The University of Queensland
School of Information Technology and Electrical Engineering

Semester 2, 2017

COMS3000/7003 – Tutorial 12 (Week 13), Answers

Q1) A nearby Access Point (AP) is using IEEE 802.11b channel 8. What channels can you use on another 802.11b AP, while avoiding significant interference with the existing AP?

Answer:
There are 14 IEEE 802.11b DSSS channels, each 22 MHz wide, with 13 spaced 5 MHz apart from 2.412 GHz to 2.472 GHz and channel 14 at 2.484 GHz. Channel 8 is centred on 2.447 GHz, occupying from 2.436 GHz to 2.458 GHz.

Thus only Channels (with centre frequencies) 1 (2.412 GHz), 2 (2.417 GHz), 3 (2.422 GHz) and 13 (2.472 GHz) are clear. Channel 14 (2.484 GHz) is not permitted in Australia.

Q2) What were the main failings of the Wired Equivalent Privacy (WEP)?

WEP One-way Authentication
WEP authentication is client-based only. This means that the client has to prove its identity to the AP but not vice versa. Thus a rogue AP may successfully authenticate the client station and then subsequently will be able to capture all the packets sent by that station through it.

Static WEP Keys
There is no concept of dynamic or per-session WEP keys in IEEE 802.11b specification. Moreover the same WEP key has to be manually entered at all the stations in the WLAN, causing key management issues. Such key management overhead may result in WEP keys that are not changed frequently.

WEP Key Vulnerabilities
Key Size
Many parties blamed 40-bit RC4 keys for WEP's weakness and recommended using 104 or 128-bit RC4 keys instead. Although using larger key size does increase the work of an intruder, it does not provide a secure solution.

Initialization Vector (IV)
Use of known “weak” IVs and also the small IV itself. Two frames that use the same IV almost certainly use the same secret key and key stream. Moreover, since the IV space is very small, repetition is guaranteed in busy networks.
Static Keys
Infrequent re-keying and frames with same IV result in a large collection of frames encrypted with same key streams that can be used to create decryption dictionaries.

Q3) What is CCMP?

CCMP: **C**tr **C**BC **M**AC **P**rotocol (CCMP): Counter Mode with Cipher Block Chaining Message Authentication Code Protocol (CCMP) is an encryption protocol in the IEEE 802.11i amendment.

Q4) How much entropy is in 64 random hexadecimal characters??

Each hexadecimal character is 4 bits, so 64 random hexadecimal characters have 256 bits of entropy.

Q5) What is the average amount of entropy in:

a) 8 printable ASCII characters?

English language: about 1.7 bits per character (Week 7) → 13.6 bits.
Truly random characters: ASCII printable characters (character code 32-127) not including Delete (127) → 95 characters → 6.57 bits per character → 52.56 bits.

b) 12 printable ASCII characters?

English language: about 1.7 bits per character → 20.4 bits.
Truly random ASCII printable characters: 6.57 bits per character → 78.84 bits.

c) 20 printable ASCII characters?

English language: about 1.7 bits per character → 34 bits.
Truly random ASCII printable characters: 6.57 bits per character → 131.4 bits.

d) 63 printable ASCII characters?

English language: about 1.7 bits per character → 107.1 bits.
Truly random ASCII printable characters: 6.57 bits per character → 413.91 bits.

These will require some research on your part prior to the final lecture on these topics (these topics are examined):

Q6) What are the (six) essential characteristics of cloud computing?

- Broad network access – services allow access by thin or thick clients or other cloud services;
- On-demand self-service – consumers can provision services as required without requiring human interaction with a provider;
- Multi-tenancy – where multiple independent instances of one or multiple applications operate in a shared environment;
- Resource pooling – provider’s resources are pooled and dynamically assigned to serve multiple consumers in a multi-tenant model;
- Rapid elasticity – resources can be quickly provisioned and released, possibly appearing unlimited; and
- Measured service – resource usage can be “monitored, controlled, and reported — providing transparency for both the provider and consumer of the service.

(Multi-tenancy is not in the NIST Guidelines but is in the ISO international standards.)

Q7) Can ***Stuxnet*** be stopped by changing all the default passwords when installing Siemens control systems?

From Eric Byres. Stuxnet Guidance: The Good, the Bad and the Ugly, Jan 17 2011. (yes, the link still works!)
http://www.tofinosecurity.com/blog/stuxnet-guidance-good-bad-and-ugly

“Top of the “Bad” list is the recent Gartner Report on Stuxnet. This paper suggested that ICS users “make sure all default passwords are changed” when installing Siemens control systems. Seems like good advice on the surface, doesn’t it? Unfortunately it’s not.
As the Siemens web site, this blog and others pointed out back in July, if users change the default password on the Siemens SQLServer databases used, the control system will cease to function correctly. The reason is Siemens hard-coded the password into its PCS7 applications. Changing the password in the database prevents legitimate PCS7 stations from accessing the central database, effectively creating a self-induced denial of service on the control system.”