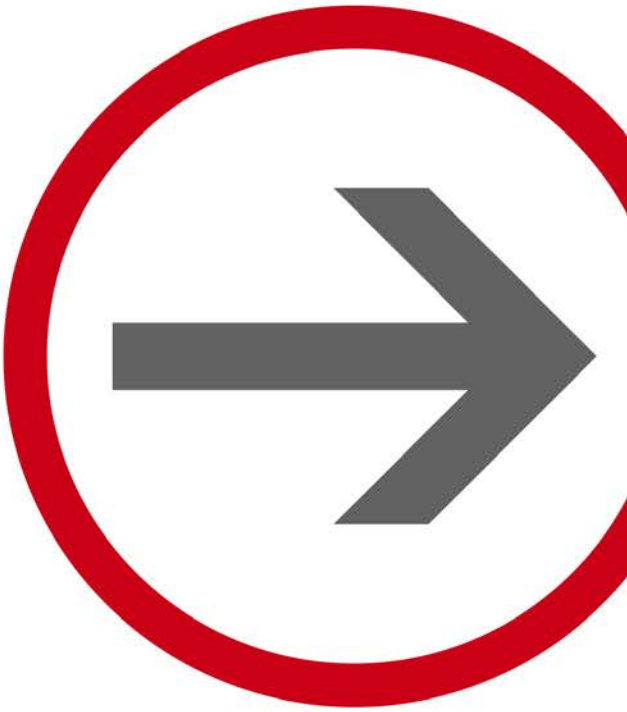
ü online



Gamificación de las prácticas de seguridad informática con una herramienta de tipo capture the flag

BANCO DE BUENAS PRÁCTICAS DOCENTES

MARTA BELTRÁN

UNIVERSIDAD REY JUAN CARLOS online
online.urjc.es

1. La práctica

- **Título:** Gamificación de las prácticas de Seguridad Informática con una herramienta de tipo Capture the Flag.
- **Curso Académico:** 2016/2017.
- **Asignatura:** Seguridad Informática.
- **Área/Titulación**: Grado en Ingeniería Informática/Grado en Ingeniería del Software.
- **Grupo de Estudiantes:** Tercer curso de Grado.

La gamificación ha demostrado en los últimos años ser una herramienta muy potente para mejorar los resultados de aprendizaje de alumnos y estudiantes en diferentes contextos. Hasta el momento los ejercicios de tipo "Capture the Flag" (CTF o Atrapa la Bandera), en los que diferentes individuos o equipos compiten por encontrar una o varias banderas escondidas en un escenario vulnerable, se han empleado con éxito en el área de la ciberseguridad en dos ámbitos muy específicos: el desarrollo de concursos en las conferencias hacker o eventos de seguridad y la concienciación o formación en entornos empresariales. Pero trasladar la mecánica y dinámica de este tipo de juegos a la enseñanza de una materia como la ciberseguridad en el marco universitario es un reto importante. El curso pasado comenzamos a utilizar estas prácticas educativas en la asignatura presencial de Seguridad Informática, proponiéndoles a los alumnos actividades gamificadas con las que practicaran lo aprendido en el aula de teoría, mejorando su capacidad para tomar decisiones en entornos lo más realistas posibles y para resolver problemas complejos en equipo, añadiendo una motivación adicional a los ejercicios realizados en el laboratorio planteando competiciones de tipo Capture the Flag**.**

2. Justificación

La mayor parte de profesores y profesionales dedicados a la concienciación, formación y enseñanza en el área de la ciberseguridad están de acuerdo en que la parte práctica del aprendizaje, el enfoque hands-on, es esencial para que los alumnos o estudiantes adquieran las competencias deseadas.

Distintos trabajos han propuesto en el pasado el uso de ejercicios prácticos de tipo Atrapa la Bandera o Búsqueda del Tesoro para mejorar los resultados de aprendizaje de los estudiantes de materias de ciberseguridad, añadiendo al enfoque práctico o técnico un componente adicional de motivación gracias a la gamificación.

Este tipo de ejercicios suele implicar el uso de laboratorios específicos para que los estudiantes puedan llevar a cabo estos ejercicios, casi siempre por equipos, con diferentes enfoques (defensivo, ofensivo, mixto, etc.).

Pero la adquisición, despliegue, administración y mantenimiento de este tipo de laboratorios implica un consumo de recursos (humanos y económicos) que muchas universidades, incluida la nuestra, no pueden permitirse hoy en día. A esto hay que sumarle la explosión de la docencia on-line o a distancia, que imposibilita la propuesta de ejercicios prácticos que impliquen el uso de este tipo de laboratorios que obligan a los estudiantes a desplazarse para usarlos de manera presencial en horarios concretos.

La solución ha sido en casi todos los casos recurrir a la virtualización de los laboratorios de ciberseguridad, ofreciendo a los alumnos o estudiantes distintos tipos de máquinas virtuales con los que practicar diferentes técnicas y mecanismos defensivos u ofensivos. Pero esta evolución ha hecho que en la mayor parte de los casos se pierda el componente de Captura la Bandera o Búsqueda del Tesoro, es decir, la gamificación. La mayoría de estos ejercicios basados en máquinas virtuales, accesibles en local u on-line se realizan de manera individual, sin ningún tipo de mecánica o dinámica de juego.

Esto nos ha llevado a dos escenarios bien diferenciados en el contexto de la formación y enseñanza en ciberseguridad. Por un lado, podemos encontrar retos, concursos y competiciones, con la componente de gamificación, cuando se dispone de presupuesto y recursos suficientes para desplegar la infraestructura necesaria para un ejercicio de tipo Captura la Bandera o Búsqueda del Tesoro. Típicamente, éste es el enfoque en conferencias y eventos de seguridad y otros contextos de búsqueda de talento o en iniciativas gubernamentales o empresariales de concienciación y formación del personal. Por otro lado, los centros educativos y universidades han optado casi siempre por el uso de máquinas virtuales para el planteamiento de ejercicios prácticos, lo que ha abaratado los costes de estos ejercicios y aumentado de manera significativa la flexibilidad de la enseñanza. Pero, esta virtualización de los laboratorios ha hecho en casi todos los casos que se pierda la gamificación. En nuestro caso habíamos intentado mantenerla utilizando la herramienta Socrative en paralelo a la realización de ejercicios con máquinas virtuales, pero no estábamos satisfechos con los resultados obtenidos en los últimos cursos.

En el curso 2016/2017 decidimos intentar disfrutar lo mejor de los dos escenarios y poder realizar ejercicios prácticos virtualizados de alguna manera para no depender de un laboratorio costoso y para no obligar a los alumnos a realizar las prácticas de manera presencial, pero sin perder la componente de gamificación y manteniendo el enfoque de Capture the Flag.

3. Desarrollo

Objetivos

Se planteó un proyecto de innovación educativa con las siguientes fases o etapas:

1. Búsqueda de un alumno que colaborara con la profesora que desarrollaba el proyecto en tareas de análisis, desarrollo, etc. Este alumno, Sergio González (del Grado en Ingeniería del Software, de manera que había estudiado la asignatura Seguridad Informática en el curso anterior y conocía la manera tradicional en la que se venían realizando las prácticas) realizó todas estas tareas como parte de su Trabajo Fin de Grado, ya que no se le podía ofrecer remuneración. Además, publicó junto a la profesora un trabajo de innovación docente en las III Jornadas Nacionales de Investigación en Ciberseguridad explicando su trabajo y tuvo la oportunidad de presentarlo durante dichas Jornadas.
2. Análisis de herramientas y plataformas que permitan cumplir con los objetivos planteados. Se realiza una comparativa en función del siguiente conjunto de criterios:

    - Escalabilidad. Se pretende que la plataforma se pueda emplear inicialmente en asignaturas con grupos de laboratorio de 30/50 alumnos, pero en el futuro en titulaciones o en MOOCs con grupos de cientos o incluso miles de alumnos.
    - Flexibilidad para generar nuevos escenarios con diferentes niveles de dificultad o complejidad o para modificar los ya generados, re-utilizando esfuerzos. La idea es generar una biblioteca o catálogo de ejercicios prácticos para todos los profesores de la universidad que imparten docencia en el área de la ciberseguridad.
    - Flexibilidad para realizar distintos tipos de ejercicios (defensivos, ofensivos, mixtos; individuales o por equipos), para proponer diferentes mecánicas y dinámicas de juego, para recompensar a los participantes de maneras diferentes, etc.
    - Reproducibilidad, de manera que se garantice justicia en los juegos y competiciones y se puedan obtener resultados fiables que permitan tener en cuenta los resultados para evaluar a los alumnos.
    - Portabilidad y uso de tecnologías estándar, de manera que no se exija a los profesores ni a los estudiantes que instalen sistemas operativos ni entornos que no utilicen ya de manera habitual.
    - Facilidad de uso, tanto para los profesores como para los estudiantes, el aprendizaje del uso de la plataforma no puede ser una barrera.

- Seguridad y privacidad, la propia plataforma no debe introducir vulnerabilidades en la infraestructura de la universidad ni provocar problemas con la protección de datos de nuestros estudiantes.
- Gratuidad y código abierto. Dado que el proyecto debe realizarse a coste cero, el análisis se debe centrar en herramientas y plataformas de libre distribución que además sean de código abierto de manera que podamos realizar las modificaciones oportunas al proyecto según las necesidades que vayamos detectando.

3. Selección de una herramienta o plataforma, adaptación para los objetivos planteados si fuera necesario y generación de manuales de uso. La plataforma seleccionada fue el Capture The Flag de Facebook (disponible en Github ya que se trata de un proyecto de código libre).
4. Generación de escenarios adecuados para las competencias que los alumnos de la asignatura Seguridad Informática deben practicar.
5. Diseño de las dinámicas y mecánicas de juego más adecuadas para añadir el componente de gamificación deseado a las prácticas de la asignatura.
6. Instalación de la herramienta o plataforma en recursos propios para realizar las primeras pruebas de concepto y ejercicios piloto. No era nuestra intención realizar prácticas evaluables en el curso 2016/2017, sólo probar con grupos piloto de alumnos que realizaran los ejercicios de manera voluntaria.
7. Realización de las primeras experiencias, validación y evaluación de las nuevas prácticas.

4. Resultados

Metodología de análisis

Se plantea practicar durante la competición los siguientes contenidos de la asignatura:

- Búsqueda de puertos abiertos y uso de la herramienta nmap.
- Hacking con buscadores (Google y Shodan).
- Análisis de scripts y de código fuente, ingeniería inversa.
- Rotura de contraseñas (fuerza bruta, ataques de diccionario).
- Esteganografía.

- Explotación de accesos remotos inseguros.
- Explotación de vulnerabilidades en sistemas de certificados.

En cuanto a la gamificación, se decide emplear técnicas mecánicas (relativas a la recompensa tras la superación de retos) como el sistema de puntuación de la plataforma y la publicación del panel con la clasificación o ranking de equipos. Para emplear técnicas dinámicas (relativas a la motivación de los alumnos) se optó por la recompensa directa (gracias al sistema de puntos ya mencionado), el estatus o reputación (gracias a la publicación de la clasificación o ranking), el logro personal (gracias a la resolución colaborativa de retos de dificultad creciente) y la propia competición (de nuevo gracias a la clasificación de equipos y a la filosofía Capture the Flag de los ejercicios).

La plataforma se instala en un servidor de la profesora con el sistema operativo Ubuntu 14.04 y trabajando sobre VirtualBox y Vagrant. Una vez instalada, permite el acceso al profesor, con rol de administrador, a los diferentes menús de configuración de equipos, retos, escenarios, competiciones y clasificaciones. Los participantes (los alumnos) acceden a la plataforma a través de cualquier navegador web y reciben las instrucciones para cada una de las competiciones en las que vayan a participar a través de diferentes medios (mensajes, tablón de anuncios, etc.). Lo fundamental es que para conquistar cada uno de los países del mapa, tienen que ir superando diferentes problemas o retos.

Todos los equipos superan los retos planteados dentro del límite de tiempo (en poco más de una hora el equipo más rápido y consumiendo las dos horas completas el equipo más lento). Se les pide que documenten durante la competición el trabajo que realizan para superar cada uno de estos retos, por lo que la profesora puede evaluar a posteriori la idoneidad de las técnicas y mecanismos empleados así como evitar plagios o atajos de otro tipo. De momento no se trata de una práctica evaluable, por lo que no se pueden comparar los resultados obtenidos con los que se obtuvieron con las prácticas realizadas de manera tradicional (que además, no se realizaban en equipos de cuatro personas) en relación con las calificaciones.

Pero sí se realiza una evaluación del impacto de la innovación educativa planteando una autoevaluación a los alumnos (para que evalúen su propio aprendizaje y los factores que intervienen en él) y de la profesora y el alumno que le ha dado soporte en todo el proyecto.

En el caso de los estudiantes, cabe destacar las siguientes observaciones de las 20 autoevaluaciones obtenidas (en forma de cuestionario sencillo y anónimo):

• 19 alumnos responden que han aprendido lo mismo o más realizando las prácticas de esta manera que de la manera tradicional.

• 16 alumnos comentan que perciben una mejora en su disposición a realizar las prácticas porque se han divertido más durante las sesiones de laboratorio.

• 14 valoran muy positivamente el cambio que creen que este tipo de ejercicios puede implicar en su forma de aprender. Piensan que les obliga a ser más creativos, a buscar soluciones eficientes, a ser más autónomos.

• 12 comentan que este tipo de prácticas mejoraría el vínculo con sus compañeros, por obligarles a trabajar en equipo y por fomentar una competencia sana con el resto de equipos.

• 5 señalan que les preocuparía que los resultados de estas competiciones contaran para la evaluación, ya que les parece que obligan a resolver problemas de manera rápida, yendo al grano, pero sin buscar la mejor manera posible de resolverlos. Algunos comentan que se estaría valorando la "idea feliz" de alguno de los miembros de cada equipo.

En cuanto a la autoevaluación realizada por la profesora y por su alumno-ayudante, cabe destacar las siguientes conclusiones:

• La plataforma escogida permite plantear ejercicios prácticos en diferentes áreas de la ciberseguridad con distintos niveles de dificultad y obteniendo el máximo beneficio posible de diferentes técnicas de gamificación. Esto de manera escalable (tanto con grupos pequeños como numerosos), portable y garantizando la reproducibilidad de los escenarios de competición, por lo que los resultados obtenidos podrían tenerse en cuenta para realizar evaluaciones.

• El hecho de que la plataforma sea gratuita es una ventaja considerable, al igual que el de su madurez, facilidad de uso y alto grado de participación de una comunidad muy motivada que actualiza y mejora constantemente el producto. Al ser de código abierto, nos ha permitido realizar las modificaciones que hemos considerado oportunas, algo que se podrá continuar haciendo en el futuro para terminar de adaptarla a un entorno educativo.

• En todas las pruebas realizadas hasta el momento se han observado dos hechos muy favorables: los profesores pueden dedicarse en exclusiva a aspectos que de verdad aportan valor a su docencia (la

propuesta de los retos y le selección de las técnicas de gamificación que mejor se adecúan a cada competición) y los estudiantes presentan una actitud mucho más positiva y participativa al realizar los ejercicios prácticos de la asignatura.

• Cabe destacar que el principal esfuerzo para utilizar la plataforma está en convertir los retos a la forma pregunta-respuesta. Es decir, el reto debe tener una solución concreta que los participantes deben subir a través del interfaz correspondiente al reto para ser validado por la plataforma y que se puedan gestionar las puntuaciones. Por lo que el reto debe tener una solución correcta. De esta manera, el enfoque siempre debe ser averiguar una dirección IP, robar una contraseña, averiguar el valor de un registro concreto en una base de datos, proponer una sentencia de código concreta para rellenar un hueco, escribir un comando concreto o recuperar un token incluido en una cookie de sesión, etc. No todos los ejercicios prácticos de la asignatura pueden plantearse de esta forma, y esta limitación debe tenerse en cuenta desde el principio.

• El otro esfuerzo importante es el relativo a la definición de unos criterios de evaluación que no tengan sólo en cuenta la rapidez de las soluciones, sino también la calidad de las soluciones, la capacidad de un equipo para trabajar de forma colaborativa, etc. Es decir, creemos que la nota de una práctica no debe obtenerse directamente de las puntuaciones obtenidas durante la competición, sino que debe ponderarse con otros aspectos del trabajo de los alumnos igualmente importantes.

• Por último, nos hemos dado cuenta de que un aspecto esencial a la hora de plantear las competiciones es el relativo al orden en el que los alumnos afrontan los retos. En las prácticas tradicionales de la asignatura, este orden estaba fijado por el profesor, y tenía un objetivo pedagógico, de manera que los alumnos se enfrentaban a ejercicios con dificultad creciente ejercitando sus competencias para resolver problemas de complejidad cada vez mayor. Pero si se plantea un ejercicio Capture the Flag puro, cada equipo decide qué territorio desea conquistar primero y esto dificulta seguir esa progresión. Después de distintas pruebas, hemos encontrado la forma de obligar a los alumnos a seguir un orden concreto en su conquista de territorios (anidando pistas en los ficheros que acompañan a las banderas de manera que uno desbloquea al siguiente en dificultad y así sucesivamente). Pero estamos seguros de que se pueden desarrollar soluciones más sofisticadas en el futuro.

En el curso 2017/2018 se ha instalado la plataforma Capture The Flag en MyApps y estamos realizando este tipo de prácticas con todos los alumnos de la asignatura de manera obligatoria. En paralelo, estamos creando un catálogo de retos lo más completo posible. Además estamos valorando la posibilidad de ofertar nuevos trabajos fin de grado, para, por ejemplo, llevar a cabo modificaciones en la plataforma que podrían ser interesantes para su utilización en nuestras aulas. Y estamos haciendo

públicos los resultados del proyecto de innovación educativa realizado en diferentes foros, jornadas y congresos.

5. Equipo docente

Marta Beltrán Pardo

Marta Beltrán es Ingeniera Electrónica (UCM 2001), Licenciada en Ciencias Físicas, rama de Física Industrial y Automática (UNED 2003) y Doctora en Informática (URJC 2005). Actualmente es Profesora Titular de Universidad en la Universidad Rey Juan Carlos de Madrid (universidad a la que se incorporó en el año 2001), donde desde hace más de quince años trabaja en sistemas distribuidos y en ciberseguridad, tanto en docencia como en I+D+i. Es una de las pocas investigadoras españolas que ha publicado trabajos en conferencias técnicas hacker internacionales como las BlackHat o las Defcon o en conferencias técnicas militares como las ICC (actuales CYCON). Además es co-fundadora del Cybersecurity Cluster de la Universidad Rey Juan Carlos, representante de esta universidad en la RENIC, directora del MOOC de Ciberseguridad en las plataformas URJCx y MiriadaX, del Máster en Ciberseguridad y Privacidad y del curso de Experto en Privacidad y Protección de Datos.