SIP GÜVENLİĞİ VE BİR UYGULAMA

Ali Yavuz ÇAKIR

Yüksek Lisans Tezi

Fen Bilimleri Enstitüsü
Bilgisayar Mühendisliği Anabilim Dalı

Temmuz 2004

JÜRİ VE ENSTİTÜ ONAYI

Ali Yavuz Çakır'ın **SIP Güvenliği ve Bir Uygulama** başlıklı **Bilgisayar Mühendisliği** Anabilim Dalındaki Yüksek Lisans tezi 16.08.2004 tarihinde, aşağıdaki jüri tarafından Anadolu Üniversitesi Lisansüstü Eğitim-Öğretim ve Sınav Yönetmeliğinin ilgili maddeleri uyarınca değerlendirilerek kabul edilmiştir.

	Adı-Soyadı	İmza
Üye (Tez Danışmanı)	**:Prof.Dr. Ali GÜNEŞ**	
Üye	**:Yard.Doç.Dr.Cüneyt AKINLAR**	
Üye	**:Doç.Dr. Ömer N. GEREK**	

Anadolu Üniversitesi Fen Bilimleri Enstitüsü Yönetim Kurulu'nun 08.09.2004 **tarih ve** ..29/20. **sayılı kararıyla onaylanmıştır.**

Enstitü Müdürü

Prof. Dr. Altuğ İFTAR
Fen Bilimleri Enstitüsü
Müdürü

ÖZET

Yüksek Lisans Tezi

SIP GÜVENLİĞİ VE BİR UYGULAMA

ALİ YAVUZ ÇAKIR

Anadolu Üniversitesi
Fen Bilimleri Enstitüsü
Bilgisayar Mühendisliği Anabilim Dalı

Danışman: Prof.Dr.Ali GÜNEŞ
2004, 82 sayfa

Bu tezde Akıllı Evler ve Ağa Bağlı Aygıtların güvenli bir şekilde kontrol ve kumandası için Session Initiation Protocol'ün kullanılması ele alınmıştır. Akıllı Evler ve Ağa Bağlı Aygıtlar'ın uzaktan kontrol ve kumandasında ortaya çıkacak güvenlik gereksinimleri belirlenmiş ve bu gereksinimleri sağlayabilmek için kullanılabilecek yöntemler sıralanmıştır. Daha sonra ise söz konusu gereksinimlerin Session Initiation Protocol kullanılarak nasıl sağlanabileceği tartışılmıştır. Bu protokolün halihazırda sunduğu güvenlik hizmetleri ele alınmış, bu hizmetlerin Akıllı Evler ve Ağa Bağlı Aygıtların uzaktan kontrol ve kumandası için kullanılması öngörülmüştür. Ayrıca bazı durumlarda sunulan hizmetlerin belli oranda değiştirilerek kullanılabileceği ve bazı durumlarda da hizmetlerin diğer katmanlardaki protokollerden alınabileceği düşünülmüştür. Geliştirilen uygulama ile güvenlik hizmetlerinden kimlik denetiminin nasıl sağlanabileceği gösterilmiştir. Yapılan incelemeler sonucunda Session Initiation Protocol'un güvenlik hizmet ve yöntemlerinin Akıllı Evler ve Ağa Bağlı Aygıtların uzaktan kontrol ve kumandasında kullanılması uygun bulunmuştur.

Anahtar Kelimeler: Akıllı Ev, Ağa Bağlı Aygıtlar, Ağ Güvenliği, SIP , HTTP Digest

ABSTRACT

Master of Science Thesis

SIP SECURITY AND AN APPLICATION

ALİ YAVUZ ÇAKIR

Anadolu University
Graduate School of Natural and Applied Sciences
Computer Engineering Program

Supervisor: Prof.Dr.Ali GÜNEŞ
2004, 82 pages

In this thesis, using SIP for securely controlling and commanding the Intelligent Houses and Networked Appliances is considered. Security requirements which occur when controlling and commanding the Intelligent Houses and Networked Appliances from remote locations are identified and the methods for fulfilling these requirements are listed. Next satisfying these requirements with the security services of SIP is discussed. The security procedures already involved in the protocol are taken into account and the usage of these procedures in remote control and command of Intelligent Houses and Networked Appliances is modeled. And in some circumstances, modifying these procedures and taking some security services from the lower layers are found to be suitable. The developed application showed how authentication can be done. After examinations, it is concluded that using security services of SIP for remote control and command of Intelligent Houses and Networked Appliances is suitable.

Keywords: Intelligent Houses, Networked Appliances, Network Security, SIP, HTTP Digest

TEŞEKKÜR

Bu tezin hazırlanmasında danışmanım olarak bana yol gösteren Anadolu Üniversitesi'nden Sayın Prof. Dr. Ali GÜNEŞ'e, konu üzerinde sahip olduğu tecrübeyi benimle paylaşan ve tavsiyeleriyle beni yönlendiren Anadolu Üniversitesi'nden Sayın Yrd. Doç. Dr. Cüneyt AKINLAR'a, desteklerini esirgemeyen Sayın Arş. Gör. Mehmet TETİK'e, Sayın Arş. Gör. Sedat TELÇEKEN'e ve Sayın Arş. Gör. Muzaffer DOĞAN'a ve her türlü çalışmamda bana destek olan aileme teşekkür ederim.

Ali Yavuz ÇAKIR
aliyavuz@anadolu.edu.tr

İÇİNDEKİLER

ŞEKİLLER DİZİNİ

ÇİZELGELER DİZİNİ

KISALTMALAR DİZİNİ

ABA	Ağa Bağlı Aygıt
AES	Advanced Encryption Standard
AKB	Aygıt Kontrol Birimi
ATM	Asynchronous Transfer Mode
CRLF	Carriege Return – Line Feed
DDP	Device Description Protocol
DES	Data Encryption Standard
DMP	Device Management Protocol
DNS	Domain Name System
DOS	Denial Of Service
HTTP	Hypertext Transfer Protocol
IETF	Internet Engineering Task Force
IPSec	Secure Internet Protocol
IPX	Internetwork Packet Exchange Protocol
MIME	Multiourpose Internet Mail Extensions
NAT	Network Address Translation
RFC	Request For Comment
RGW	Residential Gateway
RSA	Rivest Shamir Adleman
RTP	Realtime Transport Protocol
SDP	Session Description Protocol
SIP	Session Initiation Protocol
SLP	Service Location Protocol
SMTP	Simple Mail Transfer Protocol
SSH	Secure Shell
TCP	Transport Control Protocol
TLS	Transport Layer Security
UA	User Agent
UAC	User Agent Client
UAS	User Agent Server

UDP	User Datagram Protocol
UPnP	Universal Plag And Play
URI	Uniform Resource Identifier
URL	Uniform Resource Locator

1. GİRİŞ

Teknolojinin ilerlemesi ile birlikte Internet kavramı hayatımızın birçok alanına girdi ve günlük işlerimizin önemli bir kısmını Internet üzerinden yapabilir hale geldik. Buradan yola çıkarsak, Internet'in hayatımızdaki yerinin gittikçe daha da artacağı ve kullanımının yaygınlaşacağı açıktır. Bu yaygınlaşmanın bir sonucu olarak da Internet'in geleceğinin Ağa Bağlı Aygıtlar üzerinde bir yoğunlaşmaya gideceği beklenebilir. Bu sayede kullandığımız aygıtların uzaktan(tipik olarak Internet üzerinden) kontrol edilmesi ve yönetilmesi sağlanabilecektir. Biraz incelemeyle görülebilir ki, buzdolabı, fırın, kahve makinesi gibi akıllı mutfak cihazları; ağa bağlanabilen kameralar, yangın ve hırsız alarmı gibi güvenlik cihazları; TV, VCR, CD çalıcı gibi eğlence cihazları; ve bilgisayar, yazıcı, disk gibi ofis cihazlarının bir akıllı ev ağına bağlanmasının kullanıcıya birçok yeni olanak vereceği açıktır.

Tasarlanabilecek birçok uygulama arasında akla gelebilecek ve yapılması mümkün bazı uygulamalar şöyle sıralanabilir;

- Uzaktan kumanda edilebilen kameralarla sürekli evi gözetleyen ve herhangi bir hareket yakaladığında bunu güvenlik birimlerine bildiren bir güvenlik-alarm sistemi. Evdeki güvenlik sisteminin vereceği olası bir alarmın gerçek olup olmadığını anlamak için, güvenlik merkezinden evdeki kameralarla bağlantı kurularak kameralardan görüntü alınması ve bu şekilde olayın kesin değerlendirmesinin yapılabilmesi sağlanabilir.
- Ağa bağlanacak yangın algılayıcıları, bir yangın merkezini olası bir yangından haberdar edip kısa zamanda yangın ile mücadele birimlerinin olay yerine gelmelerini sağlayabilir.
- İçerisindeki malzeme listesini tutabilen, gerektiğinde sipariş verebilen veya kullanıcısına bir liste sunabilen buzdolabı çok kullanışlı olabilir. Ya da bozulan bir çamaşır makinesinin, kendi sistem kontrolleri sonucu elde ettiği arıza raporunu yetkili servise bildirip servis çağırması, kullanıcıyı hizmetten mahrum kalmaktan kurtaracaktır.

- Ev yönetim sistemleri: Buna örnek olarak da kullanıcının tatildeyken evinin bahçesindeki çimleri veya ev bitkilerini uzaktan kumanda ederek sulayabilmesini sağlayan sistem gösterilebilir.
- Uzaktan evi kontrol etme sistemi: Okuldan dönecek çocuğunun eve gelişini işyerindeki anneye bildiren ve gerekirse görüntülü olarak durumu anneye gösteren bir sistem hayal edilebilir.
- Hava, yol vs. gibi koşulları çeşitli kaynaklardan öğrenerek işe gitmek için kalkmanız gereken saati hesaplayarak alarm veren bir çalar saat oldukça faydalı olabilecektir.

Burada rahatça görülebiliyor ki bu aygıtların sözü edilen işlevleri yerine getirebilmeleri için belli bir işlem gücüne ve iletişim yeteneklerine sahip olmaları gereklidir. Örneğin sabah sizi uyandıracağı saatte odanın ışıklarını açan bir çalar saat, bu işlemi yerine getirmek için oda ışıklarıyla bir iletişim yapmak zorunda olacaktır. Ya da ev yönetim sisteminizi tatildeyken uzaktan kullanabilmek için evinizle bir iletişim kurmanız gerekecektir.

Bu tez yukarıda kısaca bahsedilen iletişimin yapılabilmesi için gerekli standartlaşmayı ele alacak, SIP[1] mimarisinin bu istekleri nasıl karşılayabileceğini ortaya koyacaktır. Bu tezde özellikle böyle bir mimari için gerekli olabilecek güvenlik gereksinimleri ve çözümleri ele alınacak, SIP mimarisinin bu konuda sunduğu çözümler ve bunların Ağa Bağlı Aygıtlar(ABA) ve Akıllı Evlerde uygulaması detaylı olarak incelenecektir. Bu inceleme yapılırken, standart SIP güvenlik yöntemleri detaylı olarak ele alınacak, bu yöntemlerin ABA kontrol ve kumandasında nasıl kullanılabileceği belirlenecektir. Bazı yöntemler direk olarak kullanılabilirken, bazıları küçük değişikliklerle kullanılabilecektir. Ayrıca bazı durumlarda diğer katmanlardan alınan hizmetler kullanılarak güvenliğin nasıl sağlamlaştırılabileceği tartışılacaktır.

ABA'lar genel olarak sınırlı işlem gücü bulunan, ağ bağlantısına sahip olan, belli bir işlevi yerine getirmek için tasarlanmış aygıtlardır. Bunlar algılayıcılara ve/veya işlevi yerine getirecek düzeneklere sahip olabilirler. Bunlara örnek olarak akıllı beyaz eşya türleri, çalar saatler, video cihazları, fırınlar, kameralar vs. ve bunların birleştirilmesiyle oluşturulan sistemler (örneğin ev güvenlik sistemi) verilebilir.

Bahsedilen akıllı aygıtların birbirine ve ağa bağlanmasıyla oluşacak ev ağında çözülmesi gereken bazı problemler ortaya çıkacaktır. Kısaca özetlenirse bu problemler ABA'ların nasıl isimlendirilip adresleneceği, ABA'ların özelliklerinin nasıl öğrenilebileceği, ABA'ların nasıl kumanda edilip programlanacağıdır.

ABA'ların isimlendirilmesi, adreslenmesi ve özelliklerinin keşfi için iki öneri göze çarpmaktadır. Bunlardan birisi Microsoft'un öncülüğündeki Universal Plug and Play[2] (uPnP) ortaklığı, diğeri ise IETF öncülüğünde geliştirilen Zero Configuration Networking[3]'dir. ABA'ların ev içerisinden veya uzaktan kumanda edilip programlanabilmesi için ise önde gelen öneri, Internet üzerinden telefon konuşmaları için tasarlanan Session Inititation Protocol (SIP) kullanımıdır. Telcordia'dan birkaç araştırmacı tarafından bazı eklemeler[4] ile kullanılması öngörülen SIP'in, ABA'ların kumandası için uygun özellikler taşıdığı açıkça görülmektedir.

Yukarıda bahsedilen sistemler göz önüne alındığında, ABA'ların SIP ile kumanda edilmesinde güvenlik kavramının büyük öneme sahip olduğu görülebilmektedir. Hiçbir kullanıcı kendi evindeki herhangi bir ABA'nın yetkisiz kişiler tarafından kontrol edilebilmesini istemez. Akıllı Evler'deki ABA'ların, ev sahibinin isteği dışındaki yetkisiz kullanıcılar tarafından erişilebilir ve yönetilebilir olması veya ev sahibinin istediği zaman kendi evine erişip kontrol ve kumanda edememesi bu tip sistemlerin ortaya çıkardığı faydaları ortadan kaldırabilir. Hatta ortaya çıkabilecek zararlar, bu tip sistemlerin kullanımının tercih edilmesini engelleyebilir. Bu tip durumlarda kullanıcıların son derece tatsız sonuçlarla karşılaşmaları söz konusu olabilir. Örneğin ısıtma sistemine yetkisiz bir kullanıcı tarafından verilen bir komut, evde yangın çıkması gibi çok tehlikeli sonuçlar oluşturabilir. Ya da evindeki bahçe sulama sistemini kapatmak isteyen, fakat bu sisteme herhangi bir saldırı nedeniyle erişemeyen ve de sisteme müdahale edemeyen kullanıcı evini su basmasını (eğer başka bir önlem alınmadıysa) engelleyemeyecektir.

Bu tezde ABA'ların geniş alan ağları (tipik olarak Internet) üzerinden kontrol edilebilmesini sağlayan SIP'in kullanım nedenleri, protokolün bu alanda nasıl kullanılabileceği ve bu protokolün sunduğu güvenlik yöntemleri ele

alınacaktır. Ayrıca bu protokolün ve sahip olduğu güvenlik yöntemlerinin ABA kontrolü için nasıl daha verimli kullanılabileceği de bu tezde tartışılacaktır.

1.1 Ağa Bağlı Aygıtlar

İnsanların hayatını kolaylaştırmak için yapılan çeşitli çalışmaların sonucu olarak teknoloji insan hayatının her alanına girmiştir. Günlük yaşantımızda teknoloji ürünü araç-gereçleri kullanmak son derece doğal bir davranıştır. Bu araç-gereçler, etrafımızdaki yaşam alanlarını daha kullanışlı hale getiren aydınlatma, ısıtma araç-gereçleri, günlük işlerimizi yerine getirmemizde bize yardımcı olan temizlik-mutfak-kişisel bakım araçları, yaptığımız hesaplama-ölçüm gibi işlerde bize yardımcı olabilen çeşitli araçlar, çeşitli eğlence araçları sayılabilir.

Teknolojinin hayatımıza eklediği diğer bir kolaylık da son derece geniş iletişim olanaklarıdır. Artık çoğu evde televizyon, radyo, telefon, Internet gibi iletişim olanakları bulunmaktadır. Bunlar sayesinde dünyanın herhangi bir noktasıyla iletişim yapmak olanaklı hale gelmiştir.

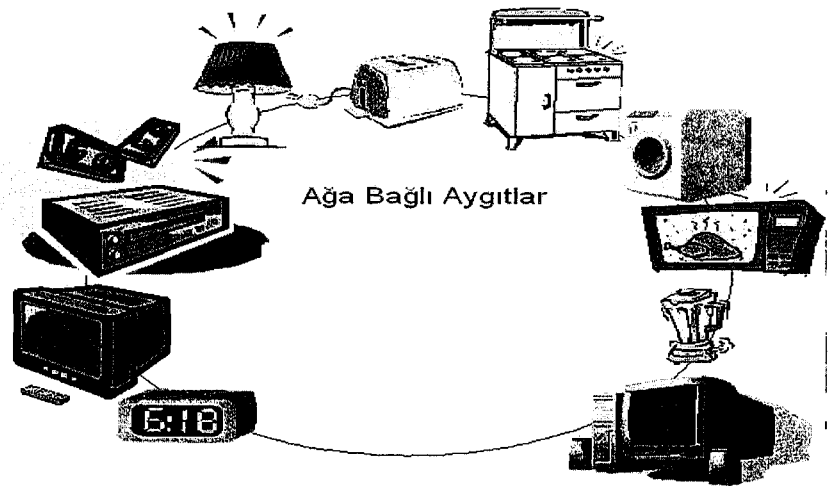
Yukarıda anlatılanlar göz önüne alındığında, teknolojinin bize sunduğu faydalı araç-gereçlerle iletişim kabiliyetlerini birleştirme fikri ortaya çıkmaktadır. Bu sayede iletişim yeteneği kazandırılan aygıtlar uzaktan kontrol ve kumanda edilebilir. Bu aygıtların birlikte kullanılması fikriyle ise akıllı evler kavramı ortaya çıkmaktadır[4].

Akıllı evler kavramıyla birlikte, bu evleri oluşturan ABA kavramı da ortaya çıkmaktadır(Şekil 1.1). Ağa Bağlı Aygıtlar(ABA) iletişim kabiliyetlerine ve belli bir seviyede işlem gücüne sahip aygıtlar şeklinde tanımlanabilir.

ABA'lara çeşitli örnekler verilebilir, aşağıda bunların bazıları ele alınmıştır.

Akıllı Beyaz eşya türleri: Bunlar genel olarak beyaz eşya olarak isimlendirilen ve çeşitli ağ yetenekleriyle belli bir işlem gücüne sahip aygıtlardır. Bu tür aygıtlara aşağıdaki örnekler verilebilir;

- Akıllı Buzdolabı: İçerisindeki malzemenin listesini tutabilen, gerektiğinde bu listeye ve kullanıcısının ihtiyaçlarına göre sipariş verebilen buzdolabı. Ayrıca içerisindeki malzemenin son kullanma tarihlerini kontrol ederek olası sorunları ortadan kaldırabilir.



Şekil 1-1 Ağa Bağlı Aygıtlar

- Öz sınama yeteneği olan beyaz eşya türleri: Çeşitli öz sınama yöntemleriyle kendi kendini kontrol edip, meydana gelen arızaları yakalayabilen aygıtlardır. Bunlar buldukları arızayla ilgili bilgileri saklayarak, olası bir müdahale gerektiğinde gerekli yetkili servislere durumu bildirebilirler. Bu sayede, belki aygıt tam olarak işlevini yitirmeden gerekli müdahale yapılabilecek, bu sayede kullanıcı hizmetten mahrum kalmayacaktır.
- Akıllı Çamaşır-Bulaşık Makinesi: Bu tip aygıtlar da uzaktan kumanda edilerek istenen saatte çalışmaları, işlemlerini gereken zamanda bitirmeleri sağlanabilir.
- Akıllı Fırın: Bu tip bir aygıtlarda zaten kullanılan programlanma özelliği, uzaktan programlanabilme ve kontrol edilebilme olanaklarına dönüştürülebilir. Bu sayede ev sahibi eve geldiğinde yemeğini fırın içerisinde pişmiş olarak bulabilir. Bu tip sistemlerin olası tehlikeleri de yine aygıtı uzaktan kontrol ederek bertaraf edilebilir.

Kişisel Eğlence Aygıtları: Bunlar da günlük hayatımızda kendisine yer açan çeşitli eğlence aygıtlarını kapsamaktadır.

- Video Kaydedici: Uzaktan programlanması mümkün olan aygıtlardır. Örneğin kullanıcı ofisinden, evindeki video kaydedicisini programlayarak istediği saatte istediği televizyon programını kaydedebilir.
- Televizyon: Televizyonunuzu istediğini program başladığında sizi uyaracak şekilde programlayabilirsiniz.

ABA Sistemleri: Bunlar da hayatımız kolaylaştırmak için birden fazla ABA'nın bir araya getirilmesiyle oluşturulmuş sistemlerdir. Aşağıda bu sistemlere çeşitli örnekler verilmiştir.

- Ev güvenlik sistemleri: Bu sistemler, evinizi belli algılayıcılar vasıtasıyla sürekli gözleyen ve olası güvenlik ihlallerini yakalayarak gerekli tepkileri veren sistemlerdir. Burada sözü edilen algılayıcılar kameralar, kapı-pencere alarm sistemleri vs. olabilir. Sistem evde herhangi bir hareket yakalandığında belli bir tepki verebilir, ev sahibine haber verebilir veya direk olarak güvenlik güçleri olaydan haberdar edebilir. Ayrıca verilen alarmın doğruluğunu teyit etmek için ev içerisindeki kameralarla bağlantı kurularak bunlardan görüntü alınabilir ve durum değerlendirmesi buna göre yapılabilir.
- Ev yönetim sistemleri: Ev sahibin evinde değilken bile evindeki bazı olayları yönetebilmesini sağlayan sistemlerdir. Örneğin seyahate çıkan birisi, evindeki rutin işleri uzaktan programlayarak yapabilir. Bu işler bahçe sulaması, evdeki bitkilerin sulanması, belli aralıklarla havalandırma sisteminin çalıştırılmasıyla evin havalandırılması vs. olabilir.
- Ev izleme sistemleri: Bu sistemler evin içindeki kameralar sayesinde izlenebilmesini sağlar. Örneğin çalışan bir anne, işyerindeki bilgisayarından evine bağlanarak çocuğunun eve gelişini kontrol edebilir. Benzer bir durum da, evde tamirat yapmak için gelecek servis elemanının, kapı zilini çaldığı zaman kapı üzerindeki kameralar vasıtasıyla izlenebildiği, beklenen kişi ise ev giriş kapısının uzaktan kumanda edilip açılmasıyla eve alınmasını sağlayan sistemdir. Yine ev içerisindeki kameralarla bu kişinin ev içerisinde ne yaptığı izlenebilecektir.
- Yangın alarm sistemleri: Evdeki yangın algılayıcıları sayesinde olası bir yangın durumunda ilgili yerlerin en kısa zamanda haberdar edilmesi

sağlanabilir. Ayrıca evin kameralarla izlenmesi sayesinde olayın gerçekliği ve nerede olduğu saptanabilir, evin kendi yangın söndürme sistemi uzaktan kumanda edilerek çalıştırılabilir. Bu sayede olaya müdahale zamanı çok kısalacak ve zarar minimuma inecektir.

Bu sayılanlara ek olarak aşağıdaki sistemler de sayılabilir, bunlar hem kendi başlarına aygıtlar ya da aygıtların birleşmesiyle oluşan sistemler olabilir;

- Akıllı iklimlendirme sistemleri: Eve geliş saatinize göre evinizin sıcaklığını istediğiniz seviyeye getirebilirsiniz.
- Akıllı çalar saat: Çeşitli kaynaklardan aldığı hava durumu, yol durumu gibi bilgileri değerlendirerek işe zamanında gitmeniz için hangi saatte kalkmanız gerektiğini hesaplayan ve bu saatte sizi uyandıran bir çalar saat.

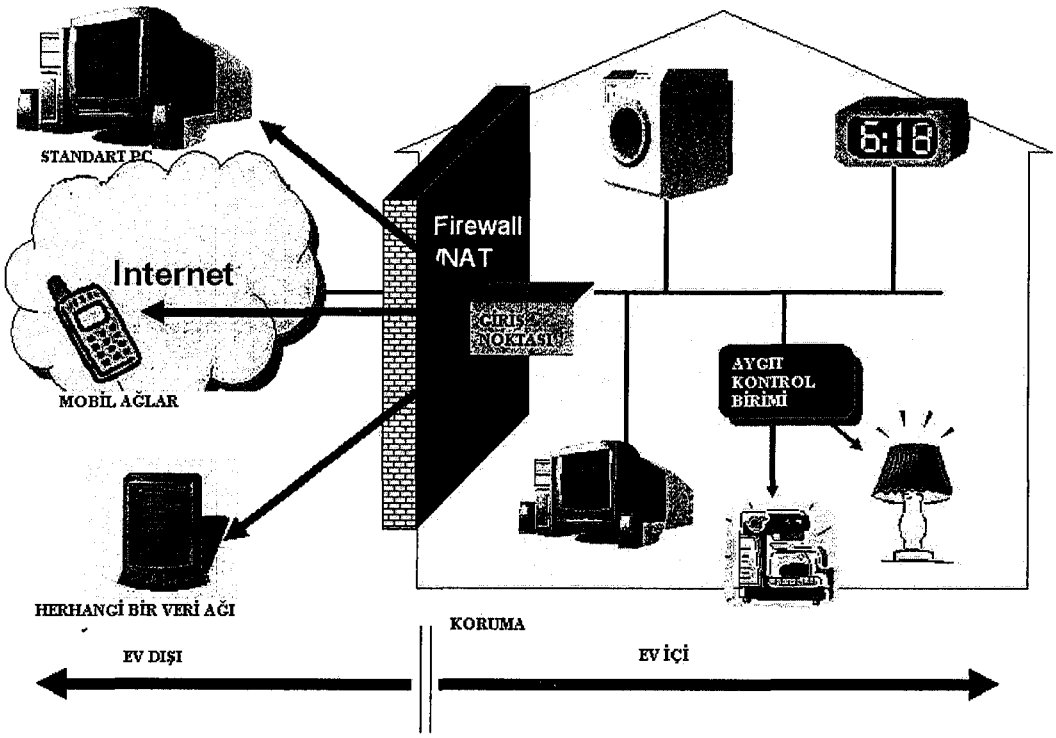
Görüldüğü gibi ABA'lar ve bunların bileşiminden oluşan sistemler kullanıcılarına birçok kolaylık getirecektir.

1.1.1 Aygıtlar arası iletişim

Daha önce de belirtildiği gibi, ABA'ların işlevleri gereği iletişim yeteneklerine sahip olmaları gerekmektedir. Bu aygıtlar iletişim yetenekleri sayesinde, ev içerisindeki veya ev dışındaki çeşitli noktalarla iletişim yapabilmektedirler. Bu şekilde oluşturulan mimari ile ev içinden ve dışından bu aygıtları kontrol ve kumanda etmek mümkün olmaktadır (Şekil 1.2). Kullanıcı kullanabileceği birçok iletişim kanalıyla eve erişebilmekte ve evindeki ABA'lardan herhangi birini kontrol veya kumanda edebilmektedir.

Ev içindeki iletişime örnek olarak bir sistemin elemanları olarak birlikte çalışan ABA'ların kendi aralarındaki iletişim gösterilebilir.

Ev dışı ile yapılan iletişim ise, ABA'ların uzaktan kontrol ve kumandası için ya da ABA'ların dışarıdan belli verileri elde edebilmesi için ev domaininin dışındaki noktalarla yapılan iletişimdir.



Şekil 1-2 Akıllı Ev ve ABA'lar Arası İletişim

1.1.1.1 Ev içi iletişim

Yukarıda da bahsedildiği gibi ABA'ların kendi aralarında iletişim yapması gerekebilir. Durumu daha da genellersek ev içerisinde de iletişim yapılması gerekecektir. Evdeki aygıtların birbirleriyle varolan X.10[5], Jini[6] gibi teknolojileri kullanarak iletişim yapması mümkündür. Bunların yanında bu aygıtların arasındaki iletişim için SIP kullanmak da uygun bir çözüm olarak gözükmektedir. Hatta SIP ve diğer protokollerin aynı ev içerisinde beraber kullanılmaları da mümkün olabilir.

ABA'ların iletişiminde SIP kullanılmasının en büyük avantajı, bu aygıtlara hem ev içerisinden hem de geniş alan ağları üzerinden erişimi sağlayabilmesidir. Bu tez genel olarak evler (domainler) arası iletişimi ele almaktadır. Bu çalışmada her evin bir domain olduğu varsayılmaktadır.

Bir domain içerisindeki aygıtlar arasındaki iletişim temelde iki bölümde incelenebilir; birincisi iletişim yapılmak istenen aygıtın yerinin bulunması ve kimliğinin belirlenmesi, ikincisi ise bu aygıtla iletişimin yapılmasıdır.

Ev içerisinde aygıtlar arası iletişimde çeşitli standartlar kullanılabilmektedir, bunlar HAVi[7], VESA Home Networking[8], JINI, UPnP gibi standartlardır. Ayrıca yer belirleme ve tanımlama işlemleri için de SLP[9] gibi protokoller kullanılabilmektedir.

Ev içerisindeki iletişim için değişik standartlar ve protokoller kullanılabilmesine rağmen, hepsinde sağlanması gereken ortak özellikler vardır. Bunları şöyle özetleyebiliriz;

- Aygıtların iletişiminde kullanılacak kurallar ya aygıtın kendi içerisinde kodlanmıştır, ya da bunları ağdan elde etmektedir.
- Bu kurallar protokollere özel bir dille yazılmıştır.
- Protokollere özel dilden kullanıcının anlayabileceği dile geçişin nasıl olacağı protokollere özel bir şekilde belirtilmektedir.

1.1.1.2 Ev dışı ile iletişim

Akıllı evler ve ABA'ların tanımlarından da anlaşılacağı gibi, bunların uzaktan erişilebilir ve kumanda edilebilir olmaları en büyük özellikleridir. Bu özelliklerinin sağlanabilmesi için ev dışı ile belli bir yapı ile iletişim yapabilmeleri gerekir. Bu iletişim için kullanılabilecek birçok protokol yanında SIP çok uygun özellikler sunmaktadır.

Ev dışı ile iletişim söz konusu olduğunda dikkate alınması gereken bazı faktörler ortaya çıkmaktadır. Bunlar kullanılan protokoller tarafından yerine getirilmesi gereken faktörlerdir. Bunlar kısaca şöyle özetlenebilir;

- Güvenlik: Eve dışarıdan erişimin söz konusu olduğu bir yapıda güvenlik hayati önem taşır. Eğer eve dışarıdan rasgele erişime izin verilirse, ihtiyaç duyulan güvenlik sağlanamayacaktır.
- Kimlik Denetimi: Eve girişe izin verilmeden önce, giriş yapmaya çalışan kişinin kimliğinin denetlenmesi ve sadece yetkisi olan kişilerin eve erişerek evdeki ABA'ları kontrol ve kumanda edebilmesi gerekmektedir.
- Güvenilirlik: Eve dışarıdan erişim, geniş alan ağı kullanımı içerdiğinden, hataların ortaya çıkabileceği nokta sayısı fazladır. Evdeki

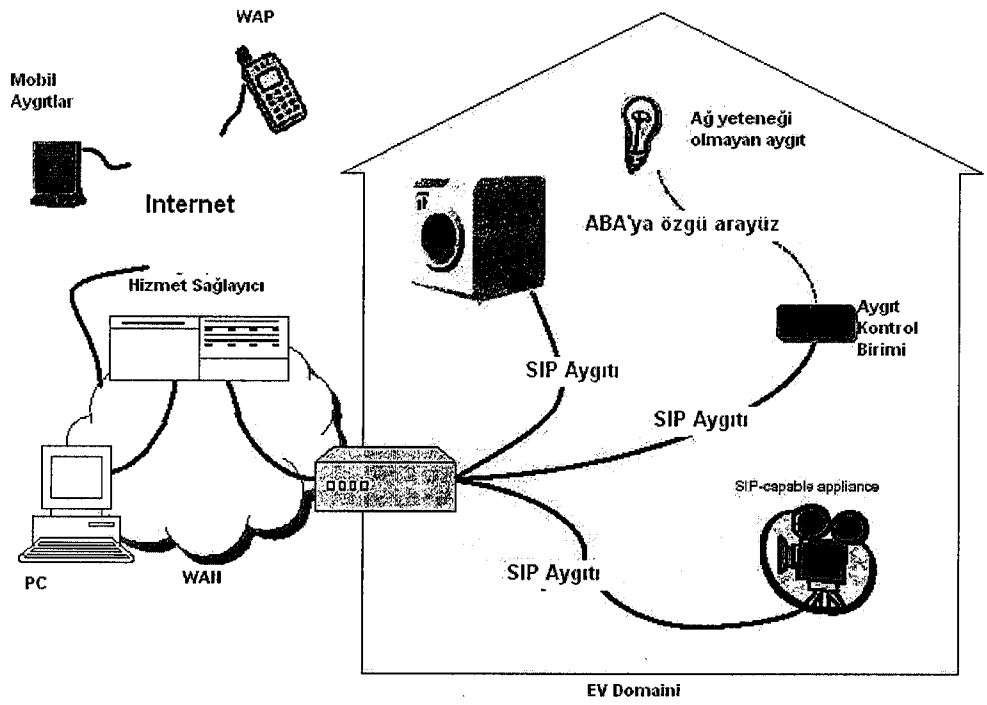
sistemler, dışarıdaki sistemlerle bağlantısı kesilse bile bağımsız olarak çalışmaya devam edebilmelidir.

- Ölçekleme: Birçok ev bulunmaktadır. Kullanılacak protokol bu şekildeki bir yapıyı desteklemelidir.
- Protokolden bağımsız olma: Bir domain içerisinde aygıtlar arası iletişimde birçok protokol kullanılabilmektedir, fakat genel alan ağları için protokollerden bağımsız bir yapı gerekmektedir. Çünkü ev içerisindeki aygıtların detaylı özellikleri dışarıdan bilinemeyebilir.
- İsimlendirme ve Yer Belirleme: Ev içerisindeki aygıtların kesin olarak isimlendirilebilmesi ve bu isimlendirmeden yerlerinin kolaylıkla çıkarılabilmesi gereklidir.

Ayrıca dışarıdan eve giriş noktası için de çeşitli teknikler geliştirilmektedir.

1.1.2 Aygıtlar arası iletişimde SIP kullanımı

Protokol yapısını incelediğimizde, SIP'in istek-yanıt mantığıyla çalışan bir protokol olduğunu görebiliriz. Bu protokol, ABA'larla iletişim için kullanılırken de aynı şekilde çalışacaktır. Oluşturulan yapı, SIP'in Akıllı Evler ve ABA kontrol ve kumandasında kullanılmasına olanak sağlamaktadır (Şekil 1.3). İsteği yapan taraf, karşısındaki SIP varlığına içerisinde istenen olayla ilgili komutu taşıyan bir mesaj yollar. Bu mesaj, olayı gerçekleştirecek aygıtın adını ve adresini, taşıyacağı veri olarak ise gerçekleştirilecek olayla ilgili komutu içerir. Bu mesaj hedefine ilerlerken, adresi çözümlenerek noktadan noktaya iletilir ve en son olarak hedefine iletilir.



Şekil 1-3 ABA Kontrol ve Kumandasında SIP Kullanımı

Örneğin, Ali'nin evindeki yatak odası lambasının yanması istenmektedir. Bunu yapabilmek için bu işle ilgili komutu taşıyacak bir mesaj oluşturulacaktır. Bu mesaj ayrıca Ali'nin evindeki lambanın tam adresini ve adını taşıyacaktır. Gönderilen mesaj, ilk olarak Ali'nin evinin yerini bilen bir sunucuya gönderilir. Bu sunucu bizim yerimize mesajı Ali'nin evine yönlendirir. Buradan sonra mesaj ilk olarak Ali'nin evinin girişindeki Firewall'a gelir ve burada kimlik denetimi ve yetkilendirme yapılır. Eğer bu işlemler başarılı ise, komut ev içerisindeki aygıta gönderilir ve istenen olayın gerçekleştirilmesi sağlanır.

SIP'in yapısını incelersek, yukarıda bahsedilenlerin zaten bu mimaride desteklendiğini kolayca görebiliriz. INVITE[1] mesajları hedeflerine aynen yukarıda anlatıldığı şekilde iletilmektedir. INVITE mesajı ilk olarak isim için bir ajana veya proxy sunucusuna yollanır. Proxy gerekirse bu mesajdaki ismi değiştirebilir ve mesajı hedefe doğru olan yolda bir sonraki noktaya geçirir, ve taşınan içerik hedefe iletilir. Yer belirleme ile ilgili kısımlar ve gerçekleştirilmek istenen olay aynı prosedürde bulunmaktadır. Ayrıca SIP güvenlik mimarisi, yüksek seviyeli isimlendirmeye bağlı kimlik denetimine izin vermektedir.

Belirlenen gereksinimlerle SIP arasında bir fark bulunmaktadır, bu da adreslemedir. SIP URI'leri Internet DNS adresleri şeklindedir. Eğer bu farklılık üzerinde çalışılırsa, SIP aygıtlarla iletişim için pratik bir çözüm olabilir.

1.2 ABA Güvenliği

Uzaktan Akıllı Ev ve ABA kontrol ve kumandasını içeren bir sistem, kişilerin evlerinin üzerinde kullanılacağı için, bu tip uygulamalarda güvenlik çok büyük bir öneme sahiptir. Bu tezde böyle bir sistemin karşı karşıya kalabileceği güvenlik tehditleri ele alınacak, uygulamalarda bunların üstesinden gelebilmek için ne tür yöntemler kullanılacağı ve ne tip önlemler alınabileceği tartışılacaktır.

1.2.1 ABA kontrol ve kumandasında güvenliğin önemi

Bir eve uzaktan erişime izin veren bir sistemin tasarımında güvenliğin önemi son derece büyüktür. Örneğin bir kullanıcının evindeki herhangi bir aygıta gönderilen yanlış bir komut telafi edilmesi imkansız sonuçları beraberinde getirebilir. Bundan dolayı eve uzaktan erişimi sağlayan bir yapıda(yada protokolde) kimlik denetim mekanizmalarının desteklenmesi şarttır. Kısaca durumu şöyle özetleyebiliriz, evdeki aygıtlara erişmek isteyen (yani kontrol ve kumanda etmek isteyen) bütün mesajlar, evin girişindeki bir güvenlik noktasında (tipik olarak RGW/Firewall tarafından) kimlik denetiminden geçirilmek zorundadır ve ayrıca kimlik denetiminden geçmiş bir kullanıcının yapmak istediği işlemi yapmaya hakkının olup olmadığı da denetlenmeli ve bu hakka sahip kullanıcıların işlemi yapmalarına izin verilmelidir.

Çoğu kullanıcı için gizlilik de önemli bir ihtiyaçtır, çünkü iletilen mesajların içeriğine bakılarak evdeki sistemler, aygıtlar, bunların ev içerisindeki yerleşimi gibi bilgilerin elde edilmesi mümkündür. Ev kontrol ve kumandasının söz konusu olduğu bir yapıda, ev içerisindeki durumla ilgili mesajlar ve/veya görüntüler taşıyan bir protokol bu tip içerikleri şifreleyebilmelidir. Çünkü bu tip içeriklerin doğrudan erişilebilir biçimde iletilmesi kullanıcının özel hayatında isteyeceği gizliliği ortadan kaldırabilir. Bundan dolayı uygulamalar şifreli iletişimi

desteklemek zorundadır. Fakat kullanıcılar bazı durumlarda bu seçeneği kullanmamak da isteyebilirler.

Sayılanlara ek olarak ABA'lar tarafından belli kumanda komutlarına verilen yanıt mesajlarının güvenliği de büyük öneme sahiptir. Bu yanıtlar durum bilgisi taşıyabileceği için bunların de güven altına alınması gereklidir. Bu yanıtların içeriğine bakan bir saldırgan evle ilgili belli durumları keşfederek (örneğin alarm sisteminin evin kedisinin girişi için kapalı duruma getirilmesini onaylayan bir yanıt) bu durumlardan fayda sağlayabilir. Buna ek olarak durum bilgisi taşıyan bir yanıt kötü niyetli biri tarafından değiştirilerek ev sahibinin istenilen bir olayı gerçekleştirmek için yönlendirilmesi sağlanabilir.

Aşağıda akıllı evler ve ABA'ların kontrol ve kumandasında ihtiyaç duyulabilecek güvenlik hizmetleri detaylı olarak sıralanmıştır.

1.2.1.1 Gizlilik

Genel olarak hiçbir kullanıcı, iletişim yapmakta olduğu hattı dinlemekte olan birisinin mesajlarının içeriğini görmesini istemez. Örneğin kişi evindeki güvenlik sistemi kameralarının kaydettiği ve muhtemel olarak kendisine ilettiği görüntülerin iletimde iken başkaları tarafından görülebilmesini istemez. Bu direk olarak kişinin ev içindeki özel hayatının açığa vurulması demektir. Bahsettiğimiz gizlilik ihtiyacı, sadece mesajın gövdesine değil aynı zamanda başlık alanlarına da erişimi kapsar. Bu alanlardan elde edilebilecek bilgilerle evde bulunan aygıtlar (ki bunlar değerli elektronik cihazlar vs. olabilir) ve bunların ev içerisindeki yerleri hakkında bilgi edinilebilir.

Diğer bir konu da iletişim için kullanılan Proxy sunucularına güvenme gerekliliğidir. Eğer kullanılan mimari ev domainin direk olarak kontrol edilmesini içeriyorsa, yani eve ulaşmak için aracı proxy sunucularından belli bir hizmet alma ihtiyacı yoksa, aracı proxylere güvenme ihtiyacı doğmayacaktır. Çünkü bu sayede belli alanlar şifrelenerek gönderilebilecektir. Fakat eğer kullanılan mimari Proxy üzerinden iletim içeriyorsa, arada bulunan proxylere güvenmek gerekli olacaktır. Her durumda kullanıcı, mesajının içeriğinin (güvendiği biri olsa bile) proxy sunucusu ve doğal olarak bu sunucunun yöneticisi tarafından görülebilmesini istemez.

Eğer ABA'ların yerini belirlemede kullanılan kayıt işlemi ev dışındaki bir ağdan yapılıyorsa, REGISTER mesajlarının de şifrelenmesi gerekli olabilir. Bu sayede bu mesajların içeriğinin daha sonra kötü niyetle kullanılmak üzere saklanması ihtimalinin önüne geçilebilir. Hem de aygıtların yeri ile ilgili bilgi elde edilemez.

1.2.1.2 Kimlik denetimi

Yukarıda da bahsedildiği gibi, akıllı ev ve ABA kontrolünde, evdeki kaynaklara erişim ve evdeki ABA'ların kontrol ve kumandası değerlidir. Çünkü bunlar sadece ev sahibine veya kullanma yetkisine sahip kullanıcılara ait olması gereken haklardır. Peki bu hakları sadece hak sahiplerinin kullanması nasıl sağlanabilir? Bu sorunun cevabı güvenlik hizmetlerinden olan "Kimlik Denetimi" sayesinde verilebilir. Bu hizmet, sadece yeterli haklara sahip olan kişilerin bu kaynaklardan ve yetkilerden yaralanabilmesini sağlar.

Kullanıcı bakış açısından ele aldığımızda, ABA kontrol ve kumanda mesajlarına kimlik denetimi yapmak çok önemlidir. Burada dikkat edilmesi gereken konulardan birisi de kimlik denetiminin iki yönlü yapılması gerekliliğidir (kullanıcı evi, ev de kullanıcıyı denetlemelidir). Kullanıcıdan eve giden mesajlar evde belli işlevleri yerine getireceklerinden dolayı bunların kimliğini denetleme gerekliliği açıktır. Bunun yanında kullanıcıya dönen 100 ve 200 kodlu yanıt mesajları kimlik denetiminden geçmek zorundadır. Bunun nedeni de, hiç hedefe iletilmemiş bir mesaj için oluşturulabilecek sahte yanıtları yakalayabilme gerekliliğidir. Ayrıca yanıt mesajları durum bilgisi taşıyabileceği için bunların kimden geldiğinden emin olunabilmesi gereklidir.

Kontrol ve kumanda mesajlarının kimlik denetiminden geçmesinin yanında, kayıt için kullanılan "REGISTER" mesajları da kimlik denetiminden geçirilebilir. Eğer kayıt işlemi ev domaini içerisinde RGW ile yapılıyorsa, şifreleme işlemleri kullanmadan bu işlem yapılabilir, çünkü bu durumda ev içerisindeki fiziksel güvenlik sayesinde bu mesajlar korunur. Eğer kayıt işlemi dışarıdan yapılıyorsa (örneğin iletişim bir Proxy üzerinden yapılıyorsa), bu durumda REGISTER mesajlarına kimlik denetimi yapılmak zorundadır. Bu sayede kötü niyetli bir yanlış kayıt engellenerek bunu neden olabileceği zararların önüne geçilebilir.

Mesajların kimlik denetiminden geçirilmesi, sahte mesajların oluşturulması, mesajların değiştirilmesi, ve taklit edilmesi gibi saldırıları engeller. Direk olarak kimlik denetimiyle engellenemeyen saldırılar ise tekrarlama saldırılarıdır. Bunların önüne geçmek için iki yol vardır, birincisi mesajlarda bulunan zaman etiketlerine veya sıra numaralarına bakarak tekrarlanan mesajları yakalamaktır. Burada sorun daha önceden kullanılmış olan zaman etiketlerinin değerlerinin sadece belli bir kısmının saklanabileceğidir. Bir diğer çözüm ise, o andaki sistem saatine bakarak eski mesajları (daha doğrusu tekrar gönderilmek istenen eski mesajları) yakalamaktır. Bu durumda da saatlerin senkronizasyonu gereklidir.

1.2.1.3 Mevcudiyet

Akıllı eve ve ABA'lara uzaktan kontrol ve kumanda eden bir sistemde mevcudiyet (yani hizmetin kullanılabilir olması) önemlidir. Herhangi bir yetkili kullanıcı evindeki herhangi bir ABA'ya erişmek istediğinde, evinden herhangi bir ABA hakkında bilgi almak istediğinde veya herhangi bir ABA'ya kumanda etmek istediğinde bunu yerine getirebilmelidir. Yani dışarıdan herhangi bir etki nedeniyle evdeki kaynaklar kullanılamaz hale gelmemelidir.

Mevcudiyet genel olarak hizmetin engellenmesi saldırılarına karşı alınan önlemlerdir. Bu saldırılar çeşitli şekillerde ortaya çıkabilmektedir. Bunlardan biri, eve erişim için kullanılması zorunlu olan iletişim kanallarının işlevini yerine getiremez bir hale getirilmesidir. Bu tip saldırıları engellemek için, sadece kimliği denetlenmiş trafiğin bu iletişim kanallarında yer alması sağlanabilir. Bu tip saldırıların diğer bir türü de yer belirleme veritabanına sahte kayıtlar girilmesi sayesinde belli noktaların erişilemez hale getirilmesidir. Ayrıca bu kayıtları tutan sunucuların veritabanlarının çok fazla kayıtla doldurulması ile kaynaklarını tüketilmesi ve görevini yerine getirememesi sağlanabilir. Bu tip saldırıların önüne geçmek için ise kayıt işlemleri kimlik denetimi sonrasında yapılabilir.

2. GÜVENLİK GEREKSİNİMLERİ VE ABA GÜVENLİĞİ

İletişim sistemlerinin artan bir hızla yaygınlaştığı, bu yaygınlaşma sonucu sistemlerin kullanıcılarına sunduğu hizmetlerin daha kapsamlı hale geldiği daha önceki bölümlerde belirtilmişti. Bunun sonucu olarak iletişimde taşınan veri bazen kişiye özel olabilmekte, saklanması gereken bir bilgi içerebilmektedir. Bazı durumlarda ağ üzerinden sağlanan hizmetin sadece istenilen kişiler tarafından kullanılabilir olması, diğer kullanıcılar tarafından kullanılamaz olması tercih edilebilir. Hatta bazı durumlarda istenmeyen kullanıcıların bu hizmetin varlığından bile haberdar olmaması istenebilir. Ayrıca hizmeti alacak kullanıcının, ihtiyaç duyduğu anda herhangi bir engelle karşılaşmadan hizmete erişebilmesi büyük önem taşır.

Yukarıda sayılan bütün bu ihtiyaçlar, bilgi güvenliği sayesinde sağlanabilmektedir. Bilgi güvenliği verinin hem bulunduğu yerde, hem de iletimi sırasında sağlanabilir.

Akıllı Evler ve ABA kontrol ve kumandası ise güvenliğin büyük öneme sahip olduğu uygulamalardır. Bu tip uygulamaların varolabilmesi ve kullanım alanı bulabilmesi için kullanıcılarına belli bir seviyede güvenliği garanti edebilmeleri gereklidir. Bu bölümde ilk olarak genel güvenlik kavramları ve gereksinimleri anlatılacaktır. Daha sonra ise ABA ve ev ağlarındaki güvenlik konuları ele alınacaktır.

2.1 Bilgi Güvenliği

İlk önce kullanılacak kavramlar kısaca şöyle tanımlanabilir[10];

- Bilgi: Araştırma, çalışma veya öğrenmeyle elde edilen malumat, haber, olgu, veri, veri ifade eden sinyal veya karakter.
- Güvenlik: Tehlikeden uzak olmak, emniyette olmak, korku ve endişeden uzak olmak.

Bu durumda "Bilgi Güvenliği", bilginin, olguların, verinin veya yeteneklerin yetkisiz kullanımının, suistimal edilmesinin, değiştirilmesinin, hak sahipleri tarafından kullanımının engellenmesinin önüne geçmek için alınan tedbirlerdir.

Yani daha kısa bir tanımlamayla bilgi güvenliği, bilgi ve yeteneklerimizi korumak için aldığımız tedbirlerdir. Bilgiyi tehditlerden ve açıklıkların kötüye kullanılmasından korumaya çalışırız.

2.1.1 Saldırılar

Bir organizasyonun, kişinin sahip olduğu verilerin veya bilgisayar sistemlerinin başına çeşitli şekillerde kötü olaylar gelebilir. Bu olaylar kasıtlı veya yanlışlıkla meydana gelebilirler, fakat yine de hepsi "saldırı" olarak adlandırılır. Temelde verinin karşılaşabileceği saldırılar dört çeşittir;

- Erişim saldırıları (Access)
- Değiştirme saldırıları (Modification)
- Hizmetin engellenmesi saldırıları (Denial of service)
- Yapılanların reddedilmesi (Repudiation)

Genelde saldırılar teknik olarak veya insan ilişkilerine bağlı olarak oluşabilmektedir. Teknik saldırılar, güvenliğin çeşitli teknikler kullanılarak aşılması şeklindedir. Örnek olarak belli yöntemlerle bir şifrenin kırılmaya çalışılması verilebilir. Bu tip saldırıların önüne geçebilmek için yine teknik yöntemlerin kullanılması veya yöntemlerin güçlendirilmesi gereklidir. İnsan ilişkilerine bağlı saldırılar ise insanların zayıf yönleri kullanılarak yapılır. Buna örnek olarak ise bir kullanıcının sahte bir e-ileti ile yanlış yönlendirilmesi sonucu kullanıcı ismi ve şifresini saldırgana yollaması verilebilir. Bu sayede saldırgan çok büyük bir çaba harcamadan istediği saldırıyı yapabilecektir. Bu tip saldırıların önüne geçebilmek için ise, kullanıcıların bilgilendirilmesi ve belirli güvenlik kurallarının koyulması yoluna gidilebilir.

Elektronik bilginin bir özelliği de kopyalanmasının orijinal bilgiye zarar vermemesidir. Yani çoğu zaman bilginin kopyalandığını (yani çalındığını) anlamak mümkün olmayabilir.

2.1.1.1 Erişim (Access) saldırıları

Saldırganın erişim yetkisi olmayan bilgiyi görmesi şeklindedir. Bilgi bulunduğu yerde veya iletim sırasında bu saldırılarla karşılaşabilir.

- Casusluk (Snooping): Saldırganın belli bir bilgiyi buluncaya kadar veya ilgisini çeken herhangi bir bilgi buluncaya kadar bilgiyi (örneğin dosyaları tek tek açıp içlerine bakarak) taraması şeklinde yer alır.
- Dinlemek (Eavesdropping): Saldırganın bilgiyi yetkisiz olarak görebilmesi için bilginin geçeceği bir yerde durup beklemesi ve veriyi izlemesi şeklinde olan saldırılardır.
- Durdurma (Interception): Saldırgan kendisini bilginin geçeceği yolda araya sokarak hedefe ulaşmadan önce eline geçirir. İsterse bilgiyi inceler, değiştirir, yollar veya yollamaz.

2.1.1.2 Değiştirme(Modification) saldırıları

Bu tip saldırılarda saldırgan, değiştirmeye yetkili olmadığı bilgiyi değiştirmeye çalışır. Bu bilginin bulunduğu yerde veya iletim sırasında olabilir. Bu saldırı bilginin bütünlüğüne karşı bir saldırıdır.

- Değişiklik yapma (Changes): Varolan bilginin üzerinde değişiklik yapma şeklindedir. Yani varolan bilgi doğru olmayan bir hale çevrilir.
- Ekleme (Insertion): Daha önceden olmayan bilgiyi eklemek şeklindedir. Mesela kişinin adına para aktarımı eklenmesi gibi.
- Silme (Deletion): Yetkisi olmayan kişilerin kayıtları silmesi şeklinde meydana gelir. Buna örnek olarak da kişinin hesabından yapılan para aktarımının silinmesi gösterilebilir.

2.1.1.3 Hizmetin engellenmesi saldırıları (Denial of Service – DoS)

Aslında direk olarak bilgiyi hedef alan bir saldırı türü değildir. Sistemdeki bilgiye, kaynaklara veya yeteneklere erişim hakkı bulunan kullanıcıların bu haklarından yararlanmalarını engellemek şeklinde yer alan saldırılardır. Yani bu

saldırılar nedeniyle sistemin gerçek kullanıcıları sisteme erişemez, ve gerektiğinde bilgiyi ve hizmetleri kullanamaz.

- Bilgiye erişimin engellenmesi: Bilginin kullanılabilir halde bulunmasını engellemek şeklindeki saldırılardır. Bu bilginin bozulması, kullanılamaz bir hale getirilmesi veya erişilemeyecek bir yere taşınması şeklinde ortaya çıkabilir.
- Uygulamalara erişimin engellenmesi: Bilgiyi işleyen veya sunan uygulamalara erişimi engellemek şeklindeki saldırılardır. Genelde uygulamayı çalıştıran bilgisayara karşı yapılırlar.
- Sistemlere erişimin engellenmesi: Bu saldırılarda bütün uygulamaları ve bilgiyi tutan sistemlere saldırılarak bunların çökmesi sağlanır. Bu sayede sistemdeki bütün bilgi erişilemez hale gelir.
- İletişime erişimin engellenmesi: Bu saldırılar iletişim sistemlerinin kullanılamaz hale getirilmesiyle oluşur. Bu hattın kesilmesi, ağların taşkınlarla boğulması gibi yollarla yapılır. Burada bilgi sistemi ve bilgiye zarar verilmez ama iletişimin engellenmesiyle veri erişilemez hale gelir.

2.1.1.4 Yapılanların reddedilmesi (Repudiation)

Bilginin izlenebilirliğine karşı yapılan saldırılardır. Yani kısaca yanlış bilgi verme veya kaydedilmiş bir olayın veya işlemin reddedilmesi şeklindedir.

- Başkasının yerine geçme (Masquerade): Bu saldırılarda saldırgan bir kişiyi taklit eder veya onun yerine geçmeye çalışır. Bu saldırılar kişisel iletimde, parasal işlemlerde veya sistemler arası iletişimde meydana gelebilir.
- İnkar etme (Denying): Bir olayın kaydının tutulduğu biçimde kabul edilmemesi şeklindedir. Mesela kötü niyetli bir müşterinin internet üzerinden verdiği siparişi kendisinin vermediğini iddia etmesi bu tip bir saldırıdır.

2.1.2 Bilgi güvenliği hizmetleri

Bu hizmetler yukarıda belirlediğimiz saldırılara karşı koyabilmek için ortaya çıkarılmıştır. Buradaki hizmetler bilgi güvenliği yöntemlerinden farklıdır.

Bu hizmetleri kısaca bilginin güvende olması için sağlanması gereken şartlar olarak tanımlayabiliriz.

Bilginin güvende olduğunu, bütün bu gereksinimler sağlanıyorsa söyleyebiliriz. Bazı durumlarda bu hizmetlerin sağlanması birbirini etkileyebilir. Yani sağlanmayan bir hizmet nedeniyle, başka bir hizmet de sağlanamayabilir. Onun için bu hizmetlerin hepsinin sağlanması tercih edilir.

2.1.2.1 Gizlilik (Confidentiality)

Bilginin istenmeyen kişilerden saklanmasını sağlar. Yani sadece bilgiye erişmesi istenen kişi bilgiye erişebilir, bilgiyi kullanabilir veya değiştirebilir. Bu hizmet işlevini tam olarak yerine getirebilmek için sorumluluk hizmetiyle beraber çalışmak zorundadır.

Gizlilik hizmeti sayesinde bilgi istenmeyen kişilerden saklanarak erişim saldırılarına karşı koyulabilir.

2.1.2.2 Bütünlük (Integrity)

Bilginin doğruluğunu sağlayan hizmettir. Yani bilginin herhangi bir şekilde değiştirilmediğini, üzerinde herhangi bir oynama, eklenti vs. yapılmadığını garanti eder. Bu hizmet doğru olarak sağlandığında kullanıcıların bilginin doğruluğuna güvenebilmelerini sağlar. Bu hizmet de Sorumluluk hizmetiyle beraber kullanılmak zorundadır.

Bütünlük hizmeti, değiştirme ve yapılanları reddetme saldırılarına karşı koruma sağlar. Bütünlük hizmeti sayesinde yetkisi olmayan kişiler veriyi değiştirdiğinde bu fark edilebilir ve yetkisiz değiştirmelerin önüne geçilebilir.

Ayrıca sayısal imzalar sayesinde kişilerin yaptıklarını inkar edememesi sağlanarak yapılanların reddedilmesi engellenebilir.

2.1.2.3 Kullanıma uygunluk (Availability)

Bilginin kullanılabilir bir halde bulunmasını sağlayan hizmettir. Bu hizmet kullanıcıların bilgisayar sistemlerine, sistemlerdeki bilgiye, bilgi üzerinde çalışan uygulamalara erişimini sağlar. Ayrıca bilginin iletilebilmesini de bu hizmet sağlar.

- Yedekleme: Önemli bilgilerin fazladan bir veya birkaç kopyasının güvenli bir yerde saklanması şeklindedir. Bu bilgiler belli aralıklarla yedeklenebilirler. Buradaki en büyük problem en son yedeklemeden itibaren olan değişikliklerin kaybedilmesidir.
- Yedek sistemler kullanma: Bilgi veya yeteneklerin yeniden kurulabilmeleri için fazladan kaynaklar atanması şeklindedir. Bu yöntemde hatalar otomatik olarak yakalanıp, bilgi ve yetenekler tekrar kullanılabilir duruma getirilebilmektedir.
- Yıkımdan kurtarma: Sistemleri, yetenekleri ve bilgiyi büyük kapsamlı yıkımlardan kurtarmak için kullanılacak kapsamlı bir süreçtir.

Kullanıma uygunluk hizmeti sayesinde hizmeti engelleme saldırılarına karşı koyulabilmektedir. Aslında bu tip saldırılar tam olarak engellenememekte, fakat bunların etkilerinin en az seviyede yaşanması sağlanmaktadır.

2.1.2.4 Sorumluluk (Accountability)

Genelde sorumluluk hizmeti direk olarak güvenlik sağlamaz, ama diğer hizmetlerle birlikte çalışarak bu hizmetlerin işlevlerini yerine getirebilmesini sağlar.

- Tanımlama ve Kimlik denetimi(identification & authentication): Bu görevler temelde iki amaca hizmet ederler; ilk olarak belli bir işi yapmak isteyenin kim olduğunu belirlemek, ikinci olarak ise bu kişinin gerçekten iddia ettiği kişi olduğunu kanıtlamak. Kimlik denetimi yaparken kimliğinizi kanıtlamak için genelde "bildiğiniz bir şey", "sahip olduğunuz bir şey" veya "size özgü bir şey" kullanılabilir. Genelde bir kullanıcı ismi ve şifre kullanımı yaygındır. Aslında bunlardan birden fazlasını kullanımı daha uygun olabilir.

- Hesap Denetimi: Kullanıcıların ve yapılan işlerin ilişkilendirilerek kaydedilmesidir.

2.1.3 Bilgi güvenliği için kullanılan yöntemler

Yukarıda da değinildiği gibi bilgi ve iletişim sistemlerinin kullanılabilir olmaları için güvenli olmaları gereklidir. Bu güvenli olma bazı şartlara bağlıdır. Bu şartlar da Bilgi Güvenliği Hizmetleri olarak tanımlanmıştı. Bu bölümde de bu hizmetlerin nasıl sağlanabileceği ele alınacaktır. Yani kısaca güvenli bir ortam sağlayabilmek için kullanılabilecek yöntemler anlatılacaktır.

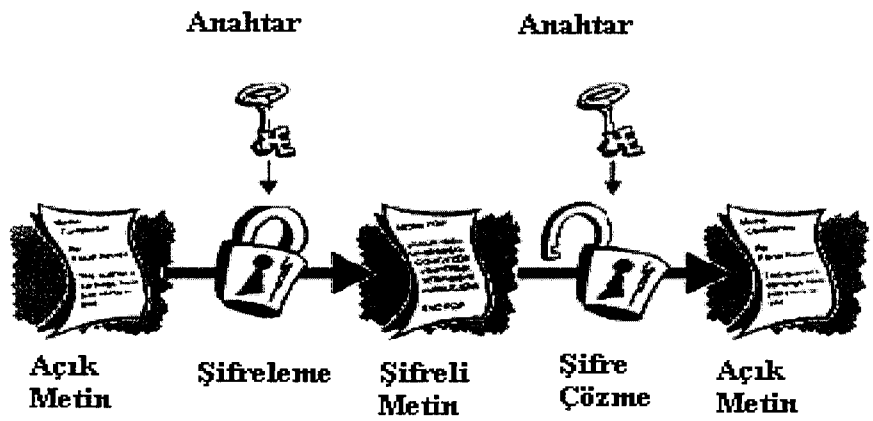
2.1.3.1 Şifreleme (Encryption)

Şifrelemeyi kısaca şöyle tanımlayabiliriz; Bilginin sadece yetkili olan kişiler tarafından okunabilecek, yetkisiz kişiler tarafından okunamayacak şekilde belli bir yöntemle gizlenmesi. Burada yetkili kişiler olarak şifreyi çözecek anahtara sahip olan kullanıcılar ifade edilmektedir. Yani şifrelenmiş bilgiyi sadece elinde gerekli anahtarı bulunduranlar okuyabilir. Bu sayede gizlilik hizmeti sağlanabilmektedir.

Şifrelemede önemli bir nokta da herhangi bir yetkisiz kullanıcının, şifrelenmiş bilgi ve şifreleme yöntemini bilse bile orijinal bilgiye erişiminin son derece zor olmasını sağlayabilmektir. Yani kişi bir şekilde şifrelenmiş bilgiyi ele geçirse, ve aynı zamanda şifreleme için kullanılan yöntemi de öğrenebilse bile, bu ikisini kullanarak açık veriyi ortaya çıkaramamalıdır.

Şifreleme ile;

- Gizlilik: Bilginin depolama veya iletim sırasında yetkisiz kullanıcılardan saklanmasını sağlayabiliriz,
- Bütünlük: Bilginin depolama veya iletim sırasında değiştirilip değiştirilmediğini anlayabiliriz, bu da bütünlüğü bozulan bilginin şifresi çözüldüğünde manasız bir bilgi haline gelmesinden anlaşılabilir.
- Sorumluluk: Bilginin kaynağının kimliğinin belirlenmesi sağlanabilir, ve daha sonra bu kaynağın bilginin kaynağı olduğunu inkar etmesi gibi durumların önüne geçilebilir.



Şekil 2-1 Şifreleme Sistemleri

Şifreleme konusunu daha iyi anlayabilmek için, bu konuyla ilgili terimler iyi bilinmelidir. Temel olarak çalışması yukarıda gösterilen (Şekil 2.1) şifreleme sistemleri ve şifreleme işlemi sırasında kullanılan çeşitli terimler kısaca açıklanmıştır.

- **Açık Metin (Plaintext)**: Şifrelenecek özgün bilgi.
- **Şifreli Metin (Ciphertext)**: Şifrelemeden sonra ortaya çıkan gizlenmiş bilgi.
- **Algoritma (Algorithm)**: Açık metini, şifreli metin haline getirmek için kullanılan yöntem.
- **Anahtar (Key)**: Açık metinden şifreli metin elde edilirken veya şifreli metinden açık metin elde edilirken algoritmaya giren veri.
- **Şifreleme (Encryption)**: Açık metini şifreli metine çevirme işlemi.
- **Şifre çözme (Decryption)**: Şifreli metinden açık metni elde etme işlemi.

2.1.3.2 Şifrelemeye karşı saldırılar

Her güvenlik yönteminde olduğu gibi şifreleme sistemlerine karşı da çeşitli şekillerde saldırılar olabilir. Bu saldırılar sonucunda, saldırgan mutlaka bilgiye erişecektir. Ama şifreleme sistemlerinin başarısı, bu bilgiye erişim zamanının bilginin değerli olduğu süreden daha fazla olması veya bilginin maddi değerinin saldırı için harcanandan daha düşük olması şeklinde ifade edilebilir.

Genelde şifreleme sistemlerine üç şekilde saldırılabilir;

- Algoritmadaki zayıflıklar kullanılarak: Algoritmadaki zayıflıkların bulunmasıyla birlikte anahtar olmadan açık metini ortaya çıkarmak için çalışırlar. Bu tip zayıflıkları olan algoritmaların kullanılması, şifrelemenin kullanılma amaçlarını yerine getiremez. Yani kısaca bu tip yöntemleri kullanmak genelde işe yaramaz.
- Kaba kuvvet kullanılarak (Brute force): Şifre çözmede kullanılacak anahtar için bütün olasılıkların denenmesi şeklindeki saldırılardır. İstatistiksel olarak bakıldığında, saldırgan başarılı olabilmek için ortalama olarak mümkün olan bütün anahtarların yarısını denemek zorundadır. Burada anahtar ne kadar uzunsa, saldırının başarılı olabilmesi, yani anahtarın bulunması için gerekli süre de o kadar uzayacaktır. Bu saldırılarda başarı kaçınılmazdır, ama önemli olan bilgiye değerli olduğu süre içerisinde erişebilmektir. Bu engellenebilirse, şifreleme başarılıdır denebilir.
- Çevre sistemlerdeki zayıflıklar kullanılarak: Bu yöntem direk olarak şifrelemeye saldırı içermez. Burada saldırgan şifreyi çözmek yerine daha kolay yollardan şifreyi ele geçirmeyi yeğler. Örneğin iletiler yoluyla ağ üzerinde dağıtılan bir anahtarı iletinin içinde bulmak, bu anahtarı kaba kuvvetle çözmekten daha kolay olacaktır. Ya da çözülmesi neredeyse imkansız olan bir anahtarın, içerisinde bir dosyada saklı olarak bulunduğu düşük güvenlikli(kullanıcı adı ve şifre ile korunan) bir bilgisayardan çalınması çok kolay olabilir.

2.1.3.3 Şifreleme çeşitleri

Şifreleme temel olarak açık metin ile anahtarın bir algoritmaya beraber girmesiyle şifreli bir metin ortaya çıkarma şeklindedir. Şifre çözme ise yine şifreli metin ile bir anahtarın algoritmaya girmesi, ve yapılan işlemler sonucu açık metnin ortaya çıkarılması şeklindedir. Temelde mantık değişmese de, bu işlemlerin nasıl yapıldığı değişebilir.

Temelde iki çeşit şifrelemeden söz edebiliriz, özel anahtar şifrelemesi (Private Key Encryption) ve ortak anahtar şifrelemesi (Public Key Encryption).

Özel anahtar şifrelemesinde, bilgiyi şifreleyen ve çözen taraflar aynı anahtarı kullanırlar. Yani ortada bir tek anahtar vardır.

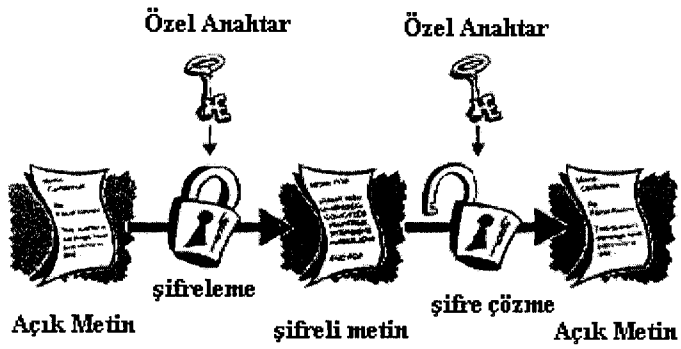
Ortak anahtar şifrelemesinde ise şifreleyen ve şifreyi çözen tarafların elinde farklı anahtarlar vardır. Fakat bu anahtarlar birbirleriyle ilişkilidir.

- **Özel anahtar şifrelemesi (Private Key Encryption)**

Hem şifreleme hem de şifre çözmede aynı anahtarın kullanıldığı şifreleme yöntemlerinin genel adıdır. Diğer bir adı da simetrik anahtar şifrelemesidir (Symmetric Key Encryption). En fazla kullanılan şifreleme çeşididir (Şekil 2.2).

Bu tip şifrelemede hem gönderen hem de alan taraf aynı anahtara sahiptir. Bu tip şifreleme ile bilginin iletim sırasındaki gizliliği sağlanabilir ve iletim sırasında bilgi üzerinde yapılacak herhangi bir değişiklik şifre çözme algoritmasının yanlış sonuçlar ortaya çıkarmasını sağlayacağından dolayı kolayca fark edilebilir. Anahtara sahip olan herkes şifreli bir metin oluşturup gönderebileceğinden dolayı bu tip şifreleme ile kimlik denetimi sağlanamaz.

- Değiştirme şifreleri (Substitution Ciphers)
- Tek seferlik bloklar (One-Time Pads)
- Veri Şifreleme Standardı (Data Encryption Standard – DES[11])
- Üçlü DES (Triple DES[11])
- Gelişmiş Şifreleme Standardı (Advanced Encryption Standard – AES[12])



Şekil 2-2 Özel Anahtar Şifrelemesi

- **Ortak Anahtar Şifrelemesi (Public Key Encryption)**

Bu tip şifrelemede iki farklı, fakat birbiriyle ilişkili anahtar kullanılır. Yani şifreleme için ayrı, şifre çözme için ayrı anahtar kullanılır (Şekil 2.3). Bu anahtarlardan birincisiyle şifrelenen veri, sadece ikinci anahtarla açılabilir, ve de ikinci anahtarla şifresi çözülebilen bir metin sadece birinci anahtarla oluşturulmuş olabilir.

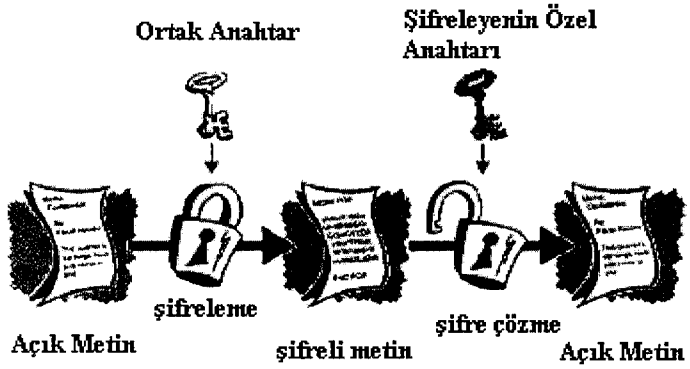
Genel olarak birinci (şifreleme anahtarı) özel anahtar (private key) ikinci anahtar (şifre çözme anahtarı) ise ortak anahtar (public key) olarak adlandırılır.

Eğer gizlilik gerekli ise şifreleme ortak anahtarla yapılır ve sadece özel anahtara sahip olan kişi veriyi görebilir. Eğer kimlik denetimi gerekli ise veri özel anahtarla şifrelenir ve sadece onun dağıttığı ortak anahtara sahip olanlar şifreyi çözebileceği için kimlik denetimi sağlanmış olur. Bütünlük gereksinimi de iki yöntemle de sağlanır.

Bu tip şifrelemenin dezavantajı işlemsel yoğunluk getirmesi ve iletişimi daha yavaş bir hale getirmesidir. Bu yönlerden iletişimin şifrelenmesi için kullanmaya uygun değildir. Fakat bu tip şifreleme ile kimlik denetimi ve anahtar dağıtımı için kullanılabilir. Bu işlemler yapıldıktan sonra veri iletimi özel anahtar şifrelemesi ile yapılabilir.

Aşağıda en sık kullanılan ortak anahtar şifreleme yöntemleri gösterilmiştir;

- Diffie-Hellman Anahtar Değişimi (Diffie-Hellman Key Exchange[13])
- RSA[14]



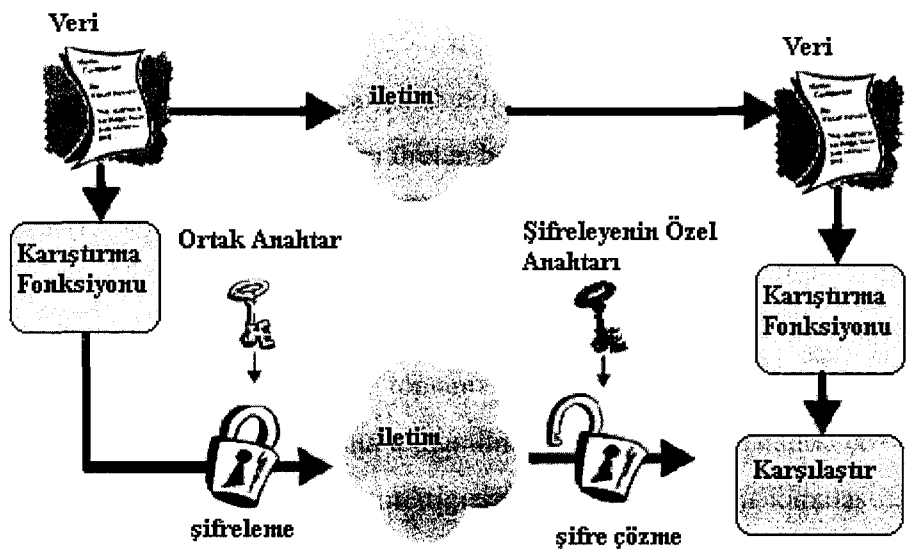
Şekil 2-3 Ortak Anahtar Şifrelemesi

2.1.3.4 Sayısal imza

Kimlik denetimi sağlamak için kullanılan bir çeşit şifrelemedir. Eğer bilgi bir kullanıcının özel anahtarıyla şifrelenmiş ise bu şifrelemeyi onun yaptığı bellidir. Ve eğer bu şifreli metin birisinin ortak anahtarıyla çözülebiliyorsa, bu durum veriyi onun şifrelediğini kanıtlar. Ayrıca bilginin iletim sırasında değiştirilmediği de bu şekilde anlaşılabilir.

Sayısal imza ile bu güvenlik geliştirilmiş ve veri alındıktan ve şifresi çözüldükten sonra bile verinin değiştirilip değiştirilmediği kontrol edilebilir hale getirilmiştir. Bu yöntem şöyle çalışır (Şekil 2.4);

- Veri önce sağlama toplamı üreten bir fonksiyona sokulur.
- Üretilen bu sağlama toplamı, göndericinin özel anahtarıyla şifrelenir.
- Veri ve de şifrelenmiş sağlama toplamı mesaj içerisinde karşı tarafa yollanır.
- Alıcı aldığı veriyi sağlama toplamı üreten fonksiyona sokar.
- Alıcı aldığı şifreli sağlama toplamının şifresini ortak anahtarla çözer.
- Şifresi çözülen ve kendi ürettiği sağlama toplamlarını karşılaştıran alıcı, bunların aynı olması durumunda verinin iddia edilen kişiden geldiğini ve yolda değişime uğramadığını belirler.



Şekil 2-4 Sayısal İmza

2.1.3.5 Anahtar yönetimi

Anahtar yönetimi, şifreleme için hayati önem taşır. Ne kadar iyi şifreleme yöntemleri kullanırsanız kullanın bu yöntemlerle anahtar üretmek ve dağıtmak, direk olarak yöntemlerin güvenilirliğini etkileyecektir. Yani kırılması çok zor bir yöntemde, anahtar olarak kullanıcının ismi kullanılırsa, bu anahtarı tahmin etmek çok kolay olacak ve yöntemin güvenilirliği hiçbir işe yaramayacaktır. Ya da aynı yöntemle üretilen güçlü bir anahtar, kullanıcının masaüstündeki bir dosyada kayıtlı ise, basit bir incelemeyle bu güçlü anahtar bulunabilecek, yine yöntemin güvenilirliği arka planda kalacaktır. Güçlü anahtar üretmek ne kadar önemli ise bu anahtarları yönetmek o kadar önemlidir.

Anahtar yönetimi temelde iki adımda incelenebilir. Birincisi, kullanılan yöntemi kuvvetlendirmek için anahtarları doğru bir şekilde üretmeyi amaçlayan anahtar üretimidir. İkinci adım ise, üretilmiş bir anahtarın istenilen yerlerde kullanılabilmesi için hedeflere dağıtılmasıdır.

- **Anahtar Üretimi**

Bilindiği gibi şifreleme sistemlerinin başarısı, kullanılan yöntemin gücü ve yöntemin başarıyla uygulanmasına bağlıdır. Bu uygulama sırasında, anahtarların belli özelliklere dikkat edilerek oluşturulması, sistemi daha da güçlendirecektir. Anahtar üretiminde aşağıdaki faktörlere dikkat edilmelidir;

- Anahtarların üretiminde kullanılacak yönteme göre bazı özelliklere dikkat etmek önemlidir. Güçlü anahtarlar bu şekilde oluşturulabilir.
  Örn: DES kullanılırken 0'lardan oluşan bir anahtar çok zayıf olacaktır.
  Örn: RSA kullanılırken p ve q sayıları asal sayı olmalıdır.
- Bazı durumlarda anahtarların kullanıcı tarafından belirlenmesi istenebilir, bu durumlarda kullanıcıların bu anahtarları (şifreleri) dikkatli seçmeleri için yönlendirilmesi gerekir. Oluşturulan anahtarlar belli kurallara uymalı (örneğin en az bir sayı ve karakter içermeli), sözlük kelimelerinden oluşmamalı (programlarla bir şifre için sözlükteki kelimeler tek tek denenebilir), kullanıcısının çeşitli bilgilerini içermemelidir (isim, soy isim

vs). Bu sayede kolay tahmin edilemeyen veya bulunamayan anahtarlar oluşturulabilir.

- Anahtar uzunlukları özenle belirlenmelidir. Çok kısa anahtarların tahmin edilmesi daha kolay olacaktır (örneğin 3 karakterlik bir anahtar için olası değerlerin tek tek denenmesi, günümüz bilgisayarları için çok kısa sürecektir).
- Ayrıca bazı ek yöntemlerle ilave dayanıklılık sağlanabilir (örneğin kullanıcı ismi-anahtar denetimi yapılan bir pencerede belli bir sayıdaki başarısız deneme ardından ortam kilitlenebilir veya en azından belli bir süre için dondurulabilir).

- **Anahtar Dağıtımı**

Yukarıda bahsedildiği gibi anahtarların üretilmesi yanında, üretilen anahtarların dağıtımı da çok önemlidir.

- Anahtarlar elle dağıtılabilir. Ama uzak mesafeler ve zaman problemleri bunu başarısız kılar.
- Diffie-Hellman gibi yöntemlerle anahtar dağıtımı sağlanabilir.

- **Anahtar Belgelendirme**

Üretilip dağıtılan anahtarların, iddia edilen kişiye ait olup olmadığı, iletimde değiştirilmediği kontrol edilebilmelidir. Bunun kontrolü de sayısal imza kullanılarak yapılabilmektedir. Belli organizasyonlar tarafından anahtarların ve sahiplerinin sertifikalandırılması yoluna gidilebilir.

3. SIP VE AĞA BAĞLI AYGITLAR ARASI İLETİŞİMDE KULLANIMI

Daha önceki bölümlerde, ABA'ların iletişiminde SIP kullanımının uygun olacağından bahsedilmişti. Bu protokolün kullanımıyla birlikte sağladığı birçok olanaktan yararlanılabilecek, birçok özelliği kullanılabilecektir. Bu protokolün ABA'lar için nasıl kullanılabileceğine bakmadan önce, protokol yapısını ve çalışmasını incelemekte fayda görülmektedir.

3.1 SIP – Session Itiation Protocol

SIP bir veya birden fazla taraf arasında oturum oluşturmak, yönetmek ve sonlandırmak için kullanılan bir kontrol protokolüdür.

Aslında SIP direk olarak oturumları tanımlamaz, SIP ile taşınan mesajlar oturumları tanımlar.

Genel olarak SIP oturum oluşturmakla ilgilenir. Bunu yapabilmek için de bir oturumu başlatacak tarafın, karşısındaki tarafın nerede olduğunu bilmesi gereklidir. Burada karşı tarafın yerinin, karşı taraf hareket etse bile bulunabilmesi gerekliliği ortaya çıkar. Bu sayede bir kişiye bulunabileceği olası yerlerden herhangi birisinde ulaşılabilir.

Karşı tarafın yeri belirlendikten sonra, sıra karşı tarafa davet edileceği oturumla ilgili bilgi vermeye gelir. SIP oturumları oluşturan protokoller hakkında bilgi taşır. Bunu mesajlarda taşıdığı MIME[15] uzantıları sayesinde yapabilmektedir. Oturumları tanımlamak için ise diğer protokoller kullanılır, en sık kullanılan oturum tanımlama protokolü SDP[16] dir.

Davet karşı tarafa gönderildikten sonra, sıra karşı tarafın bu davete bir yanıt yollamasındadır. Bu yanıt kabul, red, meşgul gibi yanıtlar olabilir. Eğer bir kabul yanıtı gelirse, oturum başlatılmış demektir ve karşı tarafa yanıtın alındığına dair bir onay mesajı yollanır. Eğer diğer yanıtlar geldiyse, gerekli tepki oluşturulur.

SIP ayrıca devam eden oturumları değiştirebilir. Bunu oturumu başlatan davetin belli yerlerini değiştirip tekrar yollayarak sağlar. Yani devam eden oturumu yeni davet mesajlarıyla istenilen biçimde devam ettirebilir.

SIP'in en son görevi ise devam eden oturumları sonlandırmaktır. Bunu da göndereceği sonlandırma mesajlarıyla yapacaktır.

3.1.1 SIP nasıl çalışır

Temelde SIP istekler ve yanıtları kullanarak çalışır. Oturum başlatmak için kaynak bir davet (INVITE) mesajını hedefe yollar. Bunu yönlendirme ve paketleri hedefe iletmeyle görevli SIP Proxy sunucuları denilen aygıtlar vasıtasıyla yapar. Yanıt da isteğin hedefe gittiği yoldan geriye döner.

SIP'te kullanılan adresleme URL formatına benzer bir yapıdadır. Genel biçim: sip:kisiismi@domain.uzantı şeklindedir.

İki taraf arasında oturumu başlatan ve yöneten UA (User Agent) araçlarıdır. Oturumu başlatacak tarafta bulunan, yani isteği yapan UAC (User Agent Client), oturum açma isteğine yanıt veren ise UAS (User Agent Server) ismi verilen uygulamalardır.

Bazı durumlarda bir kullanıcının birden fazla yerde bulunması ihtimaline karşı bazı proxy sunucular, istekleri birden fazla hedefe gidecek şekilde çoğaltabilirler (forking). Bu sayede kullanıcı muhtemel konumlarından herhangi birinde bu isteği alabilir.

SIP kendisinden daha alttaki iletim (Transport) ve ağ (Network) katmanlarıyla ilgilenmez. Kendi güvenilir iletimini sağlamakla yükümlüdür. TCP[17], UDP[18] ve de gerekirse ATM[19], IPX[20], Frame Relay[21] protokollerini de kullanabilir.

3.1.2 SIP işleyişi

SIP'in istek-yanıt mesajlarına bağlı olarak çalıştığını söylemiştik. Yani bir oturum oluşturmak isteyen taraf bu isteğini karşı tarafa bir istek mesajıyla gönderir. Bu mesajın hedefe iletilmesi, SIP ara elemanları tarafından sağlanır. Bu isteğe ise bir yanıt mesajıyla uygun cevap verilir ve bu mesaj da aynı istek mesajıyla aynı şekilde (ama ters yoldan) hedefine iletilir. Protokolün çalışmasını daha iyi anlayabilmek için işleyişini adım adım inceleyelim. Burada "anadolu.edu.tr" domainindeki Ahmet, "ogu.edu.tr" domainindeki Mehmet ile bir

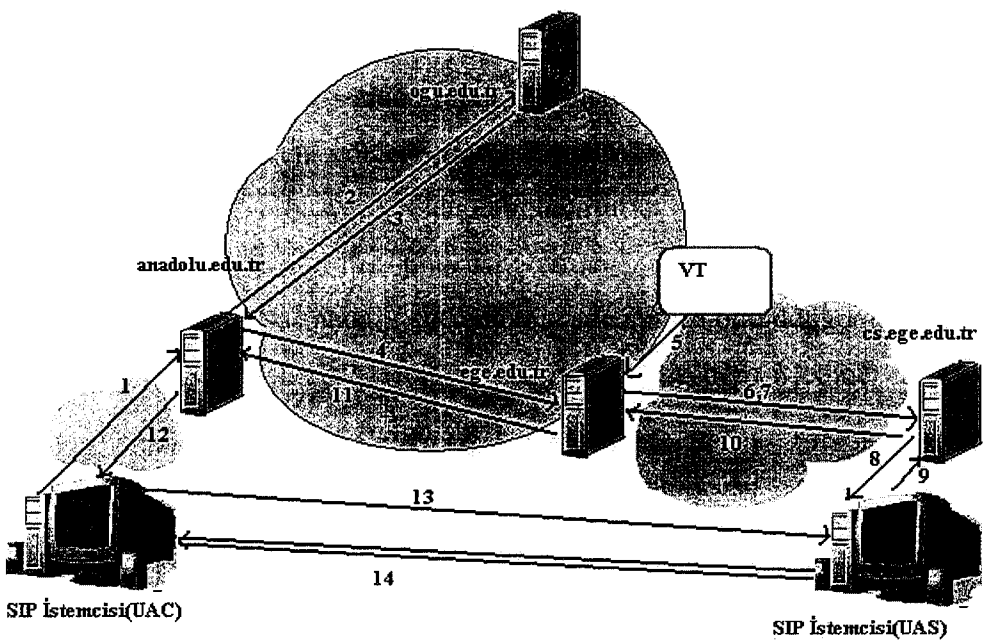
oturum başlatmak istiyor. Bu oturumun başlatılmasındaki adımları(Şekil 3.1) tek tek inceleyelim;

Adım 1.Ahmet (ahmet@anadolu.edu.tr) oturum açma isteğinin Mehmet'e (mehmet@ogu.edu.tr) iletilebilmesi için, isteğini kendisine en yakın noktada bulunan proxy sunucusuna (üniversitenin proxy sunucusu olan "anadolu.edu.tr") iletir.

Adım 2.Bu proxy Mehmet'ten aldığı istek mesajını hedefin bulunduğu domain olan "ogu.edu.tr" sunucusuna kadar iletir. Bu bir proxy sunucusu değildir. Bu bir yeniden yönlendirme (redirect) sunucusudur ve istek sahibine hedefin başka bir yerde olduğunu belirtir.

Adım 3.Yeniden yönlendirme sunucusu veritabanlarını inceleyerek istek sahibine, Mehmet'in şu anda "ege.edu.tr" adresinde bulunduğunu bildirir. Bu sunucu söz konusu bilgiyi ise daha önceden Mehmet'in kendisine bildirmesi sonucu öğrenmiştir.

Adım 4.Bu durumda "anadolu.edu.tr" proxy sunucusu, isteği direk olarak Mehmet'in şu anda bulunduğu "ege.edu.tr" domainin sunucusuna iletir.(mehmet@ege.edu.tr)



Şekil 3-1 SIP İşleyişi

Adım 5."ege.edu.tr" sunucusu kendi veritabanına bakarak Mehmet'in o anda nerede olduğunu bulur.

Adım 6.Veritabanından gelen bilgiye göre Mehmet'in yeri bulunur ve isteğin gideceği adres ortaya çıkarılır. (mehmet@cs.ege.edu.tr)

Adım 7.İstek belirlenen adrese yollanır. Mesaj hedefine giderken ilk olarak cs bölümünün proxy sunucusuna gelir.(cs.ege.edu.tr)

Adım 8. cs bölümünün proxy sunucusu kendi veritabanına bakarak Mehmet'in hangi bilgisayarda (veya SIP aygıtında) bulunduğunu belirler. Bu bilgiyi de daha önceden kullanıcıların gerçekleştirdiği kayıt (REGISTER) işlemlerinin sonucunda oluşan veritabanından elde eder. Ve istek Mehmet'in o anda başında oturduğu bilgisayarın UAS'ına iletilir.

Adım 9-10-11. Mehmet kendisine en uygun yanıtı oluşturur. Bu yanıt kabul, red, yönlendirme olabilir. Bu yanıt istek sahibine proxy sunucuları aracılığıyla geldiği yoldan geri iletilir.

Adım 13.İstek sahibi, yanıtı aldıktan sonra karşı tarafa yanıtı aldığına dair bir alındı bilgisi yollar. Bununla birlikte artık oturum oluşturulmuş olur.

Adım 14.İletişim başlar.

3.1.3 SIP'in avantajları

Bir protokolün veya teknolojinin kullanılabilmesi için, kullanım amaçlarına uygun çeşitli özellikleri olmalı ve benzer protokollere göre bazı avantajlar sunmalıdır. SIP'in sahip olduğu avantajları şöyle özetleyebiliriz.[22]

- Sağlayabileceği Hizmetler: URL lerin kullanılması, MIME içerikleri taşıyabilmesi, e-mail tarzı yönlendirme desteklemesi (sip:ahmet@anadolu.edu.tr) gibi nedenlerle diğer uygulamalarla uyumluluk sağlayabilen bir protokoldür. Bu sayede birçok hizmeti rahatlıkla sağlayabilir.
- Ölçeklenebilirlik: Genelde Internet'in ölçeklenebilirliğine benzer bir yapı sunar. Merkezde basit işlevler hızlı bir şekilde yerine getirilirken, dışta

daha akıllı ama daha az yoğun hizmetler yerine getirilir. Bunun için de çeşitli proxy sunucu tipleri tanımlanmıştır;

- Çağrı durumunu tutan proxyler (call-stateful): Genelde yapının kenarlarına yakın yerleştirilen, çağrıların durumlarını tutarak bunlara göre hizmetler sunan proxylerdir.
- Hareket durumu tutan proxyler (transaction-stateful): Merkeze yakın bulunan, sadece istek ve yanıtları izleyen proxylerdir. Çağrı durumu veya oturum hakkında bilgi tutmazlar. Çağrı kabul edildiğinde bununla ilgili tutulan bilgiler unutulur.
- Durum tutmayan proxyler (stateles): İstekleri yönlendiren ve unutan proxy sunuculardır. Merkezde bulunurlar.

- Genişletilebilirlik: SIP genişlemeleri destekleyebilecek bir yapıya sahiptir. Bu genişlemeler genel olarak yeni mesajlar tanımlanması yoluyla meydana getirilir. Bu mesajları kullanacak tarafların oturum başında hangi mesajları kullanacaklarını belirlemesi gereklidir. Bu sayede her durumda oturum oluşturmak mümkün olmaktadır.
- Esneklik: SIP genel ağ yapısını, ağda bulunan aygıtları vs. belirlemez, bunları uygulamalara bırakır. Bu sayede uygulamaların genel olarak esnek bir yapıya sahip olması sağlanmış olur.

3.1.4 SIP mesajları

SIP temelde metin bazlı ve HTTP[23] temelli bir protokoldür. Kullanılan mesajlar ve bunların başlık alanları HTTP'de kullanılanlara çok benzer. Daha önce de belirttiğimiz gibi SIP mesajları ya bir istemciden sunucuya yapılan bir istek, ya da sunucudan istemciye gönderilen bir yanıttır.

- İstek Mesajları: İstek mesajları, bir istemcinin karşı taraftan almak istediği hizmeti(tipik olarak oturum başlatma) bildirmek için kullandığı mesajlardır. Temel SIP mesajlarının yanında (Çizelge 3.1), protokole yapılabilecek eklentilerle ihtiyaca göre yeni istek mesajları da tanımlanabilir. İstek mesajları, mesajın tipini belirten yöntem ismiyle başlarlar.

Çizelge 3.1 SIP İstek Mesajları

Yöntem	Amacı
INVITE	Oturum başlatma
ACK	Oturum başlangıcı için alındı bilgisi
OPTIONS	Sunucunun desteklediği yöntemleri öğrenmek
BYE	Oturumu sonlandırmak
CANCEL	Bekleyen bir çağrıyı sonlandırmak
REGISTER	Kullanıcının konumunu kaydetmek

- Yanıt Mesajları: Yanıt mesajları (Çizelge 3.2), isteği alan tarafın isteğe verdiği yanıtla ilgili bir durum kodu taşır. Bunlarda da HTTP yanıt kodlarına benzer bir yapı vardır. SIP yanıt kodları genişletilebilir bir yapıya sahiptir, ve bunlar belli sınıflara aittir. Bir yanıt kesin olarak anlaşılmasa bile hangi sınıfta olduğunun anlaşılması yeterlidir. Genel olarak iki tip kod vardır, nihai ve nihai olmayan kodlar. Bunlardan ilki kesin karar bildirirken, ikincisi bilgilendirme amaçlı kullanılır ve nihai kod taşıyan bir mesajla takip edilirler.

Çizelge 3.2 SIP Yanıt Mesajları

Durum Kodu	Anlamı	Örnek
1xx	Bilgi mesajı	100-Trying:Deneniyor
2xx	Başarı	200-OK:İstek kabul edildi.
3xx	Yönlendirme	300-Multiple choices:Birden fazla olası konum
4xx	İstemci hatası	401-Unauthorized:Kullanıcı yetkisiz
5xx	Sunucu hatası	503-Service Unavailable:Hizmet kullanılabilir değil
6xx	Genel başarısızlık	600-Busy everywhere:Bütün olası konumlarda meşgul.

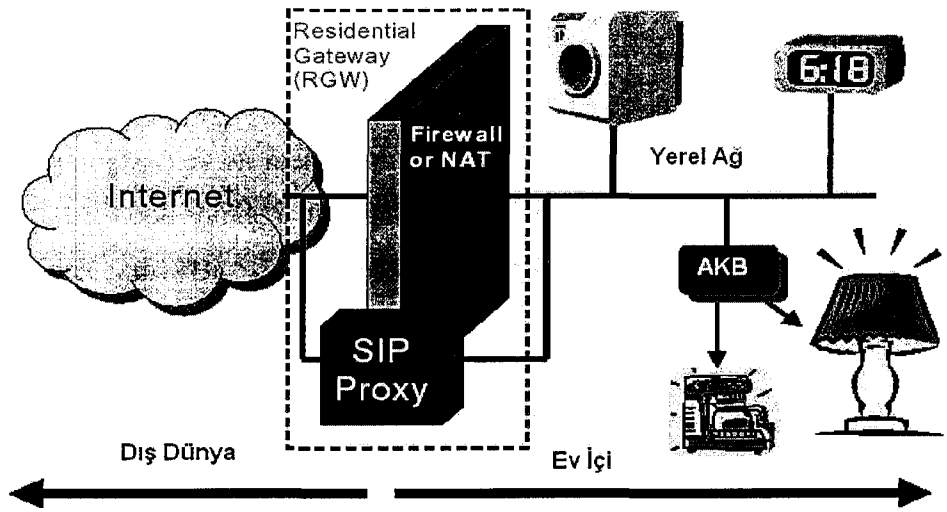
3.2 ABA Kontrol ve Kumandası için SIP Kullanımı

Daha önceden de bahsedildiği gibi, SIP istek ve yanıt mesajları ABA kontrol ve kumandası için kullanılabilir. Tipik bir uygulamayı aşağıda görebiliriz(Şekil 3.2). Aygıtlara komutları göndermek için davet (INVITE) mesajları kullanılabilir. Taşınacak komut, bu mesaj içerisinde hedefe iletilebilir. Bu komut sonucu ortaya çıkan yanıt da yine SIP yanıt (REPLY) mesajları içerisinde isteği yapana iletilir. Bu şekilde yapılmak istenen iş (tipik olarak ABA kontrol veya kumandası) ek bir mekanizmaya gerek kalmadan yerine getirilebilir.

SIP'in ABA kontrolünde kullanılabilmesi için üzerinde bazı uyarlamalar yapılması gerekecektir. Bu sayede protokol, daha önceden sıralanmış olan gereksinimleri karşılayabilecek hale gelecektir.

3.2.1 Değişiklikler ve eklentiler

Yukarıda ele alınan beklentileri yerine getirebilmek için, SIP üzerinde şu değişikliklerin yapılması önerilmektedir[4].



Şekil 3-2 ABA Kontrol ve Kumandasında SIP Kullanımı

3.2.1.1 Adresleme

SIP'te To ve From başlık alanlarındaki isimler URL olarak kodlanmıştır. Varolan uygulamalar SIP ve PHONE URL'lerini desteklemektedir. Protokolün doğası değiştirilmeden kullanılan URL tipi değiştirilebilir. Bu da kullanıcı dostu adreslemeye izin verir. Örneğin kısaltmalar kullanılabilir.

Kullanılacak Base64 kodlaması sayesinde kısaltmalar belli bir adresin dışarıdan anlaşılamayacak şekle girmesini sağlayabilir,

Örn: a454545545@ali.ev.net

Bu sayede varolan <varlık>@<yer> şeklindeki yapı korunmuş olur.

Bunun yerine standart SIP URL de kullanılabilir. Hatta hiyerarşik bir adresleme de kullanılabilir(örn: lamba.yatakodasi@ali.ev.net)

3.2.1.2 Yeni uyarım yöntemleri

SIP ilk olarak çağrı başlatma işlemleri için ortaya çıkarılmıştır. Temelde iki taraf arasında devam edecek iletim kanallarını oluşturabilmek için, bunlar arasında bir ilişki veya oturum oluşturmak amaçlanmıştır. Bu yapı, eğer bağlantı kurma kısmı kaldırılırsa, kısa süreli iletişimler için de destek sunabilir.

SIP'i ABA'larda kullanabilmek için yeni bir yöntem tanımlanmıştır[4]. Bu yeni yöntem DO yöntemidir. Bu yöntem, yukarıda belirlenen gereksinimleri sağlar ve SDP dışındaki yükleri de taşıyabilir. Yük olarak her türlü MIME tipi kullanılabilir ve de özel aygıtlar için kullanılacak belli hareket dilleri de yeni tanımlanacak MIME tipleri sayesinde taşınabilir. DO hedefteki aygıt için geçerli komutu taşır(örn: Lambayı aç). Bu komut basit bir yanıtı tetikler, bu yanıtta işlemin sonucu da bulunur ve standart SIP yanıt mekanizmasıyla isteği yapana iletilir.

3.2.1.3 Yeni yük tipleri

SIP INVITE mesajları için tipik MIME yükü SDP'dir(Session Description Protocol)[16]. ABA'lar için, aygıtlarla iletişime özel bir yük tipi gerekmektedir.

Bunun için de DMP (Device Management Protocol) isimli yeni bir MIME tipi tanımlanmaktadır.

Buna ek olarak, bir aygıt proxy sunucusuna yer kaydı yaptırdığı zaman(REGISTER mesajıyla), bu aygıta ait tanımlamalar söz konusu proxy sunucusuna taşınmalıdır. Bunun için de tanımlama için kullanılacak protokol DDP(Device Description Protocol) kullanılabilir.

3.2.1.4 Bildirim/Olaylar

ABA'larla senkron iletişim yanında, asenkron bir iletim de gereklidir. Örneğin evinizdeki bir alarm çalıştığında, ev sıcaklığı belli değerleri aştığında ya da ön kapı zili çaldığında ev sahibinin haberdar edilmesi gerekecektir.

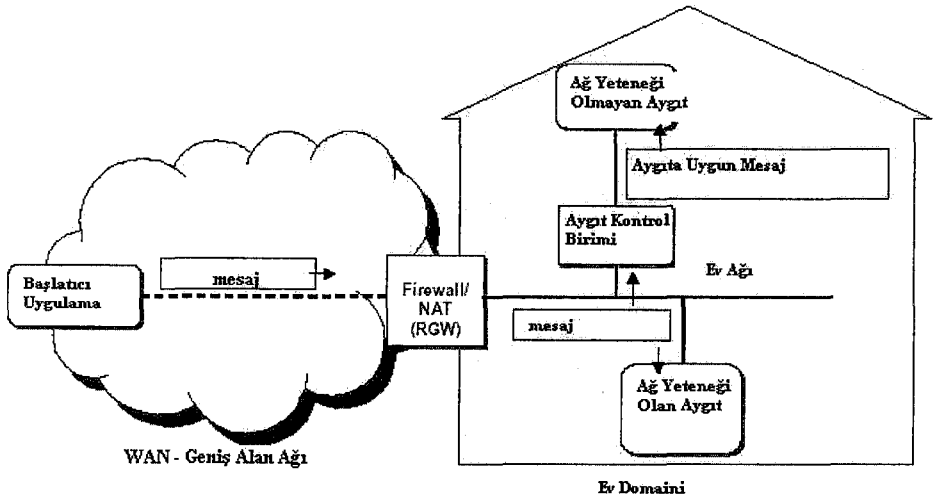
SIP olay bildirim yapısı, temel olarak SUBSCRIBE ve NOTIFY mesajlarına bağlıdır.Bu mesajlar düzgün bir adresleme yapısıyla kullanıldığında aygıtların olay bildirimi yapması mümkün olacaktır.

3.3 Örnek Ağ mimarileri

SIP kullanılarak ABA kontrolünde, temel olarak iki tipteki mimari kullanılır. İlk mimaride, istemciler direk olarak ev domaini ile iletişim yapabilmektedirler. Bu durumda eve erişim için herhangi bir ara noktaya erişme gereksinimi ortaya çıkmamaktadır. İkinci mimaride ise, istemciler evdeki aygıtlarla iletişim yapabilmek için eve giriş noktasındaki proxy sunucu ile iletişim yapmaktadırlar.

3.3.1 Ev domaini ile direk olarak iletişim

Bu mimari istemcilerin direk olarak ev domainindeki aygıtlarla iletişim yapmasına izin verir (Şekil 3.3). Geniş alan ağı, mesajları istemciden evin giriş noktası olan Firewall/NAT'a kadar iletir. Bu mesajlar firewall tarafından incelenir ve eğer istenen kurallara uygunsa içeri girmelerine izin verilir. Ev domaini içerisinde de mesajlar yerel alan ağı tarafından hedef aygıta kadar iletilir.



Şekil 3-3 Eve Direk Erişim

Bu aygıtlar kendileri halihazırda ağ yeteneğine sahip olabilecekleri gibi, aygıt kontrol arabirimleri aracılığıyla da bu ağ yeteneklerini elde edebilirler ve bu sayede iletişim yapabilirler.

3.3.2 Geçit proxy sunucusu üzerinden iletişim

Çoğu durumda istemcilerin direk olarak eve erişimine ve aygıtları yönetmesine izin vermek mümkün olmayabilir yada istenmeyebilir. Bu birkaç nedenden dolayı olabilir;

- Erişilmek istenen aygıtın IP adresi, bu aygıt bir NAT arkasında olduğundan dolayı belirlenemeyebilir.
- Erişilmek istenen aygıtın geçerli bir IP adresi yoktur.
- Belli güvenlik nedenlerinden dolayı evdeki aygıtların dışarıdan görünebilmeleri istenmeyebilir.
- Evdeki Firewall/NAT bilinmeyen kaynaklardan gelen iletişimi filtreleyebilir ve engelleyebilir.
- Daha yüksek seviyede güvenlik istenebilir(aygıt/mesaj bazında kimlik denetimi, erişim kontrolü vs.)

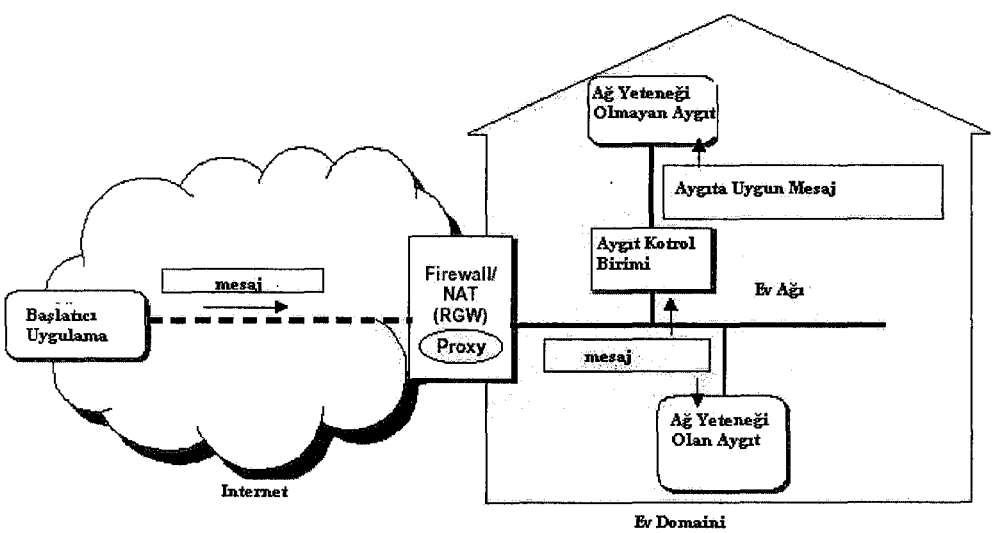
Bu durumda istemcinin gönderdiği kontrol mesajları ilk olarak ev içerisini görebilen, güvenilir bir proxy sunucusuna gönderilir (Şekil 3.4). Burada bu proxy

ve evdeki Firewall/NAT arasındaki iletişimin zaten güvenli olduğu varsayılmaktadır. Bu durumda Proxy ev girişindeki ağ geçidinin içerisine yerleştirilmiştir. Bu proxy aşağıda sıralanan işlevleri yerine getirmektedir;

- Her istek/mesajın kimliğini denetlemek ve yetkilendirmek,
- Ev domaini içerisindeki adresleme eşleştirmesi/çözümlemesini yapmak,
- Dış dünyayla iletişimde Firewall/NAT güvenli bir proxy rolü üstlenmek,
- ABA'ların taşınabilirlik ve izlenebilme hizmetlerini sağlamak,
- İstemci uygulamaları için mesaj protokol eşleştirmesi yapmak,
- Hizmetler için bir yükleme noktası olmak

3.3.3 SIP mimarisinin temel bileşenleri

Bu bölümde ABA kontrol ve kumandası için SIP kullanılarak oluşturulacak mimaride kullanılabilecek temel bileşenler ele alınacaktır. Bu bileşenleri daha iyi anlayabilmek için bir örnek mimari kullanılacaktır. Burada bu bileşenler işlevsel bloklar olarak gösterilecek, daha sonra da bunların fiziksel olarak nasıl gerçekleştirilebileceğine dair örnekler verilecektir.



Şekil 3-4 Geçit Proxy Sunucusu Üzerinden Erişim

- SIP UA (Başlatıcı domain): Bu SIP UA'sı, başlatıcı uygulama tarafından aygıtlara gönderilecek mesajların oluşturulması ve bunların ev RGW'si veya Hizmet Sağlayıcı tarafından sağlanan SIP Proxy sunucusuna gönderilmesinde kullanılır. Kısacası istemci tarafındaki uygulamadır.
- SIP Proxy (Hizmet sağlayıcı domaini): Bu SIP Proxy, yer belirleme veritabanına bakarak iletişim kurulmak istenen aygıtın nerede bulunduğunu(ev domain RGW sinin yerini de içerir) çözümler. İstemcinin SIP UA'sından gelen aygıt mesajları, ev domainindeki RGW'nin SIP Proxy'sine iletir veya güvenli bir kanaldan hedefteki aygıtın UA'sına iletir.
- Yer belirleme veritabanı (Hizmet sağlayıcı veritabanı): Ev domainindeki bütün kayıtlı aygıtların yer bilgileri bu veritabanında tutulur. Bu veritabanındaki bilgiler, Hizmet sağlayıcı SIP Proxy'si ve/veya diğer ev içi yer belirleme hizmetleriyle elde edilen bilgilerin toplanmasıyla oluşturulur.
- SIP Proxy (Ev domain RGW): Ev domain RGW'si içerisindeki SIP Proxy, ev domainindeki aygıtlar ve geniş alan ağındaki varlıklar arasındaki ağ geçididir. Firewall veya NAT gibi diğer RGW işlevleri de RGW SIP Proxy'si ile birlikte yer alabilir.
- SIP UA (Aygıt Kontrol Birimi/RGW): Başlatıcı SIP UA'sından gelen aygıt mesajları, bu SIP UA'sında sonlandırılır. Mesajlaşmayla ilgili bilgileri SIP mesajının içerisinden alır ve bunu Interworking Unit'e iletir. Bu SIP UA'sı RGW içerisinde veya Aygıt Kontrol Birimi içerisinde yer alabilir. SIP UA'lardan Aygıt Kontrol Birimine yapılan eşleştirme (mantıksal) 1:N dir.
- Aracı Birim (Aygıt Kontrol Birimi-AKB): SIP mesajı içerisinde taşınan Aygıt mesajını, aygıta özel protokole eşleştirir. Kısaca ağ yeteneği olmayan aygıtlara ağ yeteneği kazandırır.
- SIP UA (Ağ yeteneği olan aygıt): Bu SIP UA'sı ağ yeteneği olan aygıtlarda bulunur. Başlatıcıdan gelen SIP Aygıt Kontrol mesajlarının

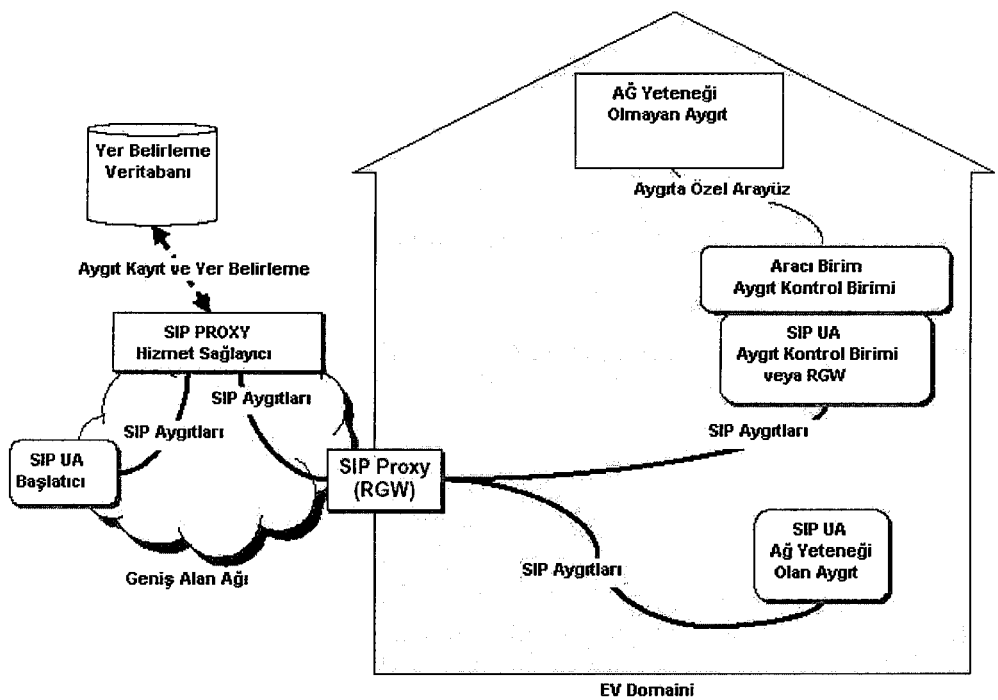
sonlandırıldığı noktadır ve aygıt uygulaması için gerekli aygıt kontrol verisini bu mesajlardan çıkarıp başka bir aracı ağ biriminin yardımına ihtiyaç duymadan işleyebilir.

- Ağ yeteneği olmayan aygıtlar: Bunlar herhangi bir ağ yeteneğine sahip olmayan, Aygıt Kontrol Birimleri tarafından kontrol edilen ve istemci uygulamalarıyla iletişim için aracı birimlere ihtiyaç duyan aygıtlardır.

Yukarıda tanımlayabileceğimiz en önemli ara yüzler;

- SIP[Aygıtlar]: Bu ara yüz kullanılan yöntemle birlikte SIP'i ifade etmektedir.
- Aygıt Kayıt ve Yer Belirlemesi: Yer belirleme veritabanına erişmek için kullanılacak herhangi bir veritabanı güncelleme ve arama protokolüdür.
- Aygıta özel ara yüzler: Interworking Unit sayesinde SIP mesajları aygıtın anlayabileceği kendi özel dile çevrilir.

Yukarıda anlatılan bileşenler ve evdeki kullanımları Şekil 3.5'te görülebilir.



Şekil 3-5 SIP Mimarisinin Temel Bileşenleri

3.4 SIP Güvenlik Hizmetleri ve ABA İletişiminde Kullanımı

Çalışma mantığına, iletişim biçimlerine, taşıdığı içeriğe bakıldığında SIP temelde güvenli hale getirilmesi gayet zor bir protokoldür. İletimde aracılar kullanması (Proxy sunucular), kurulması gereken çok yüzlü güven ilişkileri, protokolün aralarında güven ilişkisi bulunmayan elemanlarla çalışmasının beklenmesi güvenliğin sağlanabilmesini basitlikten uzaklaştırır. Değişik seviyedeki ve kapsamdaki ihtiyaçlara cevap verebilmek için, birçok faklı mekanizma geliştirilmiştir.

SIP iletişim güvenliği, SIP ile birlikte kullanılan protokollerin (RTP[24] gibi) güvenliği ile yada SIP ile taşınan gövdelerin güvenlik uygulamalarıyla (MIME[15] güvenliği SIP güvenliğinde önemli rol sahibi olduğu halde) ilgilenmez. Bir oturumla ilgili herhangi bir iletim ortamı, ilgili SIP iletişiminden bağımsız olarak uçtan uca şifrelenebilir.

SIP güvenliği konusunda ilk olarak klasik tehditler ele alınacak sonra bunların çözümü için gerekli hizmetler anlatılacaktır. Bundan sonra ise bu hizmetlerin sağlanabilmesi için kullanılabilecek yöntemler detaylandırılacaktır. En son olarak da SIP uygulayıcılarının yerine getirmesi gereken beklentiler sıralanacak ve bunların yerine getirilmesiyle ilgili örnek durumlar sıralanacaktır.

3.4.1 Saldırılar ve tehdit modelleri

Bu konuda birçok SIP uygulaması için ortak olan tehditler ele alınacaktır. Burada gösterilen tehditler, SIP'in ihtiyaç duyduğu güvenlik hizmetlerini daha iyi gösterebilmek için özel olarak seçilmiştir.

Burada sözü edilen tehditler, direk olarak sadece SIP'i etkileyen tehditler değildir, bunların çoğu tehditleri engelleyebilecek güvenlik hizmetlerini gösterebilecek niteliklere sahip klasik tehditlerdir.

Burada sözü edilen saldırılarda, herhangi bir saldırganın ağdaki bütün paketleri alıp okuyabildiği, SIP'in Internet üzerinde kullanıldığı bir yapı varsayılmıştır. Saldırganlar, ağda yol alan paketleri değiştirebilir, (kullanmaya hakkının olmadığı) hizmetleri çalabilir, iletişimi dinleyebilir veya oturumlara zarar verebilir.

3.4.1.1 Sahte yer kayıtları

SIP kayıt mekanizması, UA'ların kendilerini kayıt edilecekleri yere (Registrar) belli bir kullanıcının bulunduğu adres olarak tanıtmasına izin verir. Yani kayıt işleminden sonra, söz konusu kullanıcının erişilebileceği adres veya olası adreslerden birisi, kaydedilen UA olacaktır. Registrar, From başlık alanıyla iddia edilen kimliği değerlendirir ve bu kayıt ("REGISTER") isteğinin To başlık alanındaki kayıtlı adresi değiştirme yetkisi olup olmadığını kontrol eder. Bu iki başlık alanı genelde aynıdır ama bazen başkasının yerine üçüncü bir kişi kayıt işlemini yapabilir.

SIP isteklerinin From başlık alanındaki değer, UA sahibi tarafından gelişigüzel olarak değiştirilebilir, bu da kötü niyetli kayıt işlemlerine açık kapı bırakmaktadır. Mesela bir saldırgan, herhangi bir kayıtlı adres üzerinde değiştirme yetkisi olan bir kullanıcıyı taklit ederek, bir kullanıcı için daha önceden kaydedilmiş bütün bağlantı adreslerini kaldırıp, kendi kontrolündeki bir aygıtı bu kullanıcının bağlantı adresi olarak kaydedebilir. Bundan sonra söz konusu kullanıcıya ait bütün mesajlar saldırganın belirlediği noktaya gidecek ve gerçek sahibine ulaşamayacaktır. Bunun sonucu olarak ya söz konusu kullanıcı hizmetlerden yararlanamayacak, ya da bu durumdakine benzer birçok yanlış kaydın tek bir noktayı hedeflemesi ile hedefteki noktaya büyük miktarda veri yollanacaktır.

Söz konusu tehdit, bir isteğin sahibinin kim olduğunu garanti etmek için kullanılan kriptografik yöntemlerin sistemde yer almaması sonucu ortaya çıkan tehditlerdendir. Herhangi bir hizmet sunan UAS, bu hizmetini kullanmak isteyen kişinin kimliğini denetleyerek kaynaklarına erişimi kontrol altına alabilir. Hatta son kullanıcıların UA'ları bile istek sahiplerinin kim olduğunu ortaya çıkarmaya ve kimliğini denetlemeye çalışır.

Bu tehdit, istek sahiplerine kimlik denetimi uygulama zorunluluğunu ortaya çıkarır. Bu sayede sahte ve kötü niyetli kayıt işlemlerinin önüne geçilebilir.

3.4.1.2 Sunucu taklidi

Bir isteğin hangi domaine gittiğini genellikle isteğin Request-URI başlık alanındaki değer belirler. UA'lar isteklerini iletebilmek için genellikle hedefin bulunduğu etki alanındaki bir sunucuya direk olarak bağlanırlar. Böyle bir yapıda her zaman bir saldırganın uzaktaki sunucuyu taklit etmesi yani UA'nın isteğinin yolunun kötü niyetli ara elemanlarca kesilmesi mümkündür.

Örneğin bir domaindeki Redirect sunucusu (chicago.com), başka bir domaindeki sunucuyu taklit edebilir (biloxi.com). Bir UA isteğini biloxi.com'a yollar, fakat chicago.com bu isteğe sanki biloxi.com dan geliyormuş havasını vermek için uygun başlık alanlarını kullanarak oluşturduğu yanıtı yollar. Bu sayede yanlış bağlantı adresini istek sahibine bildirerek, istek sahibinin yanlış yere yönlenmesini veya en azından istediği yere erişemeyerek hizmetten yararlanamamasını sağlar.

Bu tehditler ailesinin çok sayıda üyesi vardır ve de bunların çoğu kritik öneme sahiptir. Sahte kayıt yapma saldırısına karşı olarak, şu durum ele alınabilir. Gönderilen bir kayıt isteği (biloxi.com'a), başka biri tarafından karşılanabilir (chicago.com) ve bu isteğe sahte bir 301 (Moved Permanently – Kalıcı olarak yer değiştirmiş) mesajıyla yanıt verilebilir. Bu durumda yanıt biloxi.com dan gelmiş gibi gözükür ve bundan sonraki registrar olarak chicago.com gösterilebilir. Bundan sonraki bütün kayıt işlemlerinin bu adrese yönlendirilmesi sağlanabilir.

Bu tip tehditleri önlemenin yolu ise, kayıt yaptırmak isteyen UA'ların kayıt isteklerini yollayacakları sunucuların kimliklerini denetlemesidir.

3.4.1.3 Mesaj gövdelerini değiştirmek

Olağan olarak UA'lar isteklerini güvendikleri sunucular üzerinden yollarlar. Bu güvenin nasıl oluştuğuna bakılmaksızın bu sunucunun mesaj gövdesine izinsiz olarak bakmadan ve değiştirmeden bu mesajı yönlendireceğine güvenilir. Bu durum da bazı hallerde açıklara meydan bırakabilmektedir.

Farz edelim ki bir UA, oturumu şifrelemek için kullanacağı anahtarları SIP mesajları ile iletiyor. Bu UA erişmek istediği domaindeki sunuculara güvense bile, bu sunucuların yöneticilerinin mesajların içerisinde taşınan oturum şifrelerini

görebilmesini istemez. Böyle bir durumda eğer bu sunucu kötü niyetli ise, oturum anahtarlarını değiştirebilir. Bu işlemi aradaki adam saldırısıyla ya da bu oturumu başlatacak tarafın istediği güvenlik özelliklerini değiştirerek yapabilir.

Bu tip tehditler sadece oturum anahtarlarına değil, SIP mesaj gövdeleriyle taşınan diğer içerik tiplerine de etki edebilmektedir. Bu içerik, kullanıcıya sunulacak MIME gövdeleri, SDP, telefon sinyalleri vs. olabilir. Saldırganlar, konuşmaları dinleyebilmek için SDP gövdelerini değiştirip oturumun kendi istedikleri(muhtemelen rahat dinleme olanaklarına sahip oldukları bir iletim ortamı) tarafa yönlendirilmesini sağlayabilirler.

Ayrıca şuna da dikkat edilmelidir ki bazı SIP başlık alanları uçtan-uca anlamlıdır (örneğin Subject). UA'lar bu alanlar için mesaj gövdelerine oldukları kadar koruyucu olabilirler. Çünkü bu başlık alanı değerleri iletimde ara elemanlar tarafından kullanılmamaktadır. Bunların koruma altın alınmaması çeşitli saldırılara açık kapı bırakabilir (örneğin kötü niyetle değiştirilen bir Subjet başlık alan değeri nedeniyle önemli bir istek Spam olarak algılanabilir). Bu tip alanlar iletimde şifrelenerek gönderilebilirler. Fakat birçok başlık alanı ara elemanlar tarafından kurallara uygun şekilde değiştirilebildiğinden, bütün başlık alanları uçtan uca güven altına alınmamalıdır (yani şifrelenmemelidir). Bu tip alanların açık olarak kalması, SIP çalışması için gereklidir.

Bu nedenlerden dolayı UA'lar SIP mesaj gövdelerini ve sadece bazı başlık alanlarını uçtan uca güven altına almak isterler. Mesaj gövdeleri için sunulan güvenlik hizmetleri, gizlilik, bütünlük ve kimlik denetimini kapsar. Bu uçtan-uca hizmetler, ara elemanlarla (proxy sunucular gibi) iletimde kullanılan hizmetlerden farklı olmalıdır.

3.4.1.4 Oturumların düşürülmesi

Daha önceden de sözü edildiği gibi, devam eden oturumlara SIP mesajları kullanılarak müdahale edilebilir ve oturumların çeşitli özellikleri değiştirilebilir. İlk mesajlaşmayla oturum kurulduktan sonra, oturumun (veya diyalogun) durumu yeni mesajlar kullanılarak değiştirilebilir. Bu tip mesajların taklit edilmesi de olasıdır. Oturumdaki kuralların belli olması bu tip isteklerin taklit edilememesini sağlar.

Farz edelim bir saldırgan iki taraf arasında oturum oluşturmak için iletilen mesajları topluyor. Saldırgan bunlar içerisinden belli başlık alanlarının (To, From, v.s.) değerlerini kopyalayıp kendi oluşturacağı oturum sonlandırma (BYE) mesajı içerisinde kullanabilir. Bu sayede saldırgan, bu mesajın oturumun taraflarından herhangi birinden geldiği izlenimi vererek oturumu zamanından önce sonlandırabilir.

Benzer oturum içi tehditler, devam eden oturumların taklit edilen re-INVITE mesajlarıyla değişik oturum özellikleriyle devam etmesini sağlayabilir. Burada oturumun sahip olduğu güvenlik seviyesi düşürülebilir, yada oturum başka bir yöne(tipik olarak saldırganın kontrolü altında olan bir yön) yönlendirilebilir.

Bu tip saldırılarla başa çıkmanın en etkili yolu, BYE mesajlarını gönderen kullanıcının kimliğini denetlemektir. Burada BYE mesajını alan tarafın denetlemesi gereken şey, bu mesajın oturumu başlatan UA'dan gelip gelmediğidir. Karşı tarafın kimliğini tamamen denetlemek gereksizdir, çünkü sadece oturumu sonlandırmak isteyenin oturumu başlatan kişi olduğunu bilmek yeterli olacaktır. Ayrıca, gizlilik özellikleri nedeniyle bir saldırganın oturumla ilgili özellikleri öğrenememesi de sahte BYE mesajlarının oluşturulabilmesini engeller. Burada yine SIP'in çalışması için gereken bir özellik karşımıza çıkmaktadır. Bazı ara elemanlar, işlevlerini yerine getirebilmek için başlık alanlarındaki çeşitli parametreleri incelemek zorundadır. Bu nedenle bunların şifrelenerek saklanması mümkün değildir.

3.4.1.5 Hizmetin engellenmesi ve çoğaltma

Hizmetin engellenmesi saldırıları temelde, bir ağ elemanının üzerine büyük miktarda trafik yönlendirilerek kaynaklarının yetersiz kalması ve bu sayede kullanılamaz hale getirilmesi şeklinde meydana gelir. Dağıtık hizmetin engellenmesi saldırılarında ise birçok ağ kullanıcısını belli bir noktaya çok miktarda paket yollaması bir tek kullanıcı tarafından tetiklenir.

Çoğu yapıda SIP proxy sunucuları tüm dünyadan erişimi sağlayabilmek için Internet ara yüzlerine sahiptir. Bu yapı göz önüne alındığında, SIP'in dağıtık hizmetin engellenmesi saldırılarına birçok yönden uygun olduğu görülebilir. Bu duruma özellikle dikkat edilmelidir.

Saldırganlar yanıltıcı bir kaynak IP adresine ve buna uygun Via başlık alan değerine sahip sahte bir istek hazırlayıp bu isteği birçok SIP elemanına yollayabilirler. Bu durumda bunların hepsi istekte bulunan yanıltıcı IP adresine (saldırının hedefine) yanıtlarını yollayacaktır. Bu da hedefte son derece fazla trafik oluşturarak hedefin ağ kaynaklarının tüketilmesini sağlayacaktır.

Benzer şekilde, saldırganlar yanıltıcı Route başlık alan değerine sahip istekler hazırlayabilirler. Bu alana hedef seçilen kullanıcının adresi yazılarak, bu isteklerin forking proxyler tarafından çoğaltılması ve de hedefe gönderilmesi sağlanabilir.

Record-Route başlık alanı da benzer şekilde kullanılabilir. Burada saldırgan başlatılan SIP diyaloğunun, diyaloğu başlatan isteğin ters yönünde birçok iletim yapacağını biliyorsa, bu başlık alanına hedefin adresi verilerek üzerine çok miktarda trafik gitmesi sağlanabilir.

Bazı hizmeti engelleme saldırıları da, REGISTER isteklerinin kimlik denetiminden geçirilmemesi veya yetkilendirilmemesi sonucu ortaya çıkmaktadır. Saldırganlar belli kullanıcıların kayıtlarını silebilir ve bu şekilde bunların erişilebilir olmasını engelleyebilir. Ayrıca saldırganlar aynı kullanıcı için birçok bağlantı noktası tanımlayarak isteklerin birçok noktaya gitmesini sağlayabilirler, bu sayede bu registrarları çoğaltıcı olarak kullanabilirler. Ayrıca saldırganlar çok fazla sayıda kayıt yaparak kayıtları tutan sistemdeki kaynakların tükenmesini ve bu sistemin işlevini yerine getiremez hale gelmesini sağlayabilir.

SIP isteklerinin çoklu gönderimle (multicast) yollanması hizmetin engellenmesi tipindeki saldırılara potansiyel sağlar.

Bütün bu problemler, hizmetin engellenmesi saldırı riskini azaltmak için genel gereksinimi ortaya koymaktadır. Ve ayrıca bu tipteki saldırıların önlenmesi için tavsiyelerin dikkatlice belirlenmesinin gerektiği anlaşılmaktadır.

3.4.2 Güvenlik Mekanizmaları

Yukarıda SIP mimarisinin karşı karşıya kalabileceği güvenlik tehditleri açıklandı. Anlatılan tehditler göz önüne alındığında SIP için gerekli temel güvenlik hizmetleri şöyle sıralanabilir[1]; mesajların gizliliğini ve bütünlüğünü korumak, tekrarlama saldırılarını ve sahte mesajları engellemek, oturumlarda

taraflar arası kimlik denetimini ve gizliliği sağlamak ve de hizmeti engelleme saldırılarını engellemek. SIP mesajlarının içerisindeki gövdeler için de ayrıca gizlilik, bütünlük ve kimlik denetimi hizmetleri sağlanmalıdır.

SIP, kendisi için yeni mekanizmalar belirlemek yerine, daha önceden HTTP[23] ve SMTP[25] için geliştirilmiş mekanizmaları uygun yerlerde ve şekillerde kullanır. Bu protokoller için zaten kendisini kanıtlamış olan ve uyumluluk problemlerini aşmış olan mekanizmalar, uygulamada kolaylık sağlamaktadır.

Aslında basit düşünülürse, mesajların tamamen şifrelenmesi iletişimin gizli olmasını en iyi şekilde sağlamaktadır, ayrıca bu sayede mesajların iletimde üzerinden geçtiği ara elemanlar tarafından değiştirilmediği de garanti edilebilir. Fakat SIP mesajları uçtan uca tamamen şifrelenemez çünkü Request-URI, Route ve Via gibi başlık alanları mesajların başarıyla iletilebilmesi için ara elemanlar tarafından görülebilir olmak zorundadır. Aynı zamanda bazı başlık alanlarının Proxy sunucular tarafından değiştirilmesi gereklidir (örneğin Via başlık alanına kendi adreslerini eklemek gibi). Bundan dolayı Proxy sunucularının belli bir seviyeye kadar güvenilir olması zorunludur. Bunun sağlanabilmesi için ise alt katman güvenlik mekanizmalarına ihtiyaç duyulur. Bunlar SIP mesajlarının tamamını noktalar arası şifreleyerek uç noktaların isteklerini yolladıkları sunucuların kim olduğunu doğrulayabilmelerine olanak sağlar.

SIP elemanları ayrıca karşılarındakini güvenli bir yolla tanımlayabilmeye ihtiyaç duyarlar. Bir SIP uç noktası kullanıcısının kimliğini karşıdaki bir UA'ya veya Proxy sunucusuna beyan ettiğinde, bu kimlik bir şekilde doğrulanabilir olmalıdır. SIP'te bu ihtiyacı gidermek için kriptografik bir kimlik denetim mekanizması sunulmuştur.

Ayrıca bağımsız bir güvenlik mekanizması uçtan uca karşılıklı kimlik denetimi için bir alternatif sağlanmaktadır. Bunun yanında UA'ların ara aygıtlara ne kadar güvenmesi gerektiğini de belirlemektedir.

3.4.2.1 Transport ve Network katmanı güvenliği

Daha önceden de belirtildiği gibi bazen güvenlik gereksinimlerini daha alt katmanların sağlaması beklenebilir. SIP de Transport ve Network katmanlarından

bazı güvenlik hizmetleri alır. Bu hizmetler TLS[26] ve IPSec[27] mekanizmalarıyla sağlanır. Bu iki katman şifreleme sayesinde mesaj bütünlüğü ve gizliliğini korur.

Çoğu zaman alt katman güvenliğini sağlamak için sertifikalar kullanılmaktadır, ve bu sertifikalar birçok mimaride kimlik denetimi için de kullanılabilir.

Yukarıda da belirttiğimiz gibi transport ve network katmanlarında güvenlik sağlayan iki protokol TLS ve IPSec'tir.

IPSec, geleneksel IP protokolünün yerine güvenlik amacıyla kullanılabilecek, network katmanında çalışan araçlardan oluşmuştur. Bu yapı genel olarak daha önceden kurulmuş güven ilişkilerine sahip hostlar veya yönetim alanlarında kullanılır. Genellikle hostun işletim sistemi seviyesinde uygulanır, ya da belli bir ara yüzden aldığı trafik üzerinde gizlilik ve bütünlük sağlayan ağ geçitlerinde kullanılabilir. IPSec ayrıca noktalar arasında da kullanılabilir.

Birçok yapıda IPSec in SIP uygulamalarıyla entegre olması gereksizdir, kullanımı SIP hostlarına direk olarak güvenlik eklemenin zor olduğu durumlarda daha uygundur. Ayrıca kendilerine en yakın Proxy sunucusu ile önceden paylaşılmış anahtar ilişkisine sahip UA'lar da IPSec için uygun adaylardır. IPSec'in SIP için her bir kullanımı, SIP'i güvenli hale getirmek için kullanılacak protokol araçlarının tanımlandığı bir IPSec profiline ihtiyaç duyar.

TLS ise bağlantı temelli (connection oriented) protokoller üzerinden transport katmanı güvenliği sağlar (özellikle TCP); "tls" (TCP üzerinden TLS in kısaltılması diyebiliriz), bir Via başlık alanı veya SIP-URI içerisinde istenen transport katmanı olarak tanımlanabilir. TLS, daha önceden herhangi bir güvenlik ilişkisine sahip olmayan hostlar arasında noktalar arası güvenlik kurmak için uygundur. Örneğin Ali kendi yerel Proxy sunucusuna güvenmektedir ve bu Proxy de bir sertifika alışverişinden sonra Ahmet'in yerel Proxy sunucusuna güvenmektedir, son olarak da Ahmet kendi yerel Proxy sunucusuna güvenmektedir. Bu durumda Ali ve Ahmet arasında güvenli bir iletişim yolunun varlığından söz edilebilir, yani bu iki kullanıcı güvenle iletişim yapabilirler.

TLS, SIP uygulamalarıyla sıkıca birleştirilmek zorundadır. Şu not edilmelidir ki SIP'te transport mekanizmaları noktalar arası olacak şekilde

belirlenmiştir, bundan dolayı isteklerini bir Proxy sunucusuna TLS bağlantısı üzerinden yollayan bir UA, TLS'in uçtan uca kullanılacağından emin olamaz.

3.4.2.2 SIPS URI yapısı

Güvenli bir iletim için SIPS URI yapısı kullanılabilir[1]. SIPS URI yapısı temelde SIP URI yapısına sadık kalmaktadır. Burada sadece yapıyı belirten string "sip" yerine "sips" tir. SIPS'in anlamsal yapısı ise SIP URI den çok farklıdır. SIPS çeşitli kaynakların güvenli olarak erişilmek istenmesine olanak sağlar.

SIPS URI kullanıcıların kayıtlı adresi olarak kullanılabilir. Yani o kullanıcının tanınmasını sağlayacak URI olarak kullanılabilir (kartvizitlerinde, isteklerinin From başlık alanında, REGISTER isteklerinin To başlık alanında kullanılabilir). Bir isteğin Request-URI başlık alanında SIPS yapısı kullanıldığında, mesajın Request-URI başlık alanının domain kısmıyla ilgili kısmını işleyecek SIP varlığına giderken geçeceği bütün noktalarda, TLS kullanılarak güvenlik sağlanmak zorunda olduğunu belirtir. Mesaj domaine girdikten sonra ise, bu domainin yerel güvenlik ve yönlendirme planına göre ele alınır. Yine burada da UAS'a ulaşacak son noktaya kadar TLS kullanılması muhtemeldir. SIPS bir isteğin göndericisi tarafından kullanılırsa (SIPS URI'nin hedefin kayıtlı adresi olarak belirlendiği durumdaki gibi), isteğin hedef domaine gidinceye kadar geçeceği yolun güvenli olmasını ister.

SIPS yapısı, SIP URI'lerinin kullanıldığı çoğu yerde kullanılabilir (Request-URI'ye ek olarak). Buna kayıtlı adres, Contact-Address, Route başlık alanları dahildir. Bu durumların her birinde, SIPS URI yapısı bu alanların güvenilir kaynaklar olduğunu gösterir.

SIPS kullanımı karşılıklı kimlik denetimi yapılmasını gerektirir. Kimlik denetimi sırasında elde edilen sertifikalar, istemcide tutulan kök sertifikalarla doğrulanmalı ve bu işlemdeki hatalar, isteğin başarısız olmasını beraberinde getirmelidir.

SIPS URI'leri kimlik olarak kullanan ve dağıtan kullanıcılar, aygıtlarını güvensiz iletimle gelen istekleri reddedecek şekilde kullanmayı tercih edebilirler.

3.4.2.3 HTTP kimlik denetimi

SIP, HTTP Kimlik Denetimi[28] temelli, 401 ve 407 kodlu yanıt kodlarına ve kimlik denetim istekleriyle kimlik denetim bilgilerini taşıyan başlık alanlarına dayalı bir kimlik denetim yapısı sunar. HTTP Digest Kimlik Denetim yapısının üzerinde belirgin değişiklikler gerekmeksizin kullanılması tekrarlama saldırılarından koruma ve tek yönlü kimlik denetimini sağlamaktadır.

SIP'te bir UAS istek aldığı zaman karşısındaki UAC'nin kimliğini denetlemek isteyebilir. Bunun için 401 (Unauthorized) yanıtıyla kimlik denetim isteğini karşıya bildirir. Buna ek olarak Registrarlar ve redirect sunucuları da aynı şekilde kimlik denetim isteği yaparlar. Fakat Proxy sunucuları için durum değişiktir. Bunlar 401 (Unauthorized) mesajını kullanamazlar, bunun yerine 407(Proxy Authentication Required) yanıtını kullanarak kimlik denetimi isteyebilirler. Ayrıca Proxy-Authenticate, Proxy-Authorization, WWW-Authenticate ve Authorization alanlarının çeşitli mesajlarda kullanılması da RFC2617'deki kullanım gibidir.

3.4.2.4 S/MIME

Daha önce de belirtildiği gibi SIP mesajlarını uçtan uca tamamen şifrelemek protokolün çalışması açısından uygun değildir, çünkü bu masajların bazı başlık alanları SIP elemanlarının doğru çalışabilmesi için okunabilir veya değiştirilebilir olmalıdır. Bu SIP elemanları göz önüne alınmadığı taktirde, SIP mesajları yönlendirilebilir olmaktan çıkar.

S/MIME[29], UA'ların SIP mesaj gövdeleri içerisinde şifrelenmiş MIME gövdeleri gönderebilmesine olanak tanır, bu sayede mesaj başlık alanları etkilenmeden bu gövdeler uçtan uca şifrelenebilir. S/MIME mesaj gövdeleri için uçtan uca gizlilik ve bütünlük ve de ayrıca karşılıklı kimlik denetimi sağlayabilir. S/MIME'ın ayrıca SIP başlık alanlarının belli bir formda gizlilik ve bütünlüğünü sağlaması SIP mesaj tünellemesi ile mümkün olmaktadır. Bu yöntemde istenilen alanlar mesaj S/MIME gövdesi içerisinde yer alabilmektedir.

3.4.3 Güvenlik mekanizmalarının uygulanması

Bu bölümde bahsedilen SIP güvenlik mekanizmalarının uygulanmasıyla ilgili konular ele alınacaktır.

3.4.3.1 SIP uygulayıcılarından beklenenler

Proxy sunucuları, redirect sunucuları, registrarlar TLS uygulamak zorundadır. Buna ek olarak hem tek yönlü hem de karşılıklı kimlik denetimini desteklemek zorundadır. UA'ların TLS başlatma yeteneğine sahip olmaları da şiddetle tavsiye edilmektedir, ayrıca bu UA ların TLS sunucusu olarak görev yapabilmeleri de mümkündür. Proxy sunucular, redirect sunucular ve registrarlar, subject kısmı kendi kurallara uygun isimlerine karşılık gelen birer site sertifikasına sahip olmalıdırlar. UA'lar da TLS ile birlikte karşılıklı kimlik denetimi için kendi sertifikalarına sahip olabilirler, fakat bunların kullanımı burada ele alınmamıştır. TLS destekleyen bütün SIP elemanları, TLS oturum başlatılması sırasında kullanılmak üzere alınan sertifikaları doğrulamak için mekanizmalara sahip olmak zorundadır; bu da sertifika otoritelerince yayınlamış bir veya birden fazla kök sertifikasına sahip olma zorunluluğunu getirir.

TLS destekleyen bütün SIP elemanları, ayrıca SIPS URI desteğine de sahip olmak zorundadır.

Proxy sunucular, redirect sunucular, registrarlar ve UA'lar, ayrıca IPSec veya daha alt katman güvenlik protokolleri de uygulayabilirler.

Bir UA, bir proxy sunucusu, redirect sunucusu veya registrara bağlantı kurmak istediğinde, UAC üzerinden SIP mesajlarını göndereceği bir TLS bağlantısı kurmalıdır. Bazı mimarilerde, UAS'lar istekleri bu tip bağlantılar üzerinden alabilirler.

Proxy sunucular, redirect sunucular, registrarlar ve UA'lar Digest Kimlik Denetim yapısını uygulamak zorundadır. Proxy sunucular, redirect sunucular, registrarlar en azından bir Digest realmi için yapılandırılmalı, ve verilen sunucu tarafından desteklenen en azından bir "realm" stringi sunucunun kullanıcı ismi ve domain ismine karşılık gelmelidir.

UA'lar, MIME gövdelerinin imzalanmasını ve şifrelenmesini ve de kimlik denetim bilgilerinin S/MIME iletilmesini destekleyebilirler. Eğer bir UA TLS veya IPSec sertifikalarını doğrulayabilmek için, otoritelerce yayınlanmış bir veya birden fazla kök sertifikasına sahip ise, gerektiğinde bunları SMIME sertifikaları için de kullanabilmelidir. UA özel olarak S/MIME sertifikalarını doğrulamak için de kök sertifikaları bulundurabilir.

Şu da not edilmelidir ki, ileride uygulamaların daha fazla yaygınlaşması ve problem uzayının daha iyi anlaşılması sonucu, S/MIME güvenliğinin iyileştirileceği beklenmektedir.

3.4.3.2 Güvenlik çözümleri

Bahsedilen güvenlik mekanizmalarının çalışması, halihazırda varolan WEB ve e-mail güvenlik modellerini belli oranda takip eder. Yüksek seviyede, UA'lar kendilerini sunuculara(proxy, redirect, registrar) tanıtır, bunu bir Digest kullanıcı ismi ve şifresiyle yaparlar. Bu sunucular da kendilerini bir sonraki noktada bulunan UA'lara veya sunuculara TLS kullanılarak dağıtılan bir sertifikayla tanıtır. Bu sayede iletim yolu üzerinde bir güven zinciri oluşturulur.

Eşler arası seviyede ise, UA'lar karşılarındakilerin kimliğinin denetlenmesi için ağa güvenirler. Fakat ağın bu tip hizmetleri sunmadığı ya da ağa güven duyulmadığı zaman, S/MIME kullanılarak direk olarak kimlik denetimi sağlanabilir.

Aşağıda belirtilen güvenlik mekanizmalarınn bahsedilen tehditleri ortadan kaldırmak için UA ve sunucular tarafından nasıl kullanılabileceğini gösteren bir örnek verilmiştir. Uygulayıcılar ve ağ yöneticileri bu yöntemleri kullanabilirler fakat bunlar sadece örnek uygulamalar olarak verilmiştir.

3.4.3.3 Kayıt güvenliği

Bir UA çevrimiçi duruma geçtiğinde ve kendi yerel yönetim domainine kayıt olduğunda (register işlemi), kendisini kayıt eden registrar ile bir TLS bağlantısı kurmalıdır. Bu registrar ise TLS için söz konusu UA'ya bir sertifika sunmalıdır. Bu sertifikanın tanımladığı site, UA'nın kayıt olmak istediği domainle

aynı olmak zorundadır. Örneğin söz konusu UA, "ali@anadolu.edu.tr" adresini kaydetmek istesin, sunulan sertifika "anadolu.edu.tr" domainindeki bir hostu göstermek zorundadır. UA, TLS sertifika mesajını alınca, bu sertifikayı doğrulamalı ve de sertifikada tanımlanan siteyi incelemelidir. Eğer sertifika geçerli değilse, eskiyse ya da istenen yeri tanımlamıyorsa, UA kesinlikle REGISTER mesajını göndermemelidir. Ancak sertifika geçerli, kullanım zamanı geçmemiş ve istenen yeri tanımlıyorsa o zaman kayıt işlemine devam etmelidir.

Registrar tarafından geçerli bir sertifika sağlandığında, UA karşısındaki registrarın yeniden yönlendirme, şifre çalma vs. gibi saldırıla yapacak bir saldırgan olmadığından emin olur.

Bundan sonra UA, registrardan aldığı site sertifikasına göre bir Request-URI ye adreslenecek REGISTER isteğini oluşturur. UA isteğini daha önceden oluşturulmuş bulunan TLS bağlantısı üzerinden yolladığında, registrar bu mesaja 401 (Proxy Authorization Required) yanıtı vererek kimlik denetim isteğini belirtir. Burada Proxy-Authenticate başlık alanındaki "realm" parametresi, daha önceden site sertifikasında belirtilen domaine ait olmalıdır. UAC kimlik denetim isteğini aldığında ya gerekli kimlik denetim bilgilerini kullanıcıya sormalı, ya da daha önceden oluşturulmuş anahtar dizisinden kimlik denetim isteğinin "realm" parametresindeki değere karşılık gelen kimlik denetim bilgilerini almalıdır. Bu kimlik denetim bilgilerindeki "username" parametresi, REGISTER isteğinde bulunan To başlık alanının içerisindeki URI'nin "userinfo" kısmıyla eşleşmelidir. Digest kimlik denetim bilgileri Proxy-Authorization başlık alanına eklendikten sonra, REGISTER mesajı tekrar registrar'a yollanmalıdır.

Registrar, UA'nın kendi kimliğini doğrulamasını istediği için, saldırganların belli bir kullanıcının kayıtlı adresiyle bir REGISTER taklidi yapması zor olacaktır. Ayrıca REGISTER gizli bir TLS üzerinden yollandığı için, saldırganların tekrarlama saldırısı yapmak için kimlik denetim bilgilerini ele geçirmesi mümkün olamayacaktır.

Kayıt işlemi registrar tarafından kabul edildikten sonra, UA bu TLS bağlantısını açık bırakmalıdır. Bu sayede registrar bu yönetim domainindeki kullanıcılara gelen istekleri ele alacak olan proxy sunucusu olarak da görev

yapabilir. TLS bağlantısı kullanılarak yeni kaydolmuş kullanıcıya gelen istekler kendisine iletilebilir.

UA karşısındaki sunucunun kimliğini denetlediğinden, bu TLS bağlantısı üzerinden gelen bütün isteklerin söz konusu proxyden geçtiğinden emindir. Bu nedenle saldırganlar, sanki bu proxyden geliyormuş gibi görünen sahte mesajlar gönderemezler.

3.4.3.4 Domainler arası istekler

Şimdi varsayalım Ali'nin UA'sı başka bir yönetim domaininde bulunan "ahmet@ogu.edu.tr" kullanıcısıyla oturum oluşturmak istiyor. Ayrıca yerel yönetim domaininde bir çıkış proxy sunucusu bulunmakta.

Bir yönetim domaininde, dışarıdan gelen istekleri işleyen proxy sunucusu ayrıca dışarıya giden istekleri işleyen çıkış proxy sunucusu olarak da görev yapabilir. Basitlik için, bu durumun "anadolu.edu.tr" adresinde de geçerli olduğunu varsayalım (aksi durumda UA başka bir sunucuya da TLS bağlantısı kurmak zorunda kalacaktır). Yukarıda anlatıldığı şekilde bu istemcinin kayıt işlemini tamamladığını varsayarsak, başka bir kullanıcıya INVITE isteğini yollarken yerel proxy sunucusuna kurduğu TLS bağlantısını kullanmalıdır. Burada UA, kullanıcıyı gereksiz yere işlemden haberdar etmemek için daha önceden sakladığı kimlik denetim bilgilerini oluşturacağı INVITE mesajı içerisinde kullanmalıdır.

Çıkış proxy sunucusu, INVITE içerisindeki kimlik denetim bilgilerini doğruladıktan sonra, mesajın nasıl yönlendirileceğini belirlemek için mesajın Request-URI başlık alanını incelemelidir. Eğer Request-URI'nin "domainname" kısmı "ogu.edu.tr" yerine yerel domaine (anadolu.edu.tr) karşılık geliyorsa, bu durumda proxy kendi yer belirleme hizmetinden yararlanarak bu kullanıcıya giden en uygun yolu öğrenir.

Eğer "ali@anadolu.edu.tr", "ahmet@ogu.edu.tr" ile iletişim kurmaya çalışıyorsa, yerel proxy bu isteği Ahmet'in kayıt sırasında registrar ile kurduğu TLS bağlantısına gönderecektir. Burada Ahmet, bu isteği kendi kimliği denetlenmiş kanalından alacağı için, Ali'nin isteğinin yerel yönetim domaindeki

proxy sunucusu tarafından kimlik denetiminden geçirildiğinden ve yetkilendirildiğinden emin olabilecektir.

Ancak bu durumda Request-URI bir dış domaini göstermektedir. Bunun için yerel çıkış proxy sunucusu "anadolu.edu.tr" karşıdaki domainin proxy sunucusu ile TLS bağlantısı kurmalıdır. Bu iki sunucu da site sertifikasına sahip olduğundan, karşılıklı TLS kimlik denetimi yapılmalıdır. İki taraf da karşısındakinin sertifikasını doğrulamalı ve incelemeli, daha sonra SIP mesajlarındaki başlık alanlarıyla karşılaştırmak için domain ismini kaydetmelidir. Örneğimizdeki "anadolu.edu.tr" sunucusu, karşıdan gelen sertifikanın "ogu.edu.tr" domainine ait olup olmadığını doğrulamalıdır. Bu yapıldıktan sonra, TLS bağlantısı sağlandıktan ve iki proxy arasında güvenli bir kanal açıldıktan sonra "anadolu.edu.tr" proxy sunucusu isteği (INVITE) karşıdaki "ogu.edu.tr" sunucusuna yollayabilir.

Bundan sonra "ogu.edu.tr" domainindeki proxy sunucusu, "anadolu.edu.tr" domainindeki proxy sunucusunun sertifikasını incelemeli ve INVITE mesajındaki From başlık alanının "domainname" kısmıyla sertifikanın gösterdiği domainin aynı olup olmadığına bakmalıdır. "ogu.edu.tr" proxy sunucusunda gönderildikleri yönetim domainiyle uyuşmayan isteklerin reddedilmesini isteyen güvenlik politikaları olabilir. Bu tip güvenlik politikaları Spam'i engellemek için ortaya çıkmıştır. Fakat bu tip politikalar, sadece isteğin kendisine atfettiği domainden geldiğini garanti edebilir, ama "anadolu.edu.tr" bu politikalarla Ali'nin kimliğinin "ogu.edu.tr" tarafından nasıl denetlediğinden emin olamaz. Sadece eğer "anadolu.edu.tr" , "ogu.edu.tr" domainin kimlik denetim yapısını başka bir yolla biliyorsa, Ali'nin kimliğinin nasıl denetlendiğinden emin olabilir. Bu durumda "ogu.edu.tr", yönetimsel olarak bilinmeyen domainlerden gelen ve "ogu.edu.tr" ile ortak kimlik denetim politikaları kullanmayan domainlerden gelen istekleri reddeden daha katı güvenlik politikaları kullanabilir.

INVITE "ogu.edu.tr" domainin proxy sunucusu tarafından onaylandıktan sonra bu proxy, istekteki hedefle (ahmet@ogu.edu.tr) ilişkili daha önceden oluşturulmuş bir TLS bağlantısı olup olmadığını belirlemelidir. Eğer böyle bir bağlantı varsa, INVITE bu kanal üzerinden Ahmet'e yönlendirilmelidir. İstek daha önceden kimlik denetiminden geçmiş bir TLS bağlantısı üzerinden geldiği

için, Ahmet bu istekteki From başlık alanının değiştirilmediğini, ve de Ali'nin kimliğinin "anadolu.edu.tr" tarafından doğrulandığını bilir. Buna göre Ali'ye güvenme veya güvenmeme kararı verebilir.

Her iki proxy sunucusu da, istekleri göndermeden önce bunlara Record-Route başlık alanlarını ekleyerek ileride bu diyalog dahilinde gönderilecek isteklerin kendileri üzerinden olmasını sağlamalıdır. Bu sayede her iki proxy sunucusu da devam etmekte olan diyaloğa güvenlik hizmetleri sağlayabilir. Eğer bu proxyler kendilerini Record-Route alanına eklemezlerse, bundan sonraki mesajlar uçtan uca (Ali-Ahmet arasında) iletilecek, bu durumda (eğer Ali ve Ahmet arasında belirlenmiş S/MIME gibi uçtan uca bir güvenlik yöntemi yoksa) güvenlik hizmetlerinden yararlanamayacakladır. Bu açıdan bakıldığında, SIP trapezoid modeli, site proxy sunucuları arasındaki anlaşma eğiliminin iki taraf arasında güvenli bir kanal sağlamasıyla güzel bir yapı oluşturmaktadır.

Bu mimaride bir saldırgan, bir BYE mesajını taklit edip iletişim kanalı üzerinden yollayamaz. Çünkü saldırganın oturum parametrelerini bilme gibi bir şansı yoktur. Bunun nedeni ise Ali ile Ahmet arasındaki iletimi koruyan gizlilik ve bütünlük mekanizmalarıdır.

3.4.3.5 Eşler arası istekler

Alternatif olarak, varsayalım isteklerini "ayse@ege.edu.tr" kimliğini sunarak yapan UA'nın yerel çıkış proxy sunucusu olmasın. Ayşe, "ali@anadolu.edu.tr" adresine bir INVITE mesajı yollamak istediğinde, UA'sı "anadolu.edu.tr" domainin proxy sunucusu ile direk olarak bir TLS bağlantısı kurmalıdır. Söz konusu kullanıcının UA'sı "anadolu.edu.tr" proxy sunucusundan bir sertifika aldığında, bu sertifika INVITE mesajı TLS bağlantısı üzerinden yollanmadan önce doğrulanmalıdır. Fakat Ayşe'nin kendisini "anadolu.edu.tr" proxy sunucusuna tanıtabilmesi için herhangi bir yol yoktur, yalnız INVITE mesajı içerisindeki "message/sip" tipindeki MIME gövdesinde CMS-Detached imzası vardır. Bu durumda, Ayşe'nin "anadolu.edu.tr" ile hiçbir formal ilişkisi olmadığı için, bu domainde geçerli olacak kimlik denetim bilgilerine sahip olması beklenmez. Hatta "anadolu.edu.tr" proxy sunucusu, From başlık alanı içerisindeki "domainname" kısmında "anadolu.edu.tr" değeri olmayan istekler için kimlik

denetimi yapma isteği bile yollamamasını isteyen güvenlik mekanizmalarına sahip olabilir. Bunları kimlik denetiminden geçmemiş olarak kabul edebilir.

"anadolu.edu.tr" proxy sunucusunun Ali için bir güvenlik kuralı vardır, buna göre kimlik denetimi yapılmamış bütün istekler ali@anadolu.edu.tr adresine karşılık gelen kaydedilmiş bir adrese, örneğin "<sip:bob@193.140.21.42>" adresine gönderilir. Ayşe TLS bağlantısı üzerinden yeniden yönlendirme (redirection) yanıtını alır ve bağlantı adresinin doğruluğuna güvenir.Bundan sonra Ayşe, verilen adresle bir TCP bağlantısı kurmalı ve yeni bir INVITE mesajını, alınan bağlantı adresini içeren bir Request-URI ile birlikte yollamalıdır (ve imzayı mesaj üzerinden yeniden hesaplamalıdır). Ali bu isteği güvenli olmayan bir ara yüzden alır ama UA'sı incelemeler sonucu From başlık alanındaki değeri tanır ve bu değere ait önceden kaydedilmiş sertifikayı bulur. Ve de INVITE mesajının gövdesindeki imzayla bu bulduğu sertifikayı eşleştirir. Ali de aynı şekilde cevap verir ve kendisini Ayşe'ye tanıtır (kimliğin kanıtlar) ve diyalog güvenli bir yolla başlar.

Bazen belli bir yönetim domainindeki firewallar veya NAT'lar belli bir UA'ya direk olarak TCP bağlantısı kurulmasını engelleyebilir. Bu durumlarda proxy sunucular bu istekleri UA'lara herhangi bir güven içermeyen yollarla aktarabilirler (örneğin, bir TLS bağlantısında vazgeçip, mesajı açık olarak TCP üzerinden yollamak gibi).

3.4.3.6 Hizmeti engelleme saldırılarından korunma

Hizmeti engelleme saldırıları daha önceden de belirtildiği gibi en yaygın ve etkili saldırılardan birisidir. Uygulamalarda kullanılan mimarilerde ve güvenlik çözümlerinde, hizmeti engelleme tipindeki saldırı riskini en aza indirebilmek için aşağıdaki tavsiyeler uygulayıcılar tarafından dikkate alınmalıdır.

Üzerinde SIP Proxy sunucusu çalışan bir host direk olarak Internet'ten genel erişime açık ise, bu host güvenlik politikaları (belli kaynaklardan gelen trafiğin engellenmesi, ping trafiğinin engellenmesi gibi) olan bir yönetim domainine yerleştirilmelidir. Yönetim domaini içerisindeki belli hostlar güvenlik amacıyla yapılandırılabilir, bunlara savunma hostları diyebiliriz. Hem TLS hem de IPSec kullanan savunma hostları yönetim domainlerinin uç noktalarında kullanılarak

güvenli tüneller veya soketleri oluşturabilir. Ayrıca bu savunma hostları, hizmeti engelleme saldırılarının darbesini kendi üzerlerine alarak domain içerisindeki kullanıcıların gereksiz trafikten etkilenmemesini sağlayabilirler.

Hangi güvenlik yöntemleri kullanılırsa kullanılsın, proxy sunucularına yönlendirilmiş mesaj taşkınları, proxy sunucularının kaynaklarını tüketebilir ve gerekli trafiğin hedefine ulaşmasına engel olabilir. SIP iletimlerinin proxy sunucularında işlenmesi belli bir işlem gücü gerektirir, bu gereksinim stateful proxylerde daha fazladır. Bundan dolayı stateful proxyler mesaj taşkınlarına karşı daha dayanıksızdır.

UA'lar ve proxy sunucuları, şüpheli istekleri sadece bir tek 401 (Unauthorized) veya 407 (Proxy Authorization Required) yanıtıyla kimlik denetimine zorlamalıdır. Bu arada yanıtların normal olarak yeniden gönderilmesinden vazgeçilmeli ve kimlik denetiminden geçmeyen kullanıcılar için durum bilgisi tutmayan proxyler gibi davranmalıdır.

401 (Unauthorized) veya 407 (Proxy Authorization Required) yanıtlarını tekrar yollamak, bir saldırganın değiştirilmiş başlık alanları(Via gibi) kullanarak trafiği üçüncü bir adrese yönlendirmesini kolaylaştırabilir.

Özet olarak, proxy sunucularının karşılıklı olarak kimlik denetimi yapması (TLS gibi mekanizmalarla), kötü niyetli ara elemanların değiştirilmiş istek veya yanıtları kullanarak hizmetin engellenmesi saldırısı yapmaları riskini azaltır. Bu sayede suçsuz SIP elemanlarının çoğaltma saldırılarında kullanılması engellenebilir.

3.4.4 Sınırlamalar

Yukarıda bahsi geçen güvenlik mekanizmaları akıllıca uygulanırsa, birçok tehdidi engelleyebilmektedir. Fakat bu yöntemlerin de belli sınırlamaları vardır. Aşağıda bu sınırlamalar özetlenmiştir.

3.4.4.1 HTTP Digest

SIP'te Digest kimlik denetimi kullanımının en temel sınırlaması, Digest içerisindeki bütünlük mekanizmasının SIP ile çok iyi çalışamamasıdır. Digest

kimlik denetim yapısı özellikle Request-URI ve mesaj yöntemi üzerinde koruma sağlar, ama UA'ların çoğunlukla güven altına almak isteyeceği diğer alanlar üzerinde herhangi bir koruma sağlamaz.

RFC 2617[28] de tanımlanan, tekrarlama saldırılarından korunma mekanizmaları da SIP ile bazı sınırlamalara sahiptir. Örneğin next-nonce mekanizması tünellenmiş istek mesajlarını desteklememektedir. Burada tekrarlamalardan korunmak için nonce-count mekanizması kullanılmalıdır.

Digest ile ilgili diğer bir sınırlama da realmlerin kapsamıdır. Digest, bir kullanıcı daha önceden kendisiyle herhangi bir ilişkisi olan bir kaynağa kimliğini kanıtlamak istediğinde önem kazanır (örneğin kullanıcının müşterisi olduğu hizmet sağlayıcısına). Aradaki farkı göstermek gerekirse, TLS kapsam olarak domainler arası ve birden çok realmlidir. Sertifikalar global olarak doğrulanabilir olduklarından, UA karşısındaki sunucunun kimliğini daha önceden kurulmuş bir ilişkiye sahip olmaksızın denetleyebilir.

3.4.4.2 S/MIME

S/MIME'in en büyük eksikliği ise, son kullanıcılar için yaygın bir ortak anahtar mekanizmasının olmamasıdır. Eğer kişisel imzalı sertifikalar kullanılırsa (yani kullanılan sertifika tanınan bir sertifika kuruluşu tarafından sağlanmak yerine kullanıcılardan birisi tarafından sağlanmışsa ve diğer tarafta doğrulanamıyorsa) daha önceden anlatılmış olan SIP-temelli anahtar değişim mekanizması, aradaki adam türündeki saldırılara açık olacaktır. Ve burada saldırgan, S/MIME gövdelerini inceleyip değiştirebilecektir. Saldırganın ilk olarak iki taraf arasındaki anahtar değişiminin yolunu kesmesi, istek ve yanıtta varolan CMS-Detached imzalarını çıkarması, ve bunların yerine kendisi tarafından sağlanan (fakat gerekli adreslerden geliyormuş gibi görünen) bir sertifika içeren CMS-Detached imzasını koyması gerekmektedir. Burada iletim yapan iki taraf da karşısındakiyle anahtar değişimi yaptığını sanacaktır. Fakat ikisi de güvenle kullanabileceklerini sandıkları saldırganın ortak anahtarını almış olacaktır.

Ama burada saldırgan bu açığı sadece iki taraf arasındaki ilk anahtar değişimi sırasında kullanabilir, diğer zamanlarda herhangi bir değişiklik hemen

fark edilecektir. Ayrıca ilerideki bütün diyaloglar boyunca saldırganın aynı hat üzerinde bulunarak iletimin yolunu kesmesi zor olacaktır.

SSH[30] da aynı şekilde ilk anahtar alışverişi sırasında aradaki adam saldırılarına karşı hassastır, fakat mükemmel olmasa da bağlantıların güvenliğini arttırmaktadır. Key Fingerprint kullanımı SSH'da olduğu gibi SIP'e de belli seviyede destek sağlamaktadır. Örneğin iki taraf sesli bir oturum başlatmak için SIP kullanıyorsa, iki taraf da karşı taraftan aldığı anahtarın fingerprintini okuyabilir, ve orijinaliyle karşılaştırabilir. Burada iki tarafın seslerinin taklit edilmesi, onların iletişimini taklit etmekten zor olacaktır.

S/MIME mekanizması UA'lara, eğer hedef adresi için anahtar dizilerinde bir kayıtlı-adres varsa, şifrelenmiş mesajları preamble alanı olmadan yollama olanağı verir. Fakat şu da mümkündür ki, belli bir kayıtlı adres için kayıt edilmiş aygıtın şu andaki kullanıcısı o sertifikayı tutmayabilir, bu da şifrelenmemiş bir isteğin doğru olarak işlenmesini engeller, bu da bazı iletişimin göz ardı edilmesini beraberinde getirebilir. Bu durum genelde şifrelenmiş mesajlar forking ile çoğaltıldığında meydana gelir.

S/MIME ile ilintili anahtarlar, belli bir aygıt (UA) yerinde belli bir kayıtlı adrese ait olursa daha kullanışlı olmaktadır. Kullanıcılar aygıtlarda yer değiştirdiğinde, UA'lar arasında özel anahtarlarını güvenli bir şekilde taşımak zor olacaktır.

S/MIME ile ilgili diğer bir sıkıcı zorluk da, oluşabilecek çok büyük mesajlardır. Bunlar özellikle SIP tünellemesi kullanıldığında ortaya çıkmaktadır. Burada S/MIME tünellemesi kullanıldığında, TCP'nin transport protokolü olarak kullanılması önerilmektedir.

3.4.4.3 TLS

TLS mekanizmasının üzerinde en çok konuşulan yönü, UDP üzerinde çalışmaması, sadece bağlantı temelli TCP üzerinden çalışabilmesidir.

Çıkış proxy sunucuları için, aynı anda birçok UA ile kurulmuş uzun ömürlü TLS bağlantılarının yönetimi güç olacaktır. Bu özellikle hassas şifre yöntemleri için ölçeklenebilirlik konusunu ortaya çıkarmaktadır. Uzun ömürlü TLS

bağlantılarının fazlalığıyla ilgilenmek de bunları oluşturan UA'lar için sıkıntı verici olabilir.

TLS, SIP varlıklarının sadece komşu oldukları sunucuların kimliklerini denetlemesine izin verir. Kısaca noktalar arası kimlik denetimi sağlar. Ne TLS ne de bahsedilen diğer mekanizmalar, istemcilerin direk olarak TCP bağlantısı kuramadıkları sunucuların kimliğini denetlemesine izin verir.

3.4.4.4 SIPS URI'leri

TLS'i bir isteğin yolu üstündeki bütün segmentlerde kullanabilmek için uçlardaki UA'lar, TLS üzerinde erişilebilir olmalıdır (belki de bir SIPS URI yi bağlantı adresi olarak kaydederek). Bu SIPS'in tercih edilen kullanımıdır. Birçok geçerli mimaride ise TLS isteğin yolunun belli bir kısmını güven altına almakta, fakat son noktadaki UA'lara erişim başka mekanizmalarla ele alınmaktadır. Bundan dolayı SIPS, gerçek manada uçtan uca TLS kullanımını garanti edemez. Birçok UA gelen TLS isteklerini kabul etmez, hatta destekleyenlerin bile kalıcı TLS bağlantıları oluşturmaları gerekebilir (daha önceden anlatılan sınırlamalara göre). Bu sayede TLS üzerinden istekleri alabilirler.

Yer belirleme hizmetlerinin bir SIPS Request-URI için SIPS bağlantısı kurması gerekmez. Yer belirleme hizmetleri genel olarak kullanıcı kayıtlarının toplanmasıyla sağlanırlar, fakat diğer protokoller ve ara yüzler de belli bir kayıtlı adres için bağlantı adresi sağlamakta kullanılabilir ve bu araçlar gerektiğinde SIPS URI'lerini SIP URI'leriyle eşleştirebilirler. Yer belirleme hizmetleri bu bağlantılar için sorgulandıklarında, gelen isteğin SIPS Request-URI ile gelip gelmediğine bakmaksızın bağlantı adreslerini döndürür. Eğer yer belirleme hizmetini bir redirect sunucusu kullanıyorsa, bu bağlantı adresinin uygunluğunu kontrol etmek, redirection mesajının Contact başlık alanını işleyen elemanın görevidir.

İsteğin gideceği hedef domaine kadar olan yolda bütün noktalarda TLS kullandığından emin olabilmek biraz güçtür. Ayrıca iletim yolundaki, kimliği şifreli olarak denetlenmiş sunucular SIP'in yönlendirme kurallarına uyumlu olmayabilir veya bu kuralları yerine getirmemeyi seçebilir. Bu tip kötü niyetli ara

elemanlar, istekleri SIPS URI den SIP URI ye yönlendirerek güvenlik seviyesinin düşürülmesini sağlayabilir.

Alternatif olarak, bir ara eleman istekleri kurallara uygun olarak SIP URI'den SIPS URI'ye yönlendirebilir. Yine de bu istekleri alanlar, bu isteklerin Request-URI kısmında SIPS URI kullanılıp kullanılmadığına bakarak, SIPS'in bu isteğin bütün yolu boyunca kullanıldığından emin olamaz.

Bu endişeleri ele almak için, bir isteği alanların bu isteğin Request-URI'sinde SIP veya SIPS URI kullanılmasına bakarak, To başlık alanındaki değerin SIPS URI içerip içermediğine bakması önerilmektedir. Şu da not edilmelidir ki, eğer bu iki alandaki değerler aynı yapıyı kullanıyorsa fakat değerleri farklı ise bu bir güvenlik ihlali belirtmez. UA'lar isteklerin Request-URI ve To başlık alan değerlerini farklı yollarla toplasalar da, SIPS URI kullanıldığında bu faklılık bir güvenlik ihlali olarak değerlendirilebilir ve istek alıcısı tarafından reddedilebilir. Ayrıca alıcılar, Via başlık alanındaki değerleri inceleyerek isteğin yerel yönetim domainine girinceye kadar geçtiği yolda TLS üzerinden gelip gelmediğini ikinci kez denetleyebilirler. Ayrıca isteğin To başlık alanının değişmeden uçtan uca gittiğini garanti etmek için UAC tarafından S/MIME da kullanılabilir.

Eğer UAS'ın Request-URI'nin güvenlik yapısının iletim sırasında değiştiğine inanmak için nedeni varsa, kullanıcısını potansiyel bir güvenlik ihlali konusunda uyarmalıdır.

Güvenlik seviyesini azaltma türündeki saldırılardan korunmak için, sadece SIPS isteklerini kabul eden SIP elemanları, buna ek olarak güvenli olmayan yönlerden gelecek istekleri de reddedebilirler.

Son kullanıcılar, SIPS ve SIP URI'leri arasındaki farkı ayırt edebilirler ve bunları elle düzenleyebilirler. Bu hem fayda hem de zarar getirebilir. Örneğin, varsayalım bir saldırgan DNS bilgilerini bozuyor, bu şekilde bir proxy için varolan bütün SIPS adreslerini siliyor. Bundan sonra bu sunucuya giden bütün istekler başarısız olacaktır. SIPS kayıtlı adresine defalarca kez yapılan isteklerin başarısız olduğunu gören kullanıcı, bazı aygıtlarda isteğin kullandığı yapısı SIPS'ten SIP'e çevirebilir. Buna karşı bazı önlemler olmasına rağmen, dikkate

değer bir durumdur. Diğer yanda ise, kullanıcılar SIP URI ile gösterilseler bile 'SIPS' geçerli olabilecektir.

3.5 ABA Güvenliğinde SIP Güvenlik Mekanizmalarının Kullanımı

Daha önceden de belirtildiği gibi Akıllı evler ile ABA kontrol ve kumandasında güvenlik hayati önem taşır. Bu tip sistemlerde sağlanması gereken gereksinimler ve karşı karşıya kalınan tehditler daha önceden ele alınmıştı. Bu kısımda ise bu gereksinimlerin ve tehditlerin SIP güvenlik mekanizmalarıyla nasıl ele alınabileceği tartışılacaktır. SIP güvenliğinin hangi durumlarda Akıllı Evler ve ABA kontrol ve kumandasında direk olarak kullanılabileceği, hangi durumlarda bazı değişikliklerle kullanılabileceği, hangi durumlarda da diğer katmanlardan yardım isteneceği tartışılacaktır.

3.5.1 ABA güvenliği ve genel SIP güvenliğinde farklılıklar

Ele alınan konu Akıllı evler ve ABA kontrol ve kumandasında SIP kullanımı olduğu için, bu protokolün güvenlik hizmetlerininin ABA güvenlik gereksinimlerini karşılayabilmesi gereklidir. Fakat protokol Akıllı evler ve ABA kontrol ve kumandasına özel olarak kullanılacağından, bazı özel güvenlik gereksinimleri ve yöntemleri de ortaya çıkabilir. Bu konu SIP güvenliği ile ABA güvenliğinin birbirinden ayrıldığı noktaları ABA güvenliği açısından ele alacaktır.

RFC3261'de[1] tanımlanan SIP kimlik denetim ve gizlilik yöntemleri, ABA kontrol ve kumandasında da geçerlidir. Fakat burada genel SIP mesajları ile ABA'ların kontrolünde kullanılacak SIP mesajlarının güvenliği birkaç konuda farklılık göstermektedir. Bu bölüm de bu faklılıkları ele almaktadır.

3.5.1.1 Paylaşılan anahtar kullanarak güvenlik

Genel SIP güvenliği, ortak anahtar kullanımını gerektirmektedir. Bu tip şifrelemede şifreleme ve şifre çözme ayrı anahtarlarla yapılır Bir eve dışarıdan erişimin sağlandığı mimarilerde ise paylaşılan anahtar (diğer adıyla özel anahtar) kullanımıyla gizlilik ve kimlik denetimi sağlanabilmektedir. Bu farklılık için iki

ana neden vardır; birincisi genel SIP iletişimi herhangi iki nokta arasında birebir olurken, evle iletişimde aynı eve birden fazla yetki sahibi kullanıcının iletişimiyle çok noktadan tek bir noktaya şeklinde olacaktır. Yani bunların her biri için kullanılabilecek anahtarlar belirlenerek daha sonra kullanılması uygun olacaktır. İkinci olarak ise, genelde SIP iletişimleri daha önceden herhangi bir bağlantısı olmayan taraflar arasında olur, bu yüzden herhangi bir paylaşılan anahtar oluşturulması şansı yoktur. Ama akıllı evlere uzaktan erişimde ise kullanıcılar tipik olarak evle daha önceden bir bağlantı kurmuş olacaktır. Yani eve ulaşmak isteyen kişi zaten eve daha önceden herhangi bir şekilde bağlantısı olan ev sahibi veya ev sahibi tarafından yetkilendirilmiş bir kullanıcı olacaktır. Eve bağlanmak isteyen kullanıcılar, daha sonra evle kuracakları iletişimde kullanabilecekleri paylaşılan anahtarı atayabilirler. Bu anahtar hem RGW/Firewall ile hem de hizmet sağlayıcı Proxy Sunucusu ile paylaşılmış olabilir.

Genelde gizli-anahtar yöntemleri yüksek güvenlik seviyeleri ve verimlilikleri nedeniyle ortak anahtar yöntemlerine tercih edilirler.

Şu da not edilmelidir ki bazı durumlarda ortak anahtar kullanımı tercih edilebilir.

3.5.1.2 Uçtan-uca şifreleme

SIP RFC23261 gizlilik için iki yöntem tanımlamaktadır; uçtan uca veya noktalar arası şifreleme. Akıllı evlere dışarıdan erişimin sağlandığı sistemlerde ise uçtan uca şifreleme önerilmektedir. Uçtan uca şifreleme daha verimlidir ve eğer kullanıcı ile RGW/Firewall (ya da hizmet sağlayıcı Proxy sunucusu) bir anahtarı paylaşıyorsa, bu durumda noktalar arası şifrelemeyi kullanmak gereksiz olacaktır. Ayrıca noktalar arası şifrelemede yol üzerindeki bütün proxylere güvenme gereksinimi vardır, fakat uçtan uca şifrelemede sadece son noktadaki şifreyi çözecek UA'ya güvenmek yeterlidir (hem RGW/Firewall hem de hizmet sağlayıcı Proxy'de). Bu nedenlerden dolayı uçtan-uca şifreleme, iletim yolunda bulunan olası tehdit noktalarının iletimde gizli kalması gereken bilgiye erişimini engelleyebilecektir.

Burada iki durum birbirinden ayırt edilmelidir; birincisi kullanıcının eve direk olarak bağlantı kurabildiği durumdur. Burada şifre çözme ve kimlik

doğrulaması RGW/Firewall tarafından yapılmaktadır. Bu durumda kullanıcının mesajı, kullanıcı ve ev arasında paylaşılan anahtarla şifrelenebilir ve mesajın kimliği denetlenebilir. İkinci durumda ise iletişim ev dışarısında bulunan bir proxy üzerinden yapılmaktadır (hizmet sağlayıcı tarafından sağlanmış Proxy sunucusu). Bu durumda ise mesajlar, kullanıcı ve hizmet sağlayıcı arasında paylaşılan bir anahtarla şifrelenecek ve bu mesajların kimliği denetlenecektir. Bu şifreli mesajı alan hizmet sağlayıcı Proxy sunucusu, mesajın şifresini çözer ve kimliğini doğrular. Bundan sonra ise mesaj hizmet sağlayıcının Proxy sunucusu ve ev arasında paylaşılan anahtarla şifrelenir ve mesajın kimliği denetlenir. Daha sonra eve yollanır (bu iletim ayrıca kurulacak güvenli bir IPSec bağlantısı üzerinden de yapılabilir). Evde ise iletilen mesajın kimliği RGW/Firewall'da doğrulanır ve şifresi çözülür, bundan sonra eve girişine izin verilir. Burada bu işlemlerin artık uçtan uca olmadığı görülebilir, ama bu durum aradaki bütün Proxylerin kullanılmasını ve bunlara güvenmek gerekliliğini ortaya çıkarmadığından uçtan uca şifreleme olarak düşünebiliriz. Sonuçta hizmet sağlayıcı bu yapıda güvenilen bir nokta olarak düşünülebilir. Bu durumda da araya başka bir olası tehdit noktası girmemiş olur.

3.5.1.3 To: Başlık alanının şifrelenmesi

SIP RFC3261'de bahsedilen durumlardan farklı olarak ABA kontrolünde SIP kullanırken To başlık alanın içeriği özel bir önem kazanır. Bu alana bakılarak ev içerisindeki aygıtların varlığı, yeri, ismi vs öğrenilebilir. Bu bilgilerin açık olarak yollanması, yani iletimde saldırganlar tarafından görülebilecek olması istenmeyen bir durumdur. Bundan dolayı bu başlık alanının şifrelenmesi gerekliliği ortaya çıkmaktadır. Mesaj gövdelerinin ve bazı başlık alanlarının nasıl şifrelenebileceği SIP RFC3261'de anlatılmaktadır. To başlık alanının şifrelenmesi, gövdenin şifrelenmesinden ayrı olarak ele alınmalıdır. Çünkü To başlık alanının tamamının şifrelenmesi, SIP işleyişi açısından mümkün değildir. Bu alandaki değerler, mesajların hedefe yönlendirilebilmesi için gereklidir, bundan dolayı sadece "@" karakterinin solundaki kısımda şifreleme yapılabilir. Bu alan da bildiğimiz gibi SIP varlığını belirten kısımdır. Diğer kısım ise varlığın yer aldığı domaini belirtir ki bu alanın şifrelenmeden kalması gereklidir.

Başta bu yaklaşım problemli olabilecek gibi gözükür, ama bu engellenebilir. Gerçekte yönlendirme işlemi To: başlık alanının iki kısmına göre yapılır, birincisi SIP varlığının ismi ("@" işaretinin solunda kalan kısım), ikincisi ise bu varlığın bulunduğu yeri belirten kısım ("@" işaretinin sağında kalan kısım). Yer bildiren kısım(tipik olarak Domain ismi) ağdaki bütün Proxy'ler tarafından görülebilirdir. Fakat SIP varlığıyla ilgili bilgiler, sadece belirli Proxy'ler (direk olarak eve erişim sağlayan mimaride RGW/Firewall, hizmet sağlayıcı üzerinden eve erişim sağlayan mimaride ise hizmet sağlayıcı Proxy) tarafından görülebilir olmalıdır. Bu şekilde çoğu proxy yönlendirme işlemi için sadece yer bildiren kısımları kullanacaktır. SIP varlığına özel kısımları ise zaten paylaşılan anahtara sahip olan Proxyler kullanmak isteyecek ve şifreyi çözerek kullanabilecektir. Bu durumda da yönlendirme işlemleri SIP varlığıyla ilgili bilgileri çözebilecek Proxy'ye gelene kadar To: başlık alanının yer bildiren (açık metin olarak bulunan) kısmına göre yapılacaktır. Bu Proxy sunucuya gelindiğinde ise SIP varlığına ait olan kısmın şifresi gerekli anahtarla çözülecek ve bundan sonraki yönlendirme bu kısımdan elde edilen değere göre yapılacaktır.

3.5.2 SIP ve ABA güvenliğinde ortak noktalar

Akıllı ev ve ABA kontrol ve kumandasında SIP kullanımında, bu protokolün güvenlik hizmetlerinin ABA güvenlik gereksinimlerini karşılayabilmesi önemlidir. Protokol belli oranda uyarlanarak kullanılacağından bazı noktalarda farklı yöntemlerin kullanılması kaçınılmazdır. Bir önceki konuda bu farklılıklar ele alınmıştır. Fakat kullanılacak protokolün güvenlik hizmetleri gereksinimleri ne kadar karşılayabilirse, bu protokolün kullanıma o kadar uygun olduğu söylenebilir. Bu bölümde ise SIP'le gelen standart yöntemlerin ABA güvenliğinde kullanılması ele alınacaktır. Bunlar standart SIP uygulamalarıyla Akıllı Evler ve ABA kontrol ve kumandasındaki ortak noktaları da göz önüne sermektedir.

3.5.2.1 ABA güvenliğinde Transport ve Network katmanı hizmetleri

Standart SIP uygulamalarında olduğu gibi bazen güvenlik gereksinimlerini daha alt katmanlardan alınan hizmetlerle sağlamak mümkün olabilir. Bu hizmetler TLS[26] ve IPSec[27] mekanizmalarıyla sağlanır. Bu iki katman şifreleme sayesinde mesaj bütünlüğü ve gizliliğini korur.

Çoğu zaman alt katman güvenliğini sağlamak için sertifikalar kullanılmaktadır, ve bu sertifikalar birçok mimaride kimlik denetimi için de kullanılabilir.

Yukarıda da belirttiğimiz gibi transport ve network katmanlarında güvenlik sağlayan iki protokol TLS ve IPSec'tir.

IPSec, geleneksel IP protokolünün yerine güvenlik amacıyla kullanılabilecek, network katmanında çalışan araçlardan oluşmuştur. Bu yapı genel olarak daha önceden kurulmuş güven ilişkilerine sahip hostlar veya yönetim alanlarında kullanılır. Genellikle hostun işletim sistemi seviyesinde uygulanır. IPSec ayrıca noktalar arasında da kullanılabilir.

Birçok yapıda IPSec in SIP uygulamalarıyla entegre olması gereksizdir, kullanımı SIP hostlarına direk olarak güvenlik eklemenin zor olduğu durumlarda daha uygundur. ABA kontrol ve kumandasında kullanımı da aynı özellikleri gösterir. Ayrıca kendilerine en yakın Proxy sunucusu ile önceden paylaşılmış anahtar ilişkisine sahip UA'lar da IPSec için uygun adaylardır. Buradan da ABA'lar bu özelliğe sahip oldukları için IPSec kullanımına uygun aday olarak tanımlanabilir.

TLS ise bağlantı temelli (connection oriented) protokoller üzerinden transport katmanı güvenliği sağlar (özellikle TCP). TLS, daha önceden herhangi bir güvenlik ilişkisine sahip olmayan hostlar arasında noktalar arası güvenlik kurmak için uygundur. Örneğin, Ali kendi yerel Proxy sunucusuna güvenmektedir ve bu Proxy de bir sertifika alışverişinden sonra Ahmet'in yerel Proxy sunucusuna güvenmektedir, son olarak da Ahmet kendi yerel Proxy sunucusuna güvenmektedir. Bu durumda Ali ve Ahmet arasında güvenli bir iletişim yolunun varlığından söz edilebilir, yani bu iki kullanıcı güvenle iletişim yapabilirler. ABA kontrol ve kumandasında TLS kullanımı ise, birkaç değişik şekilde olabilir. Örneğin, evle iletişimin hizmet sağlayıcı üzerinden olduğu durumlarda, evle

hizmet sağlayıcı arasındaki iletişim güvenli TLS bağlantıları üzerinden yürütülebilir. Bu sayede bu iletişimin güvenli olduğuna güvenilebilir. Buna ek olarak eve ulaşmak isteyen kullanıcı ve hizmet sağlayıcı arasında da TLS bağlantıları oluşturularak bu iletişimin güvenlik altına alınması sağlanabilir. Bu tip mimarilerde, hizmet sağlayıcının güvenli bir nokta olduğu düşünülebilir ve uçtan-uca güvenliğin sekteye uğramayacağı varsayılır.

3.5.2.2 ABA kontrol ve kumandasında SIPS URI yapısı kullanımı

Güvenli bir iletim için SIPS URI yapısı[1] kullanılabilir. SIPS URI yapısı, temelde SIP URI yapısına sadık kalmaktadır. Burada sadece yapıyı belirten string "sip" yerine "sips" tir. ABA kontrol ve kumandasında da SIPS URI yapısı kullanılarak güvenli bir iletim sağlanabilir.

SIPS URI ABA'ların ve kullanıcıların kayıtlı adresi olarak kullanılabilir. Bir isteğin Request-URI başlık alanında kullanıldığında, kullanılan SIPS yapısı, mesajın Request-URI başlık alanının domain kısmıyla ilgili kısmını işleyecek SIP varlığına giderken geçeceği bütün noktalarda TLS kullanılarak güvenlik sağlanmak zorunda olduğunu belirtir. Mesaj hizmet sağlayıcı domainine girdikten sonra ise, bu domainin yerel güvenlik ve yönlendirme planına göre ele alınır. Yine burada da UAS'a ulaşacak son noktaya kadar TLS kullanılması muhtemeldir. SIPS bir ABA'yı kontrol veya kumanda etmek isteyen bir kullanıcı UA'sı tarafından kullanılırsa isteğin hedef domaine gidinceye kadar geçeceği yolun güvenli olmasının isteneceğini belirtir.

SIPS URI'leri kimlik olarak kullanan ve dağıtan kullanıcılar, aygıtlarını güvensiz iletimle gelen istekleri reddedecek şekilde kullanmayı tercih edebilirler. Yani bu durumda ABA'lar veya hizmet sağlayıcı domaini SIPS URI kullanmayan istekleri kabul etmeyerek güvensiz bir iletimi en baştan reddedebilirler. Bu sayede istenilen güvenlik seviyesi belirlenebilir.

3.5.2.3 HTTP kimlik denetimi

SIP, HTTP Kimlik Denetimi[28] temelli, 401 ve 407 kodlu yanıt kodlarına ve kimlik denetim istekleriyle kimlik denetim bilgilerini taşıyan başlık alanlarına

dayalı bir kimlik denetim yapısı sunar. HTTP Digest Kimlik Denetim yapısının üzerinde belirgin değişiklikler gerekmeksizin kullanılması tekrarlama saldırılarından koruma ve tek yönlü kimlik denetimini sağlamaktadır. ABA kontrol ve kumandasında da aynı kimlik denetim yapısı kullanılabilir. Bu yöntemlerle hem hizmet sağlayıcı-ABA'lar arasında, hem hizmet sağlayıcı-kullanıcılar arasında hem de direk olarak ABA-kullanıcı arasında kimlik denetimi yapılabilir.

Herhangi bir ABA belli bir komut taşıyan bir istek aldığı zaman karşısındaki kullanıcının kimliğini denetlemek isteyebilir. Bunun için 401 (Unauthorized) yanıtıyla kimlik denetim isteğini karşıya bildirir. Buna ek olarak Registrarlar ve redirect sunucuları da aynı şekilde kimlik denetim isteği yaparlar. Fakat Proxy sunucuları 407 (Proxy Authentication Reguired) yanıtını kullanarak kimlik denetimi isterler. Ayrıca Proxy-Authenticate, Proxy-Authorization, WWW-Authenticate ve Authorization alanları da kimlik denetimini sağlamak için kullanılır. [1]

3.5.2.4 ABA kontrol ve kumandasında S/MIME kullanımı

Daha önce de belirtildiği gibi SIP mesajlarını uçtan uca tamamen şifrelemek protokolün çalışması açısından uygun değildir, çünkü bu mesajların bazı başlık alanları SIP elemanlarının doğru çalışabilmesi için okunabilir veya değiştirilebilir olmalıdır. Bu SIP elemanları göz önüne alınmadığı taktirde, SIP mesajları yönlendirilebilir olmaktan çıkar. Fakat daha önceden de belirtildiği gibi Akıllı Ev ve ABA'ların kontrol ve kumandasında bazı başlık alanlarının görülebilir olması istenmemektedir. Bundan dolayı bu alanları saklamak için bazı mekanizmalar kullanmak kaçınılmazdır. ABA kontrol ve kumandasında SIP mesajları kullanılacağı için S/MIME kullanımı uygundur.

S/MIME sayesinde mesaj gövdeleri içerisinde şifrelenmiş MIME gövdeleri gönderilebilir. Bu gövdeler mesajın başlık alanlarını içerebilir. Bu sayede istenen alanlar uçtan uca şifreli olarak gönderilebilir. S/MIME mesaj gövdeleri için uçtan uca gizlilik ve bütünlük ve de ayrıca karşılıklı kimlik denetimi sağlayabilir. S/MIME'ın ayrıca SIP başlık alanlarının belli bir formda gizlilik ve bütünlüğünü sağlaması SIP mesaj tünellemesi ile mümkün olmaktadır. Bu yöntemde istenilen

alanlar S/MIME gövdesi içerisinde yer alabilmektedir. Bu sayede hem bütün alanların şifrelenmesi ile ortaya çıkacak yük ortadan kalkacak hem de istenilen özellikler elde edilmiş olacaktır.

4. UYGULAMA

Daha önceki bölümlerde bahsedildiği gibi Akıllı Evler ve ABA kontrol ve kumandasında SIP kullanımı uygun görülmektedir. Söz konusu protokolün kullanılması ile bu protokolün sunduğu birçok olanaktan yararlanılabilecektir. Bu tezde geliştirilen uygulama da SIP'in güvenlik hizmetlerinden kimlik denetimini kullanarak çalışan basit bir UA uygulamasıdır. Daha önceki bölümlerde değinildiği gibi SIP, HTTP Digest kimlik denetim yapısını kullanmaktadır.

Uygulama sonucunda, Akıllı Ev ve ABA kontrol ve kumandasında SIP kullanımının getirdiği kolaylık rahatça görülmüştür. Bu protokolün kullandığı Digest kimlik denetim yapısı, uçtan uca kimlik denetimi için uygun bir altyapı sağlamaktadır. Bu yapının iki taraflı olarak kullanılması sonucu her iki tarafın da iletişim yaptığı tarafın kimliğinden emin olması sağlanmıştır.

4.1 Uzaktan Oda Lambası Kontrolü

Geliştirilen uygulamada, kullanıcının evinde bulunan oda lambasını uzaktan kontrol ve kumanda etmesi sağlanmıştır. Söz konusu işlevi yerine getirmek için iki ayrı uygulama geliştirilmiştir. Bunlardan birincisi, kullanıcının dışarıdan bağlantı kurarken kullanacağı UAC uygulamasıdır. Diğeri ise kontrol ve kumanda edilecek aygıtla bağlantıyı sağlayacak ara yüz olan UAS uygulamasıdır. Internet üzerinden telefon konuşmalarının desteklendiği bir yapıda UAS ve UAC aynı uygulama içerisinde yer alabilir. Yani iki taraf arasında çok büyük fark yoktur ve iki taraf da oturum başlatma ve kabul etme yeteneklerine sahip olmak isteyecektir. Ama aygıt kontrolünde aygıtın UAC uygulamasına sahip olması gereksizdir. Ayrıca kullanıcının da UAS uygulamasına sahip olması kullanıcıyı herhangi bir fayda sağlamayacaktır. Bu nedenlerden dolayı UAC ve UAS ayrı uygulamalar olarak geliştirilmiş ve UAC kullanıcı tarafına, UAS aygıt tarafına yerleştirilmiştir.

Uygulama geliştirme platformu olarak Visual Basic 6.0 uygulama geliştirme ortamı kullanılmıştır. Bu sayede gerekli işlevleri yerine getirebilecek bir ara yüz kolaylıkla tasarlanmıştır. Ayrıca uygulamaya iletişim yeteneklerini eklemek için de Winsock nesnelerinden yararlanılmıştır.

Geliştirilecek UAC uygulaması tipik olarak kullanıcının bulunabileceği ortamda ya bir kişisel bilgisayarda yada bu uygulamanın çalışabileceği kaynaklara ve iletişim yeteneklerine sahip taşınabilir bir aygıtta bulunabilir. Geliştirilen UAC uygulaması bir kişisel bilgisayar üzerinde çalışabilecek şekilde tasarlanmıştır.

Aygıtın ağ ile ara yüzünü oluşturan UAS uygulaması, yine bir kişisel bilgisayar üzerinde çalışabilecek ve gelen mesajları işleyebilecek şekilde tasarlanmıştır. Kontrol ve kumanda edilmek istenen aygıt (oda lambası), ağ yeteneğine sahip olmadığından bu yeteneği bir Aygıt Kontrol Birimi vasıtasıyla kazanabilir. Sistemin bu kısmı çalışmanın dışında bırakılmış, bu işlemin yerine getirildiği varsayılarak bir benzetim yapılmıştır.

4.1.1 UAC (User Agent Client)

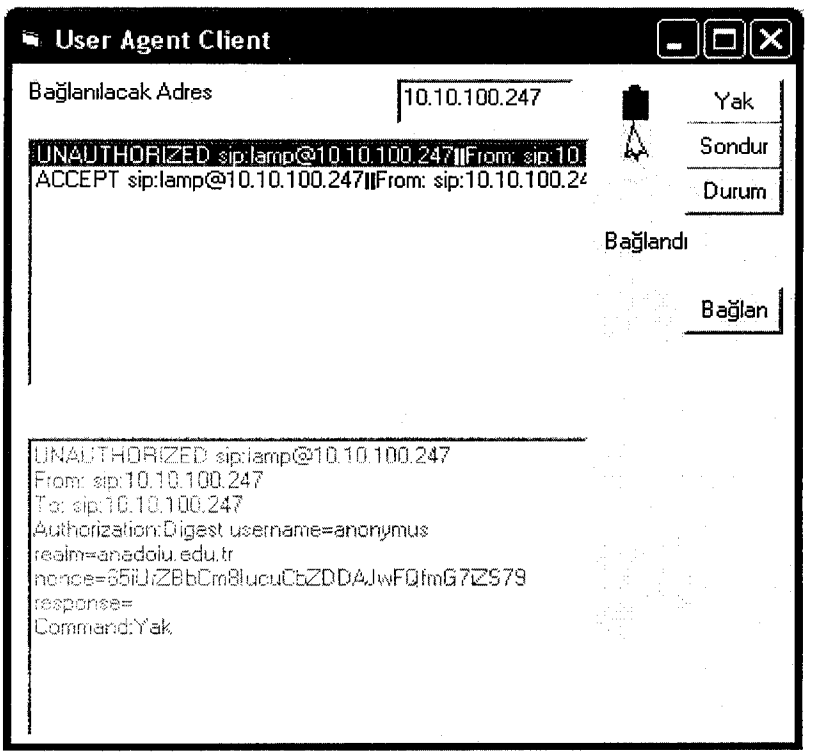
Geliştirilen UAC uygulaması, kullanıcının istediği kontrol veya kumanda mesajını istediği aygıta yollayabilmesini sağlayan bir ara yüz olarak tasarlanmıştır. Bu uygulama gerekli komutlar verildiğinde uygun mesajı oluşturup karşı tarafa yollar. Bu uygulamanın geliştirilmesindeki amaç SIP'in kimlik denetim yapısını kullanmak olduğundan, iletilen mesajlar son derece basit tutulmuş ve sadece hayati öneme sahip başlık alanları mesaja dahil edilmiştir. Taşınan mesaj olarak ise yine basit komutlar (Yak, Söndür, Durum) kullanılmıştır.

UAC tarafından karşı tarafa ilk defa istek iletilirken, bu isteğin içerisinde kimlik denetim bilgileri yer almamaktadır. Yani ilk istek mesajında kimlik denetimi için herhangi bir çaba yoktur. Bu mesaja karşı taraftan (UAS) gelen kimlik denetim isteğine ise, ilk yollanan mesaja kimlik denetim bilgileri eklenerek yanıt verilir ve karşı tarafa kimlik kanıtlanır. Bu arada karşı tarafa kimlik denetim isteği belirtilir (mesaja bir nonce değeri ekleyerek). Daha sonra ise karşı taraftan gelecek yanıt alınır ve gelen kimlik denetim bilgilerine bakılarak karşı tarafın kimliği denetlenir. Ve en son olarak da yanıtın alındığına dair bir mesaj (ACK mesajı) karşı tarafa daha önceden kullanılmış olan kimlik denetim bilgilerini kullanarak yollanır.

Uygulamanın kullanıcısına sunduğu ara yüz son derece basittir(Şekil 4.1). Form üzerinde bağlanılacak aygıtın ağ adresinin girileceği bir alan bulunmaktadır. Bu alana adres girildikten sonra karşı tarafla bir ağ bağlantısı kurulmakta ve

iletime hazır hale getirilmektedir. Bundan sonra ise yapılması gereken kullanıcının ilgili komut düğmesine basarak isteğini belirtmesidir. Bu komut düğmelerinden Yak ve Sondur başlıklı olanlar lambanın durumunu değiştirmek için, Durum başlıklı olan ise lambanın o anda sağlam olup olmadığını sorgulamak için kullanılmaktadır. Bu istek belirtildikten sonra mesaj uygulama tarafından oluşturulup karşı tarafa iletilmektedir. İletim sırasında kimlik denetimi işlemleri de yerine getirilmektedir. Eğer bağlantı kurulan aygıta (ya da bu aygıtın bulunduğu bölgeye) ait kullanıcı ismi ve şifre daha önceden veritabanına kaydedilmemişse, bu bilgiler kullanıcıdan istenmektedir. Ve bu bilgiler ileride kullanılmak üzere, isteğe bağlı olarak veritabanına eklenmektedir. Kimlik denetim işlemlerinden sonra yapılması istenen işleme karşılık gelen yanıt işlenmekte, ve aygıtın durumu ekran üzerinde görsel olarak kullanıcıya iletilmektedir.

Uygulamada ayrıca iletilen mesajların izlenebilmesi için bu mesajlar direk olarak form üzerinde gösterilmektedir. Bu sayede iletilen mesajların içeriği kolayca takip edilebilmektedir. Bu tip bir özellik son kullanıcıya dağıtılacak bir uygulamada gereksiz olacaktır.



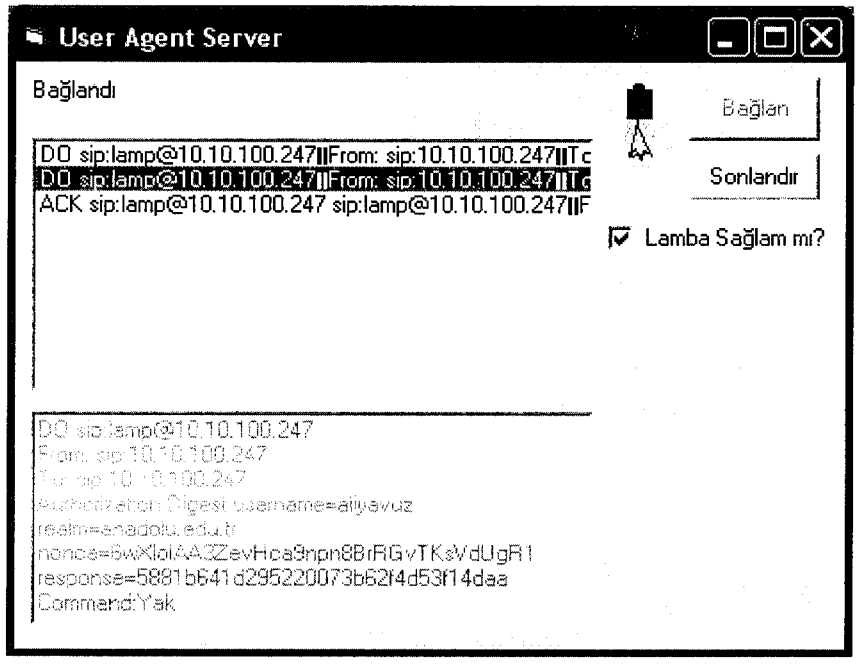
Şekil 4-1 UAC Kullanıcı Ara yüzü

4.1.2 UAS (User Agent Server)

Geliştirilen UAS uygulaması ise UAC'den gelen mesajları işleyerek gerekli işlemleri yerine getirmektedir. Bu uygulama ağ ile aygıt arasında bir ara yüz olarak tasarlanmıştır. Fakat burada uygulama kolaylığı açısından aygıt benzetim yapılarak ifade edilmiştir.

Karşı taraftan alınan mesaj ilk olarak kimlik denetiminden geçirilmektedir. Eğer kimlik denetim bilgileri mesaj içerisinde yer almıyorsa, bu bilgiler bir yanıt mesajıyla isteği yapan taraftan istenir (Unauthorized yanıtıyla). Bu yanıta karşılık olarak gelen mesajdaki (eğer varsa) kimlik denetim bilgileri kontrol edilerek karşı tarafın kimliği denetlenir. Kimliği denetlenen isteğe karşılık gelen işlemler yerine getirildikten sonra, bu isteklerin yerine getirildiğine (bazen de başarısız olduğuna) dair bir yanıt karşı tarafa yollanır. Bu yanıtta da UAS'in kendi kimlik denetim bilgileri eklenerek karşı tarafa kimlik kanıtlanır.

Uygulamada kullanıcıya sunulan ara yüz son derece basittir (Şekil 4.2). Form üzerinde karşı taraftan gelecek bağlantıyı kabul etmek veya varolan bağlantıyı sonlandırmak için iki komut düğmesi bulunmaktadır. Bunların yanında lambayı ifade eden bir resim bulunmakta ve bu resmin durumu (görüntüsü) gelen isteklere göre gerçek lambanın vermesi gereken tepkileri gösterecek şekilde değiştirilmektedir. Ayrıca lambanın bozuk veya sağlam olduğunu gösteren bir algılayıcı da bir seçenek düğmesi ile ifade edilmiş ve buna göre lambanın verebileceği tepkiler belirlenmiştir (bozuk bir lambanın yakılması veya söndürülmesi mümkün değildir, ayrıca durum bilgisi soran mesajlara da lambanın durumu hakkında yanıt verilmesi gerekebilir). Uygulamaya gelen bütün mesajlar form üzerinde gösterilerek mesajların takip edilmesi kolaylaştırılmıştır. Bu sayede mesajın başlık alanları ve taşıdığı komut kolayca incelenebilmektedir.



Şekil 4-2 UAS Kullanıcı Ara yüzü

4.1.3 Digest kimlik denetim yapısının uygulanması

Daha önceki konularda ele alındığı gibi HTTP Digest kimlik denetim yapısı istek-yanıt mantığıyla çalışmaktadır. Yani bir mesajda kimlik denetim bilgilerinin bulunması için bu mesajı gönderen, söz konusu bilgileri mesaja koymak için zorlanmalıdır. Geliştirilen uygulamada da aynı yapı oluşturulmuş ve karşılıklı kimlik denetimi sağlanmıştır.

Kimlik denetimi bilgilerini doğrulamak için belli bir alan için geçerli kullanıcı ismi ve şifre kullanılmıştır. Bu kullanıcı ismi ve şifrenin daha önceden aygıt ve kullanıcı arasında belirlenmiş olduğu varsayılmaktadır. Kullanıcı ismi ve şifre direk olarak mesaj içerisinde iletilmemektedir. Bunun yerine mesajın belli alanları ve şifre belli bir karıştırma fonksiyonu içerisine sokulmakta ve geri dönen değer mesaj içerisinde karşı tarafa yollanmaktadır. Bu mesajı alan başlık alanlarını ve kendi veritabanındaki şifreyi aynı fonksiyona sokarak bir değer elde etmektedir. Karşı taraftan gelen hesaplanmış değer ile kendi hesapladığı değeri karşılaştırdıktan sonra, eğer iki değer aynı ise kullanıcının kimliği denetlenmiş olmaktadır.

Geliştirilen uygulamada bu karıştırma fonksiyonu, MD5[31] algoritmasıdır. Yani başlık alanları ve şifre MD5 algoritması kullanılarak karıştırılmakta ve kimlik denetimi için kullanılacak değer elde edilmektedir. Bu değer daha sonra kimlik denetim bilgisi olarak gönderilecek mesaja eklenmekte ve karşı tarafın bu değere bakarak kimlik denetim yapması sağlanmaktadır.

Burada kullanılan kimlik denetimi direk olarak kullanıcı-kullanıcı arasındaki kimlik denetimidir. Küçük değişikliklerle bu yapının kullanıcı-proxy sunucu arasındaki kimlik denetimi için de kullanılması mümkündür.

5. SONUÇLAR

Bu tezde Akıllı Evler ve Ağa Bağlı Aygıt (ABA) kontrol ve kumandasında SIP protokolünün kullanılması çeşitli açılardan ele alınmış ve yapılan incelemeler sonucu kullanımı uygun görülmüştür. Söz konusu protokol temel çalışma mantığı ve işleyişi ile Akıllı Evler ve ABA kontrol ve kumandasında ihtiyaç duyulan işlevleri rahatça yerine getirebilecektir. Fakat bu tezin esas dikkat ettiği husus, Akıllı Evler ve ABA kontrol ve kumandasında ihtiyaç duyulacak güvenlik gereksinimleridir. Bu gereksinimlerin SIP protokolü tarafından ne kadar başarıyla karşılanabileceği, protokolün söz konusu ihtiyaçları karşılamak için nasıl kullanılabileceği tezin esas konudur.

Yapılan incelemeler sonucu SIP protokolünün güvenlik hizmetlerinin genel olarak Akıllı Evler ve ABA kontrol ve kumandasında ihtiyaç duyulan güvenliği büyük oranda sağladığı belirlenmiştir. Protokolün sağlayamayacağı hizmetler ise ya protokolün küçük değişikliklerle kullanılması ile yada başka protokol ve teknolojilerden hizmet alınması yoluyla elde edilebilmektedir. Bu sayede güvenlik yeterli bir seviyede sağlanabilmektedir.

SIP temel olarak HTTP temelli bir protokol olduğu için güvenlik hizmetleri de bu protokolün hizmetleriyle paralellik gösterir. Zaten varolan ve çok fazla uygulaması olan bir protokolün hizmetlerine paralel yöntemler kullanılacağı için hem uygulama daha kolay olmaktadır, hem de uyumluluk problemleri daha az olmaktadır. SIP hizmetleri Akıllı Ev ve ABA kontrol ve kumandasında kullanılırken de bu özellikler uygulayıcılara kolaylıklar getirecektir.

Bu konu ele alındıktan sonra basit bir uygulamayla SIP güvenlik hizmetlerinden Digest kimlik denetim yapısı aygıt kontrolü için iki yönlü olarak kullanılmıştır. Uygulama geliştirilirken SIP güvenliğinin kolayca Akıllı Ev ve ABA kontrol ve kumandasına uyarlanabileceği görülmüştür.

Sonuç olarak Akıllı Evler ve ABA kontrol ve kumandasında SIP uygun biçimde kullanılarak kullanıcılara hizmet sağlayabilecek bir protokoldür. Bu protokolün kullanımı ve ortaya çıkacak daha yeni teknolojilerle birleştirilmesi sayesinde istenilen hizmetler elde edilebilecektir.

KAYNAKLAR

[1] ROSENBERG, J., SCHULZRINNE, H., CAMARILLO, G., JOHNSTON, A., PETERSON, J, SPARKS, R., HANDLEY, M. ve SCHOOLER, E., *SIP: session initiation protocol*, RFC 3261, Internet Engineering Task Force (IETF), (2002)

[2] Universal Plug and Play, http://www.upnp.org/

[3] Zero Configuration Networking, http://www.zeroconf.org/

[4] TSANG, S. MOYER, S., MARPLES, D., SCHULZRINNE, H., KATZ, J., GURUNG, P., CHENG, T., DUTTA, A. ve ROYCHOWDHURY, A., "*Framework Draft for Networked Appliance using the Session Initiation Protocol*", Internet Draft, Internet Engineering Task Force , (2000).

[5] X10 Remote Control, www.x10.org

[6] The Community Resource for Jini Technology, www.jini.org

[7] Home Audio Video Interconnectivity Organisation, www.havi.org

[8] VESA Home Networking, www.vesa.org

[9] GUTTMAN, E., PERKINS, C., VEIZADES J. ve DAY, M., *Service Location Protocol, Version 2*, RFC2608, (1999)

[10] STALLINGS, W., *Network and interwork security*, Prentice Hall, (1995)

[11] National Institute of Standards and Technology, *Data Encryption Standard*, FIPS 46-3, (1999)

[12] National Institute of Standards and Technology , *Specification for the ADVANCED ENCRYPTION STANDARD(AES)*, Federal Information Processing Standard (FIPS)Publication 197, (2001)

[13] RESCORLA, E., *Diffie-Hellman Key Agreement Method*, RFC2631, (1999)

[14] JONSSON J. ve KALISKI, B., *Public-Key Cryptography Standards (PKCS)#1:RSA Cryptography Specifications Version 2.1*, RFC3447, (2003)

[15] FREED, N. ve BORENSTEIN, N., "*Multipurpose Internet Mail Extensions(MIME) Part One-Five*",RFC2045-RFC2046-RFC2047-RFC2048-RFC2049, (1996)

[16] HANDLEY, M. ve JACOBSON, V., "*SDP: Session Description Protocol*", RFC2327, (1998)

[17] INFORMATION SCIENCES INSTITUTE UNIVERSITY OF SOUTHERN CALIFORNIA, "*Transmission Control Protocol*", RFC793, (1981)

[18] POSTEL, J., *UDP: User Datagram Protocol*, RFC768, (1980)

[19] ATM(Asynchronuos Transfer Mode), www.atmforum.org

[20] Internetwork Packet Exchange Protocol , http://www.novell.com/documentation/nw5/docui/index.html#../uscomm/rtcn_enu/data/hofxxkto.html

[21] BROWN, C. ve MALIS, A., *Multiprotocol Interconnect over Frame Relay*, RFC2427, (1998)

[22] KOCH, D., *SIP Security*, University Of Waterloo, (2001)

[23] FIELDING, R., GETTYS, J., MOGUL, J., FRYSTYK, H., MASINTER, L., LEACH, P. ve BERNERS-LEE, T., *Hypertext Transfer Protocol -- HTTP/1.1*, RFC2616, (1999)

[24] SCHULZRINNE, H., CASNER, S., FREDERICK, R. ve JACOBSON, V., *RTP: A Transport Protocol for Real-Time Applications*, RFC3550, (2003)

[25] KLENSIN, J., *Simple Mail Transfer Protocol*, RFC2821, (2001)

[26] DIERKS, T. ve ALLEN, C., *The TLS Protocol Version 1.0*, RFC2246, (1999)

[27] KENT, S. ve ATKINSON, R., *Security Architecture for the Internet Protocol*, RFC2401, (1998)

[28] FRANKS, J., HALLAM-BAKER, P, HOSTETLER, J., LAWRENCE, S., LEACH, P., LUOTONEN, A. ve STEWART, L., *HTTP Authentication : Basic and Digest Access Authentication*, RFC2617, (1999)

[29] GALVIN, J., MURPHY, S., CROCKER S. ve FREED, N., *Security Multiparts for MIME: Multipart/Signed and Multipart/Encrypted*, RFC 1847, (1995)

[30] Secure Shell Communications Security, www.ssh.com

[31] RIVEST, R., *The MD5 Message-Digest Algorithm*, RFC 1321, (1992)