1 Introdución a internet

1.1 Sumario

1.2 ¿Que é Internet?

Internet é unha rede mundial formada por dispositivos que se comunican entre si ó traveso dun idioma común (protocolo) e que ten como misión principal o intercambio de información.

O conxunto de medios físicos e información que forma Internet non ten dono. Un usuario poderá ver a páxina desexada pagando só ó seu provedor de telefonía e de Internet.

1.2.1 Funcionamento da Internet

Internet funciona grazas a que os dispositivos conectados entre si falan unha linguaxe común que se denomina **protocolo**. Un protocolo de comunicación é un conxunto de regras que permite que dispositivos diferentes se comuniquen entre si.

Algúns dos protocolos de comunicación máis empregados na internet son:

◊ TCP/IP. **A Familia de Potocolos de Internet** é un conxunto de protocolos de rede que implementa a pila de potocolos na que se basea Internet e que permiten a transmisión de datos entre redes de computadoras. O nome ven en referencia ós dous protocolos mais importantes que a compoñen: **Protocolo de Control de Transmisión (TCP)** e **Protocolo de Internet (IP),** que foron os dous primeiros en definirse, e que son os mais utilizados da familia.

◊ PPP **(*Point-to-point Protocol* - Protocolo punto a punto),** protocolo de nivel de enlace estandarizado no documento RFC **1661**. Polo tanto, trátase dun protocolo asociado á pila TCP/IP.
- Xeralmente, este protocolo se emprega para establecer a conexión a Internet dun particular có seu provedor (ISP) ó traveso dun módem telefónico ou, tamén, empregando conexións de banda ancha (PPPoE ou PPPoA)
- Ademais do simple transporte de datos, PPP facilita dúas funcións importantes:
  _ *Autenticación.* Xeralmente mediante unha chave de acceso.
  _ *Asignación dinámica de IP.*

Para poder facer uso da Rede, precísanse certas ferramentas básicas: un ordenador ou dispositivo dende o que se accede, un módem ou *router*, unha liña telefónica ou o seu equivalente nas empresas de cable e un navegador.

◊ **Módem.** Un módem é un equipo que serve para modular e demodular (en amplitude, frecuencia, fase ou otro sistema) unha sinal chamada *portadora* mediante outra sinal chamada *moduladora* e que ven sendo, por decilo dalgún xeito, a representación dos datos que nos interesa transmitir por unha liña.
◊ **Router.** Un router, ou enrutador, defínese como un dispositivo que ten como misión encamiñar os paquetes IP que lle cheguen cara o camiño (interface) correspondente que lle leve ó seu destino.

Neste tema que estamos a tratar, mais que enrutador en xeral nos interesan os **Enrutadores ADSL** que, en realidade, son varios compoñentes nun: unha porta de enlace (*gateway*), un *router*, un *módem* ADSL e, na maioría dos casos hoxe en día, un punto de acceso *Wireless*.

◊ **Navegador.** Un navegador web é unha aplicación *software* que permite ó usuario visualizar documentos de hipertexto, escritos comunmente en HTML. Calquera navegador actual permite mostrar ou executar gráficos, secuencias de vídeo, son, animacións e programas diversos ademais do texto e os hipervínculos ou enlaces.

◊ **Provedor de servizos (ISP).** Un (Proveedor de Servicios de Internet) (ou ISP polas siglas en inglés de *Internet Service Provider*) é unha empresa adicada a conectar a Internet ós usuarios, tanto se se fai a nivel individual ou dende unha rede de área local. Estas empresas tamén ofrecen servicios relacionados, como aloxamento web e rexistro de dominios entre outros.

1.2.2 Estrutura da Internet

Como xa vimos, Internet non é unha rede centralizada nen está rexida por un só organismo. A súa estrutura parécese a unha *tea de araña* na que se conectan unhas redes a outras formando unha gran rede mundial.

Así e todo hai unha serie de organizacións responsables da adxudicación de recursos e a evolución dos protocolos precisos para que Internet evolucione. Así temos:

- **A *Internet Engineering Task Force* (IETF)** encárgase de redactar os protocolos que usa Internet.
- **A Corporación de Internet para os Nomes e os Números Asignados (ICANN)** É a autoridade que coordina a asignación de identificadores únicos en Internet, incluíndo nomes de dominio, direccións IP, etc.

Un punto interesante na estrutura de Internet é o xeito de identificar as máquinas, usuarios e recursos en xeral que están conectadas a ela:

- En Internet empréganse direccións numéricas para identificar máquinas, son **as direccións IP** que, como sabemos dos temas de redes, trátase dun conxunto de 32 bits que se representan, para mellor manexo polos humanos, por catro números, de 0 a 255, separados por puntos.

  Cada máquina conectada directamente a Internet debe ter unha IP única no mundo.

- Como é máis sinxelo recordar un nome que un conxunto de catro números, as direccións "tradúcense" a nomes, os denominados "nomes de dominio". Este servicio de internet que se encarga da traducción é o **DNS (*Domain Name System*).**

- Para identificar a usuarios de correo electrónico empréganse as **direccións de correo electrónico,** que teñen o seguinte formato:

  usuario@servidor_de_correo.dominio

- Para identificar recursos en Internet, empréganse dirección URL (*Uniform Resource Locator*, Localizador Uniforme de Recursos). Unha dirección URL tene a forma:

  http://nome_da_maquina.nombre_da_empresa.dominio_primario/paxina_web.htm

Sendo "http://" o protocolo, "nome_da_maquina" é o nome do servidor que nos vai a enviar a páxina web que queremos ver, nome_da_empresa" é o nome de dominio que escolleu a empresa, institución, persoa,... có que se da a coñecer en Internet, "dominio_primario" é un dos dominios dos que están regulados, e "paxina_web.htm" ó recurso ó que se accede.

1.3 Servizos da Internet

Internet é unha ferramenta moi potente que permite acceder a información que estea en calquera lugar do mundo.

Dependendo da forma na que se accede á información, xurden distintas posibilidades de uso da Internet. A estas diferentes posibilidades coñécenselles como **Servizos da Internet** e, entre eles, podemos destacar varios que sen dúbida son recoñecidas por calquera aficionado a Internet: navegación web, correo electrónico, FTP, etc. A continuación veremos cada un destes servizos.

1.3.1 Navegación web

Ó navegar pola Rede, accédese a documentos electrónicos ou páxinas web. Normalmente, estas páxinas non son simples documentos individuais senón que están relacionadas con outras formando o que se denomina un **sitio web.** A ferramenta *software* para navegar pola rede é o Navegador web. Un navegador web (explorador web ou, do inglés, *navigator* ou *browser*) é unha aplicación *software* que permite ó usuario visualizar documentos

de hipertexto, normalmente escritos en (X)HTML, e enviados por unha liña de comunicacións dende un servidor web, que poden estar en calquera parte do mundo. Esta rede de documentos denomínase ***World Wide Web* (WWW)**. Calquera navegador actual permite mostrar ou executar gráficas, secuencias de vídeo, son, animacións e programas de moitos tipos, ademais do texto e os enlaces (hipervínculos).

Para acceder a un sitio web débese coñecer a súa URL. URL é o acrónimo de *Universal Resource Locator* (Localizador universal de recursos), unha dirección única que posúe toda páxina web e permite o acceso dos usuarios a ela. Por exemplo, a URL do instituto San Clemente é http://www.iessanclemente.net (formada polo protocolo que se emprega, http, e a dirección).

1.3.2 Correo electrónico

Este servizo de Internet, que en inglés recibe o nome de e-mail (*electronic mail*), permite recibir e enviar correspondencia de xeito electrónico dende e cara calquera parte do mundo grazas ós servidores de correo.

O acceso a este servizo pódese realizar de dous xeitos distintos: ó traveso da web (*webmail*), ou mediante *software* de xestión de correo (Outlook Express, Thunderbird,...).

Tanto para o envío como para a recepción de correo con *software* de xestión, empréganse unha serie de protocolos específicos para que o servidor e dito programa se entendan. No caso de envío de correo, emprégase o protocolo SMTP (*Simple Mail Transfer Protocol*, Protocolo para a transferencia de correo simple); no caso da recepción de correo, o traballo recae sobre o protocolo POP3 (*Post Office Protocol* 3, Protocolo da oficina de correos 3). Tamén se pode empregar o protocolo IMAP (*Internet Message Access Protocol*, Protocolo de acceso a mensaxes de Internet) que permite acceder a mensaxes gardados no servidor de correo como si estivesen no propio ordenador. Poderíase dicir, por tanto, que é unha mestura entre *webmail* e POP3, adoptando certas ventaxas de cada un deles.

1.3.3 Transferencia de arquivos

Os protocolos FTP (*File Transfer Protocol*, Protocolo de transferencia de arquivos) e TFTP (*Trivial File Transfer Protocol*, Protocolo de transferencia de arquivos trivial) permiten a transferencia de arquivos entre ordenadores ou dispositivos. O usuario fai a descarga e a subida de información mediante un programa cliente instalado no ordenador.

1.3.4 Mensaxería instantánea

Este servizo baséase no uso de *software* que permite, empregando a pila de protocolos TCP/IP, enviar e recibir mensaxes en tempo real entre un ou mais usuarios conectados a Internet e que posúan dito programa. Este tipo de *software* dispón dunha lista de contactos na que se indica se os outros usuarios están conectados ou non en cada momento. Só algúns programas permiten enviar mensaxes a usuarios desconectados. Ademais os programas de mensaxería actuais incorporan cada vez mais servizos como, por exemplo, a transferencia de ficheiros. Algúns dos máis coñecidos son: Messenger, aMSN, Miranda, Pidgin, Trillian,...

1.3.5 Foros e chats

Os foros permiten a un grupo de usuarios ler e escribir sobre diferentes temas. Non son un servizo en tempo real xa que cando un usuario escribe unha mensaxe e a envía ó servidor, queda aí almacenada, podendo ser lida en calquera momento por outros usuarios. Como é de supoñer, na maioría dos foros é necesario contar con autorización para acceder a el e ler as mensaxes.

A diferenza dos foros, os chats (*chat*, charla) permiten a comunicación escrita en tempo real. Se un usuario escribe algo nun *chat*, só poderán velo aqueles usuarios que tamén estean conectados nese intre.

Un exemplo especial de *chat* é o **IRC** (*Internet Relay Chat*), un protocolo que permite a comunicación escrita en tempo real entre varios usuarios. Nel hai diversas canles ás que un usuario pode acceder se lle interesa o tema do que se trata en dita canle. Tamén existen charlas privadas entre dous ou mais usuarios ás que só teñen acceso os que reciben permisos axeitados. Para conectarse a este tipo de servidores de *chat* é preciso empregar un programa cliente.

1.3.6 Grupos de novas

Os grupos de novas ou *newsgroups* empregan o protocolo NNTP (*Networks News Transport Protocol*). Son un servizo que permite a un grupo de usuarios ler e enviar mensaxes de texto sobre un tema concreto. Ditas mensaxes mantéñense en servidores de novas, podendo ser descargadas e enviadas empregando programas específicos (*XNews*) ou programas de xestión de correo que inclúan dita posibilidade (*Outlook Express*).

1.3.7 Servizos de telefonía

Estes servizos permiten, mediante o *software* apropiado e, nalgúns casos, algún dispositivo *hardware*, manter conversas de voz entre dous usuarios a través de Internet. Se á voz se lle engaden tamén imaxes captadas por unha *webcam*, esta conexión denomínase videoconferenza. O programa máis amplamente empregado para este tipo de servizo é sen dúbida o Skype.

1.3.8 Terminais virtuais

Telnet é un protocolo de concexión remota que empregan un cliente e un servidor para unha conexión. Con el, podemos acceder dende o ordenador A ó ordenador remoto B e traballar con este como se estivésemos diante del.

Como Telnet ten moitos problemas de seguridade, unha boa práctica é empregar o protocolo SSH. **SSH (*Secure SHell*)** traballa de forma similar a como o fai Telnet. A diferencia principal é que SSH emprega técnicas de cifrado que fan que a información que viaxe de modo non lexible, e así ningunha terceira persoa poida descubrir o usuario e o contrasinal da conexión nin o que se se escribe durante toda a sesión.

Para traballar con estes protocolos é moi habitual utilizar o *software* libre PuTTY que é un cliente para SSH, Telnet, rlogin, e TCP raw. Este *software* estaba dispoñible, orixinalmente, só para Windows, pero agora tamén está dispoñible en varias plataformas Unix, e para Mac OS X.

1.4 Seguridade en Internet

Na actualidade son moi comúns os ataques á intimidade e á propiedade privada ó traveso de Internet. Por este motivo, debe considerarse de vital importancia coñecer o concepto de seguridade e o funcionamento das ferramentas que a proporcionan, tales como o cifrado dos datos ou os certificados de seguridade, así como aprender a diferenciar as conexións seguras de aquelas que non o son. Un sistema seguro sería aquel que non vai fallar nunca e que sempre terá o comportamento esperado. Pódese dicir que un sistema seguro é básicamente un sistema fiable Esta fiabilidade pódese resumir nunha serie de propiedades básicas:

1.4.1 Confidencialidade

A confidencialidade impide que usuarios non autorizados accedan a información privada. Só terán aceso a esta información aqueles usuarios que fosen autorizados no sistema, debendo cumplir as normas de privacidade impostas polo administrador da información.

1.4.2 Control de acceso

Impide que usuarios non autorizados accedan a recursos do sistema para os que non dispoñen dos permisos necesarios

1.4.3 Integridade

Impide o cambio ou modificación da información por parte de usuarios non autorizados no transcurso dunha comunicación.

1.4.4 Autenticación

A autenticación certifica a identidade dos usuarios que interveñen nunha transmisión de datos.

A. Tipos de ataque contra un sistema web.

Hai moitos tipos de ataque contra un sistema pero, en xeral, os principais modos de ataque pódense agrupar en catro:

- **Interrupción.**
  É un ataque á disponibilidade, xa que implica que a información non estea disponible por perda ou modificación que a inutilice.
- **Interceptación (*sniffing*).**
  É un ataque á confidencialidade no que un usuario non autorizado consegue acceder a información privada que se transmite entre usuarios autorizados.
  Os programas que empregan estes usuarios denomínanse sniffer.
- **Modificación.**
  É un ataque á integridade posto que un usuario non autorizado consegue o acceso a información privada e a modifica. Pódese considerar a destrucción como un tipo especial de modificación no que a información queda inutilizable.
- **Fabricación (*spoofing*).**
  O spoofing é un ataque á integridade similar á modificación. Un usuario non autorizado (X) suplanta a identidade dun autorizado (A) e crea información similar á que este proporcionaría. Dita información é enviada ó usuario autorizado (B), quen cree recibir a información do usuario autorizado (A).

B. Riscos na Internet.

Ademais dos coñecidos riscos físicos ós que se enfrontan os equipos, hai unha serie de riscos de carácter lóxico que hai que ter en conta. Os riscos lóxicos son aqueles de tipo *software* que danan os sistemas, sexa cal sexa a forma na que levan a cabo a súa acción. Poder ser creados de forma intencionada, o que recibe o nome de ***malware***, ou ben ser simplemente erros propios do desenrolo de calquera *software*, o que se coñece como *bugs* ou buracos.

◊ Entre os riscos lóxicos mais importantes destacan as **portas traseiras** ou *backdoors*. Pertencen ó tipo *bug* e son "atallos" de autenticación creados polos programadores durante o período de desenrolo dos programadores e que despois non son eliminados.

◊ As **bombas lóxicas,** son do tipo *malware* e consisten en introducir dentro do código dun programa, fragmentos de código que son "disparados" por algunha acción determinada provocando efectos prexudiciais para o sistema.

◊ Outro tipo de *malware* son os **virus**. Consisten en partes de código que se inclúen dentro de ficheiros executables de maneira que, cando é executado o ficheiro, o virus tamén entra en funcionamento realizando operacións mal intencionadas para as que foi creado.

◊ Tamén os **gusanos** son de tipo *malware* e consisten en programas que se executan e se propagan ó traveso das redes, por eles mesmos, aproveitando os buratos de seguridade nos sistemas.

◊ Finalmente, entre os riscos de tipo *malware*, estarían os **troianos.** Así os troianos, consisten en programas ocultos en outros programas de forma que cando son executados, o troiano realiza as accións para as que foi creado.

C. Comunicacións cifradas. Tipos de cifrado.

Conforme a Rede foi crecendo, a codificación chegou a ser unha das ferramentas mais importantes no que respecta a preservar a privacidade e a intimidade. Actualmente, a seguridade dos sistemas e a privacidade dos datos son primordiais debido ó aumento do número de persoas interesadas en conseguir información. En definitiva, a confidencialidade está en perigo constante, sobre todo se a información se transmite ó traveso de canles pouco seguros como é o caso de Internet.

Por esa misma razón codifícase a información. Para realizar dita codificación emprégase un código secreto denominao **chave** e ecuacións matemáticas que cifran e descifran os datos a partir de dita chave.

A ciencia que se encarga da codificación segura de mensaxes para que só o destinatario poida descifralo é a criptografía. Principalmente hai dous tipos de criptografía: a criptografía simétrica e asimétrica.

◊ **Cifrado simétrico.**
A criptografía simétrica, tamén chamada de chave secreta ou simple, baséase no uso dunha soa chave para cifrar e descifrar a información, o que conleva que os usuarios deben intercambiarse a chave con anterioridade ó traveso de canles seguros, có risco que isto supón.
Algúns exemplos de algoritmos simétricos son 3DES, AES, Blowfish e IDEA.

◊ **Cifrado asimétrico.**
A criptografía asimétrica ou de chave pública, baséase na existencia dunha chave para o cifrado da información, chamada **chave pública,** e outra chave para a decodificación dos datos, que recibe o nome de **chave privada.** A chave pública móstrase nun directorio ó que todo o mundo ten acceso mentres que a privada só a coñece un usuario e non debe ser revelada baixo ningún concepto.
Algúns algoritmos de técnicas de clave asimétrica son: Diffie-Hellman, RSA, DSA e ElGamal.

D. HTTP fronte a HTTPS.

Non se pode falar de navegación web sen o protocolo **HTTP (*HyperText Transfer Protocol*).** Este protocolo serve para a comunicación entre servidor e navegador.

A forma en que se indica ó navegador que o protocolo que se vai empregar é HTTP é escribindo **http://** seguido da URL do sitio web na barra de direccións do navegador. Deste xeito, diferénciase doutros servizos ós que tamén se pode acceder có navegador como, por exemplo, o servizo de FTP. No caso de que non se indique na URL o protocolo empregado, a maioría de navegadores entenderán que se trata de HTTP.

Como a maioría dos servizos de Internet, HTTP ten a súa versión segura, HTTPS. Esta versión segura do protocolo cifra a comunicación entre o cliente e o servidor mediante o uso de certificados dixitais. Na barra de direccións do navegador aparecerá neste caso **https://** seguido da URL, indicando así que a comunicación có servidor efectúase cifrada.

E. Certificados dixitais.
En toda transacción comercial que se leve a cabo ó traveso da Internet, o mais importante é o uso dun certificado dixital que avale a seguridade de dita transacción.

Cando se accede a unha páxina web segura, o normal é que na fiestra do navegador apareza un pequeno cadeado na parte inferior. Dende el pódese comprobar si, realmente, a páxina dispón dun certificado dixital de seguridade. Poñendo o rato sobre dita icona, aparecerá un *tooltip* cunha lenda parecida a "Seguridade SSL 128 bits". Así se indicará o tipo de codificación coa que chega dita páxina web, que no caso do exemplo anterior sería cifrado de 128 bits baseado no protocolo de seguridade SSL **(*Secure Socket Layers*).** Deste protocolo tamén existen cifrados de 40, 56 ou 256 bits.

Os certificados dixitais son únicos, é dicir, cada usuario terá o seu propio certificado. De xeito parecido a un DNI electrónico, o certificado permite identificar plenamente a un usuario. Ademais, ten a vantaxe de que se trata dunha certificación internacional e non só restrinxida ó país de residencia do usuario.

Estes documentos de identificación son proporcionados polas entidades certificadoras. Son entidades certificadoras:

- ◊ Verisign
- ◊ Fábrica Nacional de Moeda e Timbre
- ◊ TrustCenter
- ◊ Thawte
- ◊ ...

Estas entidades testemuñan que o usuario que a posúe é quen di ser dándolle un certificado dixital. Cada vez que o usuario emprega o certificado (firmando unha mensaxe cifrado ou codificando unha mensaxe), é coma si amosase ante o receptor o seu DNI particular.

Para que estas entidades concedan un certificado a un usuario ou empresa, é necesario que estes cubran un certificado de certificación. un documento no que se facilitan os datos necesarios á entidade certificadora para que esta poida asegurarse de que o solicitante cumpre cós requisitos precisos para obter o certificado.

Para ver cal é a entidade certificadora que resposta por un usuario ou por unha empresa, e os datos en xeral dun certificado dixital concreto, tan só hai que facer dobre clic sobre o cadeado.

Por último, é importante saber que os certificados poden ser de diferentes tipos dependendo do uso que se lles vaia dar e de quen os solicite. Así, se solicitas un **certificado de clase 0**, que son os mais sinxelos de obter, a entidade certificadora realizará unha serie de comprobacións e pedirá moitos menos datos que os que requirirá se o certificado é de clase superior.

--Vieites 27 sep 2007