novática
Revista de la Asociación de Técnicos de Informática

Novática, revista fundada en 1975 y decana de la prensa informática española, es el órgano oficial de expresión y formación continua de **ATI** (Asociación de Técnicos de Informática), organización que edita también la revista **REICIS** (Revista Española de Innovación, Calidad e Ingeniería del Software).

<http://www.ati.es/novatica/>
<http://www.ati.es/reicis/>

ATI es miembro fundador de **CEPIS** *(Council of European Professional Informatics Societies)* y es representante de España en **IFIP** *(International Federation for Information Processing)*; tiene un acuerdo de colaboración con **ACM** *(Association for Computing Machinery)*, así como acuerdos de vinculación o colaboración con **AdaSpain**, **AI2**, **ASTIC**, **RITSI** e **Hispalinux**, junto a la que participa en **ProInnova**.

Coordinación Editorial, Redacción Central y Redacción ATI Madrid
Padilla 66, 3º, dcha., 28006 Madrid
Tlfn.914029391; fax.913093685 <novatica@ati.es>
Composición, Edición y Redacción ATI Valencia
Av. del Reino de Valencia 23, 46005 Valencia
Tlfn. 963740173 <novatica_prod@ati.es>
Administración y Redacción ATI Cataluña
Via Laietana 46, ppal. 1ª, 08003 Barcelona
Tlfn.934125235; fax 934127713 <secregen@ati.es>
Redacción ATI Aragón
Lagasca 9, 3-B, 50006 Zaragoza.
Tlfn./fax 976235181 <secreara@ati.es>
Redacción ATI Andalucía <secreand@ati.es>
Redacción ATI Galicia <secregal@ati.es>
Suscripción y Ventas <novatica.subscripciones@atinet.es>
Publicidad Padilla 66, 3º, dcha., 28006 Madrid.
Tlnf.914029391; fax.913093685 <novatica@ati.es>
Imprenta: Derra S.A., Juan de Austria 66, 08005 Barcelona.
Depósito legal: B 15.154-1975 -- ISSN: 0211-2124; CODEN NOVAEC
Portada: Corredor de hierba - Concha Arias Pérez / © ATI
Diseño: Fernando Agresta / © ATI 2003

sumario

Nº 220, noviembre-diciembre 2012, año XXXVIII

Tema del próximo número: "Modularidad en el diseño de software"

Wilmer Pereira
Escuela de Ingeniería Informática, Universidad Católica Andrés Bello (UCAB), Caracas (Venezuela)

<wpereira@ucab.edu.ve>

Enseñanza de la Seguridad Computacional como instrumento de la ética profesional

Este artículo fue seleccionado de entre las mejores ponencias presentadas en el Congreso Iberoamericano de Educación Superior en Computación (CIESC 2011) celebrado en Quito (Ecuador) en octubre de 2011.

Resumen: *La Seguridad Computacional como asignatura se basa en la teoría que sustenta las técnicas de cifrado para asegurar, entre otras características: privacidad de los datos (confidencialidad), verificación de identidad (autenticación), evitar rechazo de compromisos (no repudio) y respeto a los derechos de autor (copyright). Así se protege la información de los usuarios en un entorno de red abierto. Sin duda hay aspectos éticos que subyacen y deben orientar el proceso educativo. La perspectiva educativa es importante debido al conocido atractivo que ejerce sobre los estudiantes el conocer las técnicas de ataques a sitios o servidores informáticos, realizados por intrusos o atacantes maliciosos. Los estudiantes centran mucho su atención en como se realizan los ataques más que en conocer lo que el atacante hace, sus efectos y sobre todo como prevenir las consecuencias nefasta de los ataques. En este artículo presentamos una estrategia de enseñanza basada en el hacking blanco o preventivo en contraposición al hacking negro o destructivo. Para ello inducimos al estudiante en el uso de herramientas de prevención, respetando la privacidad, la identidad y las responsabilidades asumidas. Además de la estrategia educativa en el aula, utilizamos una competencia interuniversitaria para reforzar el compromiso ético del estudiante. Este evento sobre delito digital se celebra cada dos años en Venezuela y participan estudiantes de ingeniería, derecho y comunicación social. Tanto en el curso de seguridad computacional como en la competencia, el objetivo es mostrar qué hace el atacante sin necesariamente hacer explícito como lo hace, bajo la perspectiva de la prevención, del compromiso ante los usuarios y, en el caso de la competencia, descubrir los culpables de un delito digital.*

Palabras clave: *Ataques Informáticos, autentificación, confidencialidad, copyleft, ética profesional, no repudio, Seguridad Computacional.*

1. Introducción

La ética profesional es sin ninguna duda uno de los aspectos fundamentales para el buen desempeño de los profesionales egresados de nuestras universidades latinoamericanas públicas y privadas.

Además de graduar ingenieros de calidad debemos formar buenos ciudadanos, íntegros, honestos y responsables de su compromiso con la sociedad. En consecuencia, la enseñanza debe estar reforzada con valores que afiancen los principios éticos dada la importancia del rol que juegan, específicamente los ingenieros, en el aparato productivo de cada país.

En este sentido el docente universitario juega un papel fundamental al impartir principios directivos que orienten los juicios y la ética del profesional. Annie Cohen-Solal, en su libro titulado "*Jean-Paul Sastre*", recoge testimonios de alumnos del conocido filosofo en el liceo de Havre, entre los que resalta el de Pierre Brument: "*Con Sartre se ponían en duda las ideas preconcebidas, se desarrollaba el espíritu crítico, la exigencia de un pensamiento personal y la honestidad intelectual*" [2].

Es decir, creatividad y no seguir al pie de la letra modelos preconcebidos, no implica el rompimiento de normas de respeto al individuo que impone la sociedad. Más aún Nussbaum, también conocida profesora del área de filosofía clásica y ética, cita en un artículo: "*Como dijo Heráclito hace 2.500 años: aprender sobre muchas cosas no da lugar al entendimiento. Marco Aurelio insistía en que, para llegar a ser ciudadanos del mundo, no bastaba con acumular conocimientos; también debíamos cultivar una capacidad de imaginación receptiva que nos permitiera comprender los motivos y opciones de personas diferentes a nosotros, sin verlas como extraños que nos amenazan, sino como seres que comparten con nosotros muchos problemas y oportunidades*" [2].

De estos argumentos se intuye que para el docente, estrechamente ligado al proceso de aprendizaje, no basta con impartir los conocimientos del área, sino, también, debe enseñar principios de comprensión y aceptación para lograr mejores profesionales con amplitud de criterio, aptitud crítica y una posición de compromiso ante la sociedad.

El caso particular de un profesional egresado del área de Ingeniería Informática o Computación, debe manejar información sensible o confidencial de la compañía para la cual trabaja y proteger tanto los datos como el software. Por ejemplo el ingeniero tiene los medios para acceder al sueldo de cada empleado, datos de cualquier computadora de la empresa (sobre todo si trabaja en el servicio de soporte de hardware y software), uso de cualquier recurso, en fin puede conocer mucha información de la empresa. Ante este panorama es vital que el ingeniero muestre integridad y honestidad para poder ser depositario de la confianza de sus empleadores, clientes y personal subalterno.

En la Facultad de Ingeniería de la Universidad Católica Andrés Bello, existe un curso obligatorio de Ética y Ejercicio Profesional (impartida para las ingenierías: informática, civil, industrial y telecomunicaciones) donde los estudiantes toman conciencia de que su bienestar individual descansa sobre su compromiso con el entorno. Allí examinan casos de estudio para reforzar los conceptos éticos desde distintos puntos de vista o teorías.

El curso de Seguridad Computacional ofrece un marco de experimentación ideal para aplicar principios éticos en casos específicos y directamente ligados con el ejercicio profesional. Durante el curso se tienen presente ciertas premisas como la prevención y resguardo de la información ante intrusos y ataques informáticos. El docente enseña las técnicas de protección de los canales de comunicación y la información local de los computadores, siempre tomando en consideración que el ingeniero es el garante de la seguridad en el medio informático donde se desenvuelve.

Así, en esta asignatura, hemos ideado una estrategia para inducir al estudiante sobre la importancia de asegurar cuatros aspectos fundamentales: la confidencialidad, la autentificación, el no repudio y el respeto a los derechos de autor. Con la estrategia propuesta para la enseñanza de estos conceptos, se motiva en el estudiante principios éticos y se desmotivan intenciones de exploración insana, sin la autorización debida, de centros y servidores informáticos. Se induce al estudiante a asumir la responsabilidad que

> “En la Facultad de Ingeniería de la Universidad Católica Andrés Bello, existe un curso obligatorio de Ética y Ejercicio Profesional… donde los estudiantes toman conciencia de que su bienestar individual descansa sobre su compromiso con el entorno”

implican las promesas y los compromisos, siempre respetando los derechos de los demás.

De hecho, intentamos convencerlos de lo inútil que resulta mostrar como se realizan los ataques e incitarlos a asumir una actitud apegada a la ley, que vele por la seguridad e integridad de los datos, personas y recursos de las instituciones para las cuales trabajarán.

Además organizamos, cada dos años, una competencia de simulación de juicio sobre delito informático, donde participan estudiantes de las escuelas de derecho, informática y comunicación social. El objetivo es definir equipos interdisciplinarios donde las habilidades a nivel legal se complementan con la experticia técnica, para conducir una acusación, en el caso del fiscal, o probar la inocencia de un implicado, valiéndose de la evidencia digital, en el caso de la defensa. Todo reseñado por comunicadores sociales que siguen las incidencias del juicio y el comportamiento de sus actores.

2. Motivación y objetivos

Desde hace un buen tiempo hay consenso en el área de informática sobre la importancia de la seguridad de la información. Gradualmente muchos *pensum*[1] de pregrado están incluyendo una asignatura específica aunque en la mayoría de los casos como materia electiva. Por otro lado, en Venezuela, unas pocas universidades tienen muy recientemente ofertas de postgrado cortos en seguridad y hasta una conocida compañía de seguros armó una formación de un año.

Sin embargo, la oferta sigue siendo poca para las exigencias del mercado. Ante esta situación diversas instituciones y compañías privadas, a nivel internacional, están ofreciendo certificaciones. Algunas de las más conocidas son: CISM (*Certified Information Security Manager*) y CISA (*Certified Information System Auditor*) de ISACA, CEH (*Certified Ethical Hacker*) y CHFI (*Certified Hacking Forensic Investigator*) de EC-Council, GSEC (*GIAC Security Essential*) de GIAC, CSSP (*Cisco Certified Security Professional)* de CISCO, entre las más conocidas. Esta situación no sólo se presenta en Venezuela sino en buena parte de Iberoamérica [9].

Este estudio no pretende competir con el nivel de detalle de las certificaciones sino más bien, en una asignatura, reforzar los principios éticos impartidos, mostrando las herramientas de seguridad y sólo considerando la posibilidad de intrusión como punto de partida para definir detalladamente las políticas de defensa.

Durante la materia se siguen los siguientes lineamientos para lograr que el docente obtenga el objetivo general antes enunciado:
1) Presentar las herramientas de prevención y protección ante intrusiones y ataques informáticos.
2) Mostrar como desarrollar políticas de seguridad conociendo las debilidades y cuales son los puntos vulnerables, sin mencionar como se realizan los ataques.
3) Mostrar en clases, generalmente a partir de exposiciones de los estudiantes, casos reales de antiguos intrusos y como se desenvuelven sus actividades y vida una vez descubiertos.
4) Preparar semanalmente talleres cerrados sobre el uso práctico (instalación y configuración) de herramientas de protección y prevención ante ataques.
5) Montar un proyecto de seguridad en computadores, de ser posible individualmente, con fines meramente preventivo, con protección de servidores, y usando herramientas de código abierto. En ese proyecto se debe prevenir o proteger contra:

- Suplantación de identidad.
- Violación de la privacidad de la información.
- Rechazo a los compromisos asumidos.
- Irrespeto a los derechos de autor.

6) Incentivar la participación en el modelo de simulación de delito informático para que el estudiante perciba la importancia de los grupos interdisciplinarios y aplique sus conocimientos y principios éticos.

En esta asignatura, la estrategia se desarrolla a todo lo largo del semestre y se culmina con la presentación del proyecto que utiliza: certificados digitales para la autentificación, cifrado de canales para la confidencialidad, firma digital para evitar el rechazo de los compromisos y código *copyleft* como alternativa para no utilizar herramientas propietarias que irrespeten el *copyrigth*.

3. Marco teórico

Inicialmente en esta sección se presentan los principios básicos de seguridad computacional y posteriormente los fundamentos que rigen la ética en informática.

3.1. Seguridad Computacional

La seguridad, desde el punto de vista técnico, se aboca a los mismos desafíos que debe afrontar la seguridad convencional. De hecho, siempre han existido aspectos vitales para el resguardo de la información entre los que se encuentran: la confidencialidad, la autentificación, el no repudio y el respeto por los derechos de autor.

El primer concepto tiene que ver con la privacidad de los datos, ya sea mientras se transmite información o cuando los datos se colocan en algún medio de almacenamiento del computador. El cifrado normalmente se realiza con algoritmos de clave simétrica dado que son 1.000 veces más rápidos que los algoritmos de clave pública.

Por otro lado, la autentificación se vale de los certificados digitales que contienen la clave pública, única para cada usuario, y acoplada con su clave privada. Justamente es esta última clave la que permite firmar documentos que, en contrapartida, se verifican gracias a la clave pública que contienen los certificados. Por último, el *copyleft*, en contraposición al *copyright*, permite la distribución y uso de software que puede ser usado sin costo, modificado y a su vez redistribuido sin irrespetar ningún derecho de autor.

Un ejemplo práctico donde se combinan todos estos conceptos, en el ámbito digital, es en el comercio electrónico, cuando se cancela mediante el número de la tarjeta de crédito. Ante todo, es necesario entregar el número de la tarjeta de crédito con la previa verificación de la identidad del ente comercial. La autentificación debe preceder al intercambio de información, de ser requerido cifrado, para asegurar que los datos son entregados y recibidos con privacidad para las personas o los entes autorizados.

Una vez llegado a un acuerdo sobre el bien recibido y el descuento de dinero sobre la tarjeta de crédito, el cliente espera una factura firmada para avalar el compromiso de venta del sitio de comercio electrónico (aunque la mayoría de las veces este último paso no se realiza) [7].

3.1.1. Autentificación y certificados digitales

Para lograr verificar la identidad de una persona existen tres métodos importantes [8]:

“ Justamente estas dos vertientes perfilan, según los propios *hackers*, a los primeros como *hackers de sombrero blanco* o simplemente *hackers* y a los segundos como *hackers de sombrero negro o crackers* ”

- Bajo el conocimiento de una secuencia de seguridad o clave.
- Con el porte de un documento o carnet de identificación.
- Verificando características propias del usuario mediante aparatos especializados.

El primer método es el más utilizado y se basa en el conocimiento que tiene el usuario de una secuencia de dígitos y/o caracteres para ser autenticado. Se parte del principio de que sólo el propietario conoce esta clave, lo cual permite asegurar su identidad. Sin embargo, presenta el inconveniente del olvido de la clave o que, bajo coacción o descuido, un usuario no autorizado puede obtener dicha clave.

Debido a estos problemas se ha desarrollado el segundo método, que consiste en exhibir un documento que avala la identidad del portador. Así se logra la autentificación sin que el usuario deba recordar ninguna información. No obstante, se presenta el problema de que sin exhibir el documento el usuario pierde su identidad pues, en realidad, a quien se autoriza es al documento y por ende al portador actual (no necesariamente al propietario). Además, está el problema de la falsificación o clonación de documentos.

Estas deficiencias conducen a un tercer método, más personal, donde el titular no depende ni de una clave que debe recordar ni de un documento que está obligado a exhibir. Aquí se cuenta con un aparato especializado capaz de leer información propia del titular: huella dactilar o palmar, secuencia de ADN, registro del iris, etc. Esta estrategia de autenticación se conoce como *biometría* y, en principio, resuelve algunas de las deficiencias de los dos primeros métodos. Sin embargo, tampoco es infalible: los dispositivos lectores son aún muy costosos y, desafortunadamente, no son capaces de impedir que bajo coacción un titular sea obligado a exhibir alguna parte de su cuerpo para facilitar el acceso a un intruso.

Dado que ninguno de los métodos es infalible, resulta común que se usen combinados para elaborar sistemas de seguridad más robustos y difíciles de violar [7].

El método de portar un documento o prenda también se puede emular con un documento digital, no físico, que avala la identidad de su portador. Así, en una transacción electrónica el propietario exhibe un documento digital que permite al receptor constatar la identidad del emisor. Este tipo de documento se conoce como *certificado digital*, el cual usa técnicas de cifrado conocidas como algoritmos de clave pública o asimétricos comúnmente usados para la autentificación y negociado de las claves simétricas [8].

Dado que este documento digital es público, para evitar suplantación de identidad, algún ente confiable debe avalar los certificados digitales para detectar si son alterados. Estas entidades, también conocidas como *Autoridades de Certificación*, son organismos confiables que avalan la identidad de personas y entes comerciales. Así, la mayor parte de las transacciones bancarias y comercio electrónico se sustenta en esta infraestructura (conocida como PKI: *Private Key Infraestructure*) para validar la identidad de los entes que participan en un intercambio comercial [8].

3.1.2. Firma digital y *copyleft*

Para avalar la autoría de un documento digital, se requiere del uso de la clave privada ya que esa clave está bien resguardada y sólo le pertenece al usuario portador. La verificación de la firma digital es posible gracias a la clave pública ya que con ella se extrae el compendio o *hash* original del mensaje y se compara con el compendio del mensaje recibido. Si son iguales se acepta el documento. En caso contrario, se rechaza el mensaje.

La firma digital tiene múltiples usos. Uno de ellos es el aval que las autoridades de certificación dan al certificado, firmando con su clave privada, las claves públicas de sus clientes. Es decir, el certificado es distribuido con la firma de la autoridad de certificación y la verificación se obtiene usando la clave pública de la propia autoridad.

Por otro lado, el uso de software de libre distribución, en particular con las licencias *copyleft* [13], es útil cuando no se desea o no es posible utilizar el software propietario, protegido por *copyrigth.* El estudiante desarrolla el proyecto sin infringir derechos comerciales de empresas desarrolladoras de software. De hecho el software de libre distribución ha generado todo un movimiento con el patrocinio de licencia *copyleft*, el cual, en contraposición a *copyrigth,* tiene como condición que los códigos fuente son abiertos es decir a disposición de quien lo desee. En la mayoría de los casos se puede comercializar, siempre bajo la condición de que el código debe estar disponible (aunque hay variantes dentro de la filosofía *copyleft* como el caso de las opciones débil o fuerte).

3.1.3. Benefactores e intrusos

Todos estos mecanismos, junto con la confidencialidad o cifrado de la información, se definen para evitar y prevenir los ataques informáticos realizados por personas con alto nivel técnico pero posiciones ideológicas muy cuestionables.

En términos generales, personas con un alto nivel de experticia son conocidas como *hackers*. Ellos encuentran su motivo de vida en alcanzar un nivel técnico alto para, en el mejor de los casos, explorar y diagnosticar fallas en los sistemas. En su peor faceta, son delincuentes que se apropian de información para obtener beneficio personal en detrimento de los auténticos propietarios de la información o bienes.

Justamente estas dos vertientes perfilan, según los propios *hackers*, a los primeros como *hackers de sombrero blanco* o simplemente *hackers* y a los segundos como *hackers de sombrero negro* o *crackers*. La existencia de ambas corrientes justamente antepone principios éticos y permite ver en muchos casos que la frontera es difusa. De hecho hay autores [12] que argumentan que no existen *hackers* éticos pues las típicas posiciones que asumen como benefactores pueden ser fácilmente refutadas.

Por ejemplo, los argumentos más comunes que presentan los *hackers* para justificar sus acciones son:

- Mostrar debilidades de los sistemas para que sean corregidos.
- La información es libre de fluir por Internet sin censura.
- Los estudiantes pueden practicar *hacking* para adquirir habilidades que les permitirán conseguir cierto tipo de empleos.
- Los *hackers* son protectores de la omnipresencia del sector público fuertemente regulador.

Ninguno de estos argumentos supera un examen exhaustivo desde el punto de vista ético por lo que algunos autores aseguran que bajo ninguna circunstancia los *hackers* generan algún beneficio a la sociedad. Para más detalles ver [12].

Por otro lado, a pesar de la comprobada nocividad de las actividades de los *crackers*, aún existen muchos inconvenientes para poder enjuiciarlos y acusarlos de daños a los sistemas informáticos. El problema está en el gran nivel de experticia que debe poseer el

“Por último, está la irresistible atracción que ejercen estos personajes sobre los adolescentes pues se circundan de una ‘aureola heróica’ y contra el sistema que les hace ganar la admiración de adolescentes inconformes”

investigador policial, junto con el fiscal, para poder levantar pruebas y evidencias sobre un medio virtual y bien resguardar la cadena de custodia. Esta cadena es el conjunto de medidas que deben adoptarse a fin de preservar la identidad e integridad de objetos o muestras que pueden ser fuente de prueba de hechos criminales, para su total eficacia procesal [4]. Otro aspecto que influye es que, en general, las leyes sobre delito informática son muy genéricas, lo cual es un factor que dificulta la aplicación de la justicia [1].

Por último, está la irresistible atracción que ejercen estos personajes sobre los adolescentes pues se circundan de una “aureola heróica” y contra el sistema que les hace ganar la admiración de adolescentes inconformes [10]. Justamente éste es el punto sobre el cual se enfoca el curso de Seguridad Computacional para desincentivar actitudes nocivas y destructivas en nuestros estudiantes.

3.2. Ética en Informática

Desde el punto de vista más general la ética define los principios directivos que orientan a las personas en su concepción de vida para lidiar con los juicios, los hechos y la moral. La informática, como su nombre indica, maneja diversos tipos de información y por su potencial de acceso y uso, aunado a las posibilidades que ofrece Internet, genera problemas éticos. Estos se agravan en muchos casos por la ambigüedad de las leyes y regulaciones [6].

Algunos estudios se han abocado a la tarea de definir códigos éticos que llenen los vacíos jurídicos que existen en algunos ámbitos del problema. Algunos trabajos exploran las perspectivas de distintas organizaciones en diferentes países para encontrar puntos coincidentes [3].

Es de notar que las leyes de casi cualquier país, cubren de alguna manera los aspectos más importantes. En particular, la ley sobre delitos informáticos venezolana [1] contempla aspectos como violaciones a la autenticación, privacidad, derechos de autor, etc.

Sin embargo las ambigüedades surgen cuando los delitos traspasan fronteras, algo muy común por el uso de Internet. Otro problema es al levantar pruebas sin que se “contaminen” para que no sean anuladas en los juicios. De hecho en la UCAB hemos dictado cursos a agentes policiales y fiscales donde hemos podido constatar esta dificultad.

La principal dificultad se centra en el resguardo de la cadena de custodia, sobre todo cuando hay evidencia digital. Ésta debe, como mínimo, estar firmada digitalmente por el investigador en presencia de testigos. Esto requiere un conocimiento técnico del investigador policial con el que desafortunadamente no siempre se cuenta.

En otros casos, un investigador contamina la escena digital, es decir, toca el computador antes de hacer el respaldo del disco y firmarlo digitalmente. En consecuencia, en algunos casos, se enturbia la comunicación entre los investigadores y los fiscales. En la competencia justamente interactúan estos dos actores: abogados y especialistas en informática. Antes del evento, el especialista técnico debe levantar la evidencia digital, procesarla y definir la cadena de custodia. A posteriori los abogados, con ese insumo, levantar el caso para la acusación o la defensa.

4. Metodología educativa

Como se mencionó en la introducción y objetivos, la estrategia en la cátedra de Seguridad Computacional es mediante una preparación continua y progresiva con material teórico, talleres prácticos de herramientas de protección/prevención y un proyecto a desarrollar a todo lo largo del semestre. También se realiza un evento, estilo competencia, donde se ejercitan habilidades adquiridas por los estudiantes durante su formación.

4.1. Estrategia docente

Para la asignatura las clases teóricas son en un aula con el apoyo de videoBeam[2] y las clases prácticas en un laboratorio con computadores. En la parte teórica, a grandes rasgos, se cubre en la primera parte del semestre los temas de criptografía simétrica y asimétrica, firma digital y certificación digital.

En la segunda parte se presentan las herramientas de protección clásica: cortafuegos, sistemas de detección de intrusos, redes privadas virtuales, etc. A modo de complemento, en la parte práctica, se hacen 10 talleres en el semestre para reforzar la teoría impartida.

Los temas que abordan los talleres son:

- Seguridad básica (en el sistema operativo Linux).
- Comandos de red seguros (para comandos como ssh, sftp, scp, etc).
- Cifrado simétrico y asimétrico (con GPG).
- Certificación digital (con openSSL).
- Husmeadores y monitoreo de red (con el *sniffer* wireshark y NESSUS).
- Redes privadas virtuales (usando open VPN).
- Cortafuegos (bajo Linux con iptables).
- Sistemas de detección de intrusos (bajo snort).
- Servidores seguros (instalando http+SSL y DNSSec).
- Programación cliente/servidor segura (usando el *security manager* de Java).

Es de notar el fuerte énfasis en el uso de herramientas preventivas, por ejemplo, el preferir NESSUS (práctica 5) en lugar de nmap. Aunque ofrecen las mismas funcionalidades para exploración de vulnerabilidades, NESSUS indica sugerencias de cómo mejorar o cerrar brechas ante “huecos de seguridad”.

Por otro lado está la realización de un proyecto práctico con estrategias de enseñanza controladas, utilizando las herramientas necesarias para la prevención y protección ante ataques e intrusiones informáticas. Éste incluye la instalación conjunta de las herramientas utilizadas en las prácticas, bajo una aplicación cliente/servidor, para proteger tanto el equipo, como los componentes del software y el usuario del sistema. En este proyecto es necesario asegurar los servicios básicos como son la confidencialidad, la autentificación, el no repudio y preservar los derechos de autor.

Entre los proyectos que se han desarrollado están: sitios de comercio electrónico, repositorios seguros de datos y claves, instalación de un segmento de una LAN segura con servidores de red, etc.

4.2. Competencia interuniversitaria

Este evento de simulación de un juicio define el marco para poner en práctica las ideas trabajadas por el estudiante en un ámbito más general, situado dentro del contexto jurídico-técnico-comunicacional.

Inicialmente se le entrega a cada universidad información sobre un fraude o delito del cual se tiene evidencia en documentos físicos y

electrónicos. Las instituciones participantes preparan al menos 5 equipos: defensa y fiscalía conformado por estudiantes de derecho, peritos informáticos para la defensa y la fiscalía, con estudiantes de computación y estudiantes en comunicación social quienes preparan entrevistas y redactan un pequeño instrumento informativo reseñando el juicio.

Cada universidad, un mes antes del evento, debe entregar la acusación para que el resto de las universidades sepan los cargos que se le imputan a cada uno de los acusados.

El día del evento se realiza un sorteo de como se mezclarán los equipos en cada juicio. Evidentemente habrá varios juicios en simultáneo y cada uno presidido por jueces voluntarios, jubilados o aún en ejercicio. Esto para asegurar la completa imparcialidad del personaje cuyo rol conciliador y rector de cada juicio es asegurar un desarrollo satisfactorio de la actividad. Además al momento del cierre del evento, se aprovecha la gran experiencia de los jueces, para mostrar a cada universidad sus fortalezas y debilidades.

Para cada juicio se conforma un grupo de expertos, en cada área del conocimiento, y se les entrega un instrumento de evaluación. Cada miembro de ese grupo, en función a su experticia, evalúa los equipos estudiantiles del juicio que presencia.

Finalmente, al dictarse sentencia en todas las salas, los grupos de expertos se reúnen y, con las puntuaciones, se entregan reconocimientos por área (derecho, informática y comunicación social) y un premio para la universidad con mayor puntuación de todos sus equipos.

5. Discusión

Los aspectos explícitamente trabajados durante el dictado de la asignatura se refieren a: La estrategia educativa, las habilidades técnicas y las consideraciones subjetivas. El rol del profesor, entre otras consideraciones, evita personificarse con el atacante, y siempre asume una posición que respete los derechos de los demás. Esto es de vital importancia para la percepción del estudiante sobre la seguridad informática.

5.1. Estrategia educativa

La interdependencia entre las clases teóricas y los talleres en el laboratorio afianzan y consolidan la relación entre la teoría y la praxis. Cada taller se realiza una vez que el tema es cubierto en clases. Para esta asignatura se exige que el estudiante debe aprobar tanto los exámenes teóricos como el trabajo práctico (talleres + proyecto). A nuestro juicio esta relación vincula estrechamente los conocimientos impartidos con su aplicación en el mundo real.

El material de apoyo se vale de libros de texto, láminas e información en Internet. Entre los medios de difusión de seguridad en el mundo iberoamericano, está la red Criptored, con el patrocinio de la Agencia Española de Cooperación Iberoamericana y coordinado principalmente por la Universidad Politécnica de Madrid. Su principal función es la difusión y enseñanza de la seguridad no sólo en el ámbito universitario sino también empresarial [9].

5.2. Habilidades técnicas

Tanto en los talleres como en el proyecto se deben trabajar y evaluar cuatro aspectos que resumen las pautas que debe seguir cualquier sistema seguro:

- Resguardo de la privacidad y verificación fidedigna de la identidad.
- Evitar ataques e intrusiones en los sistemas informáticos.
- Asumir las responsabilidades y compromisos.
- Protección de la propiedad intelectual de información y bienes.

Para asegurar la autentificación se exige que el proyecto use certificados digitales reforzado con el uso de buenas prácticas de palabras claves seguras al momento de la conexión. Esta última se maneja con palabras claves suficientemente largas, con caracteres diferentes y controlando el número de intentos para evitar ataques de fuerza bruta. Todo esto concientiza al estudiante sobre la importancia de una verificación sólida de la identidad.

El cifrado se trabaja tanto en los talleres como en el proyecto y generalmente se hace montando herramientas que hagan el negociado de la clave simétrica al momento del establecimiento de la conexión, justo después de la autentificación. El resguardo de la privacidad es vital para mantener la confianza del usuario sobre la plataforma y aplicaciones que utiliza. Tener plena certeza que la información no será visible por terceros, aumenta la confianza en los medios digitales.

La firma digital es exigida también para el proyecto pues en principio da tranquilidad al eventual cliente de la aplicación. Así se sabe que si la persona que realizó el intercambio no acepta su compromiso, se dispone de un medio legal para demandarlo ante el incumplimiento de sus obligaciones.

El uso de software *copyleft*, tanto en el proyecto como en los talleres, evita caer en el uso indebido de aplicaciones y programas informáticos privativos, usados sin pago, ya que el *copyleft* es una alternativa para desarrollar aplicaciones económicas con el aval de toda la comunidad GNU.

Todo esto se amalgama con la utilización de una librería (sobre todo en el proyecto) para potenciar servidores y aplicaciones, como lo es SSL (*Secure Sockets Layer*). Esta librería es ampliamente usada para la navegación segura vía Web. También se ofrece al estudiante la posibilidad de usar otras librerías de seguridad de los lenguajes de programación más conocidos, como lo es el caso del *security manager* de Java.

5.3. Posturas éticas del docente

En primer lugar, a todo lo largo del curso de Seguridad Computacional se utiliza un vocabulario donde se habla de *crackers* siempre en tercera persona, evitando cualquier asociación con el docente o algún estudiante. Lo ideal es no asumir roles que inadecuadamente propicien conductas de *crackers*.

También se evita, en lo posible, presentar como se realizan los ataques informáticos. Siempre se indica qué hace el ataque y sólo se explica como se realizan cuando son ataques muy conocidos de los cuales se tienen herramientas de protección. Esto permite que el estudiante se concentre inmediatamente en jugar un rol opuesto al *crackers* para asumir una posición de protector de la seguridad.

Un argumento, que permite justificar al docente en su negativa de explicación de los ataques, es que la rapidez con la que cada ataque es tomado en cuenta, en las herramientas de protección, es tal que puede hacer extremadamente largo y arduo para hacer el seguimiento. Es decir, se puede dedicar mucho tiempo a explicar un ataque que a fin de cuentas cuando se hace público ya no es un ataque que atente contra la integridad de un servidor o computador permanentemente actualizado.

Otro aspecto es convencerlos, con ejemplos de *hackers* famosos, que este camino no siempre lleva al éxito. Ellos mismos constatan que un estudiante a punto de graduarse no se proyecta a futuro realizando *hacking* negro. Este estilo de vida implica vivir en el anonimato, sin poder sacar provecho directo de su gran nivel de experticia a menos que revelen su identidad. Y si mientras el *hacker* está en el proceso de aprendizaje, se ha dedicado a actividades ilícitas, hacer pública su identidad sólo puede traerles múltiples inconvenientes. Con ejemplos de casos reales, los estudiantes verifican que cada es más común el poco reconocimiento que tienen esas personas dada la gran cantidad de profesionales honestos, con buenos niveles de experticias, y que liberan a las empresas de contratar "delincuentes digitales".

Otro aspecto a considerar es mostrar al estudiante los límites entre sus derechos y el de los demás. Un ejemplo claro es el derecho a la privacidad que se contrapone a la libertad

> “ También se evita, en lo posible, presentar como se realizan los ataques informáticos. Siempre se indica qué hace el ataque y sólo se explica como se realizan cuando son ataques muy conocidos de los cuales se tienen herramientas de protección ”

de información. Es decir la información, en principio, es privada para quien la posee pero debe ser pública en la medida que beneficia a la sociedad y que resultaría inadecuado ocultar. De manera análoga ocurre con el derecho al anonimato que es diametralmente opuesto al deber de la responsabilidad del individuo. Es decir, tengo derecho a no divulgar mi identidad mientras con ello no esté evadiendo responsabilidades. Es de notar que la primera dualidad tiene que ver con la confidencialidad mientras que la segunda está relacionada con la autenticación. Estos son dos conceptos claves en el curso y se afianzan y refuerzan en todo momento.

Es de notar que estos aspectos (confidencialidad, autenticación y ataques) son abordados por la Ley venezolana contra Delitos Informáticos en particular la privacidad en los artículos 11, 20, 21 y 22, autentificación en los artículos 6 y 12 y sanciones contra los ataques informáticos en los artículos 7, 8 ,9 y 10 [1].

Por último en lo que concierne a la competencia, no tenemos ninguna duda que esta actividad fomenta la interdisciplinaridad sobre todo en dos áreas que deben interactuar en busca de un beneficio común durante el ejercicio profesional. Debido a la mala relación que existe entre los investigadores y los fiscales, hemos querido hacer explícita esta dificultad, para incitar al estudiante a esforzarse por la importancia del trabajo en equipo, en la búsqueda de la verdad, cuando se está ante un delito electrónico.

6. Conclusiones y recomendaciones

Estos intentos son los primeros pasos para reforzar aptitudes y actitudes éticas en nuestros estudiantes, en primer lugar, con ejemplos prácticos y desarrollo de un proyecto que inmediatamente aplican en bien de la protección y resguardo de información y bienes. En segundo lugar, la competencia es un ambiente motivante y lleno de retos que implican resolver los enigmas que plantea el caso. De hecho allí constatan como proteger antes de aprender como atacar, lo cual, sitúa al estudiante del bando adecuado.

Durante el curso se genera también la conciencia de que la seguridad no es sólo responsabilidad del ingeniero informático sino también de los usuarios de los sistemas. El ingeniero debe impulsar al usuario o cliente a tomar medidas que resguarden sus datos personales y que definan mecanismos seguros locales, por ejemplo, adoptar claves no ingenuas que puedan ser fácilmente adivinadas por terceros mal intencionados.

A lo largo de nuestra experiencia hemos notado menor interés del estudiante por las técnicas de ataques que típicamente usan los *crackers*. Antes teníamos casos donde, abiertamente en el aula, nos solicitaban que les enseñásemos como atacar, pero ante nuestra clara posición ahora es muy poco frecuente. De hecho en nuestra primera experiencia dictando el curso formamos grupos de ataque y de defensa y, realmente, fue una pésima idea que hasta generó enemistades entre los alumnos. Sin embargo, la experiencia nos concientizó sobre la necesidad de una estrategia ética en la cátedra de Seguridad Computacional.

En trabajos futuros estudiaremos el problema de los sistemas espías (*Spyware*) [5] y troyanos que representan una intromisión a la privacidad y definir estrategias educativas que muestren al estudiante los límites entre el deseo de informar y proteger sin violentar los derechos ciudadanos. También estamos por definir una estrategia educativa para que nuestros estudiantes desarrollen hábitos para el uso de herramientas de compartir recursos (P2P) como kazza, e-mule, limewire, etc, sin violentar los derechos de propiedad.

Por último vale la pena mencionar los esfuerzos recientes que se están haciendo para consolidar un plan de educación para la seguridad en informática [11]. Cuando estas líneas lleguen al lector, se habrá realizando el Primer Taller Latinoamericano de Enseñanza e Innovación Educativa en Seguridad de la Información (TIBETS 2011) que tendrá lugar a finales del año 2011 en Bucaramanga, Colombia. El principal instrumento de trabajo será una encuesta que permitirá emitir un primer informe sobre el estado del arte en enseñanza y formación en Seguridad de la Información en los paises iberoamericanos. Este evento cuenta con el apoyo de Criptored, cuyo coordinador es el Prof. Jorge Ramió de la Universidad Politécnica de Madrid.

Agradecimientos

Este trabajo contó con la participación de los profesores Jorge García y Rafael Andara en la realización de los talleres del laboratorio de seguridad.

Referencias

[1] Asamblea Nacional de Venezuela. Ley Especial contra los Delitos Informáticos, *Gaceta oficial N. 37.313*, 30 de octubre de 2001.

[2] Carlos Berbosa. Elogio de la Docencia Universitaria, periódico *El País, 8/5/2006*, España.

[3] Porfirio Barroso. *Cuatro Principios de la ética*. Disponible en: <http://www.ccee.edu.uy/ensenian/catcomp/material/etica.pdf, 1997>.

[4] Jeimy J. Cano. *Computación Forense: descubriendo los rastros informáticos*. Editorial Alfaomega, 1ra. edición, 2009. ISBN 978-958-682-767-6.

[5] Otorgan Derecho a Instalar Spyware en su PC, *El Diario de Caracas, 18 de noviembre de 2005*.

[6] John Foley, Pierfranco Pastore. *Ética en Internet*. Web del Vaticano <http://www.vatican.va> (última modificación 22 de febrero de 2002).

[7] Luis Gabaldon, Wilmer Pereira. Usurpación de Identidad y Certificación Digital en el Fraude Electrónico. *Revista Sociologias Universidade Federal do Rio Grande do Sul, N. 20*, Dic/2008, pp. 184-190, Porto Alegre, Brasil.

[8] Simson Garfinkel, Gene Spafford. *Seguridad y Comercio en la web*. Mc Graw Hill y O'Reilly, México, 2000.

[9] Jorge Ramió Aguirre, Pino Caballero Gil. Enseñanza de la criptografía y seguridad de la información en España: Primer informe de perfiles de asignaturas. *Revista Seguridad Informática en Comunicaciones (SIC), N.34*, abril de 1999. <http://www.criptored.upm.es/investigacion/informe.htm>.

[10] Manu Rodríguez. *Hackers: aristócratas de la red*. Disponible en <http://www.cibersociedad.net>, 2000.

[11] Miguel Rodríguez. La Seguridad Informática: Una necesidad en la docencia. Universitaria. *Revista PLAC (Publicación Latinoamericana y Caribeña de Educación), nº 1*, enero-abril, 2010.

[12] Eugene Spafford. Are Computer Hacker Breakins Ethical. *Journal of System & Software, January 1992*, Vol. 17, number 1, pp. 41-47.

[13] Richard Stallman. *El Manifiesto GNU*. <http://www.gnu.org/gnu/manifiesto.es.hml>, 1990.

Notas

[1] Nota del editor: “Conceptualmente un pensum es una descripción de algunos de los requerimientos que se aa satisfacer para obtener un grado universitario en un área del saber”, <http://universidadesymasuniversidades.com/producto.php?producto=Pensum+universitario>.

[2] El material de apoyo se encuentra en <http://www.ldc.usb.ve/~wpereira/docencia/seguridad>.