Seminar 7 – Debate Vote – Feedback and the Future of the Internet

- ➢ Announcements
- ➢ Initial (informal) Feedback
- ➢ Reflections
- ➢ Unit 12 Question /Exercise
- ➢ Q&A

Reflections:

- Emphasise what we have learned and how that helps us in the future
- Critic the own work is an important part of the reflection.
- In terms of reflective it is about making choices of evaluation.
- What went well in the team project. What was we able to learn in these terms.
- Referencing in terms of literary review.

Informal feedback on Assessment2:

- Criticality
- Sources and References
- Proof Reading – Grammar & Technical/Content
- Prior Learning
- Formats

CCN:

To edit:

- Future is more discreet distributed
- Attribute based encryption scheme

Mobility First architecture:

- It is about the separation of the level package.
- First is the GUID which is a dynamic ID, which register the names of the service.
- Secondly there is the SID for the device and also the level address
- It can support two or more level interface → useful for mobility
- This architecture is already used by the Canadian police.
- Many companies provides or uses this service in the future(e.g Nvidia, Amazon, Tesla, Windows)
- Reasons for mobility first:
  - ➔ Trust
  - ➔ Scalability

- ➔ Security: Globally unique identifier / NetFence against DoS attacks / using networks than end systems / easily construct of end to end communication
- ➔ Mobility: Allows resumption of downloads when a device moves / strengths mobile and wireless network / separation of names and network addresses
- ➔ Higher performance: Caching adopted on data delivery / IoT offer low control overheads / good packet success rate

Disadvantages of NDN and COAST in comparison to mobility first:

NDN:

- ➔ DoS detection difficulties
- ➔ Interest packets not validated
- ➔ Data Confidentiality (cached at routers)
- ➔ Privacy concerns: trust issues around signing data packets
- ➔ Information disclosure (Monitoring)
- ➔ Interest flooding and content poisoning

COAST:

- ➔ High overhead
- ➔ Difficult to construct end to end communication
- ➔ Too much processing
- ➔ Lack of access control
- ➔ Low probability of establishing session key between data consumer and producer (Host – Oblivious Network Security)
- ➔ Specific DoS attacks
- ➔ Lacks efficient in terms of active/passive crawling
- ➔

Disadvantages of peer to peer networking architecture:

- Peers are out of control and not secure. BitTorrent, Trojana and other viruses or malware can be embedded into the installation code of other software.
- One of the main cyber risk associated with TOR is that monitoring traffic is almost impossible, because all communication over TOR is encrypted.
- Mounting a Sybil attack is very easy in KAD and allows to compromise the privacy of KAD users
- Legal troubles