i310 (IAC) – Final Review 2015

Computer Labs (summary & lessons learned)

What is scanning software (in s/w assurance) and what are two basic types/classes

Enterprise IA/CyberSec versus Platform

What are threats ?

Risk Cube

Understand security policy and/versus security mechanisms (how do they complement each other)

Hurdles to overcome that limit/delay implementation of security policy/implementation

Describe Advanced Persistent Threat

SCADA (what is – why relevant)

Components and strategies of enterprise security perimeters

What makes an entity trustworthy ?

What is Software Assurance ?

Describe Formal Methods (as an Assurance Technique) for design analysis/testing/validation

Differentiate dynamic and static software scanners – on what criteria would you select a scanner ?

Describe/contrast Basic Service Set (BSS) and Extended Service Set (ESS) in 802.11 Wifi

Dd-hoc (peer to peer wireless) – why important to understand in computing security context

WiFi channel reuse patterns/model in 2.4 GHz and 5 GHz wireless networks, why important ?

Honeypots (will cover 3/3/16)

Concerns per security of RFID tags ? Two basic categories of RFID ?

What security mechanisms are used to help protect wireless systems ?

Wireless Lab demonstrated couple applications – NetStumbler and Wireless Network Monitor ? Their function/role and relevance to CyberSec/IA

Security implications of roaming in large campus or enterprise environment ?

Describe an Intrusion Detection System and other security mechanisms ?

Describe Anomaly Detection

What would you consider essential services (i.e. DNS, directory) on security perimeter ?

Memory management/protection (Bishop Chpt 29)

Cyber/IA Governance

What is role of a CISO ?

Some Use Case Scenario:

You were offered CISO position at a start-up company to build the security org how you best saw fit. What things to you need to be successful, list the policies and mechanisms that will enable you to be successful. (This relates to Cyber Sec/IA governance) – how will you verify and maintain IA ?

You are CISO and ultimately responsible for network/apps/storage/servers/access/telephony shown, list the policies and mechanisms that will enable you to be successful. All LANs also include WiFi LANs (802.11). Remote access required for all employees, HTTP for customers, Drop/Pick up files, email connectivity to companies A, B, C, D (directly linking their email server to yours)