Security in Ad Hoc Networks: Project Description

Carlos Viescas Huerta

May 13, 2018

1 Contents and key areas

The project consists studying the nature of ad hoc networks and its security issues, implementing a system with Raspberry Pi's that is able to transmit data securely with encryption methods. Among the contents, some key areas will be:

- Ad hoc routing protocols.
- Be sure that data (plain text, files) can be transmitted across the network and that nodes can obtain up to date information.
- To build the network, use 3-4 nodes: 2-3 RPi's (+ my computer).
- Confidentiality:
  - Symmetric Cryptography.
  - Asymmetric Cryptography.
- Authentication and key distribution.

2 Learning outcomes

Knowledge

- Understanding and knowledge about ad hoc networking routing protocols, symmetric and asymmetric key cryptography, man-in-the-middle attacks and network authentication.

2.1 Skills:

- Being able to implement a wireless ad hoc system with multiple devices.
- Being able to implement encryption algorithms.
- Being able to implement authentication algorithm.
- Evaluate and report a Linux-based project.

2.2 Competences

- Define, initiate and carry out independently an embedded Linux project, including management of time, knowledge and dissemination.
- Take responsibility for self professional development and specialization.
- Apply and disseminate research-based knowledge.

3 References.

3.1 Implementation

1. http://etutorials.org/Linux+systems/unix+internet+security/Part+II+Security+Building+Blocks/
2. https://en.wikipedia.org/wiki/Symmetric-key_algorithm#Implementations
3. https://cryptography.io/en/latest/hazmat/primitives/asymmetric/
4. https://docs.oracle.com/cd/E19683-01/806-4075/ipsec-ov-11/index.html
5. https://www.sciencedirect.com/science/article/pii/S2213020916301963
6. http://www.ee.ucl.ac.uk/lcs/previous/LCS2002/LCS064.pdf

3.2 Setting up the network.

1. https://adhocloopback.wordpress.com/2016/09/07/setting-upjoining-and-i
2. http://scalabilly.com/category/raspberry-pi/
3. https://hackaday.com/2012/11/14/mesh-networking-with-multiple-raspberr
4. https://raspberrypi.stackexchange.com/questions/63045/using-raspberry-
5. https://en.wikipedia.org/wiki/List_of_ad_hoc_routing_protocols
6. http://www.netlab.tkk.fi/opetus/s38030/k02/Papers/12-Petteri.pdf
7. http://www.cs.tut.fi/courses/TLT-2756/lect05.pdf

3.3 Confidentiality of data

- https://www.intechopen.com/books/mobile-ad-hoc-networks-protocol-desig
- http://encryptionhowto.sourceforge.net/previous/Encryption-HOWTO-0.2.1-5.html
- http://studyraspberrypi.blogspot.dk/2016/01/sending-rsa-encrypted-mess html
- http://www.instructables.com/id/Encrypted-Messages-With-Bitmessage-on-
- https://www.raspberrypi.org/forums/viewtopic.php?t=145155
- https://onehundred15.wordpress.com/2013/11/15/encrypting-network-traff

3.4 Authentication

1. https://pdfs.semanticscholar.org/ee4a/79a1e6b70d6b47f52843df660025998d
   pdf
2. https://ac.els-cdn.com/S0895717711000975/1-s2.0-S0895717711000975-main
   pdf?_tid=d4baada5-00a7-4a66-a3e2-a0f1d166fb9b&acdnat=1520508825_
   e680aa9e8e5a5e6964d3ffff39c7f9e9
3. http://www.comsec.uwaterloo.ca/~khoeper/cacr2004-03.pdf
4. http://staff.bath.ac.uk/masrjb/Papers/authadhoc.pdf
5. https://www.cse.unsw.edu.au/~salilk/papers/book/Auth_Ad_Hoc.pdf

3.5 External threats

1. http://www.cursodehackers.com/ManInTheMiddle.html
2. https://hipertextual.com/archivo/2014/06/ataque-man-in-the-middle/
3. https://en.wikipedia.org/wiki/Man-in-the-middle_attack
4. https://www.tutorialspoint.com/wireless_security/wireless_security_adhoc_connection_attack.htm
5. https://arxiv.org/pdf/1111.4090.pdf
6. http://onlinelibrary.wiley.com/doi/10.1002/wcm.2527/pdf