CRIPTOR ETHERNET IN TIMP REAL BAZAT PE LINUX

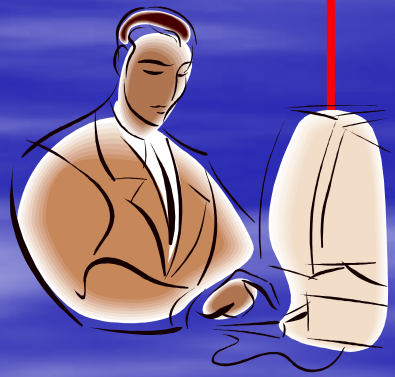
eLiberatica, *Brasov 18-19 MAI 2007*

O POVESTE DIN ZILELE NOASTRE:

A fost o data ca niciodata ca de nu ar fi, nu s-ar povesti. A fost o data o lume in care traiau doi fericiti utilizatori de SIC-uri interconectate: Ion si Maria.

O POVESTE DIN ZILELE NOASTRE...

MARIA



ION

Povestea continua:

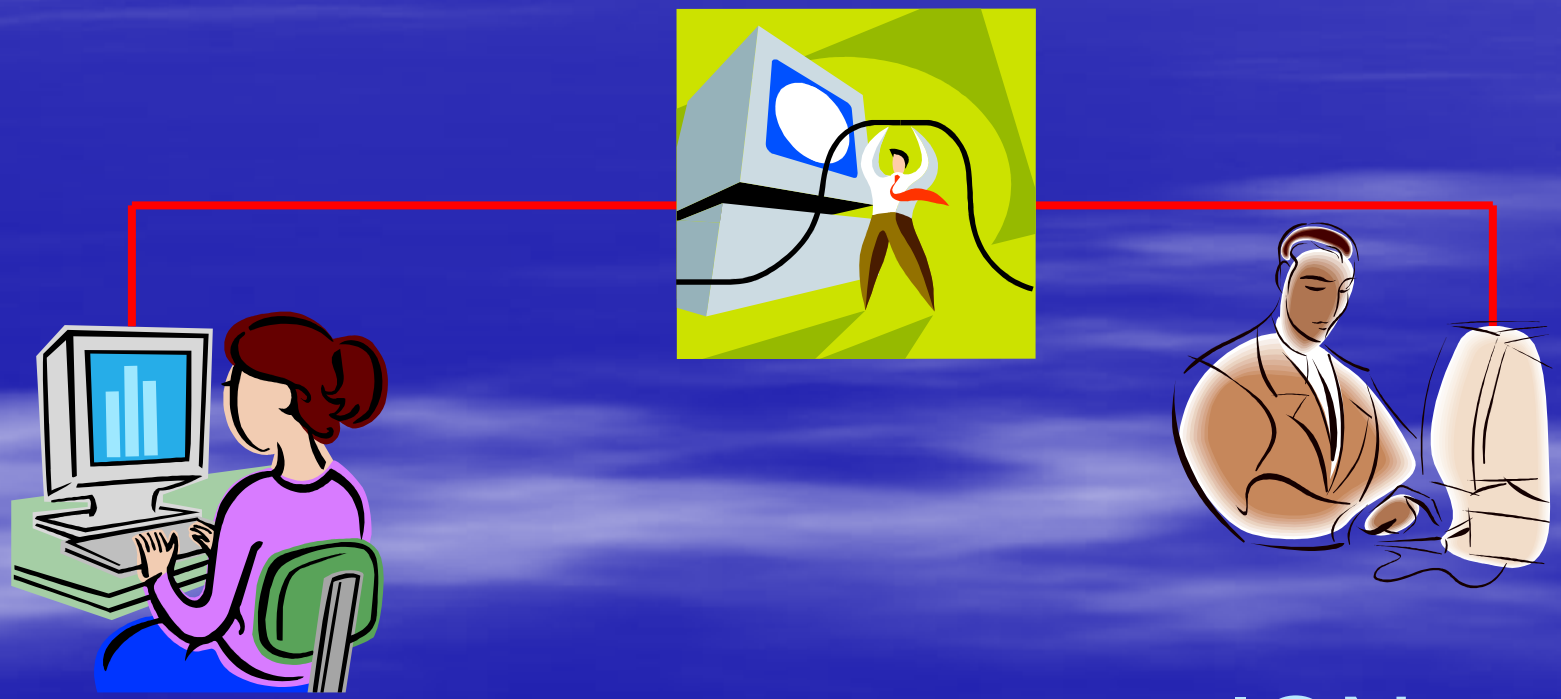
...

Povestea continua:

Si isi trimiteau ei unul altuia tot felul de chestiuni ce ii privea numai pe ei si pe altii nu. Nu se stie daca erau dulci declaratii de dragoste sau tocmai fisiere legate de munca lor. Totul a fost perfect, pana cand nu a aparut ceva de care ei nu stiau ca exista. Acel ceva a aflat despre ce faceau ei pe acolo, iar dupa cum se comportau cei doi, se pare ca nici nu stiau ce se intampla in realitate. Cine e vinovat ca

NU S-AU PROTEJAT???

O POVESTE DIN ZILELE NOASTRE...



MARIA

ION

...

VA SUNA CUNOSCUT???

CRIPTOR ETHERNET IN TIMP REAL BAZAT PE LINUX

AUTOR:

- Drd. Tiberiu Socaciu, *InfoData Cluj*

PREZINTA: TIBERIU SOCACIU

CRIPTOR ETHERNET IN TIMP REAL BAZAT PE LINUX

- *Introducere*
- *Material si metoda*
- *Rezultate, discutii*

Introducere

- Criptografia
- Necesitatea criptarii datelor
- Criptoare
- Rosu si negru
- Ethernet ca mediu de transmitere a datelor
- Criptor Ethernet

Criptografia

Criptografia reprezintă o ramură a matematicii care se ocupă cu securizarea informației precum şi cu autentificarea şi restricționarea accesului într-un sistem informatic. Conform Wikipedia, in realizarea acestora se utilizează atât metode matematice (profitând, de exemplu, de dificultatea factorizării numerelor foarte mari), cât şi metode de criptare cuantica. Termenul *criptografie* este compus din cuvintele de origine greacă κρυπτός *kryptós* (*ascuns*) şi γράφειν *gráfein* (*a scrie*).

Necesitatea criptarii datelor

Criptarea (cifrarea) este necesara in momentul in care informatia trebuie sa ajunga de la un emitor la un receptor pe un canal nesigur sau cu un grad de clasificare inferior, acest lucru impunand ca informatia sa nu circule in clar, deoarece manipulatorii informatiei nu au dreptul de acces sau deoarece canalul de comunicatie poate fi interceptat.

Criptoare

Numim criptor un echipament care realizeaza urmatoarele functii: a) *criptarea* - eventual in *timp real* - informatiei in clar pe baza unei/unor chei; b) *decriptarea* - eventual in *timp real* - informatiei criptate pe baza unei/unor chei. Constrangerile de timp real sunt necesare in mod evident datorita posibilitatii folosirii criptoarelor in sisteme de comunicatii ce pot interconecta retele in care sunt conectate echipamente de procesare si stocare a informatiilor clasificate.

Rosu si negru

Conceptul de rosu si negru presupune separarea fizica a echipamentelor si sistemelor de procesare, stocare si transmitere a informatiilor clasificate necriptate (rosu) de cele clasificate criptate sau neclasificate (negru). In principiu, locul criptorului este la interfata dintre un mediu rosu si unul negru, considerandu-se ca echipamentul de criptare este unul rosu, manipularea cheilor presupunand un nivel de securitate cel putin egal cu nivelul de clasificare a informatiilor clasificate din zona rosie

Ethernet ca mediu de transmitere a datelor

Conceptul de rosu si negru presupune separarea fizica a echipamentelor si sistemelor O data cu disparitia treptata a cablarilor tip BNC si aparitia noilor “cablarilor structurate” folosind cabluri TP din cauza noilor echipamente de tip hub Ethernet a inceput studierea posibilitatii cresterii de viteza de transmisie pe cabluri torsadate folosind tehnologii compatibile Ethernet. Asa s-au ajuns la concluzia ca s-ar putea creste viteza de transmisie de la 10Mbps la 100Mbps doar prin modificarea tipului de torsadare, deoarece transmisiile de date foloseau cate o pereche pentru transmisie de date (TX), respectiv receptie de date (RX). Noul standard s-a numit FastEthernet.

Ethernet ca mediu de transmitere a datelor (continuare)

Urmatorul pas a fost atasarea unei memorii pentru dispozitivele de tip hub in care sa se memoreze toate MAC-urile potentiale destinatie de pachete. Acest lucru se poate face printr-o banala analiza a expeditorului unui pachet ce vine pe un port oarecare. Astfel, echipamentul ar putea “invata” din mers MAC-uri, construind si intretinand in timp real o tabela cu intrari de forma (port, MAC). Probabil cea mai buna organizare a tabelei este decisa de fabricantul echipamentului in momentul in care scrie firmware-ul echipamentului. Utilitatea acestei tabele se vede in momentul in care software-ul echipamentului decide ca la primirea unui pachet, acesta sa fie transmis pe cat posibil doar pe portul care este prezumtiv conectat interfata in cauza. Acest lucru genereaza scaderi drastice ale coliziunilor de pachete in noile echipamente care se numesc switch-uri

Criptor Ethernet

Numim criptor Ethernet un criptor ale carui porturi rosii si negre se conecteaza la doua retele Ethernet una rosie, iar cealalta neagra. Managementul cheilor pentru criptoarele Ethernet ar trebui sa se faca a) fizic prin introducerea unui suport fizic de informatie ce contine cheia (gen flash-uri de memorie); b) logic, via o sesiune TELNET/SSH sau HTTP. Practic, un criptor Ethernet ar trebui sa fie un echipament gen switch, cu ajutorul caruia interconectarea unei retele rosii cu una neagra s-ar face relativ fara probleme

Material si metoda

- Bridge-uri
- Tunele
- Tuneluri TAP/TUN
- Implementarea unui criptor Ethernet

Bridge-uri

Crearea de bridge-uri in Linux se face via comanda brctl. Evident, pe un sistem putem avea mai multe bridge-uri active, diverse interfete putand fi membre intr-unul sau mai multe bridge-uri. O secventa de creare a unui bridge **br0** din interfetele **eth0**, **eth2** si **eth3** ar fi:

- # echo creare interfata bridge
- # brctl addbr br0
- # echo adaugare interfete in bridge, una cate una
- # brctl addif br0 eth0
- # brctl addif br0 eth2
- # brctl addif br0 eth3
- # echo adaugare ip pe interfata bridge (nu e obligatoriu!)
- # ifconfig br0 192.168.10.1 netmask 255.255.255.0

Tunele (Tuneluri)

Tunelele sunt mecanisme prin intermediul carora se ridica o interfata virtuala intre doua routere interconectate direct sau indirect si care pot comunica pe baza de IP. Unul din primele tunele care au aparut si s-au dezvoltat datorita promovarii de catre Cisco au fost tunelele GRE. Aceste tunele incapsuleaza un pachet de date initial intr-un alt pachet de date de tip 47/GRE

Tunele TAP/TUN

O clasa aparte de tunele sunt tunelele de tip TAP/TUN. Una din calitatile acestor tunele este ca din momentul ridicarii interfetei de tunel, aceasta se comporta ca o interfata Ethernet, pachetele transmise pe aceasta interfata fiind practic pachete Ethernet. Cea mai cunoscuta comanda pentru ridicarea de astfel de tuneluri este **openvpn.** Astfel, pentru a ridica un tunel intre masinile A si B vom folosi seturi de comenzi ca

- RouterA# ifconfig tap0 down
- RouterA# openvpn --daemon --local 80.97.70.39 --remote 86.104.30.254 --port 5009 --dev tap0 --comp-lzo
- RouterA# ifconfig tap0 86.104.31.30 netmask 255.255.255.240
- RouterB# ifconfig tap0 down
- RouterB# openvpn --daemon --local 86.104.30.254 --remote 80.97.70.39 --port 5009 --dev tap0 --comp-lzo
- RouterB# ifconfig tap0 86.104.31.17 netmask 255.255.255.240

Implementarea unui criptor Ethernet

Din cele expuse, rezulta ca cel mai simplu mod de implementare a unui criptor Ethernet folosind un sistem Linux este ridicarea unei interfete de tip tunel TAP criptate. Folosirea unui tunel TAP criptat ne asigura posibilitatea folosirii unui canal de comunicatii sigur, chiar si peste un mediu de transmisie negru. Evident, pentru a transparentiza echipamentul care ne ofera functiile de criptare este necesar in a pune in bridge interfata rosie a echipamentului nostru cu tunelul criptat. Astfel, un sistem Linux ce are 2 interfete Ethernet, una rosie si una neagra (pentru transportul tunelului) devine un criptor Ethernet in timp real.

Implementarea unui criptor Ethernet (continuare)

Managementul cheilor unui astfel de tunel se face via o interfata HTTP bazata pe un server web (APACHE sau altul). Deoarece cheia in sine este o informatie rosie, managementul cheilor se poate face doar pe interfata rosie a echipamentului care va avea un IP ce poate fi de asemenea setat de catre administrator sau de catre custodele criptografic. Deoarece tunelul ridicat intre doua criptoare Ethernet are nevoie de IP pe interfata neagra, managementul acestui IP se poate face via aceeasi interfata de catre administrator sau custodele criptografic. De asemenea, exista posibilitatea de a face setari tehnice cu privire la structura tunelului, cum ar fi: tipul transportului (TCP/UDP), numarul portului de transport, existenta compresie LZO etc. Toate aceste date se pot seta la nivelul aceleasi interfete de catre administrator sau custodele criptografic.

Rezultate, discutii

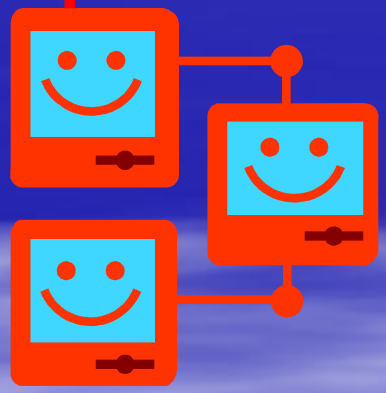
- Testarea
- Aplicatii civile
- Aplicatii militare
- Multumiri si concluzii

Testarea

Am folosit criptoarele Ethernet pentru a interconecta 2 sedii ale unui client metropolitan al firmei InfoData Telecom din Cluj. Deoarece se traversa o zona neagra, informatia rosie (din punctul de vedere al respectivului client) trebuia criptata.

Testarea

Criptor



Sediu A client

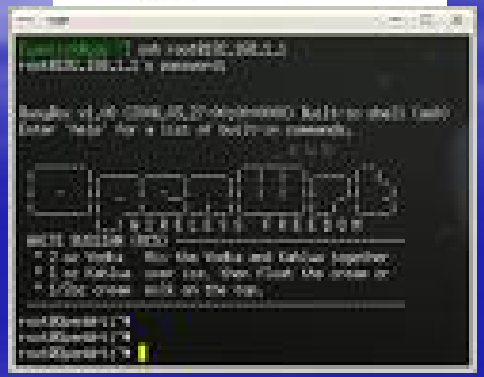
Retea transport

Criptor

Sediu B client

Implementarea

Implementarea s-a facut pe P2-uri cu Linux Slackware si pe echipamente Cisco Linksys WRT 54GL cu Linux OpenWRT.

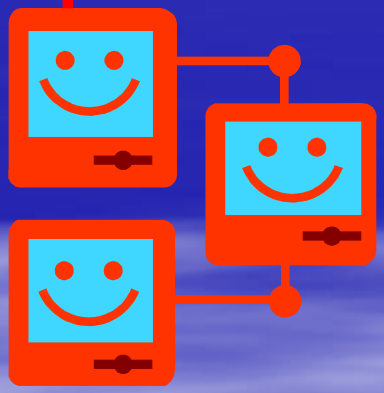


Aplicatii civile

Astfel de criptoare pot fi folosite de firme ce isi inchiriaza birouri in parcuri tehnologice, fiind cunoscut ca numarul de birouri folosite creste o data cu dezvoltarea afacerii in incubator. Presupunand ca parcul tehnologic, ca si gazda, ofera la nivel logistic posibilitatea interconectarii birourilor afacerii incubate printr-o legatura neagra (deoarece nu exista nici un fel de control asupra modalitatii de implementare a interconectarii, chiar daca de obicei este vorba de VLAN-uri), folosirea de criptoare Ethernet in fiecare birou este o solutie.

Aplicatii civile

Criptor



Incaperea #1 a clientului

Retea transport gazda

Criptor

Incaperea #2 a clientului

Aplicatii militare

Alte aplicatii ale criptoarelor Ethernet pot fi gandite in domeniul militar, unde se presupune ca in cadrul cazarmii avem zone de securitate (rosii) ce trebuie interconectate prin traversarea unor zone administrative (negre). Din nou, folosirea de criptoare Ethernet este o potentiala solutie.

Aplicatii militare

Criptor Ethernet

Criptor Ethernet

MC/WDM – fibra – MC/WDM

Zona de securitate

Zona de securitate

Multumiri si concluzii

Multumim Grupului de firme InfoData pentru suportul acordat in implementarea prototipului de criptor Ethernet: firma InfoData ne-a oferit echipamentele pe care s-a facut dezvoltarea, iar firma InfoData Telecom ne-a oferit posibilitatea testarii criptorului Ethernet intr-un mediu real, prin oferirea accesului la reteua de date metropolitane.

Multumiri si concluzii

- http://www.infodatagrup.ro

INFODATA

Intelligent IT Platforms

Multumiri si concluzii

De asemenea multumim tuturor celor care ne-au ajutat sau ne-au sustinut in realizarea acestui proiect. Consideram ca finalizarea acestui proiect este un real succes ce demonstreaza ca lumea FLOSS poate fi folosita fara probleme in zona INFOSEC, fiind o alternativa ieftina si sigura.

Incheiere

Va multumesc pentru rabdarea cu care m-ati urmarit.

INTREBARI? cu si fara raspuns ;)