attacks.html
This source will be useful when identifying supply chain attack remediation strategies. Recognising how a supply chain works and how adversaries might think in a possible attacking situation is also discussed briefly here.

"NIST SP800-22 Test Suite" - Andrew Rukhin
https://nvlpubs.nist.gov/nistpubs/Legacy/SP/nistspecialpublication800-22r1a.pdf
Publication of the NIST SP800-22 Test Suite which can be used to carry out statistical tests of randomness against a RNG. Using this document to find useful information regarding how the SP800-22 is built up, the tests the suite contains and a technical description of these tests.

"On statistical tests for randomness included in the NIST SP800-22 Test Suite and Based on the Binomial Distribution" - Fabio Pareschi
https://ieeexplore.ieee.org/abstract/document/6135498
In this document I'm able to extract information on how the SP800-22 Test Suite can be used on statistical tests of randomness and some of these tests are also lightweight. This is perfect for research on my report as I will be looking at carrying out tests using this test suite.

"Great Expectations: A Critique of Current Approaches to Random Number Generation Testing & Certification" - Darren Hurley-Smith, Julio Hernandez-Castro
https://link.springer.com/chapter/10.1007/978-3-030-04762-7_8
Through this reading I have become more aware of that the current methods used to test RNGs through statistical tests might be unreliable, and especially to the unknowing end-user of a product using an insecure or maybe even an RNG which have been tampered with. I am sure that this report will lead me to explore the more ethical aspect of how these RNGs are implemented as there must be ways that they can be exploited.