

Universidad Técnica Federico Santa María
Departamento De Electrónica

Trabajo de Seminario de Computadores I **“Autenticación de Personas”**

Profesor : Agustín González

Integrante: José Gardiazabal S.
9721008-K

Fecha : 09/11/01

Resumen

El objetivo de este informe es explicar cuáles son las principales debilidades que presenta el uso de computadores para comunicar datos que son sensibles, y cuáles son las soluciones que existen para poder suplir estas falencias.

Aquí se explican las principales formas de autenticar información, que son los sistemas de llave pública – llave privada y las firmas digitales, sus ventajas y sus limitaciones, y también se explican, a grandes rasgos, su forma de trabajo.

Para autenticar personas, se explican las ventajas y limitaciones de uso de contraseñas, llaves (PKI) y métodos biométricos más usados. También se muestra cuáles son las limitantes legales y sociales de estos sistemas.

Introducción

Con la evolución de los computadores y el creciente uso de Internet como medio de comunicación, sumado a los costos involucrados y el tiempo gastado en movilizarse de un lugar a otro, ha surgido como una alternativa cada vez más interesante el uso de formas de comunicación basadas en Internet, como forma alternativa y que para poder suplir estos problemas. Las principales ventajas de estos métodos son un bajo costo (para muchos de estos el costo está sólo en el costo de la conexión) y una disminución del tiempo requerido para entregar la información. El problema más grave que tiene esto, es que al ser Internet una red pública, cualquiera puede estar escuchando lo que decimos o, peor aún, puede estar cambiando el contenido de lo que enviamos. También es importante tener en cuenta que, aunque la transmisión de datos entre los dos computadores esté protegidos, todavía falta proteger cada uno de los computadores, ya que si aquí no existe alguna forma de identificar al usuario, cualquiera podría transmitir información desde ahí, y se vería como si lo enviado hubiese sido obra del dueño del computador.

Habiendo identificado estos problemas, se presentarán las formas más usadas para solucionarlos. El primer problema, el envío de datos de forma segura se soluciona con métodos basados en llave pública – llave privada y con sistemas de firma digital, y la autenticación de personas se realiza principalmente usando 3 métodos: contraseñas, llaves físicas y métodos biométricos.

Envío de Datos en forma segura

Sistemas de llave pública – llave privada:

Tradicionalmente la criptografía estaba esencialmente restringida a las aplicaciones militares y diplomáticas (su origen se remonta a Julio César), mediante los denominados algoritmos simétricos, en los que se utiliza la misma clave para encriptar y desencriptar. Este tipo de algoritmos tiene la desventaja de que hay que resolver el problema de la distribución de las claves a través de canales seguros. En 1976, Diffie y Hellman publicaron un trabajo fundamental sobre como distribuir claves a través de canales inseguros. Este trabajo constituyó la base de los métodos asimétricos o de clave pública. El hecho esencial es que cada usuario posee dos claves, una privada que mantiene secreta, y otra pública que es accesible a cualquier persona.

Los algoritmos de clave pública (asimétricos) utilizan dos claves diferentes y relacionadas. Una se llama clave pública y la otra clave privada. La clave privada es mantenida en secreto por el dueño de la misma y la clave pública es distribuida a quien la requiera. Cuando una clave es utilizada para encriptar, se deberá utilizar la otra clave para desencriptar el mensaje.

Los algoritmos de clave pública son más lentos que los algoritmos simétricos en varios órdenes de magnitud. En consecuencia, se utilizan en forma combinada con un algoritmo simétrico encriptando una clave de sesión con la clave pública del destinatario del mensaje. Estos sistemas se conocen como sistemas híbridos. También se utilizan para firmar digitalmente un mensaje encriptando con la clave privada del emisor. De esta manera cualquier persona puede verificar el origen del mensaje.

Sistemas de firma digital:

Las firmas digitales son utilizadas para verificar la integridad y autenticidad de un mensaje. Esto último también se puede lograr utilizando algoritmos criptográficos convencionales. La firma digital garantiza además la no repudiabilidad de un mensaje (el emisor no puede desconocer la autenticidad de éste) y por lo tanto tiene el mismo

valor legal que una firma holográfica tradicional (en los países que poseen una ley de firma digital).

Las firmas digitales son generadas utilizando un algoritmo de clave pública. Para ello se encripta con la clave privada del emisor un checksum del mensaje a firmar. Cualquier persona puede verificar la validez de la firma digital del mensaje utilizando la clave pública del emisor del mensaje.

Los algoritmos de checksum permiten verificar que un mensaje no ha sido modificado. Dado un mensaje de tamaño arbitrario, producen una salida de tamaño fijo. Este tipo de funciones se conocen como funciones sin inversa debido a que es muy fácil calcular un hash para un mensaje, pero muy difícil encontrar un mensaje que produzca un valor particular de checksum. Dado que la cardinalidad del espacio de todos los mensajes posibles es mucho mayor que el número de combinaciones distintas para un tamaño determinado de checksum, necesariamente existen diversos mensajes que producen el mismo resultado, aunque es computacionalmente imposible encontrarlos.

Cabe señalar que la participación masiva de tráfico de información, requiere la presencia de una Autoridad Certificante de reconocido prestigio, que garantice el origen de cada clave pública activa en el sistema, encargándose de difundir aquellas que queden fuera de servicio, lo que se conoce como lista de revocación.

Autenticación de personas

Contraseñas:

Este es el método más primitivo de autenticación de personas. Consiste en un grupo de símbolos (generalmente letras, números y otros caracteres) que forman una cadena de texto, que se le preguntan al usuario antes de permitirle el acceso a una determinada operación, esto es iniciar un computador, revisar o enviar un mail, etc.

Las contraseñas tienen la ventaja que es muy fácil implementarlas en los programas y su costo, por estar basadas exclusivamente en software, es casi nulo. El problema más grave de las contraseñas está en la naturaleza humana. Una persona promedio no puede recordar fácilmente más de 7 u 8 combinaciones de letras con números, si estos no tienen un sentido, lo que hace que en general las claves se conviertan en palabras, fechas de cumpleaños, etc. Además, existen sistemas que capturan las secuencias de teclas, con los que se pueden después recuperar las claves. Más grave aún es el problema que las personas acostumbran a asignar la misma clave para todas las necesidades (Redbanc, mail, alarmas de casa, etc.) Estos problemas, en conjunto, hacen que las contraseñas sean sumamente vulnerables a los ataques, ya que con un computador y un generador de claves automatizado es muy simple romper esta barrera.

Estos problemas se pueden solucionar parcialmente usando ciertas políticas en la creación de contraseñas, como son un largo mínimo, una periodicidad en el cambio de ésta (por si llegase a ser descubierta) y el uso de generadores aleatorios de claves hacen de éstas un sistema viable, pero aún así este sistema por sí sólo no garantiza un nivel de seguridad adecuado.

Llaves Físicas:

Las llaves físicas, como su nombre lo dicen, son llaves que permiten funcionar como método de autenticación de personas, en donde las llaves comúnmente se

conectan a un computador usando un puerto USB, paralelo o serial, aunque las más implementadas son las USB, debido a las ventajas que este puerto proporciona.

Cada una de estas llaves tiene un juego de llave privada – llave pública, pero a diferencia de las llaves privadas – públicas tradicionales, aquí la llave privada nunca sale del dispositivo físico, sino que son los datos los que entran, son encriptados, y salen de vuelta, por lo que el dispositivo crítico deja de ser el computador, y pasa a ser una llave que cabe en un llavero. Para cuidar esto, las soluciones basadas en llaves en general van unidas a una contraseña, lo que las hace más seguras en caso de robos o pérdidas.

La llave entonces viene a cumplir varias misiones, las cuales son verificar identidad, asegurar integridad de los datos enviados, asegurar privacidad de la información recibida, permitir el acceso a una cierta máquina, autorizar transacciones e implementar no repudiabilidad. Por supuesto, cada sistema puede incluir uno o más de estos servicios, y esta función depende de los requerimientos de las personas y los ofrecimientos de la empresa que los implementa.

Aunque estas llaves se ven como una solución prometedora, no está exenta de peligros potenciales y todavía existen dudas que resolver acerca de estos puntos. Por ejemplo, qué pasa si un virus es capaz de enviar datos hacia la llave, tomarlos de vuelta y enviarlos, haciendo que estos datos queden firmados como si el autor fuese el dueño de la llave? O quién asegura que un documento firmado por una persona en realidad está firmado por ella, que conozco, y no por otra que tiene el mismo nombre? Estos problemas y otros todavía no están completamente solucionados, pero se espera que tengan una solución en el futuro cercano.

Biometría:

La idea de los sistemas biométricos es conseguir autenticar personas usando características biológicas propias, entre las cuales se incluyen las huellas dactilares, los patrones faciales, los patrones de retina o iris, los trazados de venas y la voz.

La dactilografía es, dentro de las formas de identificación biométrica, la más utilizada. Su uso data de los egipcios, los cuales sellaban ciertos decretos con su huella dactilar. Investigaciones serias en este campo datan del siglo XIX, cuando en 1893, Sir Francis Galton demostró que no había dos huellas digitales iguales, aún en el caso de gemelos.

El sistema de identificación de huellas digitales, que es el que se usa hasta nuestros días, es el sistema Henry, creado por Sir Edward Henry, el cual clasifica los montes de las yemas de los dedos en ocho categorías: la accidental, el lazo central, el lazo doble, el arco plano, la espiral plana, el lazo radial, el arco cubierto y el lazo del hueco del codo. Analizando estos patrones y estableciendo de 8 a 16 puntos de comparación entre muestras, se puede identificar personas sin posibles dudas.

El problema más grave de la dactilografía es que existen ciertas enfermedades que hacen que no todas las personas tengan huellas digitales, como por ejemplo la epidermolisis bullosa, que hace que estas personas tengan sólo partes o simplemente carezcan totalmente de huellas dactilares.

Actualmente, la tecnología de impresión de huellas digitales es tan barata que algunas empresas están empezando a incorporarla a los PC, lo que hace que se vea como una forma prometedora de identificación personal.

Otro sistema que ha sido ampliamente estudiado tiene que ver con patrones distintivos en la retina. La retina, que controla la visión periférica, es un tejido sumamente fino que convierte la luz en señales eléctricas, las cuales son transmitidas al cerebro. La retina está compuesta de varias capas, de las cuales dos son de interés biométrico. La capa externa contiene estructuras fotorreceptivas y reflectoras llamadas conos y bastones, que procesan la luz. Por debajo de ésta, se encuentra la capa coroide, que alberga complejos sistemas de vasos sanguíneos. Para tomar una imagen, el ojo es bombardeado con luz infrarroja, las estructuras fotorreceptoras de la capa exterior responden reflejando dicha luz y la reflexión resultante produce una imagen de los patrones de los vasos sanguíneos de la retina.

Los especialistas en identificación indican que las exploraciones de retina son extraordinariamente fiables y en muchos casos superiores a la toma de huellas digitales. Por ejemplo, los patrones de retina presentan muchos más puntos de comparación que las huellas digitales (entre 700 y 4200). por este motivo las exploraciones de retina se clasifican como de alta biometría o como sistemas biométricos con un grado altísimo de precisión.

Sin embargo, las exploraciones de retina son en ocasiones insuficientes y es posible que no funcionen si los usuarios son ciegos, parcialmente ciegos o tienen cataratas. Además, dichas exploraciones tienen una tasa desproporcionadamente alta de rechazo, o falso negativo, es decir aunque hay una pequeña probabilidad e que una exploración de retina autentique a un usuario no autorizado, los usuarios no autorizados son rechazados a menudo la primera vez.

La tecnología más reciente se ha fijado en los patrones de voz. Sin embargo, estos sistemas son poco fiables, ya que el sistema es muy sensible a fallos debido a que el usuario tenía bronquitis, catarro, etcétera.

El problema más grave de los controles de acceso biométrico es que si se expanden más allá de la propia estación de trabajo, es posible que haya que enfrentarse a problemas de privacidad. Por ejemplo, se ha argumentado que en contra que las exploraciones retinales revelan información personal médica. Mediante patrones de retina se pueden detectar indicios de abuso de drogas, enfermedades hereditarias e, incluso, SIDA. De ahí que el mantenimiento de una base de datos e patrones de retina pueda llevarle a un litigio. Análogamente, las huellas dactilares pueden revelar tendencias criminales, lo que también constituye un dato sensible.

Más allá de los aspectos legales, los sistemas de control de acceso biométrico tienen implicaciones sociales. Los empleados de una compañía pueden ofenderse por estos controles y considerarlos una violación de la intimidad, lo digan o no, lo que podría fomentar un ambiente de trabajo hostil, aun cuando no se manifieste de manera abierta.

Es posible que el mayor inconveniente, que seguramente va a evitar su uso, sea su eficacia. Dichos sistemas realizan, al menos, registros rudimentarios, por lo que crean un registro incontrovertible de las personas que han llevado a cabo sus tareas y del momento en que las han realizado, lo que puede ser usado como forma de prueba en juicios.

Pese a estos problemas, los controles de acceso biométrico son excelentes cuando se usan internamente, en lugares cerrados y entre compañeros en los que se confía. Su uso es aconsejable dentro de oficinas en aquellas máquinas que se usan para el control y administración de la red.

Conclusiones

Se puede ver entonces que existen básicamente 3 puntos que vienen a solucionar estas tecnologías en conjunto:

- 1) Que los datos enviados fueron efectivamente enviados por la persona que dice haberlos enviado
- 2) Que sólo el receptor recibe los datos enviados
- 3) Que el receptor recibe exactamente lo enviado

Es importante ver que cada una de estas tecnologías viene a solucionar uno o más aspectos, pero que en general deben ser usadas en conjunto para poder obtener un mayor nivel de seguridad.

También es muy importante notar que todos los sistemas tienen sus pros y sus contras, por lo que es necesario evaluar cada caso para buscar la solución más adecuada, ya que no existe una fórmula mágica para resolver todos los problemas.

En general, en todos estos sistemas, el eslabón más débil pasa por el factor humano. Es así como las contraseñas serían mucho más efectivas si las personas tuvieran mejor memoria y los sistemas biométricos serían más precisos si las características biológicas de las personas no se vieran afectadas por cambios de humor o enfermedades.

Otro punto importante es que, al implementar estos sistemas, hay que tener claro hasta qué punto es legal y moral usar cada uno de estos sistemas, sobretodo con los sistemas biométricos, ya que las mediciones biométricas pueden arrojar información personal.

Tal vez lo que hay que finalmente destacar es que ningún sistema es infalible, así que no basta con implementar un sistema de éstos y olvidarse. Hay que estar monitoreándolo constantemente y chequeando que todo funciona como corresponde.

Bibliografía

- **Linux Máxima Seguridad, Anónimo, capítulos 2 y 5.** Habla acerca de contraseñas y biometría
- **Public Key Infrastructure, <http://www.cio.usmc.mil/c4i/cio/c4ibrief>** Explica cómo funcionan las llaves públicas y privadas y por qué conviene usarlas.
- **Firma Digital, lo que se esperaba en la red <http://www.viajuridica.com/index.asp?art=00&dc=32883>** Explica en forma bastante didáctica lo que son las firmas digitales
- **Introduction to Cryptography http://www.rainbow.com/ikey2000/ikey2_crypto_intro.html** entrega una introducción acerca de cómo funciona la criptografía.
- **Iris Scan Biometrics <http://www.iris-scan.com>** tiene información técnica acerca de cómo se generan los patrones del iris y contiene información estadística acerca de su eficacia.

Anexos

Tipos de llaves:

USB



Paralela



Serial

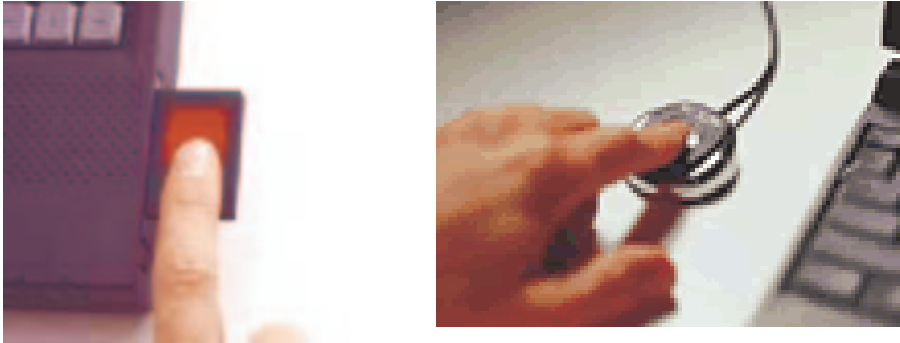


Sensores Biométricos:

Mouse con detector de huella dactilar:



Sensor de huella dactilar PCMCIA y USB



Sensor de Iris:

