Lecture 01: Course Intro and Administrivia

CS101 - Introduction to Computing

Dr. Mohammad Nauman

Assistant Professor (CS)
FAST National University of Computer and Emerging Sciences
mohammad.nauman@nu.edu.pk
http://recluze.wordpress.com

Introduction

About You

- Math. Eng.
- Army
- Architecture
- MS/PhD
- Programming
- Android
- iOS
- Animation
- UI
- Graphic Designing
- Java
- Gaming
- Medical

Let's talk!

Some things you can share with us:

1. Name
2. Interests
3. Was CS your first choice? If not CS, what was?
4. What do you want to do after your BS?

Plan

Class introduction

About the instructor

About the CS program

Course outline

Teaching method

Practice focus

About the instructor

PhD (2014) – Security and privacy

Postdoc – Android Security from Max Planck Institute for Software Systems, Germany

Research Output:

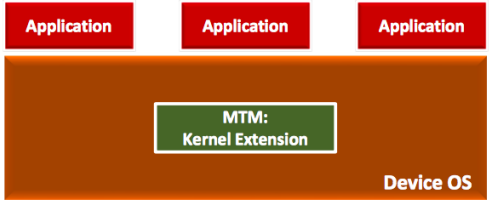
1. 15 book chapters/journal papers, 30+ conference, 2 books
2. Number of citations: 1100+ (Highest cited; 600+)
3. Collaboration at global scale

Software: `http://github.com/recluze`

Site: `http://recluze.wordpress.com`

	(Slides)		"Not So Great Expectations: Why Application Markets Haven't Failed Security," McDaniel and Enck (IEEE S&P Magazine'10) (link)
01/17/12	Rule Driven Policy		"Security-by-contract on the .NET platform," Desmet et al. (2008) (link) "On Lightweight Mobile Phone Application Certification," Enck et al. (CCS'09) (link)
01/19/12	Rule Driven Policy		"Semantically Rich Application-Centric Security in Android," Ongtang et al. (ACSAC'09) (link) "Apex: Extending Android Permission Model and Enforcement with User-defined Runtime Constraints," Nauman et al. (ASIACCS'10) (link)
01/24/12	Rule Driven Policy		"Porscha: Policy Oriented Secure Content Handling in Android," Ongtang et al. (ACSAC'10) (link) "XManDroid: A New Android Evolution to Mitigate Privilege Escalation Attacks," Bugiel et al. (link)
01/26/12	**No class (Oakland PC Meeting)**		
01/31/12	High-level Policy		"Using Labeling to Prevent Cross-Service Attacks Against Smart Phones," Mulliner et al. (DIMVA'06) (link) "Practical and Lightweight Domain Isolation on Android", Bugiel et al. (SPSM'11)
02/02/12	Research Methods (Slides)		"Reflections on Trusting Trust", Thompson (link)
02/07/12	**No class (NDSS)**		
02/08/12	**OS Report Prelim Writeups Due (11:59pm Midnight)**		
02/09/12	OS Presentations		Android iOS
02/14/12	OS Presentations		Blackberry Windows Phone
02/15/12	**OS Report Final Writeups Due (11:59pm Midnight)**		
02/15/12	**Guest Talk by Glenn Wurster (RIM Security) (11am-12n, 3211 EBII)**		
02/16/12	Research Methods (Slides)		"Reflections on Trusting Trust", Thompson (link)
02/20/12	**Project Proposal Writeups Due (11:59pm Midnight)**		
02/21/12	Project Proposals		Oral Presentations
02/23/12	Project Proposals		Oral Presentations
02/28/12	High-level Policy		"Permission Re-Delegation: Attacks and Defenses," Felt et al. (Security'11) (link) "QUIRE: Lightweight Provenance for Smart Phone Operating Systems", Dietz et al. (Security'11) (link)
03/01/12	Platform Hardening		"Measuring Integrity on Mobile Phone Systems," Muthukumaran et al. (SACMAT'08) (link) "Beyond Kernel-level Integrity Measurement: Enabling Remote Attestation for the Android Platform," Nauman et al. (TRUST'10) (link)
03/06/12	**Spring Break - No class**		

Approach 2: Kernel Module



(Nauman et. al., 2010)

- Security and Privacy Vulnerabilities of In-Car Wireless Networks: A Tire Pressure Monitoring System Case Study. Rouf et al. USENIX Security 2010. [local]
- Experimental Security Analysis of a Modern Automobile. Koscher et al. Oakland 2010. [local]
- Chip and PIN is Broken. Murdoch et al. Oakland 2010. [local]
- What's in a Name? Evaluating Statistical Attacks on Personal Knowledge Questions. Bonneau et al. FC 2010. [local]

Privacy-preserving Computation

- SEPIA: Privacy-Preserving Aggregation of Multi-Domain Network Events and Statistics. Burkhart et al. USENIX Security 2010. [local]
- P4P: Practical Large-Scale Privacy-Preserving Distributed Computation Robust against Malicious Users. Duan et al. USENIX Security 2010. [local]
- SCiFI - A System for Secure Face Identification. Osadchy et al. Oakland 2010. [local]

Differential Privacy

- Privacy Integrated Queries. McSherry. SIGMOD 2009. [local]
- Airavat: Security and Privacy for MapReduce. Roy et al. NSDi 2010. [local]
- Differentially Private Aggregation of Distributed Time-Series with Transformation and Encryption. Rastogi and Nath. SIGMOD 2010. [local]
- Differentially-Private Network Trace Analysis. McSherry and Mahajanl. SIGCOMM 2010. [local]

Privacy

- An Analysis of Private Browsing Modes in Modern Browsers. Aggarwal et al. USENIX Security 2010. [local]
- ZKPDL: A Language-Based System for Efficient Zero-Knowledge Proofs and Electronic Cash. Meiklejohn et al. USENIX Security 2010. [local]
- Privacy Diffusion on the Web: A Longitudinal Perspective. Krishnamurthy et al. WWW 2009. [local]
- Adnostic: Privacy Preserving Targeted Advertising. Toubiana et al. NDSS 2010. [local]
- The Wi-Fi Privacy Ticker: Improving Awareness & Control of Personal Information Exposure on Wi-Fi. Consolvo et al. UbiComp 2010. [local]
- Privacy-Preserving P2P Data Sharing with OneSwarm. Isdal et al. SIGCOMM 2010. [local]

Cloud Computing

- When Good Randomness Goes Bad: Virtual Machine Reset Vulnerabilities and Hedging Deployed Cryptography. Ristenpart and Yilek. NDSS 2010. [local]
- HAIL: A High-Availability and Integrity Layer for Cloud Storage. Bowers et al. CCS 2009. [local]
- Hey, You, Get Off My Cloud! Exploring Information Leakage in Third-Party Compute Clouds. Ristenpart et al. CCS 2009. [local]

Security for Smartphones

- TaintDroid: An Information-Flow Tracking System for Realtime Privacy Monitoring on Smartphones. Enck et al. OSDI 2010. [local]
- Smudge Attacks on Smartphone Touch Screens. Aviv et al. WOOT 2010. [local]
- Beyond Kernel-level Integrity Measurement: Enabling Remote Attestation for the Android Platform. Nauman et al. TRUST 2010. [local]

Voting Technologies

Spring 2010

EECS 450 Internet Security

Prof. Yan Chen and Dr. Zhichun Li

Home
Lectures

Wed 4/21	Web app vulnerability discovery	[pdf, and complementary ppt]	State of the Art: Automated Black-Box Web Application Vulnerability Testing, Jason Bau, Elie Bursztein, Divij Gupta, John Mitchell, Oakland, 2010.
Mon 4/26	Web origin policy	Vaibhav [ppt]	The Multi-Principal OS Construction of the Gazelle Web Browser, Helen Wang, Chris Grier, Alexander Moshchuk, Samuel T. King, Piali Choudhury, and Herman Venter, USENIX Security 2009. [Ref]Cross-Origin JavaScript Capability Leaks: Detection, Exploitation, and Defense, Adam Barth, Joel Weinberger, and Dawn Song, USENIX Security 2009.
Wed 4/28	JavaScript security policy	Vaibhav [ppt]	ConScript: Specifying and Enforcing Fine-Grained Security Policies for JavaScript in the Browser, IEEE Symposium on Security and Privacy, 2010. [Ref]Object Views: Fine-Grained Sharing in Browsers, Leo Meyerovich, and Adrienne Felt WWW 2010.
Mon 5/3	Midterm project presentation [Android Security] [Social Network Security Survey] [Web Origin Security] [UltraPAC]		
Wed 5/5	Web browser access control	Yi [ppt]	On the Incoherencies in Web Browser Access Control Policies, Kapil Singh, Alexander Moshchuk, Helen J. Wang, and Wenke Lee, IEEE Symposium on Security and Privacy, 2010.
Mon 5/10	Mobile System Security	Ted, Tyler [ppt]	Mobile Application Security on Android, by Jesse Burns at Black Hat 2009. Reference slides: Understanding Android's Security Framework (Tutorial) by W. Enck, and P. McDaniel.
Wed 5/12	Mobile System Security	Ted, Tyler [Kirin] [Apex]	On Lightweight Mobile Phone Application Certification, W. Enck, M. Ongtang, and P. McDaniel, ACM CCS 2009. [Ref] Apex: extending Android permission model and enforcement with user-defined runtime constraints, M. Nauman, S. Khan, and X. Zhang, ACM ASIACCS 2010.
Mon 5/17	Social Network Security/Measurement	Tuo, Jun [ppt]	Social Honeypots: Making Friends With A Spammer Near You, Steve Webb, J. Caverlee, and C. Pu, ACM CEAS 2008. [Ref]Characterizing User Behavior in Online Social Networks, F. Benevenuto et al, ACM IMC 2009.
Wed 5/19	Social Network Privacy	Jun, Jingnan	xBook: Redesigning Privacy Control in Social Networking Platforms, by Singh, et. al., USENIX Security Symposium 2009. [Ref] Persona: An Online Social Network with User-Defined Privacy, R. Baden, et al, SIGCOMM 2009.
Mon 5/24	NIDS	Jing	Outside the Closed World: On Using Machine Learning For Network Intrusion Detection, Robin Sommer and Vern Paxson, in IEEE Symposium of Security and Privacy, 2010.
Wed 5/26	Project presentation		
Mon 5/31	No class due to Memorial Day.		
Wed 6/2	Project presentation, cont`d		

Notes: You may find the brochure useful: Efficient reading of papers in Science and Technology by Michael J. Hanson, 1990, revised 2000 Dylan McNamee.

Areas I've worked in

Application programming

Mobile app development

Web development

System administration

Game development

Security and privacy

Voice over IP

Graphics design / photography / 3D designing

Operating systems

Cloud computing

Machine learning (and many other research areas)

Education

About the studies

About the CS program

Aimed at both industry and academia

Courses will be discussed in a while *inshaallah*

Some courses are more important than others

About the CS program

Aimed at both industry and academia

Courses will be discussed in a while *inshaallah*

Some courses are more important than others

Some very import soft skills:

1. Typing
2. Reading
3. Presentation and communication

How to approach the semester system

Early impressions go a long way

Doesn't really matter how well you did in the past

Do not rely fully on the instructors

- Coursera.org is a good place to start
- Alternatives: MIT OCW, Stanford, Berekely ...

For this course, follow along/ahead on `composingprograms.org`

Course outline and administrivia

Course outline is available in print

Two phases: intro and programming

Assignments are your real teacher

Semester project is your way of showing what you have learned

Quizzes are just to keep you motivated

0 tolerance for plagiarism

Things to do

Create accounts for:

- github.com
- stackoverflow.com
- Some website hosting company (e.g. wordpress.com)

Things to do

Create accounts for:

- github.com
- stackoverflow.com
- Some website hosting company (e.g. wordpress.com)

Get a notebook and take notes!

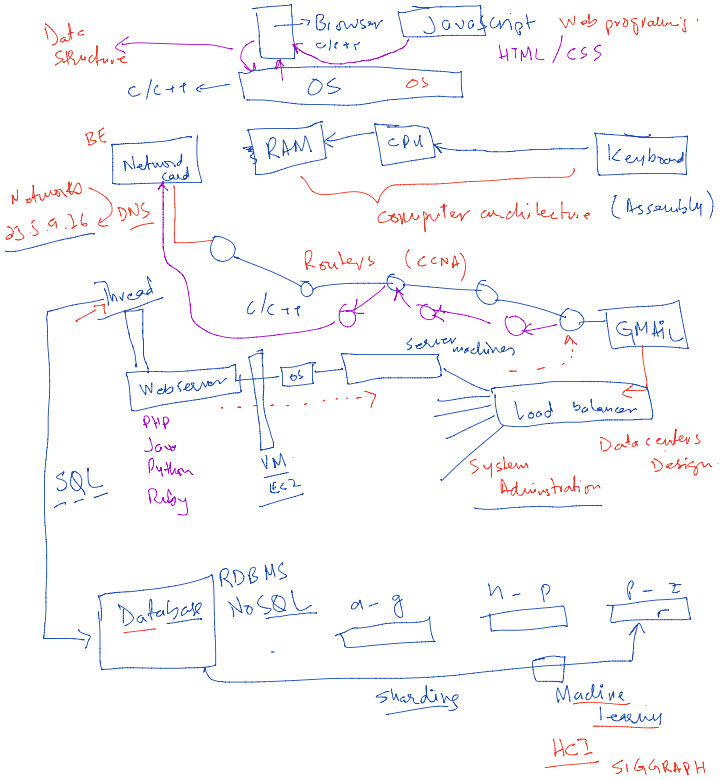
Introduction to Computer Science

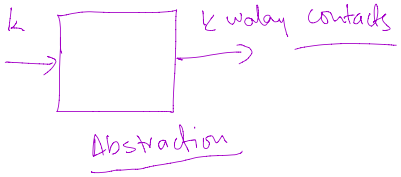
So, what is computer science?


Tools
Computer Science
— Problem Solving.

An overview case study

Let’s see what goes on when you click on a web page!


Browser
c/c++
Javascript
Web programming
HTML / CSS
Data Structure
c/c++
OS
os
BE
Network card
RAM
CPU
Keyboard
Networks
DNS
Computer architecture (Assembly)
Routers (CCNA)
c/c++
Thread
GMail
Server machines
Webserver
OS
Load balancer
PHP
Java
Python
Ruby
VM
EC2
SQL
Data centers
Design
System Administration
RDBMS
Database
NoSQL
a - g
h - p
p - z
Sharding
Machine learning
HCI
SIGGRAPH


k
k way contacts
Abstraction

CS program courses

ITC

Computer programming

Data structures

Database systems

Analysis of algorithms

Operating systems

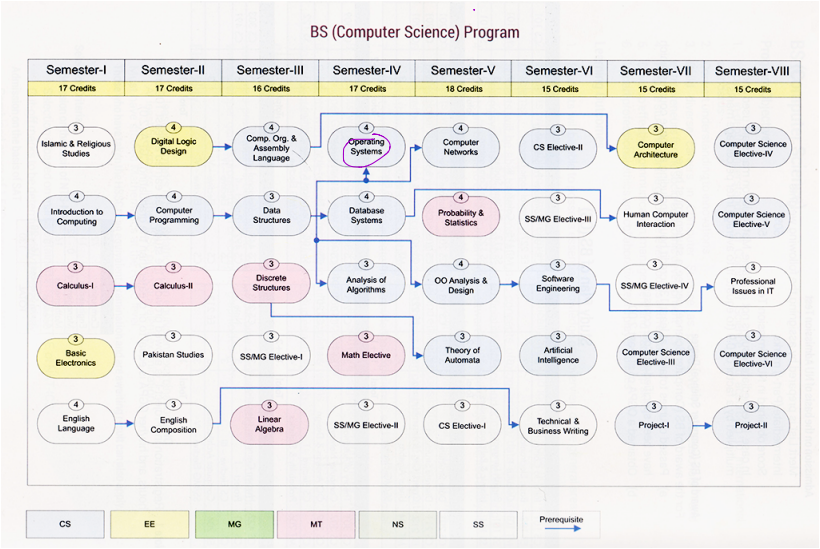
Computer networks

OOA&D / Software engineering

Human computer interaction

Computer architecture / theory of automata

Professional issues in IT


BS (Computer Science) Program
Semester-I
17 Credits
Islamic & Religious Studies 3
Introduction to Computing 4
Calculus-I 3
Basic Electronics 3
English Language 4
Semester-II
17 Credits
Digital Logic Design 4
Computer Programming 4
Calculus-II 3
Pakistan Studies 3
English Composition 3
Semester-III
16 Credits
Comp. Org. & Assembly Language 4
Data Structures 3
Discrete Structures 3
SS/MG Elective-I 3
Linear Algebra 3
Semester-IV
17 Credits
Operating Systems 4
Database Systems 4
Analysis of Algorithms 3
Math Elective 3
SS/MG Elective-II 3
Semester-V
18 Credits
Computer Networks 4
Probability & Statistics 4
OO Analysis & Design 4
Theory of Automata 3
CS Elective-I 3
Semester-VI
15 Credits
CS Elective-II 3
SS/MG Elective-III 3
Software Engineering 3
Artificial Intelligence 3
Technical & Business Writing 3
Semester-VII
15 Credits
Computer Architecture 3
Human Computer Interaction 3
SS/MG Elective-IV 3
Computer Science Elective-III 3
Project-I 3
Semester-VIII
15 Credits
Computer Science Elective-IV 3
Computer Science Elective-V 3
Professional Issues in IT 3
Computer Science Elective-VI 3
Project-II 3
CS
EE
MG
MT
NS
SS
Prerequisite