بۆ بەڕێز/ سەرۆکی زانکۆی پۆلیتەکنیک

کۆنووس/ ١

بابەت/ ڕێکخستن و پێداچوونەوەی پڕۆگرامی(مەنهەجی) قۆناغی دووی بەشەکانی تایبەتی لە سلێمانی و چەمچەماڵ و خانەقین

نامازە بە فەرمانی زانکۆمان بە ژمارە (٥٦٠١) لە ٢٠١٤/٨/١٨ و (٦٤٢٨) لە ٢٠١٤/٩/٧ بە مەبەستی پێکهێنانی لێژنەی ڕێکخستن و پێداچوونەوە بە پڕۆگرام و وانەکانی هەردوو قۆناغی یەک و دوو، لێژنەکەمان چەند کۆبوونەوەیەکی ئەنجامدا و ئەم پێشنیار و گۆڕانکاریانە کران :

یەکەم : پڕۆگرام و وانەکانی قۆناغی دوو ڕێکخران بە ڕەچاو کردنی گشت هەفتەکانی تیۆڕ و کرداری، لە هاوپێچی ژمارە یەکدا گشت وانەکان دانراون.

دووەم : لێژنە پێشنیاری گۆڕینی ناوی وانەی (**Web Design**) دەکات بۆ (**Web Programming**).

سێیەم: لێژنە پێشنیاری لابردنی بەشی پراکتیکی وانەی **Information Security** بە هۆکاری سودمەند نەبوونی خوێندکاران لە بەشەوانەی پراکتیکی.

چوارەم: بە زوونترین کات دەست دەکەین بە ڕێکخستن و پێداچوونەوەی پڕۆگرامی قۆناغی یەک.

کۆنووس داخرا.

هاوپێچ/

- وێنەیەک لە پڕۆگرامی خوێندنی قۆناغی دوو

ئەندام ڕێبوار ملا نبی	ئەندام علي جليل ابراهيم	ئەندام هيمن محي الدين كريم
ئەندام یونس محمد داود	سەرۆکی لێژنە پ.ی.د فاضل سلمان عبد	

3. Information Security

Subject Name	Stage	Number of Hours in Week		
Information Security	Second	Theory	Practical	Total
		2	-	2

3.1 Course Overview

This course focuses on the fundamentals of information security that are used in protecting both the information present in computer storage as well as information transmission over computer networks. Information security has also emerged as a national goal and homeland security issues. In this course, we will look into such topics as fundamentals of information security, computer security technology and principles, access control mechanisms, cryptography algorithms, software security, physical security, and security management and risk assessment.
By the end of this course, class members will be able to describe major information security issues and advise individuals how to protect their data.

3.2 Course objectives

Cyber security is now widely recognised as an international priority, with hacking, malicious code, and data theft being just three of the many systems, distributed systems, networks and representative applications.
Course objectives are listed below:

- Explain the challenges and scope of information security;
- Develop an understanding of security policies (such as authentication, integrity and confidentiality), as well as protocols to implement such policies in the form of message exchanges.
- Develop a basic understanding of cryptography, how it has evolved, and some key encryption techniques used today.
- Describe the access control mechanism used for user authentication and authorization;
- Explain the importance of physical security and discuss ways to improve physical security of an enterprise;
- Explain the use of security tools as firewalls, VPNs, and intrusion prevention systems;
- Explain malicious software issues and threats;
- Describe the basic process of risk management.

3.3 References

1. Principles of Information Security, 4th edition - Michael E. Whitman, Herbert J. Mattord.
2. A Practical Guide to Managing , Information Security, Steve Purser , 2004
3. NFORMATION SECURITY, Principles and Practice, Second Edition, Mark Stamp and San Jose State University , San Jose, CA, 2011

3.3.1 Web References :

- https://www.cs.purdue.edu/homes/clifton/cs526/
- http://www.utdallas.edu/~zxl111930/fall2012.html#toc2

3.4 Theoretical Syllabus

Week	Syllabus Details
1-2	***Introduction to Information Security*** • Brief History of Information Security • What Is Security? • Components of an Information System • Balancing Information Security and Access • Approaches to Information Security Implementation • System Development Life Cycle • Security System Development Life Cycle • Security Professionals and the Organization • Communities of Interest
3-5	***The Need for Security*** • **Business Needs First** • **Threats** • **Attacks** ✓ Malicious Code ✓ Hoaxes ✓ Back Doors ✓ Password Crack ✓ Brute Force ✓ Dictionary ✓ Denial-of-Service (DoS) and DistributedDenial-of-Service(DDoS) ✓ Spoofing ✓ Man-in-the-Middle ✓ Spam ✓ Mail Bombing ✓ Sniffers ✓ Social Engineering ✓ Pharming ✓ Timing Attack • **Secure Software Development**
3-5	**An Overview of Risk Management** • Risk Identification • Risk Assessment • Risk Control Strategies • Selecting a Risk Control Strategy • Quantitative Versus Qualitative Risk Control Practices

6	***Planning for Security*** • Information Security Planning and Governance • Information Security Policy, Standards, and Practices • Security Education, Training, and Awareness Program • Continuity Strategies
7-10	***Planning for Security*** • Access Control ✓ Identification ✓ Authentication ✓ Authorization ✓ Accountability • Firewalls ✓ Firewall Processing Modes ✓ Firewalls Categorized by Generation ✓ Firewalls Categorized by Structure ✓ Firewall Architectures ✓ Selecting the Right Firewall ✓ Configuring and Managing Firewalls ✓ Content Filters • Protecting Remote Connections ✓ Remote Access ✓ Virtual Private Networks (VPNs)
11-14	***Planning for Security*** • Foundations of Cryptology • Cipher Methods • Cryptographic Algorithms ✓ Symmetric Encryption ✓ Asymmetric Encryption ✓ Examples • Cryptographic Tools ✓ Public-Key Infrastructure (PKI) ✓ Digital Signatures ✓ Digital Certificates ✓ Hybrid Cryptography Systems ✓ Steganography • Protocols for Secure Communications • Securing Internet Communication with S-HTTP and SSL • Securing E-mail with S/MIME, PEM, and PGP • Securing Web Transactions with SET, SSL, and S-HTTP • Securing Wireless Networks with WEP and WPA

	• Securing TCP/IP with IPSec and PGP • Attacks on Cryptosystems ✓ Man-in-the-Middle Attack ✓ Correlation Attacks ✓ Dictionary Attacks ✓ Timing Attacks ✓ Defending Against Attacks
15-18	Intrusion Detection and Prevention Systems ✓ IDPS Terminology ✓ Why Use an IDPS? ✓ Types of IDPS ✓ IDPS Detection Methods ✓ IDPS Response Behaviour ✓ Selecting IDPS Approaches and Products ✓ Strengths and Limitations of IDPSs ✓ Deployment and Implementation of an IDPS ✓ Measuring the Effectiveness of IDPSs • Honeypots, Honeynets, and Padded Cell Systems ✓ Trap-and-Trace Systems ✓ 2.2 Active Intrusion Prevention • Scanning and Analysis Tools ✓ Port Scanners ✓ 3.2 Firewall Analysis Tools ✓ 3.3 Operating System Detection Tools ✓ 3.4 Vulnerability Scanners ✓ 3.5 Packet Sniffers ✓ 3.6 Wireless Security Tools • Biometric Access Controls ✓ Effectiveness of Biometrics ✓ Acceptability of Biometrics
19-20	***System and Network Security*** • Secure design principles (Least-privilege, fail-safe defaults, complete mediation, separation of privilege) • TCB and security kernel construction • System defense against memory exploits • UNIX security and Security-Enhanced Linux (SELinux) • Windows security • TCP/IP security issues • DNS security issues and defenses • TLS/SSL
	Software Security • Vulnerability auditing, penetration testing • Sandboxing

21	• Control flow integrity
22-23	***Web Security*** • User authentication, authentication-via-secret and session management • Cross Site Scripting, Cross Site Request Forgery, SQL Injection
24-27	***Implementing Information Security*** • Information Security Project Management ✓ Developing the Project Plan ✓ Project Planning Considerations ✓ Scope Considerations ✓ The Need for Project Management • Technical Aspects of Implementation ✓ Conversion Strategies ✓ The Bull's-Eye Model ✓ To Outsource or Not ✓ Technology Governance and Change Control • Nontechnical Aspects of Implementation ✓ The Culture of Change Management ✓ Considerations for Organizational Change • Information Systems Security Certification and Accreditation
28	***Information Security Maintenance*** • Security Management Maintenance Models • Digital Forensics