Zero Trust Networking

Prof. D. Manjunath
Prof. Gaurav S. Kasbekar
Motivation

• In traditional model for enterprise security:
  - Devices such as firewalls and Intrusion Detection Systems (IDSs) are placed at the edge of the enterprise network
  - Devices situated outside the enterprise network need to authenticate themselves, use Virtual Private Networks (VPNs), etc.,
  - Those situated inside can access resources in the network relatively freely

• However, the above traditional model is not suitable for modern enterprise networks, in which:
  - A significant part of the storage and processing occurs in a cloud,
  - Several employees connect from hotels, homes or via mobile devices while traveling, etc.

• The traditional model is also insecure since once an intruder gains access to a machine inside the enterprise network, it is easy to access other machines and various resources
Zero-Trust Networking

- Zero Trust Networking refers to a threat model that no longer assumes that devices or users operating from within the enterprise network should be automatically trusted.
- Instead, it assumes that anything and everything trying to connect to its systems must be verified before access is granted.
- How much trust to place in a user and which resources in the enterprise network the user should be allowed access to is decided based on multiple factors, e.g.:
  - the current time,
  - location of the user,
  - the device that the user is using,
  - the network the device belongs to,
  - what operating system and libraries are installed in the device,
  - the user's browsing history in the recent past, etc.
Objectives of This Project

1) To design a scheme for assigning a trust level to each user, which is a time-varying function of the history of the activities, location, etc., of the user,

2) To design an architecture for an enterprise network based on the Zero Trust Networking paradigm,

3) To design a scheme for regulating access to different parts and resources of the enterprise network based on the trust level assigned to a user.
References

• For more information, please go through the following references: