Selected Topics in Computer System Security (Wed: 18:15-20:00)

Synopsis

Computer Systems Security is a class about the design and implementation of secure computer systems. The protection of information systems from theft or damage to the hardware, the software, and to the information on them, as well as from disruption or misdirection of the services they provide. It includes controlling physical access to the hardware, as well as protecting against harm that may come via network access, data and code injection, and due to malpractice by operators, whether intentional, accidental, or due to them being tricked into deviating from secure procedures. The field is of growing importance due to the increasing reliance on computer systems in most societies and the growth of "smart" devices, including smartphones, televisions and tiny devices as part of the Internet of Things – and of the Internet and wireless network such as Bluetooth and Wi-Fi.

This course of "Selected Topics in Computer System Security" is designed to discuss the latest research going in the field of Firewalls, IDS/IPS, OS security, Physical security and Insider threats. Besides lectures covering details of these areas, there would be regular discussion sessions related to the research work done by researchers in these areas. So all assignments would be research based where each student has to present research task assigned to him on these topics. So only those students who are interested in doing research must register this course.

Pre-requisite

Students should have taken a post-grad level course of Information & Network Security

Course Contents

Lecture#	Topics
1	Introduction to System security, Vulnerabilities and threats
2	Threat models and variants
3	Firewalls intro., packet filtering router, Circuit level gateway, Application level gateway
4	Next generation Firewalls, Advanced Persistent Threats
5	Discussion session (Students presenting their assigned research tasks)
6	Intrusion detection system , IPS, Anomaly-based IDS, Threshold-based IDS
7	Expert Systems, Honey-pots, virus, worms

8	**MID-TERM**
9	**Discussion session (Students presenting their assigned research tasks)**
10	**OS security, models, Biba, La-pudalla, Chinese-Wall model**
11	**Group-based access control, Roll-based Access Control methodologies**
12	**Web Security, SSL/TLS, Browser side risks, Server side risks, Cookies**
13	**Discussion session (Students presenting their assigned research papers)**
14	**Physical security, Issues, Methodologies, Intro. to Insider threats**
15	**Insider threat assessment, detection and prevention methodologies**
16	**Discussion session (Students presenting their own research papers)**

About Instructor

Dr. Maaz Bin Ahmad is Associate Professor in Karachi Institute of Economics and Technology since Jan 2016. He received his PhD in Network Security from Center of Advanced Studies in Engineering (CASE), Islamabad, in 2014. Before that, he did his MS in Computer Engineering from CASE. He has teaching experience of around 15 years. His research interests include Networks Security, Adhoc Networks and Video processing.