İSTANBUL TEKNİK ÜNİVERSİTESİ ★ FEN BİLİMLERİ ENSTİTÜSÜ

YÜKSEK BAŞARIMLI YAZILIM TABANLI IPSEC GÜVENLİK GEÇİDİ TASARIMI

YÜKSEK LİSANS TEZİ

Müh. Ural ERDEMİR

Anabilim Dalı: Bilgisayar Mühendisliği

Programı: Bilgisayar Mühendisliği

Tez Danışmanı: Yrd. Doç. Dr. Feza BUZLUCA

MAYIS 2006

ÖNSÖZ

Tez çalışmalarım süresince göstermiş olduğu anlayış ve yardımlardan dolayı tez danışmanım sayın Yrd. Doç. Dr. Feza Buzluca' ya, katkılarından dolayı çalışma arkadaşım Umut Tekin' e, Hayatımın her anında olduğu gibi tez çalışmalarım boyunca da benden yardımlarını esirgemeyen aileme sevgi ve saygılarımı sunarım.

Mayıs 2006 Ural ERDEMİR

İÇİNDEKİLER

Sayfa No

KISALTMALAR

AES	: Advanced Encryption Standard
AH	: Authentication Header
ARP	: Address Resolution Protocol
CBC	: Cipher Block Chaining
CIDR	: Classless Inter-Domain Routing
CRC	: Cyclic Redundancy Check
CSMA / CD	: Carrier Sense Multiple Access with Collision Detection
DUT	: Device Under Test
ESP	: Encapsulating Security Payload
HMAC	: Keyed-Hashing for Message Authentication Code
Gbps	: Gigabits per second
GoF	: Gang of Four, Gamma E., Helm R., Johnson R., Vlissides J.
GRASP	: General Responsibility Assignment Software Patterns
ICMP	: Internet Control Message Protocol
ICV	: Integrity Check Value
IETF	: Internet Engineering Task Force
IP	: Internet Protocol
IPSec	: IP Security, Security Architecture for the Internet Protocol
IPv6/IPng	: IP version 6/ IP Next Generation
ISAKMP	: Internet Security Association and Key Management Protocol
IV	: Initialization Vector
MAC	: Message Authentication Code
Mbps	: Megabits per second
MD5	: Message Digest 5
NAT	: Network Address Translation
NIST	: National Institute of Standards and Technology
PPS/PBS	: Packet per second / paket bölü saniye
RED	: Random Early Detection
QoS	: Quality of Service
RFC	: Request For Comment
RSA	: Rivest-Shamir-Adleman Güvenlik Firması
SA	: Security Association
SAD	: Security Association Database
SHA1	: Secure Hash Algorithm
SPD	: Security Policy Database
SPI	: Security Parameter Index
TCP/IP	: Transmission Control Protocol / Internet Protocol
TCAM	: Ternary Content Addressable Memory
TFC	: Traffic Flow Confidentiality
TTL	: Time to Live
UP	:Unified Process
VPN	: Virtual Private Network, Sanal Özel Ağ

TABLOLAR

Sayfa No

ŞEKİLLER

Sayfa No

YÜKSEK BAŞARIMLI YAZILIM TABANLI IPSEC GÜVENLİK GEÇİDİ

ÖZET

Veri haberleşmesinde güvenlik konusu günümüzde üzerine en çok araştırma yapılan konulardan biri haline gelmiştir. Özellikle kaynak ve zaman paylaşımının yapıldığı bilgisayar ağları gibi sistemlerde, verilerin korunması ve saldırıların önlenmesi için bir çok yöntem tasarlanmıştır. Tasarlanan yöntemler temelde verinin iletimi esnasında korumasını esas almaktadır. Bugün bilgisayar ağlarında kullanılan temel iletişim protokolü IP protokolüdür ve IPSec, ağ katmanında IP protokolü için tasarlanmış yaygın kullanımlı standart güvenlik mimarisidir.

IP (IPv4) ile birlikte isteğe bağlı olarak genellikle kurumsal bazda şıkça kullanılan IPSec' in yeni nesil IP (IPv6 ya da IPng) protokolüyle birlikte kullanımı zorunlu hale getirilmiştir. Artan güvenlik gereksinimleri ve IPv6'nın yaygınlaşmasıyla beraber IPSec' in kullanımı dünya genelinde daha da artacağı düşünülmektedir. IPSec' in bu şekilde artan kullanımı sonucunda IPSec yapan güvenlik geçitlerinin başarımları konusunda bugün için düşünülmeyen yeni problemler ve araştırma konuları ortaya çıkacaktır. IPSec güvenlik politikası veritabanlarının, kullanıcı sayısı ile doğru orantılı olarak büyümesi, güvenlik politikası veritabanlarında kararlar ile paketlerin eşleşmesini zorlaştırarak, IPSec başarımında ciddi bir dar boğaz oluşturacaktır.

Bu konuda ortaya çıkan problemler için çeşitli çözümler düşünülse bile günümüz ağ cihazlarının statik ve değişime açık olmayan tasarımları bu çözümlerin gerçekleştirilmesini zorlaştırmakta hatta çoğu zaman imkansız hale getirmektedir. Ağ cihazlarının mimarilerinin donanım tabanlı olması bunun olmasının en büyük sebebidir. Ancak gelişen teknoloji sayesinde bugün işlemci hızları çok yüksek mertebelere ulaşmış ve bu gibi sistemlerin yazılım tabanlı olarak da yüksek başarımlı bir biçimde yapılabilmesine imkan vermiştir.

Bu tez çalışması kapsamında öncelikle yüksek başarımlı ve yazılım tabanlı IPSec' yapan bir güvenlik geçidi tasarlanıp gerçeklenmiştir. Tasarım nesneye dayalı bir biçimde, modülerlik ve esneklik ön planda tutularak yapılmıştır. Gerçeklenen modüler ve esnek yapı sayesinde yeni fikirlerin kısa sürede gerçeklenip sonuçlarının alınabileceği örnekler ile gösterilmiştir. IPSec' protokolünde güvenlik politikası veritabanının boyutlarının büyümesinin cihaz başarımına etkileri test sonuçları gösterilmiş. Bu problem için çeşitli çözümler önerilmiş ve test sonuçlarıyla bu çözüm önerilerin sonuçları ortaya konmuştur. Bu çalışma sonucunda karar tablosunun boyutundan çok az etkilenen yüksek başarımlı ve yazılım tabanlı modüler bir güvenlik geçidi gerçeklenmiştir. Normal bir PC donanımı üzerinde yapılan testler sonucunda 16.000 kural sayısında bile 700.000 pps gibi çok yüksek bir başarım elde edilmiştir.

HIGH PERFORMANCE SOFTWARE BASED IPSEC SECURITY GATEWAY

SUMMARY

Nowadays, security has become one of the most interesting research issues in data communication, especially in computer networks where resource and time sharing is very common. There exist many standard systems designed for protection of data and preventing attacks. They are based on protection of data at the time of transmission.

Today IP is the most popular protocol of the computer networks. Because security is not inherently built into the protocols of IP, securing IP traffic has largely been a chore for the higher layers. IPSec provides security services at the network layer. It is commonly used to refer to the secure IP packets of the AH and ESP protocols, because these provide the major security services. IPSec design is a framework for multiple services, algorithms and granularities The security services that IPSec provides can include access control, authentication (through data origin authentication and connectionless integrity), packet anti-replay protection, confidentiality through encryption, and limited traffic flow confidentiality. The new IPSec standards (IPSec version 3) defined by IETF, in December 2005.

After its proven success in IPv4 and by making IPSec a mandatory part of IPv6, it is expected that IPSec will be much more widely used. On the other hand, the bandwidth requirement and number of nodes in network is growing exponentially, these will bring up new problems and research issues. With increasing number of rules in the security policy databases, packet classification will be one of the significant performance bottlenecks for IPSec security gateways. Another important topic for security devices is the reliability of the cryptographic algorithms and protocols they use. A reliable algorithm for today can be broken and become unreliable in the near future. In these cases, there will be a need for adapting new algorithms and protocols in a short critic time interval.

Even there exist some suggestions for such problems; because of their closed, static, and inflexible designs applying them in today's network devices is very difficult and mostly impossible especially for hardware based network processors.

In this thesis, we designed a high performance, its object oriented software based IPSec security gateway. The most significant features of our design are its modularity, extensibility and flexibility. It is shown that, new ideas can be integrated easily with these features. Also in this study, a new scheme for IPSec policy search presented and its performance measured

Designed software runs in the Linux kernel and for a size of 16,000-rules security policy database, its maximum IPSec forwarding rate is 700,000 64-byte packets per second on a conventional PC hardware.

1 GİRİŞ

İçinde bulunduğumuz bilgi çağının temel gerekleri bilgiye ulaşım, bilginin paylaşımı ve etkin kullanımıdır. Dünyayı kuşatan telefon ağlarının kurulması, radyo ve televizyonun icadı, bilgisayar endüstrisinin doğuşu ve benzersiz büyümesi, iletişim uydularının fırlatılması bu çağın en önemli gelişmeleri olarak sıralanabilir. Teknolojinin gelişmesi ile artan, bilgiye hızlı ve kolay ulaşma ihtiyacı, Internet'i geçtiğimiz yüzyılın en önemli buluşlarından biri yapmıştır. Internet en genel anlamda birbirine bağlı bilgisayarların oluşturduğu ağların ağı olarak tanımlanabilir.

60'lı yılların sonunda, askeri bir araştırma projesi olarak ortaya çıkan Internet, o yıllardaki klasik devre anahtarlamalı telefon ağlarından farklı paket anahtarlamalı çalışacak şekilde tasarlanmıştı ve asıl amacı birbirine bağlı ağlar üzerinden, bu ağlardan bir kısmı çalışmasa bile bağımsız olarak haberleşmeyi sürdürebilmekti.

Internet'i kısa zamanda bu denli popüler yapan, milyonlarca insana fikirlerini, bilgilerini, çalışmalarını paylaşacak bir ortam sağlaması. ve çıkış felsefesinde yatan açık mimari, baskın bir kontrol merkezinin olmaması , herkese kolayca erişim imkanı sunma düşünceleridir[1]. 90'lı yıllarda büyük ticari şirketlerin ve akademik çevrenin Internet altyapısını toplu iletişim aracı olarak kullanmaya başlaması ve WWW' in gelişmesi IP'nin yaygınlaşmasını hızlandırmıştır.

Internet ağlarını, bir arada tutan temel yapı taşı Internet'in ağ katmanı protokolü IP[1]'dir. IP 20 yıl öncesinin ihtiyaçlarına göre tasarlanmış bir protokoldür. O yıllarda bilgisayar ağları üniversite araştırmacıları arasında elektronik posta yollama, dosya paylaşımı, haber gruplarına erişme, yazıcı paylaşma gibi uygulamalarda kullanılıyordu ve bu tür uygulamalarda öncelikli konu iletişim güvenliği değildi. Ancak 90'lı yıllardan sonra Internet'in milyonlarca kişinin bankacılık işlemlerini yaptığı, elektronik ticaret vb. parasal uygulamalarda, şirketlerin ve kurumların özel verilerini taşıyan kritik uygulamalarda kullanılmaya başlamasıyla iletişim güvenliği önemli bir boşluk olarak ortaya çıkmıştır.

[1] Tez kitapçığında IP, Internet Protokol versiyon 4'ün kısaltması olarak kullanılmaktadır. Internet Protokol versiyon 6, IPv6 olarak ayrıca vurgulanmaktadır.

Internet'in özel sektörde yaygınlaşması ile beraber çıkan diğer bir konu da iç ağ ve dış ağ kavramlarıdır. İç ağ belli bir kurumun Internet ağ teknolojilerini (TCP/IP) kullanarak oluşturduğu kurum içi özel iletişim ağıdır. Dış ağ, kurumların iç ağlarını oluştururken, coğrafi olarak birbirinden uzakta bulunan şube veya ofislerini, Internet gibi herkese açık bir iletişim ortamı üzerinden bağlamalarıyla oluşan özel ağdır. Böyle bir ağda kuruma ait özel bilgiler herkese açık bir ortamdan geçirileceği için iletişim güvenliğinin sağlanması şarttır. Bu amaçla oluşturulan Sanal Özel Ağlar (VPN) kişilere ya da kurumlara ait özel bilgilerin Internet gibi herkese açık ağlar üzerinden güvenli bir şekilde iletilmesini sağlar. Sanal özel ağlar ile sadece güvenilir ve yetkilendirilmiş sistemlerin hassas ve önemli verilere ulaşması sağlanabilir. Geleneksel ortamda kurumlar, kiralık hatlar ya da farklı ortamlar ile Internet'e açık olmayan iletişim hatlarını kullanarak güvenli haberleşmeyi sağlayabilirler. Ancak bu yöntem hem ekonomik hem de esnek olmamaktadır.

IPSec, IETF tarafından tanımlanmış Internet Protokolü güvenlik standardıdır. IPSec mimarisi ile kendi içinde güvenli ağlar, güvensiz ağlar üzerinden haberleştirilerek sanal özel ağlar oluşturulabilir. Bu tip VPN uygulamasında temelde biri kullanıcı-güvenlik geçidi ve diğeri güvenlik geçidi-güvenlik geçidi olarak adlandırılan iki tür bağlantı türü yapılabilir. Bu yapıda güvenilmeyen ağdan geçen paketler IPSec güvenlik geçidi tarafından şifrelenmesine ve diğer uçtaki güvenlik geçidinde karşı ucun kimlik kontrolü yapılıp, paketin şifresi çözülmesi dayanır. Böylece iki uç arasında dışarıya mantıksal olarak kapalı bir tünel bağlantısı oluşturulur.

Bilgisayar ağlarındaki düğüm sayısı ve band genişliği ihtiyacı üstel bir şekilde artarken, güvenlik tehditleri de artmakta ve iletim güvenliği firmalar için kaçınılmaz olmaktadır. Güvenli iletişim elbette, iletişim alt yapısı üzerinde bazı ek maliyetler de getirmektedir. Bu maliyetler başta güvenlik yönetimi işlemleri ve ağ başarımında azalmadır.

Son zamanlarda IPSec' in sanal özel ağ uygulamalarında yaygınlaşması ile IPSec güvenlik geçidi tasarımı önemli bir konu haline gelmiştir. Kullanıcılar IPSec güvenlik geçidi ürünlerinden, kolay yönetilebilirlik, ucuzluk, yüksek başarım beklerken, üretici firmalar rekabet edebilmek için bu isteklere ek olarak, hızlı ürün çıkarabilme, modüler yapılar ile tekrar kullanılabilirlik, güncelleme hata ve bakım maliyetinin azlığını istemektedir. Donanım tabanlı sistemler yüksek başarım vermelerinin yanında, yazılım tabanlı sistemlere kıyasla maliyetleri oldukça

yüksektir. Günümüzde genel amaçlı işlemcilerin başarımı giderek artmakta ve zamanla daha yüksek başarımlı işlemciler ucuza alınabilmektedir.

Güvenlik gibi kritik uygulamalarda güncelleme oldukça önemli bir konudur. Dün güvenli olan bir algoritma ya da sistem bugün güvenliliğini yitirmiş olabilir, örneğin MD5[2] ve SHA1[3] algoritmalarında zayıflıklar bulunması[4,5] bu algoritmaları kullanan güvenlik geçitlerinin, dolayısıyla haberleşme bağlantılarının güvenliğini azaltmıştır. Kritik tasarım hataları da güvenlik sistemi üzerinde güncellemeler gerektirebilir. Yazılım tabanlı sistemlerde bu tip sorunlar basit bir yazılım güncellemesi ile çözülebilecekken donanım tabanlı sistemlerde durum her zaman bu kadar kolay olmamaktadır. Hata durumlarında güncellemenin bu denli yüksek olması donanım tabanlı sistemlerin test süreçlerinin de daha uzun sürmesini gerektirmekte ve toplam maliyeti arttırmaktadır.

Bu tez çalışmasında yeni standartlarla tanımlı IPSec (versiyon 3)[6] mimarisi incelenmiş ve yazılım tabanlı yüksek başarımlı bir IPSec güvenlik geçidi tasarlanmaya çalışılmıştır. Yazılım tabanlı sistemlerin en büyük zayıf noktası olan başarım dar boğazları incelenmiş ve başarımı arttıracak çalışmalarla sistemin limitleri belirlenmeye çalışılmıştır.

Tez kitapçığında öncelikle IPSec güvenlik mimarisi hakkında kısaca bilgi verilmiştir. Üçüncü bölümde tasarlanan sistemin mimarisinde büyük etkisi olan Click yönlendirici yazılım mimarisi tanıtılmıştır. Dördüncü bölümde esnek, modüler, hata bağışıklığı yüksek hedef sistemin nesneye dayalı modellenmesi ve tasarımı anlatılmıştır. Beşinci bölümde yazılım tabanlı IPSec güvenlik geçidi başarımında ciddi bir dar boğaz oluşturan Güvenlik Politika Veritabanlarında paket eşleşmesi için çok boyutlu paket sınıflandırma problemi ve önerilen çözümler anlatılmıştır. İzleyen bölümde tasarlanan sistem üzerinde yapılan önemli iyileştirmelerden bahsedilmiştir. Son olarak yapılan iyileştirmelerin tasarlanan sistemin başarımına etkileri ölçülmüş ve sonuçlar tartışılmıştır.