Subject Description Form

Subject Code	EIE3120
Subject Title	Network Technologies and Security
Credit Value	3
Level	3
Pre-requisite	The students are expected to possess basic knowledge about network protocols (Ethernet and TCP/IP) and cryptography (public-key and private-key encryption, hash function, digital signature).
Co-requisite/ Exclusion	Nil
Objectives	This subject teaches students the features and technologies about public and private telecommunication and data networks for the provision of security services of confidentiality, integrity, availability, and authentication.
Intended Subject Learning Outcomes	**Upon completion of the subject, students will be able to:** Category A: Professional/academic knowledge and skills 1. Describe common security issues arising from the use of telecommunication and data networks for the transmission of information 2. Describe methods for dealing with security issues as described in (1) 3. Identify and solve network security problems by applying knowledge learnt and by using appropriate tools and techniques 4. Communicate effectively and understand the importance of life-learning as well as continual professional development
Subject Synopsis/ Indicative Syllabus	**Syllabus:** **Fundamentals:** 1. Basic network technologies and components: Internet, Ethernet, VPN, hub, switch, router, network layer protocols (IP, ICMP,DHCP,NAT), transport layer protocols (TCP, UDP) 2. Network security model, services, mechanisms, and threats: authentication, access control, data confidentiality, data integrity, availability, eavesdropping, DOS (denial-of-service) **Applications:** 3. Authentication and Key Distribution for protected communication: Kerberos, X.509, Public Key Infrastructure, Certification Authority 4. Firewalls: packet filtering, application level gateway, encrypted tunnels 5. Internet Protocol Security: ESP and IKE 6. Transport layer security: Secure Sockets Layer (SSL) and Transport Layer Security (TLS), SSH
Teaching/Learning Methodology	Lecture: Lectures will be used as the main instruction mechanism, to be supplemented with interactive discussion, multimedia (video, web-site information) presentation materials Tutorial: Tutorials will be used for strengthening students' understanding about taught materials through quizzes, worksheets, further reading, and discussions Labs: Laboratory exercises will be used to provide enable students apply what they have learnt through hands-on activities such as analyzing network securities issues, ethical hacking, and implementing security mechanisms Case studies: Case studies will be used to enable students to probe into a real-life security issue deeply through extensive readings and research.

<table>
<tr><td></td><td>Students communication skills will also be cultivated with presentation and report writing</td></tr>
<tr><td>Assessment Methods in Alignment with Intended Subject Learning Outcomes</td><td>
<table>
<tr><th rowspan="2">Specific Assessment Methods/Tasks</th><th rowspan="2">% Weighting</th><th colspan="4">Intended Subject Learning Outcomes to be Assessed (Please tick as appropriate)</th></tr>
<tr><th>1</th><th>2</th><th>3</th><th>4</th></tr>
<tr><td>1. Continuous Assessment (total 50%)</td><td></td><td></td><td></td><td></td><td></td></tr>
<tr><td>• Assignment</td><td>10%</td><td>√</td><td>√</td><td></td><td>√</td></tr>
<tr><td>• Case study report</td><td>20%</td><td></td><td></td><td>√</td><td></td></tr>
<tr><td>• Lab reports</td><td>10%</td><td></td><td></td><td>√</td><td></td></tr>
<tr><td>• Test</td><td>10%</td><td>√</td><td>√</td><td></td><td>√</td></tr>
<tr><td>2. Examination</td><td>50%</td><td>√</td><td>√</td><td></td><td>√</td></tr>
<tr><td>Total</td><td>100%</td><td colspan="4"></td></tr>
</table>
</td></tr>
<tr><td>Student Study Effort Expected</td><td>
<table>
<tr><td>Class contact (time-tabled):</td><td></td></tr>
<tr><td>• Lecture</td><td>24 Hours</td></tr>
<tr><td>• Tutorial/Laboratory/Practice Classes</td><td>15 Hours</td></tr>
<tr><td>Other student study effort:</td><td></td></tr>
<tr><td>• Lecture: preview/review of notes; homework/assignment; preparation for test/quizzes/examination</td><td>36 Hours</td></tr>
<tr><td>• Tutorial/Laboratory/Practice Classes: preview of materials, revision and/or reports writing</td><td>30 Hours</td></tr>
<tr><td>Total student study effort:</td><td>105 Hours</td></tr>
</table>
</td></tr>
</table>

Reading List and References	**Reference Books:** A set of comprehensive lecture notes will be provided to students for the study of this subject, together with tutorial worksheets and laboratory hand-outs. Students may refer to the following suggested reading lists for more in-depth and extensive discussion of topics covered and end-of chapter problem sets (when applicable): 1. Stallings, William, *Cryptography and Network Security: Principles and Practice (6th Edition)*: Pearson, c2014. 2. Stewart, James Michael, Burlington, *Network security, firewalls, and VPNs*, 2nd ed., Mass.: Jones & Bartlett Learning, c2014. 3. Stallings, William, Upper Saddle River, *Network security essentials: applications and standards*, 5th ed., N.J.: Pearson Education, c2014. 4. Jacobs, Stuart, Books24x7. ; Wiley (DDA)_d., Hoboken, N.J. : John Wiley & Sons ; Piscataway, *Security management of next generation telecommunications networks and services*, NJ: IEEE Press, c2014. 5. McMillan, Troy, Indianapolis, *CISSP cert guide*, Indiana: Pearson, 2014, 6. Boston, *Guide to network security*, Mass. : Course Technology/Cengage Learning, c2013. 7. Chen, Lidong, Boca Raton, *Communication system security*, FL: CRC Press/Taylor & Francis Group, c2012. **Classics reading materials:** 8. *ITU-T Recommendation X.800 Data Communication Networks: Open System Interconnection (OSI); Security, Structure and Applications*, ITU-T CCITT, Geneva, 1991 (PDF version available from *http://www.itu.int/rec/T-REC-X.800-199103-I/e*) 9. "Communication theory of secrecy systems" in *Claude Elwood Shannon: collected papers*, Shannon, Claude Elwood, 1916-2001, New York: Institute of Electrical and Electronics Engineers, c1993., PolyU Lib. Acc. No.: TK5101 .S448 1993, (p.84-143)
Last Updated	December 2015
Prepared by	Dr H. Hu