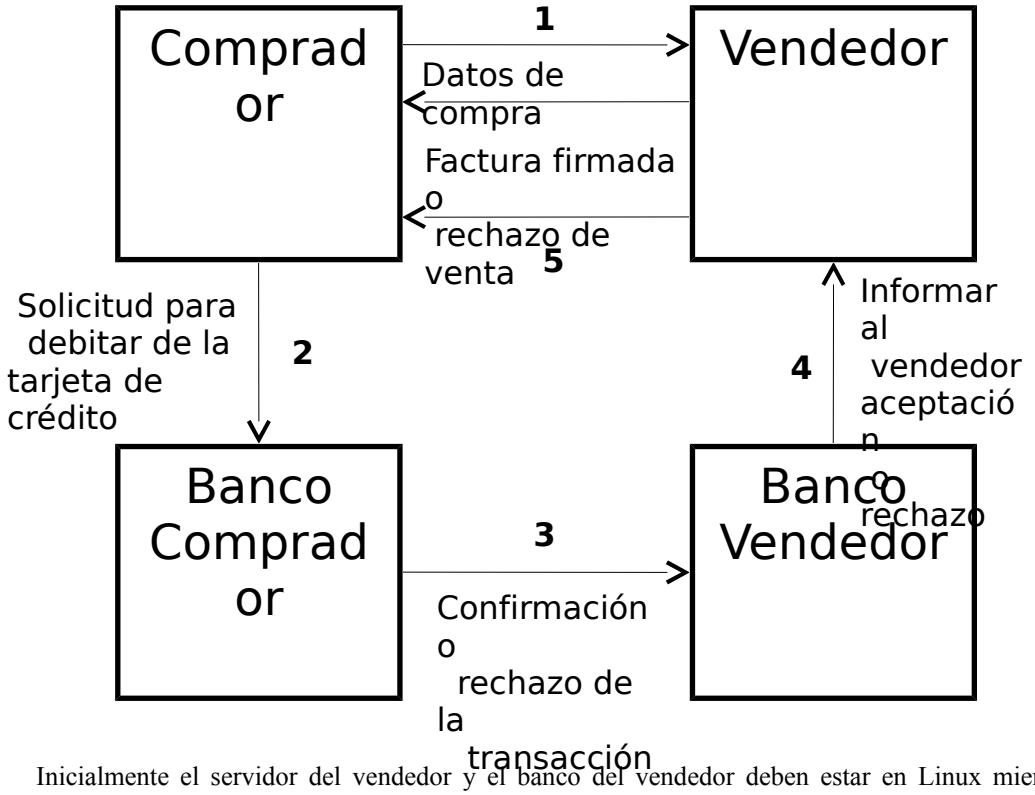
Universidad Simón Bolívar
Departamento de Computación
Redes de Computadores III
Enero/Marzo2018
Prof. Wilmer Pereira

Proyecto II (20%)

Los lineamientos para este proyecto son montar las condiciones mínimas de seguridad para un sitio de comercio electrónico emulando el protocolo 3D-Secure, propuesto hace algún tiempo por Visa/MasterCard. Esta propuesta involucra cuatro actores: comprador, vendedor, banco del comprador y banco del vendedor. A pesar de que 3D-Secure no se usa en Venezuela, por inconvenientes con el control cambiario, es un protocolo de amplio uso en otros países. En líneas generales el protocolo ofrece las siguientes funcionalidades:



- Inicialmente el servidor del vendedor y el banco del vendedor deben estar en Linux mientras que el cliente y su banco en window.

- Los enlaces entre cada máquina deben ofrecer confidencialidad (con cifrado) y autentificación (al menos con certificados digitales). La conexión 1 se asegura vía `hhtps` como en el primer proyecto. En cambio en las otras tres conexiones, al menos una debe usar sockets seguros (socketsSSL) implementados en Java, Python o el lenguaje de su preferencia. También pueden usar sockets en PHP (en ese caso deben antes cifrar el canal)

- Los certificados de vendedor, banco del vendedor y banco del comprador deben ser emitidos por una CAE y el vendedor tendrá dos certificados, uno firmado por una CAE y el otro por la CAI de su banco.

- Todos los actores deben estar en máquinas separadas, bien sea virtuales o físicas, y no debe haber *warnings*.

- La tarjeta de crédito nunca debe estar en posesión del vendedor. El cliente sólo intercambia información de compra con el vendedor. Así que es responsabilidad de los bancos manejar los datos de la tarjeta de crédito. El enlace contra las entidades bancarias debe ser seguro (confidencialidad y autentificación).

- Cada actor debe tener sus bases de datos separadas y pueden usar cualquier manejador de BD sencillo o usar archivos XM o JSON. La interfaz de usuario sólo ofrecerá unos pocos productos y tendrá el link de pago que iniciará la interacción con los bancos. Como es un proyecto de seguridad no se evaluará ni la usabilidad ni la estética de la interfaz. Dediquen sus esfuerzos a resolver los problemas de seguridad.

- Una vez confirmado por intermedio de los bancos que la transacción se puede realizar, el vendedor recibirá confirmación de bloqueo del monto facturado o rechazo de la transacción. En caso de aceptación debe enviar una factura firmada al comprador que la almacenará para acciones legales si hay incumplimiento por parte del vendedor. Si por el contrario no tiene saldo suficiente, el banco del comprador impedirá la venta y todos los actores deben ser informados.

- Cuando el cliente se conecta por primera vez con el vendedor, se le debe crear una cuenta para acceder al sitio de *e-commerce* por lo que es necesario manejar adecuadamente los *passwords* de acceso

    - Debe tener una longitud mínima, al menos un carácter no alfa numérico y una letra mayúscula

    - Al ingreso debe chequear número de intento y después de tres tentativas fallidas se bloqueará la cuenta del usuario.

    - El *password* debe almacenarse con un algoritmo sin inversa para evitar que aún el propio administrador pueda acceder a este. Más aún, nunca puede llegar en claro al sitio de comercio electrónico, es decir, debe partir protegido desde el comprador.

- Debe haber *captcha* al momento del ingreso al sitio para evitar los ataques de fuerza bruta. Puede usar los que ofrece `google` que están a disposición de los programadores

- Las conexiones de 3D-Secure usan SMS o preguntas personales para inicio de sesión o recuperar información de seguridad. Deben implementar al menos alguna de estas políticas de confirmación.

- El sitio del vendedor, que está en Linux, tendrá instalado `iptables`. El *firewall* debe correr mientras se ejecuta la aplicación de comercio electrónico. Se bloqueará `ping` entrante más no saliente, se permitirá `ssh`, `http` y `https` pero no `ftp`. El resto de los servicios debería estar bloqueado. Al momento de la corrida se intentarán conexiones de los servicios bloqueados y el *firewall* debe estar configurado para que la maquina reciba las notificaciones de cada bloqueo. Haga intentos de conexión y levante el tráfico con `wireshark`. Deberá justificar sus respuestas en el informe apoyándose en capturas de pantalla.

- Por último, también visualizando mediante `wireshark`, intente con `nmap`, escanear la máquina que tiene el *firewall*, ¿Qué observa? Al igual que la anterior debe justificar su respuesta en el informe con capturas de pantalla.

La entrega se hará la última semana del trimestre. Este proyecto es en parejas y deben explicar detalladamente, con diagramas de secuencia o máquinas de estado finito, el protocolo. Esto se colocará en el informe que sólo contendrá lo referente a la interacción entre los distintos actores y las respuestas a los dos últimos ítem de descripción del proyecto. Es muy importante el diseño de su protocolo pues la implantación es libre por lo que debe haber muy pocos puntos de coincidencia entre los proyectos. El protocolo es vital para asegurar que todos respetan las reglas de comunicación. Por último, si usan código de Internet deben indicarlo explícitamente en su programa o en el informe.