1. Ransomware Detection using Deception Models – 16th November

Questions:

* What specific ransomware strains were used to produce the data sets, and how do they reflect the diversity of real-world ransomware encounters (especially understanding how to reduce error and possibly recognize many types of files)
* Can the study provide insights into the potential implications of its findings for the development of more effective ransomware detection methods, particularly on entropy classification for values of finding more effective ways to compare files and classify them?

1. Understand humans approach to Reverse Engineering – 23rd November

Questions:

* What are the ethical considerations and implications of augmenting autonomous cyber reasoning systems with human assistance?
* How might the use of eye-tracking technology and other physiological measures help us better understand the cognitive processes involved in reverse engineering, particularly understanding what can be the techniques used to obfuscate both humans and automatic methods alike?

1. Fuzzing – 23rd November

Questions:

* How would you improve and add mutators inside the API in order to reach an even better implementation over different targets?
* How to determine if it’s OK to use persistent mode for a given app, specifically in showing it’s better than forking and in the program coverage to avoid application-specific issues?

1. Private data inference from Social Networks – 7th December

Questions:

* How would you improve the SVM model: adding some attributes or editing the existing ones, probably there would be a bias over certain categories of data gathered?

1. Social Network Analysis – 7th December

Questions:

* How do you think the aspect of social closeness can be considered valuable, given at any point anyone can become a friend, avoiding formations of “false triads” of friends?

1. IoT Security – 14th December

Questions:

* Given how the schema is composed, how would you improve the computational cost that is kept maintaining provers and aggregators? What power should the devices have in order to sustain it?

1. Misuses in Wearable Devices – 14th December

Questions:

* Do you think combining a different method for sampling for a malicious app or use a different pairing method in the context of data injection may or may not be effective or less? How would you make the user more aware of these binding related problems, combining a simple method like Bluetooth avoiding clones or excessive power consumption?

1. Lie Detection – 21st December

Questions:

* Regarding the unexpected questions, how much do you think is important to make users know in advance before completing the task? How would you formulate such questions to improve the general model?

1. Air-Ground Communication – 21st December

Questions:

* How much do you think will be impactful the usage of an open system using for example collision avoidance, combined with formal protocols from the start, for example using ACARS standard, given it has not been adopted?