Project	**IEEE 802.20 Working Group on Mobile Broadband Wireless Access** <**http://grouper.ieee.org/groups/802/mbwa**>
Title	Wireless LAN Security Threats
Date Submitted	**2003-01-12**
Source(s)	Alan Chickinsky Northrop Grumman/TASC 4801 Stonecroft Blvd Chantilly Va 20151 Voice: 703-633-8300 x8554 Fax: 703-449-4900 Email: achickinsky@northropgrumman.com
Re:	Security Tutorial
Abstract	Unlike wire based MANs, wireless MANs pose unique security problems. To monitor communications on a wire based MAN; the observer must be physically located near or in direct contact with the wire medium. In the wireless MAN, the observer must be within the broadcast signal range. Because one cannot completely control the signal broadcast pattern, there must be message encryption to limit interception. Encryption of a message requires a plain text message, an algorithm, and a key. To quickly and accurately decipher the encrypted message, one needs the algorithm, a key and the encrypted message. In an IEEE 802.20 Wireless MAN, an ease dropper has the encrypted message, and the algorithm. Therefore the IEEE 802.20 must select a method that makes it difficult for the ease dropper to discover the key. This paper proposes several methods to limit the ability to discover the key. It also proposes methods to discover data forgery of valid messages
Purpose	Address security issues for a Wireless MAN
Notice	This document has been prepared to assist IEEE 802.20 MBW. It is offered as a basis for discussion and is not binding on the contributing individual(s) or organization(s). The material in this document is subject to change in form and content after further study. The contributor(s) reserve(s) the right to add, amend or withdraw material contained herein.
Release	The contributor grants a free, irrevocable license to the IEEE to incorporate material contained in this contribution, and any modifications thereof, in the creation of an IEEE Standards publication; to copyright in the IEEE's name any IEEE Standards publication even though it may include portions of this contribution; and at the IEEE's sole discretion to permit others to reproduce in whole or in part the resulting IEEE Standards publication. The contributor also acknowledges and accepts that this contribution may be made public by IEEE 802.20 MBWA.
Patent Policy	The contributor is familiar with IEEE patent policy, as outlined in Section 6.3 of the IEEE-SA Standards Board Operations Manual <http://standards.ieee.org/guides/opman/sect6.html#6.3> and in *Understanding Patent Issues During IEEE Standards Development* <http://standards.ieee.org/board/pat/guide.html>.

Wireless LAN Security Threats

Alan Chickinsky
Northrop Grumman/TASC
January 11, 2003

Security Events

- Human Initiated Events
- Data Privacy
- Data Forgery
- Denial of Service
- Hardware Errors

Human Initiated Events

- Two common errors are
  - Administrators improperly configure systems
  - System software errors.

Data Privacy

- A Data Privacy security event occurs when an unauthorized user gains access to all the unencrypted traffic
- To decrypt the message, the user needs
  - the encrypted message
  - the algorithm
  - the key

Data Forgery

- A Data Forgery security event occurs when an unauthorized user inserts data into network as a valid user.
- There are two ways valid data enters the network
  - Replay
  - Mimicking

Denial of Service

- An intruder floods the network with either valid or invalid messages
  - Force the system to use valuable battery power
  - Flood the Access Point

Hardware Errors

- The hardware could
  - Cease to function
  - Jam the channel by sending constant
  - Send random patterns on the channel that look like valid messages

Encryption

- Encryption is composed of 4 elements
  - Plain text
  - Algorithm
  - Key
  - Encrypted message
- Given any three of the four, you can solve for the fourth

Encryption Algorithms

E (i) = k(i) <operator> p(i)

for i = 1 to number of bits in the key

Where

E(i) is the i-th bit of the Encrypted message

k(i) is the i-th bit of the key

<operator> is the mathematical operator

p(i) is the i-th bit of the plain text operator

Encryption Algorithms

E (i) = k(i) <operator> p(i) <operator> m(i)

for i = 1 to number of bits in the key

Where

E(i) is the i-th bit of the Encrypted message

k(i) is the i-th bit of the key

<operator> is the mathematical operator

p(i) is the i-th bit of the plain text message

m(i) is the i-th bit of the message sequence key

Encryption Algorithms

E (i) = F {k, p , m }

for i = 1 to number of bits in the key

Where

E(i) is the i-th bit of the Encrypted message

k is the key

<operator> is the mathematical operator

p is the plain text message

m is the message sequence key

F {..} is a mathematical function

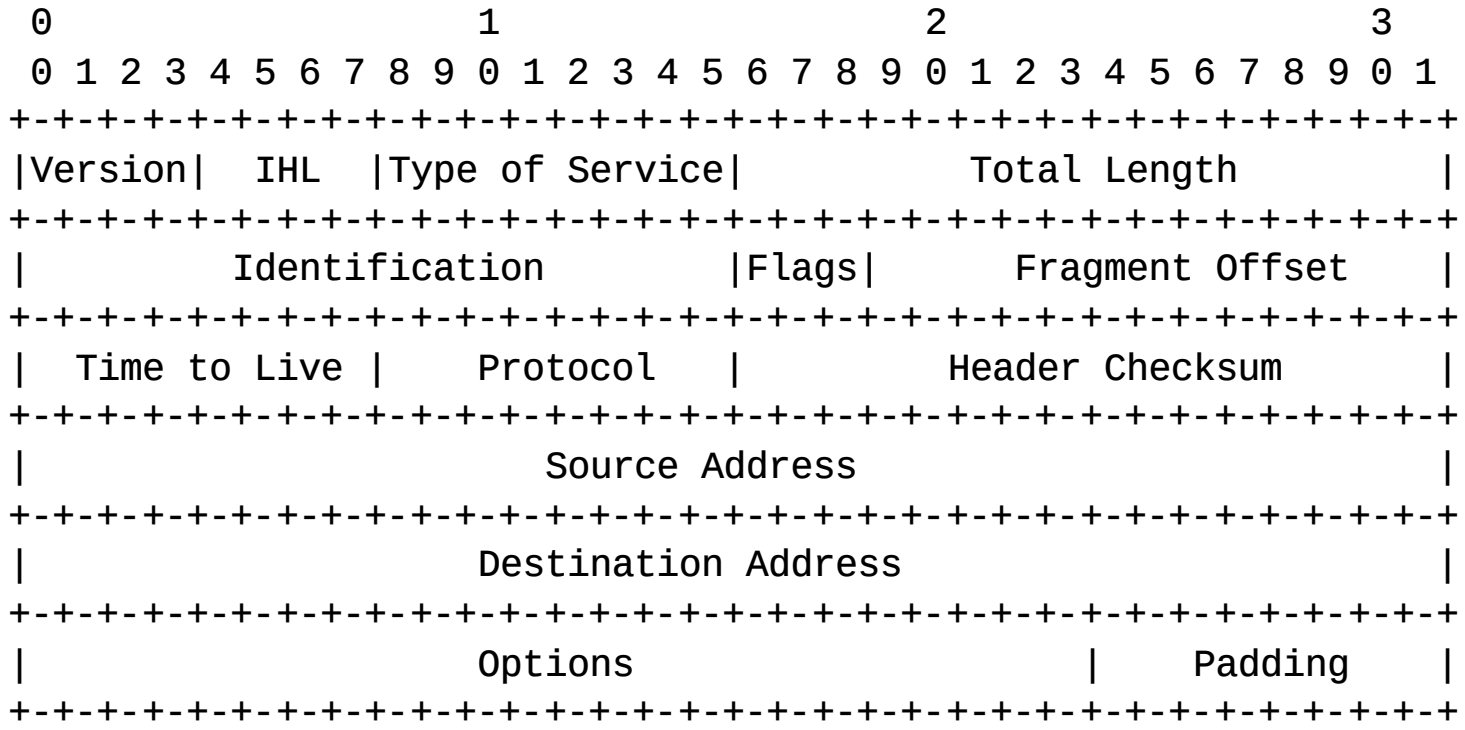
Reading the Message

- An Intruder has
  - Algorithm
  - Encrypted message
- An Intruder needs
  - Valid Plain Text (First bits only)

Encryption Algorithms

- Assume
  - Random message text
- Problem
  - IP Headers are not random
  - Of the first 128 bits, only 56 bits change

The IP Header



Determining the 56 Change Bits

- The 56 change bits
  - Identification is a sequence number
  - Time to Live is a constant
  - Message size is same as encrypted message size
  - Checksum is a created with fixed information and the items above

Assigning the First Key

- Assume a user powers on a device in a strange city
- How do both the base station and the mobile device get the “unique” first key?

Replaying a Message

- Each message has a unique sequence number
- Why?
  - A sequence of messages could give access to a portion of the network

Different Keys

- Best encryption is each message is sent using a different key
- Can create a list of keys
- Create a unique key for each message with a base and a sequence number

Increasing Security

- If we change the encryption algorithm to randomly add bytes to the plain text message - we now have an equation that always has a random pattern

Two Methods

- Prefixing each message with a fixed number of random bits, the key is randomised for each transmission
  - The prefix bits only appear on the wireless transmission.
- Randomly adding a character sequence to the message.
  - The sequence would have an escape character followed by a random character

Further Security

- Always send messages in fixed block sizes
- Multiple fixed block sizes
- Pad message with random characters
- If we are message sensitive, then use context padding

Data Forgery-Replay

- If each message sent over the wireless link has a unique message number, and there is a fixed relationship between message numbers then a replay attack would send messages with an incorrect message number.
- When all the available message numbers are used, a new encryption key is required before further data message transfer can occur.

Data Forgery-Mimicking

- We assume
  - the Hacker does not have the valid key for the current session
  - the distribution of keys and validation of any key requests are outside of this discussion.
- There is an issue on what does a system do when it “logs-off” the network.
  - Will the key would be retired on termination?

Data Forgery –PHY Layer

- The RF interface could use the subtle hardware differences in each transmitter to identify any type of data forgery.

Hardware Errors –PHY Layer

- There are numerous algorithms to methods to detect errors and minimize hardware errors

Conclusion

The paper has proposed several alternatives to create a secure environment to send data. More investigation is needed to determine if some subset of the proposed methods produce a secure environment