**Week 4: Network Security OPenSSL. Graded LabExercise. Individual.  
For Wednesday tutorial group only.!**

**Security Objectives**

Can be: Privacy, Non-Repudiation, Message Integrity, Sender Authentication, Replay.

This is the text file that need to be sent are as followed

“ Random: Nonce(YourName\_STudentID\_RandomNonce\_32Digit\_HexDecimal) : *PENGURUSAN PENDAKIAN DI SEMENANJUNG MALAYSIA : MALIM GUNUNG PERHUTANAN Mohd Yussainy MY1, Zuraida Z1, Mohamad Rizal R1, Mohammad Ifratshim MS1, Che Engku Nor Amiza CE1, Mardiana Salihah M1 and Mohd Zulkhairi Z1 1Forestry Department Peninsular Malaysia, W.P. Kuala Lumpur (MALAYSIA) E-mail: yussainy@forestry.gov.my Abstrak Sehingga tahun 2020, terdapat 116 Taman Eko Rimba dan 16 Hutan Taman Negeri telah ditubuhkan dan lebih 240 lokasi hotspot pendakian gunung dan bukit dalam Hutan Simpanan Kekal (HSK) di Semenanjung Malaysia. Aliran rekreasi masa kini telah berubah daripada santai ke arah rekreasi lasak yang penuh dengan cabaran dan memerlukan jurupandu arah yang memiliki kemahiran tertentu. Ada tanggapan dimana terdapat personaliti yang unik di kalangan pendaki yang menarik mereka ke arah menjadikan malim gunung sebagai kerjaya. Inventori personaliti Malim Gunung Perhutanan telah dibangunkan dan diuji untuk mendapatkan maklumat personaliti tersebut. Pada tahun 2018 sehingga 2021, terdapat 852 kes kehilangan di hutan telah direkodkan. Jabatan Perhutanan Semenanjung Malaysia (JPSM) menyasarkan untuk melatih 1,000 orang Malim Gunung Perhutanan (MGP) dengan modul latihan yang komprehensif. Melalui pengukuhan kemahiran di kalangan masyarakat setempat yang berperanan sebagai malim gunung, keyakinan pendaki terhadap perkhidmatan yang ditawarkan akan meningkat. Individu yang ditauliahkan sebagai MGP juga akan berperanan sebagai first responder ketika menjalankan aktiviti dalam kawasan HSK serta duta kecil JPSM dalam pengurusan pendakian di Semenanjung Malaysia. Penguatkuasaan sepenuhnya perkhidmatan MGP ini akan bermula pada tahun 2023 dijangka dapat membantu JPSM menyelesaikan isu pengurusan pendakian selain daripada membantu komuniti setempat menjana pendapatan dalam ekopelancongan melalui perkhidmatan MGP. Kata Kunci: Malim Gunung Perhutanan, Pengurusan Pendakian, Inventori Personaliti 2 1.0 PENDAHULUAN 1.1 Hutan Simpanan Kekal (HSK) kaya dengan kepelbagaian biodiversiti serta memiliki landskap yang menarik dan unik meliputi bukit bukau, gunung ganang, air terjun, jeram, gua dan geologi yang begitu sesuai untuk aktiviti rekreasi. Sehingga tahun 2020, seluas 4.8 juta hektar telah diwartakan sebagai HSK di Semenanjung Malaysia (JPSM, 2020) dan sebanyak 132 buah Taman Eko Rimba (TER) dan Hutan Taman Negeri (HTN) telah ditubuhkan di dalam HSK oleh Jabatan Perhutanan Negeri. Aktiviti mendaki bukit dan gunung merupakan aktiviti yang biasa dilakukan di dalam HSK dan dilihat mampu memberikan faedah kepada semua lapisan masyarakat. Antara faedah yang diperolehi adalah dapat meningkatkan potensi diri dari segi kecerdasan, keyakinan diri, ketahanan mental dan kepuasan diri. 1.2 Peningkatan kepada aktiviti pendakian ini dapat dilihat melalui peningkatan bilangan pengunjung ke beberapa lokasi puncak bukit dan gunung yang popular di Negeri Pahang, Perak, Terengganu dan Kelantan. Aktiviti mendaki bukit dan gunung di dalam HSK ini juga menarik minat ramai kerana keadaan faktor geografinya yang mempunyai banjaran serta landskap yang menarik serta keadaan iklim khatulistiwa yang membolehkan para pendaki menjalankan aktiviti pendakian sepanjang tahun. Antara 12 senarai gunung tertinggi di Malaysia, 7 daripada adalah merupakan yang terdapat di Semenanjung Malaysia dan menjadi kegemaran pada pendaki pada masa kini. 2.0 PERNYATAAN MASALAH 2.1 Pada masa kini, aktiviti mendaki gunung yang dahulunya hanya menjadi aktiviti riadah dan sekadar mengisi masa lapang semakin menjadi tumpuan dan telah berkembang menjadi suatu industri yang menjana pendapatan malah ada yang menjadikannya sebagai satu karier bagi penggiat aktiviti mendaki gunung. Peningkatan risiko kemalangan semasa menjalankan aktiviti menyebabkan* “

E.g :

“ Random: Nonce(ChanWaiKok\_MU12345\_RandomNonce\_12345678901234567890123456789012) : *PENGURUSAN*

**Question. Single Objective Security. Table 1.**

Just do one of the following question (StudentID)%6 = Question No.

The symmetric password is not abc123. Both Alice and Bob don’t have anything to begin with other that the private and publickey. Assume their PubKey is trustworthy. The text message to be sent is stated above.

|  |  |  |  |
| --- | --- | --- | --- |
| Q\_No | Alice send message to Bob |  |  |
| 0 | Privacy: Only Bob can decrypt the message. |  |  |
| 1 | Non-repudiation: Alice cannot denial she sent this signed message to Bob. For this case it is the same as sender authentication. |  |  |
| 2 | Message integrity: Both Alice/Bob must ensure that the message is not modified by anyone. |  |  |
| 3 | Non Replay: Nobody including Alice or Bob can replay this message again |  |  |
| 4 | Message Hiding: There is a hidden message inside the text message which Alice want to convey to Bob. Everyone can see the message but cannot know the hidden message |  |  |
| 5 | Receiver acknowledgement. Alice want to send a “saman” to Bob. She need to make sure Bob are forced to acknowledge the receipt of this message. Assume Bob has an open channel to receive any message but he is nasty and selectively choose to accept good profitable message and ignore bad/$losing message. |  |  |

Note: Question No 1,2,3,4,5: every Tom Dick and Harry can see the message content.

**Submission guidelines. Hardcopy submission.**

1. Front cover Name, ID, Tutorial Day/Time/Section
2. Submit a 2-4 pages staple report with
3. all the openssl command used by Alice to send the file.
4. All Openssl command used by Bob to receive the file
5. Screenshot of the output. Proof that your solution actually work
6. No need color printing no need plastic. Just staple will do.
7. Demo during tutorial hour. Please bring along your hardcopy during demo.

General Grading Policy: Everybody start with full mark. Each mistake there will be mark deduction.