Risico´s van internetwerken

Wietse Venema

Wiskunde en Informatica
Technische Universiteit Eindhoven
wietse@wzv.win.tue.nl

ABSTRACT

Aansluiting van een lokaal netwerk op een extern netwerk als Internet heeft diverse gevolgen voor beheer en beveiliging. Aandacht wordt besteed aan de voornaamste risico´s en oplossingen: niet afluisterbare wachtwoorden voor externe toegang, data encryptie voor veilig informatie transport, en netwerk firewalls voor een duidelijke scheiding tussen lokaal en extern netwerk.

De elektronische metropool

Staat uw auto of fiets op slot? Nu niet meteen weglopen :-) Zet u hem ook op slot als hij thuis in de schuur of garage staat? Waarschijnlijk niet. Waarom zetten we dingen op slot, of waarom zetten we ze in een afgesloten ruimte? Wel, we hebben geleerd dat het verstandig is om je spullen af te sluiten als je ze ergens onbewaakt achterlaat.

Met het Internet betreden we het tijdperk van de elektronische metropool die zich uitstrekt over alle werelddelen. Een digitale burger kan zomaar in contact komen met iemand aan de andere kant van de wereld, ook als ze niet eerder van elkaars bestaan op de hoogte waren.

In elke samenleving gelden spelregels, taboes, en andere vormen van kultuur. Dat geldt ook voor een elektronische samenleving. Een aantal van die regels is in de afgelopen jaren door pioniers ontdekt. Ik heb het voorrecht gehad om aan dat proces een klein stukje te mogen bijdragen. Er is echter nog veel niet verkend terrein.

Ik zal in mijn voordracht aandacht geven aan een aantal technieken en spelregels die kunnen helpen om al te grote brokken te voorkomen. Deze spelregels en technieken zijn nog betrekkelijk nieuw. Ik heb goede hoop dat ze over een paar jaren net zo gewoon zijn als "uitkijken voor je de straat oversteekt" of "handen wassen voor het eten".

Veiligheid: een afbakening

Alvorens in te gaan op problemen en oplossingen lijkt het een goed idee om eerst aan te geven wat ik in dit verhaal onder beveiliging versta. Over het onderwerp zijn hele boekwerken vol geschreven. Ik beperk me echter tot de volgende vereenvoudiging:

- Gecontroleerde toegang tot systemen.
- Gecontroleerde toegang tot gegevens.

Wat we onder ‘gecontroleerde toegang’ dienen te verstaan hangt af van de omstandigheden. Gecontroleerde toegang kan bijvoorbeeld inhouden prikkeldraad rondom een bomvaste bunker, een gewapende soldaat voor de deur, en herkenning door middel van een scan van het netvlies.

Zo’n mate van beveiliging is voor de meeste toepassingen overdreven. In een openbare bibliotheek verwacht je nu eenmaal geen staatsgeheimen aan te treffen. Van een ziekenhuis, daarentegen, verwacht je dat patientengevens niet voor Jan en alleman toegankelijk zijn. Welke mate van bescherming gewenst is hangt dus van Uw eigen doelen af. Als U gegevens gaat transporteren door de elektronische stad, dan kan U beter vooraf vaststellen of een bakfiets goed genoeg is, of dat je vandaag maar beter de pantserwagen kan laten voorrijden.

Het lokale netwerk: een elektronisch dorp

Om een gevoel te geven wat aansluiting op een extern netwerk inhoudt wil ik beginnen met een simpel voorbeeld: een lokaal netwerk dat een eilandje op zichzelf vormt. Men denke aan een afdeling binnen een organisatie. Stel eens, om de gedachten te bepalen, dat zo’n lokaal netwerk toegang biedt tot enkele tientallen, maar zeker niet meer dan enkele honderden, gebruikers.

Het aardige van zo’n geisoleerd netwerk is dat het relatief veel bescherming kan ontlenen aan zijn omgeving. Om toegang te krijgen tot de systemen zal je je toch eerst in levende lijve aan de apparatuur moeten presenteren. Pas als deze fysieke drempel is genomen kan er sprake van zijn toegang tot bestanden. Onder gunstige omstandigheden kunnen verdere beveiligingsmaatregelen zelfs achterwege blijven. Deze situatie is te vergelijken met een dorp waar je s´ochtends een tas met wat geld aan de deur hangt, en erop kan rekenen dat die tas in de loop van de dag netjes wordt gevuld met boodschappen.

Van elektronisch dorp naar metropool

Wat gebeurt er als lokale netwerken van verschillende afdelingen binnen de organisatie worden gekoppeld? Allereerst neemt het aantal aansluitingen dramatisch toe. Met een beetje universiteit gaat het al gauw om duizenden aansluitingen. Met zoveel aansluitingen erbij kan het lokale netwerk veel minder bescherming aan de omgeving ontlenen. Zolang er geen externe verbindingen van betekenis zijn geldt nog steeds de drempel van fysieke aanwezigheid. Het is echter duidelijk dat de gebruikersgroep heterogener zal zijn dan in het geval van een geisoleerd afdelingsnetwerk.

Bij aansluiting op het wereldwijde Internet bereiken we de tegenpool van de beginsituatie. Het lokale netwerk wordt opeens uitgebreid met ordegrootte honderdduizend aansluitingen binnen Nederland, en met nog eens zo’n 3 miljoen aansluitingen daarbuiten. Het mag duidelijk zijn dat in zo’n elektronische metropool andere regels gelden dan in het elektronische dorp waaraan ik eerder refereerde. Dit lijkt echter langzaam door te dringen tot leveranciers (en tot hun klanten!). Computersystemen worden helaas maar al te vaak afgeleverd met instellingen die uitgaan van een beschermde omgeving. Allerlei sloten hangen los, en deuren staan wijd open. Zulke systemen bevinden zich fysiek wel binnen een solide gebouw, maar eigenlijk staan die systemen buiten op straat waar ze een gemakkelijke prooi zijn voor elektronische joyriders en vandalen.

Na deze sombere woorden zal ik proberen te laten zien welke oplossingen zijn bedacht voor het probleem van gecontroleerde toegang tot netwerken, systemen en gegevens.

Afluisterbare wachtwoorden

In science-fiction films zien we soms dat mensen hun vinger in een apparaat moeten steken om te bewijzen wie ze zijn. Of ze moeten hun oog voor een apparaatje houden dat dan naar hun netvlies koekeloert. Diverse toeren worden vervolgens uitgehaald om zulke apparatuur te foppen. Dat de held van het verhaal aan deze avonturen een prettige relatie overhoudt is mooi meegenomen. De banale wekelijkheid is evenwel dat veel systemen nog steeds worden beschermd met een wachtwoord. Het is dan ook geen wonder dat hackers nog altijd veel moeite willen doen om wachtwoorden te pakken te krijgen.

Netwerk login procedures verlopen gewoonlijk als volgt. De gebruiker zit achter een computer. Dit systeem noemen we de *client*. Er is een tweede computer die diensten levert. Dit systeem noemen we een *server*. De server levert de service alleen als de gebruiker zich op de juiste wijze heeft bekendgemaakt. De gebruiker geeft een gebruikersnaam en wachtwoord in op de client computer. Beide worden door de client over een netwerk naar de server gestuurd. De server controleert gebruikersnaam en wachtwoord, en besluit om al dan niet de gevraagde dienst te verlenen.

Veel computernetwerken zijn gebaserd op ethernet. Informatie wordt als kleine pakketjes over de kabel verstuurd. Elk pakketje heeft een afzender adres dat zegt waar het vandaan komt, en een bestemming adres dat aangeeft voor welke computer het bestemd is. Op een ethernet gelden allerlei spelregels om te zorgen dat het verkeer ordelijk verloopt. Een van die spelregels is dat dat computers niet luisteren naar netwerk pakketjes bestemd voor andere systemen.

Computers zijn echter uiterst flexibele apparaten. Het is voor een hacker een kleine moeite om een programma te draaien dat ervoor zorgt dat een systeem wel luistert naar alle voorbij komende boodschappen. Op die manier kan een hacker geheel ongemerkt wachtwoorden en allerlei andere informatie meelezen.

Het meeste netwerkverkeer speelt zich af tussen systemen op hetzelfde lokale netwerk. Bij een systematische opzet van een netwerk zal lokaal verkeer het lokale netwerk dan ook niet verlaten. Het risico van afluisteren van lokaal verkeer is dus beperkt, ook als je op een extern netwerk bent aangesloten.

Afluisteren op grote schaal

De situatie wordt er niet gunstiger op met netwerk logins via externe netwerken. Gebruikersnaam en wachtwoord reizen nu via allerlei tussenliggende netwerken van andere partijen. De mogelijkheden om verkeer af te luisteren worden dan ook stukken groter.

In Februari 1994 gaf CERT/CC een perbericht uit waarin ze bekend maakte dat in de daaraan voorafgaande maanden naar schatting 10000 wachtwoorden waren afgeluisterd. Hackers hadden een aantal systemen gekraakt waarlangs veel verkeer kwam. Door subtiele veranderingen aan te brengen in systeemsoftware konden ze enige tijd ongemerkt hun gang gaan. CERT/CC is een organisatie die bemiddelt bij problemen met de veiligheid van systemen aan het Internet. CERT-NL is de Nederlandse variant en is het onderwerp van de volgende spreker.

Encryptie versus big brother

Waarom worden gegevens zoals wachtwoorden zonder enige bescherming over het netwerk gestuurd? Als de informatie versleuteld was zou afluisteren immers geen zin meer hebben. Tegen die redenering is niets in te brengen. Er zijn echter bezwaren van niet technische aard. Encryptie maakt het niet alleen lastiger om wachtwoorden af te luisteren, maar maakt ook andere informatie ontoegankelijk, en dat is de reden waarom allerlei regeringen er problemen mee hebben. Zo legt de regering van de USA allerlei beperkingen op aan de export van producten waaraan encryptie te pas komt: encryptie valt onder de munitiewet. Hoe beter de encryptie, des te sterker de restricties. Andere landen als Frankrijk verbieden zelfs het gebruik van data encryptie. En onze eigen regering had begin 1994 een wetsvoorstel in voorbereiding dat encryptie zonder vergunning illegaal zou maken. Aan het gebruik van encryptie zitten dus nogal wat haken en ogen. Dit werkt bepaald niet stimulerend op leveranciers.

Niet afluisterbare wachtwoorden.

Het ziet er dus naar uit dat data encryptie voorlopig geen standaardvoorziening zal worden. Wachtwoorden zullen nog geruime tijd op de huidige manier over het netwerk blijven reizen. Wat is hier aan te doen? Het probleem is dat iedereen die een wachtwoord kent het zovaak kan gebruiken als hij of zij wil. Hoe korter een wachtwoord geldig is, hoe kleiner het risico dat een ander er wat aan heeft. Vandaar dat sommige organisaties eisen dat gebruikers elke week of maand een nieuw wachtwoord gebruiken. Deze aanpak is nogal onvriendelijk voor de gebruiker, en het lost het probleem van afluisteren niet echt op.

Een grondiger oplossing is om een wachtwoord maar eenmaal geldig te laten zijn. Dit is alleen uitvoerbaar wanneer het wachtwoord automatisch wordt gegenereerd, bijvoorbeeld door een programmaatje of door een klein stukje hardware. Zelfs wanneer zo'n wachtwoord wordt afgeluisterd dan is er geen ramp gebeurd want het kan toch niet meer worden gebruikt.

Eenmalige wachtwoorden kunnen op diverse manieren worden gegenereerd: met speciale hardware in de vorm van een niet programmeerbare smartcard (SecurID) of met een programmeerbare encryptiebox (Digital Pathways), of met een resident miniatuur programmaatje in je PC (de S/Key software). De aanschafkosten varieren van fl 100,- per persoon per jaar in het eerste geval tot niets in het laatste geval.

Veilig informatie transport

In het voorafgaande besprak ik hoe bij het afluisteren van netwerkverkeer wachtwoorden kunnen worden opgevangen. Als je wachtwoorden kan afluisteren, dan kan je natuurlijk ook allerlei ander verkeer afluisteren.

Er zijn twee manieren om informatie veilig over een netwerk te sturen: of je beschermt het netwerk tegen ongewenste toegang, of je beschermt de informatie zelf. Bescherming van het netwerk is geen praktische oplossing als je vanuit Nederland een bericht wil sturen naar iemand in Nieuw Zeeland. Zeker niet als de transatlantische verbinding uitvalt en gebruik moet worden gemaakt van een backup verbinding via een satelliet. Bescherming van de informatie zelf vereist encryptie. Nu kan je data encryptie op allerlei niveaus doen. Voorbeelden zijn:

- Per systeem: elke individuele computer versleutelt alle informatie alvorens ze op de kabel te zetten. Dit is de meest radicale oplossing, maar ze is ook erg kostbaar qua beheer.
- Per netwerk: informatie wordt versleuteld bij het verlaten van het lokale netwerk. Dit wordt wel gebruikt om prive netwerken te koppelen via een openbaar netwerk als het Internet.
- Per applicatie: een applicatie versleutelt informatie alvorens ze aan de netwerk software te geven. De huidige generatie secure electronic mail werkt volgens deze methode.

Elk niveau heeft voor en nadelen. Bij wijze van illustratie zal ik laten zien hoe encryptie op applicatie niveau wordt gebruikt ten behoeve van electronic mail. De meeste problemen die we daar tegenkomen gelden ook voor encryptie op andere niveaus.

Traditionele versleuteling

Traditionale versleuteling maakt gebruik van precies een sleutel (soms ook wel wachtwoord genoemd). De sleutel wordt gebruikt om de informatie onleesbaar te maken. De onleesbare informatie wordt vervolgens verstuurd (in vroeger tijden met een koerier te paard). De ontvangende partij gebruikt dezelfde sleutel om het bericht weer leesbaar te maken. Als we even aannemen dat de sleutel alleen bekend is bij afzender en ontvanger, dan levert versleuteling de volgende zekerheden op:

- Privacy: alleen een bezitter van de sleutel kan het bericht leesbaar maken.
- Herkomst: alleen een bezitter van de sleutel kan het bericht aanmaken.
- Integriteit: als er in het versleutelde bericht ook maar iets is veranderd dan levert het onmiddelijk een fout op bij het ontcijferen.

Het is duidelijk dat er nogal wat voorbereiding aan te pas komt voordat je op deze wijze met iemand kunt communiceren. Allereerst moet je een veilige manier zien te vinden om met elkaar een sleutel af te spreken. Alleen dat al kan een lastig kip en ei probleem zijn. Een tweede probleem is dat je eenzelfde versleuteld bericht moeilijk aan meerdere partijen kan sturen, tenzij je ze allemaal dezelfde sleutel geeft. Dat komt de geheimhouding niet ten goede.

Een veel ernstiger probleem is dat bij gebruik op grotere schaal het aantal benodigde sleutels snel uit de hand loopt. Als je volgens de regels te werk gaat is een sleutel nodig voor ieder paar partijen. In een formule uitgedrukt: als N het aantal partijen is, dan zijn N(N-1)/2 sleutels nodig. Bij grote aantallen partijen is het benodigde aantal sleutels dus evenredig met het kwadraat van het aantal partijen. Traditionele encryptie is alleen al om deze reden ongeschikt voor grootschalige toepassing.

Publieke sleutels: een sleutel per partij, bescherming op maat

Een interessante ontwikkeling is de encryptie op basis van complementaire sleutels. Informatie die is vercijferd met de ene sleutel kan alleen leesbaar worden gemaakt met zijn wederhelft. Dat lijkt op het eerste gezicht geen vooruitgang: nu heb je twee sleutels nodig waar eerst een enkele sleutel volstond. De grap is echter dat je met dit ene sleutelpaar kan volstaan, ongeacht het aantal partijen waarmee je correspondeert.

Elke partij genereert een stel complementaire sleutels. De ene sleutel blijft geheim. De andere sleutel wordt openbaar en mag onbeperkt worden verspreid.

Voorbeeld: privacy

Stel, ik bewonder een schone dame en wil haar een liefdesbrief sturen. Daartoe hoef ik alleen haar openbare sleutel te kennen. Die sleutel kan ik via het netwerk ophalen; dat is handig voor verlegen personen. Ik versleutel mijn ontboezemingen met haar openbare sleutel en vertrouw het resultaat toe aan het netwerk. Ik kan erop vertrouwen dat mijn ontboezemingen alleen onder haar ogen komen, want alleen zij heeft de geheime sleutel waarmee het bericht leesbaar kan worden gemaakt.

Voor de ontvangende partij is dit een uiterst gerieflijke manier van communicatie: met een enkele openbare sleutel kan ze persoonlijke post ontvangen van hordes bewonderaars.

Voorbeeld: authenticiteit

Stel, ik wil een openbare aankondiging doen, en vind het belangrijk dat men weet dat het bericht echt van mij afkomstig is. Ik versleutel daartoe het bericht[1] met mijn geheime sleutel. Met mijn openbare sleutel kan vervolgens iedere lezer of lezeres zelf vaststellen dat het bericht van mij afkomstig is.

Voor maximale veiligheid combineren we de twee voorbeelden. Hiermee bereiken we dat alleen de juiste partij het bericht leesbaar kan maken. Verder kan de ontvanger vaststellen wie de afzender is. Bovendien bewijst successvolle ontcijfering dat het bericht ongewijzigd is aangekomen.

Secure electronic mail standaarden

Informatietechnologie is een gebied dat zich snel ontwikkelt. Een van de plezierige kanten is dat er altijd meerdere standaarden zijn om uit te kiezen. Zo ook met secure electronic mail. De belangrijkste standaarden zijn:

- PEM (privacy enhanced mail). Dit is een Officiele Internet Standaard. De standaard is recent, en is in Nederland nog in het stadium van proefprojecten. Buiten de UNIX omgeving is er nog niet veel voor te krijgen. Een van de handicaps van PEM is dat het afhankelijk is van een nog niet bestaand mechanisme voor distributie van openbare sleutels.
- PGP (pretty good privacy). Dit is een ‘de facto´ standaard. PGP wordt in wijde kring gebruikt, en er zijn implementaties voor de belangrijkste omgevingen. In tegenstelling tot PEM is PGP niet afhankelijk van een specifieke manier van sleutel distributie. Een handicap van PGP is dat vroegere versies het onderwerp waren van juridische controverses. Die periode is gelukkig voorbij. Er zijn nu versies beschikbaar voor gebruik binnen de USA en daarmee compatibele versies voor gebruik in de rest van de wereld.

Gelukkig wordt er naar wegen gezocht om de PEM en PGP standaarden met elkaar te koppelen. Niemand is gediend met twee incompatibele dialekten.

---

1. Of een checksum van het bericht, de zogenaamde digitale handtekening.

Firewalls: het elektronische hek rond het terrein

Aan het begin van deze voordracht liet ik zien dat bij aansluiting op het Internet een lokaal netwerk wordt uitgebreid naar zo´n 3 miljoen aansluitingen. Internet zelf biedt onbelemmerde communicatie tussen willekeurige systemen. Het gevolg is evenwel dat elk afzonderlijk lokale systeem zichzelf moet beschermen tegen pogingen tot misbruik vanuit de hele wereld. Met aansluiting op het Internet komen de lokale systemen als het ware buiten op straat te staan. Als ze niet van goede kwaliteit sloten zijn voorzien kan je vroeg of laat ongelukken verwachten.

Met schade en schande hebben pioniers geleerd dat het verstandig kan zijn om niet alle interlokale verkeer over je lokale netwerk te laten gaan, maar alleen verkeer dat wenselijk is. Firewall is de technische term voor de voorziening die zulke restricties implementeert. Een firewall wordt geinstalleerd tussen het lokale netwerk en de rest van de wereld, zodat alle interlokale verkeer de firewall moet passeren. Je kan een firewall dan ook zien als een elektronisch hek rondom het terrein, met slechts een beperkt aantal al dan niet bewaakte doorgangen. Mogelijkheden die de hedendaagse firewall technologie biedt:

- Restricties op binnenkomend verkeer. In het meest extreme geval kunnen externe systemen geen directe verbinding naar binnen maken.
- Restricties op uitgaand verkeer. In het meest extreme geval kunnen lokale systemen geen directe verbinding naar buiten maken.
- Authenticatie. Wanneer directe verbindingen naar binnen niet zijn toegestaan maken externe gebruikers zich eerst bekend aan de firewall. Dat gebeurt uiteraard met een eenmalig wachtwoord. Pas daarna mag men verder naar binnen.
- Proxies. Wanneer directe verbindingen naar buiten niet zijn toegestaan kan de firewall als doorgeefluik fungeren voor specifieke toepassingen, eventueel nadat de interne gebruiker zich eerst heeft bekendgemaakt aan de firewall.

Vanwege zijn strategische positie is de firewall bij uitstek geschikt om bij te houden wat er zoal aan verkeer de grens van het lokale netwerk passeert.

Firewalls komen in allerlei soorten en maten, en welk type geschikt is hangt af van de lokale eisen. In een universitaire omgeving worden meestal geen beperkingen opgelegd aan uitgaand verkeer. Soms wordt het binnenkomende verkeer in lichte mate gefilterd om de meest problematische diensten of systemen af te schermen. Deze mate van openheid ligt voor de hand, want de resultaten van onderwijs en onderzoek zijn of worden immers toch openbaar.

Een commerciele organisatie daarentegen zal zijn gegevens willen beschermen tegen al te nieuwsgierige ogen, en een meer gesloten beleid is dan ook gewenst met betrekking tot binnenkomend verkeer. Vaak zal verkeer naar buiten nog wel acceptabel zijn.

Het meest stringente firewall beleid staat geen enkele directe communicatie toe tussen het lokale netwerk en de buitenwereld. Deze elektronische variant op de luchtsluis bewijst zijn nut wanneer hoge eisen worden gesteld, bijvoorbeeld wanneer vertrouwelijke gegevens of industriele geheimen op het spel staan.

Tot slot

Aansluiten van een lokaal netwerk op Internet is niet iets dat je zomaar even doet. Men dient terdege rekening te houden met de mogelijke risico´s. Er is een veelheid aan technische middelen beschikbaar om het verkeer in goede banen te leiden. Uit deze middelen moet een verstandige keuze worden gemaakt. Het verdient dan ook aanbeveling om in een beleidsdocument duidelijk vast te leggen welke veiligheid is vereist, teneinde conflicten of ongelukken te voorkomen.

Literatuur

De onderstaande *RFC* documenten zijn beschikbaar op diverse ftp servers, bijvoorbeeld op ftp.nl.net in /pub/documents/rfc.

[1] R. Pethia, S. Crocker, B. Fraser, "Guidelines for the Secure Operation of the Internet", RFC 1281.

[2] J. Reynolds,J. Holbrook, "Site Security Handbook", RFC 1244.

[3] W.R. Cheswick, S.M. Bellovin, "Firewalls and Internet Security", Addison-Wesley 1994. Zie ook de bestanden in ftp.research.com:/dist/internet_security.

[4] Paul Wallich, "Wire Pirates", Scientific American, Maart 1994.

[5] W.Z. Venema, "TCP WRAPPER: Network monitoring, access control and booby traps", Proceedings of the Third Usenix UNIX Security Symposium, 1992. Zie ook de bestanden in ftp.win.tue.nl:/pub/security.