Seguridad en Arquitecturas Web mediante Certificación Digital

1. Resumen

El objetivo del tutorial es presentar los principios básicos de criptografía de clave pública como fundamento para comprender los procesos de cifrado y firma digital que, a su vez, sustenta la infraestructura de certificación digital.

2. Contenido

1. Criptografía
   1.1. Principios de básicos de cifrado
   1.2. Algoritmos de clave simétrica y clave pública (AES y RSA)
   1.3. Funciones de *hash* o compendio (MD5 y SHA)
   1.4. Firma Digital (DSS)
2. Certificados Digitales y Autoridades Certificadoras
   2.1. Certificados de Servidores, Clientes y software
   2.2. Tipos de Autoridades de Certificación: Internas y Externas
   2.3. Arquitectura de las PKI
   2.4. Ventajas y desventajas de las PKI
   2.5. Herramientas
      2.5.1. gpg
      2.5.2. openssl
3. Principios básicos de seguridad en linux
   3.1. Permisos de usuarios
   3.2. Archivos de password de cuentas de usuarios
   3.3. Conexión remota y transferencia de archivos a distancia
   3.4. Cuenta del administrador: restricciones y privilegios

3. Duración

El taller se dicta en ocho horas donde cuatro horas son de teoría y aproximadamente cuatro horas de prácticas en laboratorio sobre manejo de privilegios y transferencia y conexión segura en Linux, cifrado simétrico y asimétrico, firma digital y certificación digital.

4. Equipos

Se requiere máquinas con linux en la cuales se tenga instalado, por máquina:

- gpg
- openssl
- wireshark
- servidor apache
- Deseable aunque no imprescindible una cuenta con privilegios de administración (root)

Se harán tres laboratorios:

1. Seguridad básica en Linux,
2. Cifrado y firma digital
3. Creación de certificados

5. Público Objetivo

Estudiantes y profesores en informática o carreras de ingeniería afines: ingeniería en telecomunicaciones e ingeniería electrónica. Es deseable aunque no indispensable un cierto conocimiento en linux pues las prácticas en laboratorio serán bajo este sistema operativo.

6. CV resumido

Prof. Wílmer Efrén Pereira González PhD

Nacimiento: 13/02/61, Caracas

Dirección Trabajo: Universidad Católica Andrés Bello, Urb. Montalbán
Escuela de Ingeniería Informática, Caracas.
Universidad Simón Bolívar, Valle de Sartenejas
Dpto. de Computación, Baruta, Caracas.

Teléfono Trabajo: UCAB – 4074407, USB – 9063241

Educación

- **Post-doctorado** en la Universidad de Pierre et Marie Curie, Francia. En el seno del equipo de investigación "Sistemas Multiagentes" del Laboratorio de Informática de Paris VI (LIP6), Sep/09 - Jul/10.
- **Doctorado en Informática** (Mención de Honor) en la Universidad de Rennes I, Francia. En el área de Inteligencia Artificial: "Una Lógica Modal para el Tratamiento de la Incertidumbre", Sep/88 - Jul/92.
- **Post-Diploma en Redes de Computadoras** en la Escuela Superior de Electricidad de Rennes, Oct/87 - Jul/88.
- **Diploma de Ingeniero en Computación** de la Universidad Simón Bolívar, Caracas, Sep/79 - Jul/85.

Experiencia Laboral

- **Universidad Católica Andrés Bello**, profesor a dedicación en Ingeniería Informática y Maestría en Sistemas de Información desde Abr/00.
- **Universidad Simón Bolívar**, profesor convencional en pregrado de Ingeniería en Computación, Especialización en Telemática y Maestría en Ciencias de la Computación desde Abr/00.

- **Universidad Central de Venezuela** (Caracas). Profesor de la Maestría en Ciencias de la Computación desde Sept/05.
- **Université de Dauphine** (Paris, France), Profesor por contrato para el *Diplôme Universitaire de Gestion et d'Economie Appliquée* (DUGEAD), segundo año, tercer semestre, de Ene/10 a Jul/10.
- **Universidad Centro Occidental Lisandro Alvarado** (Barquisimeto). Profesor invitado, Ene/96 - Jul/96, Dic/01-Abr/02 y Ene/05-Abr/05.
- **Universidad de Rennes I** (Francia). Profesor-investigador. Feb/92 - Ago/93.
- **Escuela de Organización Industrial** (España). Profesor Internacional. Oct/00 – actual.
- **Oficina Central de Estadísticas e Informática**, responsable de la unidad de lectoras ópticas. May/88-Jul/88

Publicaciones y Seminarios

Expositor de 20 artículos arbitrados en conferencias internacionales, 26 artículos en conferencias nacionales y ponente invitado en seminarios y jornadas estudiantiles en la USB, UCV y UCAB en informática y telecomunicaciones.

Méritos y Afiliaciones

- Fundador de la Sociedad Venezolana de Computación y ex presidente desde Sep/2011-Sep/2015.
- Investigador acreditado por el Programa de Estímulo al Investigador (PEI) desde Jul/2011
- Miembro del Comité Editorial de la Revista Venezolana de Computación (ReVeCom) desde Jul/2013.
- Responsable de Grupo de Investigación de Inteligencia Artificial y Robótica de la UCAB.
- Director de la Revista de la Facultad de Ingeniería de la UCAB (Tekhné) desde Sept/2008.
- Miembro del comité de programa de 15 conferencias internacionales.
- Participante del proyecto iberoamericano IDEAS (Ingeniería en Ambientes de Software) Patrocinado por el CYTED (Agencia de Cooperación Española) y coordinador de un proyecto MAPFRE sobre seguridad y 3 proyectos CDCHT (Consejo de Desarrollo Científico, Tecnológico y Humanístico) en robótica
- Primer lugar en el Premio al trabajo de Investigación UCAB edición 2006-2007, con el trabajo titulado "*Evaluación de Arquitecturas de Software Locales y Distribuidas en Robótica Autónoma y Teledirigida*". También en la edición 2004-2005 con el trabajo: *Elementos Difusos para un Modelo Orientado a Objetos*.
- Presidente del Comité Organizador Conferencia Nacional en Computación, Informática y Sistemas (CoNCISa2014), UCAB, Oct/2014.
- Miembro del Comité de Asesores de la Revista Técnica de la Facultad de Ingeniería de la Universidad del Zulia desde Ene/12 -- actual.