**//UPDATE: We do not have to do every single subtopic in detail. Only four or five. We can mention the rest of them but we do not have to spend too much time on them. Just on the relevant ones.** *– Chris 23/10/2017*

**//Write whatever you have paraphrased or any quotes into the assigned section. Any quotes and references need to go to the Bibliography page. To do this, select the text/quote, click on “References” and then “Insert Citation”.** - *Chris 25/10/2017*

[**SONIA: (Cyber Security)**](#_CYBER_SECURITY)

**Anonymity**

**Authentication**

**Privacy-Enhancing Technologies**

**Security and Privacy Measurement**

**Computer Security**

[**CHRIS: (Reliability & Management)**](#_RELIABILITY_&_MANAGEMENT)

**Reliability and Dependability**

**Information Hiding**

**Trust**

**Information Security Management**

**Identity Management**

[**YIFAN: (Cryptology)**](#_CRYPTOLOGY)

**Cryptanalysis**

**Cryptography**

**Financial Cryptography**

**Steganography and Steganalysis**

**Virtual Currencies**

[**PAUL : (Humans & Cybercrime)**](#_HUMANS_&_CYBERCRIME)

**Usable Security**

**Human Aspects of Security**

**Network Security**

**Cybercrime**

**Malware**

# **CYBER SECURITY**

**Sonia**

## Anonymity:

## Authentication:

## Privacy-Enhancing Technologies:

## Security & Privacy Measurement:

## Computer Security:

# **RELIABILITY & MANAGEMENT**

**Chris**

## Reliability and Dependability:

In Information Security, Reliability and Dependability can be used interchangeably to describe the same thing. This presents the idea of having a trustworthy system throughout a given time. Or as the Institute of Electrical and Electronics Engineers (IEEE), it *is “the ability of a system or component to function under stated conditions for a specified period of time”.*

(IEEE, 1990)

Reliability engineering concentrates on the costs that would apply during system downtime. It focuses on making sure that a given system is appropriate for its purpose with respect to time. It will also aim attention at the durability of said system and its functioning when it is presented with stated condition.

Dependability in systems has three key elements:

* Characteristics: A way to evaluate how reliable a system is.
* Threats: Knowledge of the things that can affect said reliability.
* Means – Methods to improve the system’s dependability.

(<https://en.wikipedia.org/wiki/Reliability_engineering#Definitions>)

(<https://en.wikipedia.org/wiki/Dependability>)

## Information Hiding:

With respect to Information Security, Information Hiding is the limitation of access to information to entities who require it to execute certain tasks. The idea is that, the fewer the people who know the details of a system or task, the less chances this information is compromised or falls into the hands of the opposition.

A good example of this would be the Manhattan Project. Staff worked with centrifuges to isolate Uranium-235 from naturally occurring uranium, but they did not know what they were doing it for. Those that knew, did not know why they were doing it. Parts of the weapon were designed without knowing how they interacted.

(<https://en.wikipedia.org/wiki/Compartmentalization_(information_security)>)

## Trust:

(<https://en.wikipedia.org/wiki/Trusted_system>)

## Information Security Management:

## Identity Management:

# **CRYPTOLOGY**

**Yifan**

## Cryptanalysis:

## Cryptography:

## Financial Cryptography:

## Steganography and Steganalysis:

## Virtual Currencies:

# **HUMANS & CYBERCRIME**

**Paul**

## Usable Security:

## Human Aspects of Security:

## Network Security:

## Cybercrime:

## Malware:

# Bibliography

**There are no sources in the current document.**