SI110 AY 2014 Fall 12 Week Exam Review Topics

Web/HTML Client Side Scripting: Non-event driven

- Know what Client Side Scripting is and how to identify that it is being used
- Understand the risks, advantages and disadvantages with client versus server side scripting
- Know how to disable JavaScript in your browser
- Know how to use JavaScript to access and change the DOM (document.location, document.write)
- Understand the risks associated with embedded JavaScript in email and websites

Web/HTML Client Side Scripting: Event driven & Forms

- Understand what a HTML element is and how it is structured
- Be able to identify the parts of a HTML Element
- Know how to use the id attribute with JavaScript to fetch and modify other attributes of the element – although not permanently, since this is client side scripting
- Understand how user triggered event attributes are used with JavaScript instead of placing the JavaScript inside the <script> tag – user triggered scripts (event driven Client Side Scripts) – onclick, onmouseover…
- Be able to determine from the source code what type of user action will result in changes to the viewed page and what the changes are
- Understand that status popups (href URL) can mislead and how to make that happen
- Understand the parts of a HTML form, the main types of inputs used in a form, and the attributes usually used in a form
- Be able to draw what a form would look like in the browser window (from source)
- Know what a form does after the user enters information into the form
- Be able to modify parts of a form
- Know what CLIENT SIDE VALIDATION is

Web/HTML Server Side Scripting

- Understand the difference between client side and server side scripts
- Be able to determine if a web page is using server or client side script or both
- Understand how the server side script URL contains the user entered data – which may include private data (password, social security number, …), and that the URL is sent via GET, so it is saved in the server's access logs
- Understand how to bypass the form, the onclick, and/or client side validation and still send data to the server by typing the data directly into the URL
- Identify or create the URL that a form submission will generate
- Know what SERVER SIDE VALIDATION as compared to CLIENT SIDE VALIDATION, which type of validation is best, and why
- Discuss tradeoffs between client-side and server-side scripts, and explain why client-side input validation is weaker than server-side.

Web/HTML Injection attacks, XSS

- Understand how the message board works
- Understand what injection attacks are and how to attempt one
- Understand how cookies work, where they are stored, why they are stored
- Understand phishing and spear phishing attacks
- Understand how Cross Site Scripting is done and how to prevent those attacks
- Understand what sanitizing input is, the tradeoffs, and the difficulties, for example with the message board
- Explain how an email containing HTML with embedded scripts is a risk to security.
- Explain how cookies are used by both the web browser and the webserver.
- Explain how reflection, injection attack, and cross-site scripting work and why they may fail.

Networks & Protocols

- Explain the basic functioning of the Internet in terms of hosts, packets, routers and IP addresses.
- Know what a host is and how a host is identified (IP Address)
- Understand how the Internet works in a basic sense to include what a packet is and what a router does
- Know how to determine a packet's path and how to read and diagram the output from a traceroute
- Know what an IP address is comprised of and the difference between IPv4 and IPv6
- Know how to determine your IP address

- Know what a domain name is and the hierarchy of domain names
- Know how to determine the IP address for any domain name
- Know how to determine the domain name for any IP address
- Understand what the DNS is, how it works with the WWW, and security issues with name resolution.
- Explain the function of traceroute, ipconfig, and nslookup
- Understand what a protocol is
- Understand the connection between ports, protocols, and services
- List the layers in the protocol stack of the TCP/IP Model.
- Describe each layer in terms of its function and the hardware devices used.
- Be able to describe, compare and contrast, the two protocols in the Transport layer, TCP and UDP
- Understand how to use netcat
- Understand what information is available from running netstat -a
- Know the fundamental services, and specifically what service what they provide
- Match fundamental services to protocol associated with the service and the tool that is associated with the client accessing the service – COMPLETE THE TABLE FOR SERVICE, PROTOCOL, TOOLS
- Understand the difference between HTTP and HTTPS
- Know the difference between the Internet and a simple network
- Know the difference between a router, a switch and a hub
- Know what a gateway router is, how to identify it in traceroute or ipconfig outputs for the source or destination host
- Know how to determine if two hosts are on the same network, i.e. what information is needed to determine this?
- Know what the network address is and what it represents, and what is used to calculate it
- Understand how the link layer functions and how it differs from the Internet layer; Know how packets are addressed and handled at the link and Internet layers
- Know how to determine the MAC address for a network adapter and what the MAC address is used for
- Understand what the arp table displays and how to depict the results in a diagram

Networks: Build-a-lan lab

- Review the steps performed in the lab, as well as the questions and answers
- Know what is required for hosts on different networks to communicate

Networks: Wireless Networking

- Describe where in the TCP/IP stack wireless networks differ from wired networks
- Know the wireless standard
- Know how a wireless network is set up; define/describe a basic service set, the ESSID
- Understand the purpose of a base station
- Understand the different problems associated with using wireless and the solutions (how you know what network you are on, how to increase the reach or balance the load on a wireless network, how to control who joins the network and provide privacy from someone not on the network who is snooping on packets)
- Describe the purpose of encryption on a wireless network, and compare WEP, WPA, WPA2

Networks: Build-a-wireless-lan lab

- Review the steps performed in the lab, as well as the questions and answers
- Understand the attacks and what steps to take when setting up a wireless network to defend against the attacks
- Describe each of the following: IP Address, subnet mask, network address, broadcast address, private address, MAC address, BSSID, ESSID
- Appropriately use these commands and tools and explain their output: ipconfig/ifconfig, netstat, arp, ping, traceroute, nmap, nslookup, netcat. Interpret their output to deduce information about network hosts, topology and services, and to construct a physical wired network and an encrypted wireless network, both connected to a simple internet.

Symmetric Encryption, Asymmetric Encryption, Hashing, Digital Crytogtraphy

- Understand symmetric and asymmetric encryption as tools that help provide confidentiality
- Know that Symmetric Encryption uses a single, shared, secret key and what its weaknesses are
- Know the meaning of the terms: plaintext, ciphertext, encrypt, cipher, key, decrypt, Symmetric Encryption, cryptographic attack

- Understand the Alice-Bob-Eve setup
- Use and understand the traditional symmetric encryption methods: Caesar Shift, and the Vigenere Cipher
- Understand frequency analysis and that it is a form of cryptographic attack on symmetric encryption
- Understand a plaintext attack as a form of cryptographic attack on symmetric encryption
- Understand what a one-time pad is and what it provides
- Describe and contrast symmetric encryption, asymmetric encryption and hashing and explain their roles in protecting the Pillars of IA.
- Describe and contrast key management for symmetric and asymmetric encryption.
- Explain and actually use representative symmetric encryption and hashing techniques that are done "by hand" (e.g., Vigenere Cipher, Rubik's Hash).
- Identify the user's vs. the technology's responsibilities in situations where cryptography is used (e.g., HTTPS)
- Describe common tools such as AES and MD5, relate their use to Information Assurance, and demonstrate their use
- Discuss authentication by password, password attacks, hashing, salt, and password strength.
- Discuss two-factor authentication, what it is and which IA pillar it strengthens
- Explain the workings of attacks such as frequency analysis, and chosen plaintext attack
- Understand why we need Asymmetric Encryption (why isn't Symmetric Encryption adequate?)
- Understand what the public key and private keys are and how they are managed
- Be able to explain what is meant by asymmetric encryption being a commutative cryptosystem
- Describe the steps of Asymmetric Encryption with Authentication
- Identify what pillar each step of Asymmetric Encryption with Authentication strengthens and guarantees
- Know how can you use digital signatures to guarantee the integrity of a message
- Identify which additional pillar is strengthened, but not guaranteed with digital signatures
- Understand what a hash is and what IA pillars it strengthens
- Understand what makes a good hash function
- Be able to explain how hashes are used for password authentication
- Understand what salt is and what it helps defeat
- Know the difference between a dictionary attack and brute force attacks
- Describe what a rainbow table is and how it is used
- Know how to choose strong passwords and why
- Describe a website's responsibilities in protecting user passwords
- Know the difference between MD5, AES, and RSA (what do each do: hash? Encryption – what type?)
- Know what MD5 produces
- Know how AES encrypts – what a block is
- Know how to use MD5, AES, and RSA
- Understand how to combine MD5 with AES, and MD5 with RSA and why
- Be able to combine crypto tools