ESCUELA SUPERIOR POLITÉCNICA DEL LITORAL

FACULTAD DE INGENIERÍA EN ELECTRICIDAD Y COMPUTACIÓN
COMPUTACIÓN Y SOCIEDAD
SEGUNDA EVALUACIÓN - II TÉRMINO 2016-2017

Nombre:_____Matrícula:_____
Paralelo:_____

Tema 1: Programación

ESPOL (campus Las Peñas) ha decidido implementar un sistema de evacuación de emergencia usando drones para guiar al personal y estudiantes novatos a las salidas. El sistema de evacuación trabajará bajo las siguientes condiciones.

- Cada edificio tendrá alarmas para diferentes situaciones: Incendio, Terremoto y Tsunami.
- Para cada situación un dron tiene diferentes puntos de evacuación, dependiendo de la alarma guiará a las personas a un punto seguro.
    - Si ocurre un incendio el dron dirige a la gente al Malecón.
    - Si ocurre un incendio y temblor el dron dirige a la gente al Malecón.
    - Si ocurre un temblor o terremoto el dron dirige a la gente hacia el frente del edificio.
    - Si ocurre un tsunami dirige a la gente hacia las Peñas.
- Las alarmas se activan de forma automática a través de sensores de movimiento, detector de humo y movimiento de mareas respectivamente.

Diseñe una solución en pseudocódigo que implemente este sistema. Suponga que ESPOL también necesitará realizar simulacros donde se active de forma manual las alarmas.

Tema 2: Privacidad y seguridad

Las vacaciones de Miguel.

Miguel está buscando un vuelo para sus próximas vacaciones a través de Internet. Sin embargo, aún está indeciso, por ende, realiza múltiples búsquedas en el sitio oficial de la aerolínea. Luego de 5 minutos de búsquedas continuas le apareció el siguiente mensaje***: "Algo sobre tu navegador nos hizo pensar que eras un bot."***, luego de esto, la página no le permitió continuar con la búsqueda.

Mientras seguía buscando vuelos similares en varios buscadores, le apareció una oferta a través de una ventana emergente; en la misma se mencionaba ***"Eres el usuario nro. 100000 y eres ganador de la siguiente OFERTA DE VUELO"***. Sólo necesitaba llenar un formulario o autenticarse usando una red social para ver el precio real de la oferta. Para evitar llenar todos los datos Miguel dio autorización a este sitio con la clave de Facebook. Sin embargo, no se percató de todos los permisos que solicitaba el sitio. Luego de esto no pudo ver ninguna oferta, automáticamente se cerró la ventana y se descargó un archivo llamado ***instalar.exe***, el cual lo instaló, pero no pasó nada en el momento.

A partir de ese momento se percató que, en su red social, Facebook, se empezaron a compartir varios links que él no había publicado. Además, le empezaron a llegar muchos correos de todo tipo, algunos sobre productos y otros informativos sobre vuelos y tours. Los mismos que Miguel revisaba ya que pensaba que no eran reales. Sin embargo, un día le llegó un correo que parecía personal; en el mismo se mencionaba que responda si le interesaba obtener promociones, además solicitaban su número de teléfono para comunicarse con él. Al ver que no era nada peligroso Miguel respondió de forma positiva al correo.

Al día siguiente, lo llaman a Miguel, de la empresa que le solicito su número telefónico por email y le mencionan que tienen una oferta única y que dura dos días. Le mencionan que sólo necesitan conocer qué tipo de tarjeta de crédito tiene para validar si aplica a su promoción. Miguel indica que tipo de tarjeta tiene, luego de unos segundos le confirman que puede obtener la oferta pero que para la misma necesitan los datos de tarjeta (número de tarjeta, fecha de expiración, código CSV). Miguel desconfiado no entrega esta información y les menciona que desea pensarlo un poco más y pide tiempo. Luego de esto busca información en la red social de la empresa que lo contacto y se percata que hay muchos comentarios positivos en la red social de la empresa; decide escribir a uno de los usuarios de la red social quien le responde cosas positivas acerca de la empresa. Escribe a alguien más y se da cuenta que usan las mismas frases y palabras que el usuario anterior. Escribe a un tercero y la respuesta que dio fue casi idéntica que las primeras. Todo confundido prefiere dejar por ese día la búsqueda.

Al finalizar la semana le llegó un nuevo correo. Este correo mencionaba una nueva oferta increíble para Copa Airlines; Miguel dio clic en el enlace y automáticamente cargó una página con información del vuelo. Miguel al ver que el URL: www.copaairlines.com correspondía a la empresa de avión, decide navegar hasta que encuentra un vuelo barato y decide comprarlo. Ingresa sus datos de tarjeta y finaliza la compra. Sin embargo, luego de la transacción apareció un error y lo re-direccionó a otro enlace https://www.copaair.com/, confundido sigue navegando en este nuevo sitio. Esta vez ya no encontró la oferta, así que continuó buscando otro vuelo y lo encuentra; procede a comprar y nota que esta vez el pago de tarjeta lo envió a un sitio seguro y que incluso le enviaron un código. de seguridad a su teléfono cosa que no sucedió la vez anterior. Cuando le toco realizar el pago le apareció un mensaje de que no disponía de dinero. Esto fue extraño para Miguel. Enseguida ingresó a su banca virtual y se percata que efectivamente no había suficiente dinero en la tarjeta; Miguel ingresa a ver los detalles y recientemente se habían realizado varias transacciones no autorizadas por el. Llamó a la aerolínea quien negó haberlo hecho y al banco quien confirmo las transacciones, finalmente bloqueó su tarjeta.

Luego de unas semanas Miguel intenta explorar su computador y nota que se han creado accesos directos de todos sus archivos y un duplicado de los mismos. Al final Miguel realizó un reclamo escrito a su Banco, no pudo realizar su viaje y envió su computador a un técnico.

Analice cada párrafo y mencione que tipos de ataque informático ha identificado, su definición y qué método de seguridad ofrecería a la aerolínea de ser el caso. Para finalizar agregue 4 recomendaciones a Miguel para navegar de forma segura en la web.

Tema 3: Propiedad intelectual

Klever Moreira es el director de una empresa tecnológica. Como parte de sus proyectos en investigación y desarrollo, Moreira ofrece apoyo económico al Departamento de Robótica de la ESPOL para la construcción de "robots asistentes" para personas con necesidades especiales o personas de avanzada edad. A cambio, la universidad ofrece dar a la compañía de Moreira derechos exclusivos sobre la tecnología que ellos desarrollen. A manera de compensación, la universidad también recibirá regalías sobre las ganancias que la compañía obtenga por el producto cuando sea comercializado.
En la universidad, un grupo de profesores de ingeniería mecánica de la misma universidad, muestra interés en adelantar una investigación y publicar un artículo relacionado a estas tecnologías. Los profesores de Mecánica contactan a los profesores del Departamento de Robótica de la ESPOL, quienes le ofrecen datos obtenidos como resultado de su propia investigación y también de la investigación de Moreira. El grupo de Mecánica ignora que los resultados provienen de dos fuentes.
La investigación resultado todo un éxito y su artículo es publicado en una prestigiosa revista. Los resultados obtenidos por la compañía de Moreira aparecen dentro del artículo, pero no son

referenciados y únicamente los miembros del Departamento de Robótica de la ESPOL reciben crédito. Más tarde este grupo de Mecánica se entera de que la mayor parte de la información citada en su artículo fue proporcionada por la compañía de Moreira.

a) **Dentro de las acciones realizadas en el caso anterior, indique las que tienen características de plagio. ¿Por qué es plagio?**

b) **¿Cuál debería ser la actitud de Moreira, qué acciones debería tomar?**

c) **¿Cuál debería ser la actitud del Departamento de Robótica de la ESPOL, que acciones debería tomar?**

d) **¿Cómo Moreira podría prevenir situaciones parecidas?**

Tema 4: Ética Profesional

Extracto del paper "The Ethics of Using Hacked Data: Patreon's Data Hack and Academic Data Standards".

La proliferación de datos y el "big data" han causado retos tanto para periodistas como para científicos sociales. Muchos problemas, a veces ignorados, han surgido, como "el estado de consentimiento informado" en big data, donde los datos pueden ser utilizados para una variedad de estudios después de haber sido recolectados, siendo esto, fines no previstos originalmente por los individuos que proporcionan los datos.

Un ejemplo conocido sucedió cuando varios periodistas publicaron documentos clasificados de seguridad estadounidense que Edward Snowden había publicado sin autorización. Los miembros de la ACM debatieron la ética de las acciones de Snowden, y las del periodista Glenn Greenwald[1]. Como señalaron, las acciones de Snowden eran claramente ilegales y una violación de la ética profesional.

Otro ejemplo reciente es el pinchamiento de los teléfonos celulares de los ciudadanos, acción realizada por ciertos empleados de Rupert Murdoch del periódico News Corporation en el Reino Unido[2], para obtener noticias sensacionalistas. Tanto la ética periodística como la ley fueron violadas. En este caso, la expectativa de privacidad era clara, ya que los datos hackeados eran todos privados.

La ilegalidad paralela y la invasión de la privacidad no pueden pasarse por alto. Tanto el pinchamiento telefónico como el uso de los datos en los artículos de noticias publicados son un problema. Incluso los casos de compartir y mostrar datos públicos pueden causar un alboroto, como se muestra cuando un periódico estatal de Nueva York publicó nombres y direcciones de dueños de armas en su área de lectores, recuperados a través de una solicitud de libertad de información[3]. La información pública ampliamente difundida no siempre es considerada apropiada por aquellos a quienes se refieren los datos, y los datos públicos eran lo que esperábamos utilizar.

Los periodistas usan datos e información en circunstancias en las que autoridades y el público no quieren que se publiquen los datos, como con Wikileaks y Edward Snowden. Esta es una práctica

---

1 A. Adams. 2014. Report of a debate on Snowden's actions by ACM members. SIGCAS Computers & Society 44, 3: 5-7.

2 Natalie Fenton. 2012. Telling tales: Press, politics, power, and the public interest. Television & New Media 13, 1: 3-6.

3 Jim Fitzgerald. 2013. Journal News removes controversial handgun permit information from website. Associated Press. Retrieved December 16, 2015, from http://www.huffingtonpost.com/2013/01/18/journal-news-handgunremoves-information_n_2507774.html

profesionalmente aceptada si se hace por el bien público. Sin embargo, los periodistas también tienen normas profesionales sólidas y códigos de ética bien establecidos a diferencia del campo de la ciencia de los datos que por ser joven carece de un bien establecido código de etica. Aunque casos como el de Snowden son polémicos, existe una aceptación generalizada de que los periodistas tienen cierta responsabilidad con el bien público, lo que les da libertad para el juicio profesional.

Al igual que el periodismo polémico, los datos hackeados permiten a los investigadores acceder a datos que en última instancia son útiles para el público y que las empresas no están dispuestas a compartir. El investigador independiente de seguridad informática Mark Burnett había recogido durante mucho tiempo ID de usuario y contraseñas de los inicios de sesión encontrados en vertederos de datos ilegales liberados por hackers. Muchos estudiantes y académicos le pidieron su colección con el tiempo, y decidió publicar su colección de 10 millones de inicios de sesión públicamente para facilitar la investigación[4]. Las empresas con una gran base de usuarios normalmente no están dispuestas a compartir datos de acceso con nadie, ya que expone a dañar a sus usuarios.

Existen algunas diferencias paradójicas entre los datos en línea y otros tipos de datos más tradicionales utilizados por décadas por los especialistas en medios de comunicación, como los periódicos y revistas. Los investigadores han visto el contenido periodístico como juego limpio para su uso en la investigación porque se considera público. Sin embargo, no es fácil reunirse, ya que uno debe tener acceso a las bases de datos restringidas disponibles a través de una biblioteca de la universidad o el acceso al microfilme físico y microficha. Los datos en línea, por el contrario, es fácil de encontrar por cualquier persona con una conexión a Internet. Sin embargo, como Boyd y Marwick [5]han declarado, en relación con Internet, "sólo porque el contenido es accesible al público no significa que estaba destinado a ser consumido por cualquier persona".

¿Según los principios de ACM, que preceptos entrarían a favor y cuales en contra de los casos mencionados?

[4] Stuart Dredge. 2015. Security researcher publishes 10m usernames and passwords online. The Guardian, 11th February. Retrieved February 22, 2016 from: http://www.theguardian.com/technology/2015/feb/11/securityresearcher-publishes-usernames-passwords-online-mark-burnett

[5] Danah Boyd, Kate Crawford. 2011. Six provocations for big data. Retrieved from http://papers.ssrn.com/sol3/Papers.cfm?abstract_id=1926431