Segundo Certamen

Tiempo: 90 min

Nombre: _____

Si algo está poco claro, anote un supuesto razonable y responde conforme a éste.
Todas las preguntas tienen igual puntaje. Sea breve en su respuestas.

1.- ¿Qué preguntas responde todo programa GINGA-NCL? ¿Cuál de estas preguntas se responde con rótulo <media>?
¿Qué medios serán mostrados? ¿Dónde serán mostrados? ¿Cómo serán mostrados? ¿Cuándo serán mostrados?
<media> permite especificar los medios de la aplicación.

2.- ¿Para qué sirve el rótulo <port> y los distintos tipo de conectores de GINGA-NCL?
El rótulo <port> se emplea para indicar el o los medios que inician la aplicación. Es el punto de partida del programa. Los conectores permiten especificar cuándo un medio debe iniciar su reproducción. El conector especifica el inicio de un medio con alguna condición en otro medio o el control remoto. Por ejemplo, cuando un medio termine que se inicie el otro, cuando se presiona un botón del control remoto, que se inicie un medio.

3.- ¿Mencione y explique 4 diferencias entre las redes de sensores inalámbricos y las redes de computadores y/o teléfonos inteligentes que expliquen el uso de sistemas operativos y lenguajes diferentes?
Los sensores inalámbricos se vinculan con el medio de forma asíncrona, luego el sistema operativo debe proporcionar mecanismos para reaccionar ante eventos.
Las redes de sensores deben operar de forma autónoma (sin recarga de energía) por mucho tiempo, luego se debe proveer mecanismos para ahorrar energía.
Los nodos poseen, en general, pocos recursos de memoria, CPU, etc, luego se debe optimizar el código generado para operar con poca memoria.
A diferencia de los computadores y teléfonos inteligentes, las redes de sensores operan en modo ad-hoc y multihops, luego los sistemas operativos y/o lenguajes deben proveer mecanismos para facilitar la operaciones de ruteo multihops.

4.- ¿Qué explica la baja tasa de bits en las redes de sensores inalámbricos respecto a WiFi considerando que ambos operan en la banda de 2.4 GHz?
La tasa de bits no se relaciona con la frecuencia en que operan sino con la baja potencia utilizada. La tasa de bits máxima alcanzable crece con el aumento de la relación señal a ruido. En las redes de sensores se trabaja con baja potencia, lo que genera una relación señal a ruido baja y por ello la tasa es mucho más baja que en WiFi.

5.- ¿Qué significa que, en TinyOS, el límite entre hardware y software puede variar dependiendo de la aplicación y plataforma de hardware?
La arquitectura de TinyOS está basa en componentes. Cada componente puede ser un elemento de software o un elemento de hardware provisto por la plataforma a usar. Por ello el lenguaje define un conjunto de componentes implementadas por software cuando ese recurso no está el el hardware (es programado usando elementos de hardware más básico) o implementadas directamente por la plataforma. Así el límite entre software y hardware queda definido al momento de compilar cuando el usuario especifica la plataforma destino y se determina qué va en software y qué se usa directo del hardware.

6.- ¿Por qué se han desarrollado lenguajes especiales, como NesC para programar aplicaciones de redes de sensores en lugar de usar C directamente?
Porque una programación conducida por eventos es mejor que la secuencial ofrecida por C. C permite implementar la programación dirigida por eventos, pero es más fácil si el lenguaje ya ofrece esas herramientas.
NesC también entrega mecanismos para mejorar la optimización de los programas.
NesC da prioridad a ciertas tareas y con ello ofrece mecanismos para programar sistemas soft real-time.

7.- Explique en qué consiste la técnica de análisis estadístico para descifrar un mensaje. Mencione un tipo de cifrado en que esta técnica pueda ser efectiva.
Consiste en generar un histograma de frecuencia de los símbolos. Luego éste se compara con el histograma conocido de los símbolos no codificados de algún lenguaje. Así se puede reconocer qué símbolo del lenguaje debería estar mapeado a algún símbolo del código.
Esta técnica es efectiva en cifrado mono-alfabético.

8.- ¿Qué problema resuelve el cifrado de bloques en cadena respecto al cifrado de bloques?
El cifrado de bloques en cadena logra que dos bloques iguales generen mensajes cifrados distintos. Esto no se consigue con cifrado de bloques. Esto se consigue mezclando el bloque de mensaje con el bloque cifrado anterior y luego cifrando el resultado.

9.- ¿En qué consiste el ataque de reproducción? Explique la técnica que permite su detección. ¿Puede usar esta técnica para evitar la reproducción de e-mail seguros? Comente.
El ataque consiste en grabar un mensaje autenticado por una fuente y más tarde volverlo a enviar pretendiendo ser la fuente.
Para detectarlo, se ideó el uso de un número único enviado por el receptor antes de recibir el mensaje. La fuente debe incorporar ese número único en el mensaje autenticado. El receptor debe comparar si el número único del mensaje corresponde al generado por él.
En general no podría ser usada porque en correo electrónico no hay negociación entre quien escribe y quien lee el mensaje. Se puede enviar un mensaje sin que el receptor sepa que lo recibirá.
Si ambas partes lo acuerdan, sí se pueden enviar mensajes pidiendo un número único y luego usarlo en la firma del mensaje. El receptor puede así verificar que no es una reproducción.

10.- Una persona plantea que su empresa no necesita cortafuego (firewall) porque tiene un sistema de detección de intrusión. ¿Está usted de acuerdo? ¿Qué argumento a favor o en contra daría usted?
No estoy de acuerdo. Un sistema de detección de intrusión detecta ataques pero no toma acciones a menos que trabaje en conjunto con otros sistemas como, por ejemplo, un cortafuegos.