Week 0 – Introduction

DR. RICCI IEONG, CISSP, CISA, CCFP, CCSK, CCSP, CEH, ISSAP, ISSMP, ISO 27001LA, STAR AUDITOR

Class Schedule

Combined Lectures and Labs session

- Friday 10:30 – 2:20pm, room 4221 (CS Lab 1)

Tutorial Session

- TA: Monday and Wednesday 14:00-15:30, Room No.3654 b
- Instructor: Friday 15:30 – 18:00, Room 3538 (better to email me before coming)

Slides and Lab sheet download

- Check the course webpage https://course.cse.ust.hk/comp4632/

(will be updated every week)

Who am I

Working Experience

- Principal Consultant and Founder of eWalker Consulting Limited (2005 -)
- Consultant of Hewlett Packard HK SAR (2000 – 2005)
- Senior Consultant of PrivyLink HKSAR (2000)
- ACO of Cyberspace Center, HKUST (1997 – 2000)
- Demonstrator, COMP, HKUST (1996 – 1997)

Education

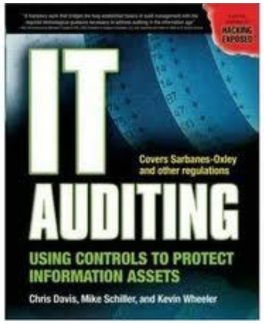
- PhD (2013) in Computer Science Dept, HKU
- MA Arb (2006) in Arbitration and Dispute Resolution, City University HK
- M.Phil (1996) in Computer Science Dept, HKUST
- B.Sc (1994) in Chemistry, CUHK

Others

- Active speaker in HK IT security industry
- Secretary of Information Security and Forensics Society
- Director of Cloud Security Alliance (HK&M) Chapter

My Current Job

Monitor
Plan
Implement
Review


HACKING EXPOSED
IT AUDITING
Covers Sarbanes-Oxley and other regulations
USING CONTROLS TO PROTECT INFORMATION ASSETS
Chris Davis, Mike Schiller, and Kevin Wheeler

Log Walker

FoxyeyⓄ

Local Industry Demand

Consultant?

IT Security Specialists?

Digital Forensics Specialists?

IT Security Manager or CISO?

IT Auditor?

Entrepreneur?

About Instructor, TA and supporting team

Role	Name	Email
Instructor	Dr. Ricci IEONG (Rm 3538)	ricci@ust.hk, ricci@cse.ust.hk or ricci.ieong@gmail.com
TA	Jmaiel Ep Louati, Abir (Rm 3654b)	ajel@ust.hk
Support team	Dr. LEE Wai Leng	leng@ewalker.com.hk
	Kenneth TSE	kenneth@ewalker.com.hk
	Jenius SHIEH	jenius@ewalker.com.hk
	Eric YUEN	eric@ewalker.com.hk
	Rafael WONG	rafael@ewalker.com.hk
	Chak Fu LAU	chakfu.lau@ewalker.com.hk

Important notes

You can use your laptop in the class as most of the lab session are operating in isolated environment within the VM environment

Please keep the original password and don't change that.

Do your assignment in lab but you can also contact us for assistance.

The course is a practical course – Practice, Practice and Practice

IT Security is ever changing and growing world – so this is just the beginning of your IT security life

Your Computer Accounts

You have two computer accounts:

- Your ITSC account
  - This is given to you when you join UST
  - This is your main email account at UST
- Your CSD account
  - This is given to you when you first join a COMP course

- All the class and labs are taught in the Computer Science Department (CSD) lab rooms (we will use room 4221, called CS lab 1)
- Before you can work in those lab rooms, you need to enable your CSD account

How to Enable Your CSD Account

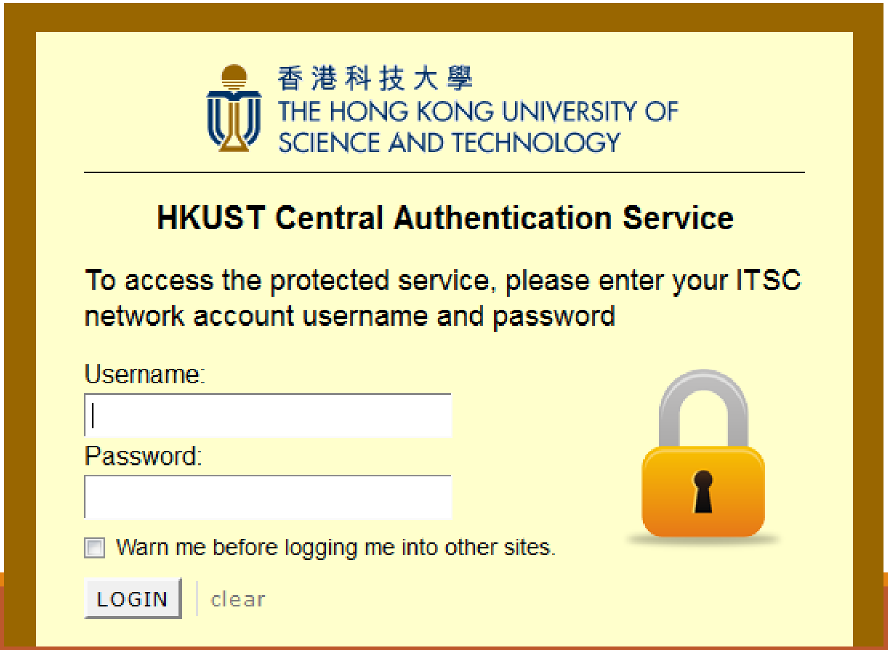
Don't wait for the day of the lab to do this!

Go to a computer in one of the Barns at UST

Start a browser, go to:

https://password.cse.ust.hk:8443/pass.html

Log on using your ITSC details



香港科技大學
THE HONG KONG UNIVERSITY OF SCIENCE AND TECHNOLOGY

HKUST Central Authentication Service

To access the protected service, please enter your ITSC network account username and password

Username:

Password:

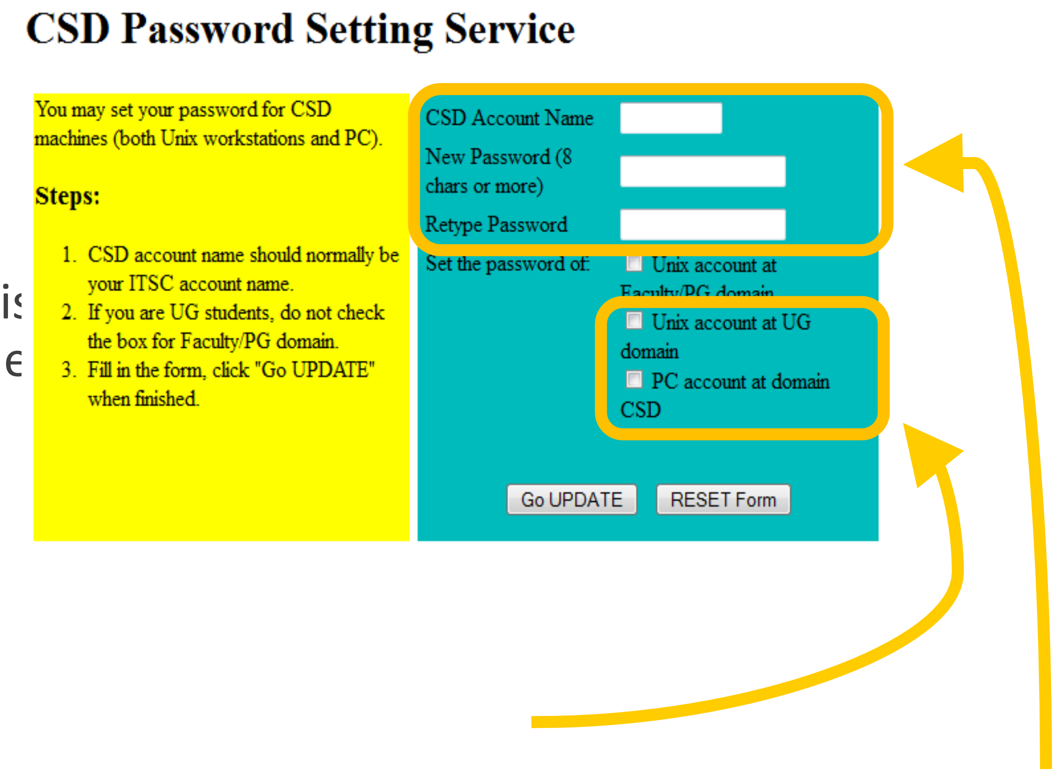
□ Warn me before logging me into other sites.

CSD Password Setting Service

Tick the bottom two check boxes ("Unix account at UG domain" and "PC account at domain CSD")

Enter your ITSC account name and password (your CSD account name is the same as your ITSC account name

Finally, click 'Go UPDATE'



CSD Password Setting Service

You may set your password for CSD machines (both Unix workstations and PC).

Steps:

1. CSD account name should normally be your ITSC account name.
2. If you are UG students, do not check the box for Faculty/PG domain.
3. Fill in the form, click "Go UPDATE" when finished.

CSD Account Name

New Password (8 chars or more)

Retype Password

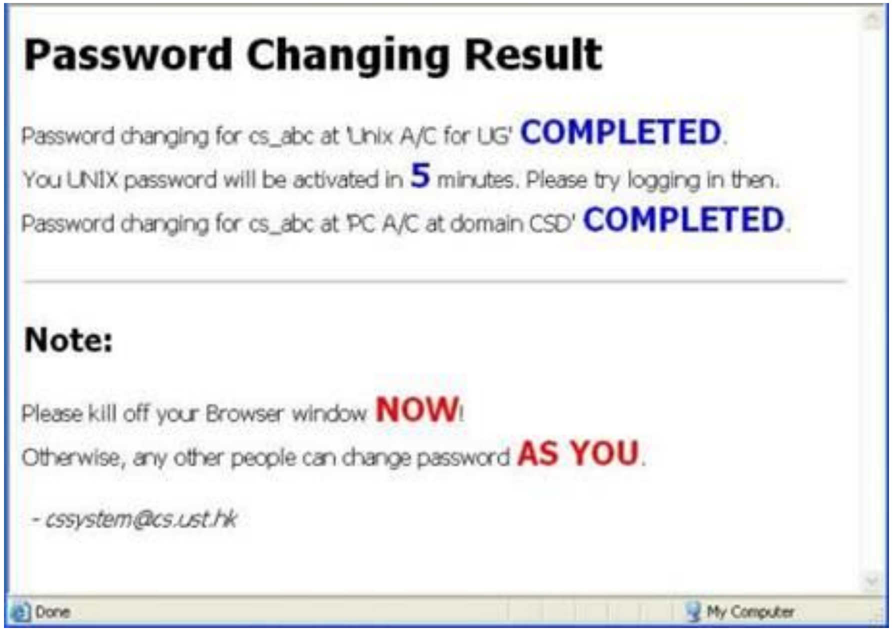
Set the password of: ☐ Unix account at Faculty/PG domain
☐ Unix account at UG domain
☐ PC account at domain CSD

CSD Password Setting Service

You may need to wait a few minutes before
your CSD account is activated

Then you can access any CSD computers
e.g. the computers you will use in CS lab 1

Enable your account before the first lab begins!



Password Changing Result

Password changing for cs_abc at 'Unix A/C for UG' **COMPLETED**.

You UNIX password will be activated in **5** minutes. Please try logging in then.

Password changing for cs_abc at 'PC A/C at domain CSD' **COMPLETED**.

Note:

Please kill off your Browser window **NOW**!

Otherwise, any other people can change password **AS YOU**.

- cssystem@cs.ust.hk

Expectation and Logistics Arrangement

Week	Date	Class Content and Descriptions
1	4-Sep-15	**Basic Concept on IT Security** (Lecture): 3 hours briefing on CyberSecurity practices, Access Control, Authentication, IT Security Principles and Risk Analysis, Threats and Vulnerabilities (Lab): Setup of ESXi server and walk through of vSphere client and VM environment
2	11-Sep-15	**Network Basics** (Lecture): Network basis, Network architecture and security architecture, DNS, LAN and WiFi Security (Lab): nmap scanning, DNS info searching, nessus usage, WiFi setup demo, Wiresharks
3	18-Sep-15	**Network Hacking** (Lecture): Network attack, scanning, sniffing, vulnerability scanning, Denial of Service attacks, malware and virus (Lab): Setup web application environment including DB, web server, ftp server, DNS server and launch nessus and vulnerability scanning
4	25-Sep-15	**Network Infrastructure Secure Design** (Lecture): Network defense mechanism, Firewall, IDS, Anti-DDoS (Lab): Launch Exploits, Setup Firewall, IDS, honeypot and Snort
5	2-Oct-15	**Network Encryption** (Lecture): Encryption basics, PKI, SSL TLS, Secure Protocol, Heartbleed and POODLE (Lab): WiFi analysis and cracking, SSL/TLS traffic analysis
6	9-Oct-15	**Web Application Programming** (Lecture): PHP, Javascript, SQL query and web authentication (Lab): web protocol, HTML, CSS, implement web application with PHP and Javascript,. Connect PHP web site to MySQL database, Setup web authentication system

Expectation and Logistics Arrangement

Week	Date	Class Content and Descriptions
7	16-Oct-15	**Mobile Application Programming** (Lecture): mobile application architecture and life cycle, android programming concept (Lab): Develop of android apps with mobile languages, coding app logic with Java and PHP web site
8	23-Oct-15	**Web Application Hacking** (Lecture): OWASP top 3/10 attack methods including SQL injection, XSS, CSRF (Lab): injection attack, Cross-site scripting and CSRF attack
9	30-Oct-15	**Web and Mobile Application Hacking** (Lecture): Other OWASP top 7/10 attack methods, securing methods, mobile security issues (Lab): attack on web application authentication, session management, web OS hardening metod and cracking of android application
10	6-Nov-15	**Application Security** (Lecture): Application security threats, Secure programming life cycle, Buffer Overflow, Application firewall, secure code review and security assessment concept (Lab) Buffer Overflow code development
11	13-Nov-15	**Hacking Examination**
12	20-Nov-15	**Incident Response and Computer Forensics** (Lecture): Incident Response, Computer Crime, Forensics Investigation and Compliance (Lab): Log analysis and attack tracing HomeWork presentation
13	27-Nov-15	**Advanced Topics on Security** (Lecture): Physical security, management and operation security, Cloud Computing Security (Lab): Actual cloud computing setup (e.g. AWS)

Upcoming Classes

Lecture	Attacks	Defenses
L2: Network Basics	DNS attack	Network architecture and WiFi Security
L3: Network Hacking	Vulnerability scanning, port scanning, Session Replay, Session Hijacking, Man in the middle attacks, Network Eavesdropping, Denial of Services attack, botnet, virus, APT	
L4: Network infrastructure secure design	Exploitation	Firewall, IDS, anti-DDoS
L5: Encryption and Usage	Crack WiFi, Heartbleed, POODLE	Encryption basics, PKI, SSL, TLS
L6: Web Application Programming		
L7: Mobile Application Programming		

Upcoming Classes (Cont.)

Lecture	Attacks	Defenses
L8: Web Application Hacking	Web hacking, injection attack, cross-site scripting, CSRF	
L9: Web and Mobile Application Hacking	Other OWASP top 10 attacks, mobile related attacks	
L10: Application Security	Buffer overflow	Secure programming life cycle, application layer firewall, secure code review, security assessment
L12: Incident Response		Log analysis, Incident Handling, compliance & risk
L13: Advanced Topics in Security – Cloud Security		Cloud security

Course Structure and Grading

Tasks	Score
In class course work	30% (3 marks per week)
Attendance	10% (1 mark per week)
3 Assignments (2 written and one survey paper)	30% (7.5, 7.5 and 15 marks)
1 Exam (on week 11, 13 Nov 2015)	30%

In class course work is expected to be submitted before the start time of following class (within the week) through **LMES**.

Reference Books

Bosworth S., Kabay M. and Whyne E. (2014). Computer Security Handbook. Sixth Edition, Volume 1. John Wiley & Sons, Inc

Donaldson S., Siegel S., Williams C. and Aslam A. (2014). Enterprise Cybersecurity, How to build a successful cyberdefense program against advanced threats. Apress Open

Kurose J. and Ross K. (2013). Computer Networking, A Top-Down Approach. Sixth Edition. Addison-Wesley

Joseph Migga Kizza (2015). Guide to Computer Network Security. Third Edition. Springer-Verlag London

OWASP (2014). OWASP Testing Guide 4.0

Umesh Hodeghatta Rao and Nayak U. (2014). The InfoSec Handbook – An Introduction to Information Security. Apress Open

National Institute of Standards and Technology (2014). Framework for Improving Critical Infrastructure Cybersecurity. Version 1.0.

Stallings, W. (2011). Cryptography and Network Security, Principles and Practice. Fifth Edition. Prentice Hall.

Stallings, W. (2012). Computer Security Principles and Practice. Second Edition. Prentice Hall.