Co-funded by the Erasmus+ Programme of the European Union

InCyT Eğitim Modülleri

Çalışanlar için Bilgi Güvenliği **Birim no: (3) 5. Hafta** **Birim (Modül) adı: (İş gezilerinde güvenlik)**	
Öğrenme aktiviteleri	❑ **Web semineri** ❑ **Egzersizler** ❑ **Atölye** ❑ **Sunum** ❑ **Diğer**
Öğrenme Sorumlusu	• Miroslaw Mazurek • Pawel Dymora
Öğrenme Etkinliği Hedefleri	1. Kablosuz Ağlar 2. VPN 3. E-posta şifreleme
Kazanılacak Beceriler	• **TS3** • **SS2**
Öğrenme faaliyetinin süresi	2 hafta
Öğrenme Gereksinimler	***İhtiyaç duyulan şey?*** • internet girişi • İnternet tarayıcısı • MS Office365

Funded by the European Union. Views and opinions expressed are however those of the author(s) only and do not necessarily reflect those of the European Union or the European Education and Culture Executive Agency (EACEA). Neither the European Union nor EACEA can be held responsible for them.

Co-funded by the Erasmus+ Programme of the European Union

Modül hakkında kısa bilgi

Tanım
Bu modülün genel ana hatları, iş gezilerinde bilgi ve pratik beceri güvenliği ile ilgili bazı teorik ve pratik konuları sağlamaktır. VPN fikri ile kablosuz ağınızı koruma ve korumalı kablosuz ağları kullanma imkanına sahip olacaksınız. Modül ayrıca, sizin izniniz olmadan kimsenin çözemeyeceği şifreli mesajlar için ücretsiz PGP protokolü kullanarak e-postaların nasıl güvenli bir şekilde gönderileceğini de kapsayacaktır.

Öğrenme Materyalinin İçeriği

1. Kablosuz ağlara giriş. Teorik temeller: çalışma prensibi, şifreleme protokolleri.

Daha önceki WEP ve WPA protokolleri, kablosuz ağların güvenliğini sağlamak için kullanılıyordu, ancak bunlar bilgisayar korsanlarının saldırılarına karşı dayanıklı değildi. WPA2 protokolünün tanıtılması, yeterli düzeyde güvenlik sağlanmasına izin verdi, ancak yine de tam güvenlik sağlamaz. Birçok ağ topolojisi, kablosuz erişim protokolü ve ağ erişim toplama teknikleri mevcuttur ve ağ anahtarı edinmede hem CPU (Merkezi İşlem Birimi) hem de GPU (Grafik İşlem Birimi) bilgi işlem mimarileri kullanılır [1,2].

WEP (Kabloluya Eşdeğer Gizlilik), en eski IEEE 802.11 kablosuz şifreleme standartlarından biridir. RC4 algoritmasının kullanımına dayalı bilgi koruması sağlar. Bilinen birçok güvenlik açığına sahiptir ve bu nedenle birden çok kez kırılmıştır. WLAN ağlarının güvenliğini sağlamak için en eski standartlardan biridir (1997'de kurulmuştur). Kurulu cihazların yüksek bilgi işlem gücüne ihtiyaç duymaz. İki kullanıcı kimlik doğrulama yöntemi kullanır: Açık Kimlik Doğrulama ve Paylaşılan Anahtar Kimlik Doğrulama. Ayrıca, ACL (Erişim Kontrol Listesi) kullanılarak fiziksel MAC adreslerine dayalı kullanıcı doğrulamasını sağlar. 64 bit WEP varyantı (40 bit anahtar ve 24 bit başlatma vektörüne dayalı) ve 128 bit WEP varyantı (104 bit anahtara dayalı) vardır. Bazı üreticiler ayrıca 256-bit WEP standardı [1,2] tanıttı.

WPA (Wi-Fi Korumalı Erişim), IEEE 802.11 kablosuz ağlarının şifrelenmesi için başka bir standarttır. WEP standardındaki bilinen güvenlik açıklarının yerini alarak WLAN ağlarının güvenlik düzeyini iyileştirmek için tanıtıldı. Protokollerin kullanımına dayanmaktadır: TKIP (Geçici Anahtar Bütünlüğü Protokolü) ve EAP (Genişletilebilir Kimlik Doğrulama Protokolü), 802.1x standardı ve MIC (Mesaj Bütünlüğü Kontrolü) mekanizması. Standart, RC4 algoritmasına dayanmaktadır. WEP standardı ile mevcut en güvenli kablosuz şifreleme standardı 802.11i arasında geçici bir çözüm olarak uygulandı. Aşağıdakileri içeren iki modda çalışma sağlar: Kurumsal (anahtarların kullanıcılara atanmasını yöneten bir RADIUS sunucusu kullanarak) ve Kişisel (paylaşılan bir PSK

Funded by the European Union. Views and opinions expressed are however those of the author(s) only and do not necessarily reflect those of the European Union or the European Education and Culture Executive Agency (EACEA). Neither the European Union nor EACEA can be held responsible for them.

Co-funded by the Erasmus+ Programme of the European Union

anahtarı kullanarak) [1,2].

WPA2 (Wi-Fi Korumalı Erişim 2) şu anda kablosuz ağlar için en güçlü şifreleme standardıdır (802.11i olarak da bilinir). AES (Gelişmiş Şifreleme Standardı) kullanımına dayalı bilgi koruması sağlar. WLAN ağlarının güvenlik düzeyini iyileştirmek için tanıtıldı, WEP standardındaki ve geçici WPA standardındaki bilinen güvenlik açıklarının yerini aldı. Ağa kullanıcı erişiminin kontrolünü iyileştiren 802.1x protokolünü uygular. Şunları içeren iki modda çalışma sağlar: Kurumsal (anahtarların kullanıcılara atanmasını yöneten bir RADIUS sunucusu kullanarak) ve Kişisel (paylaşılan bir PSK anahtarı kullanarak) - günümüzde genellikle ev çözümlerinde kullanılır [1,2].

WEP algoritması, IEEE 802.11 kablosuz ağları için en az güvenli şifreleme standardıdır. Algoritmanın güvenlik yönlerinde şu anda bilinen birçok güvenlik açığı nedeniyle çeşitli yöntemlerle birçok kez kırılmıştır. Standardın ana dezavantajları şunlardır[3]:

- Tanımlanmış bir anahtar yönetim sisteminin olmaması (genellikle bir kablosuz ağın tüm düğümleri tarafından bir ağ anahtarı kullanılır);
- Ağ anahtarının yetersiz bit boyutu (WEP standardının ilk sürümü 40 bitlik anahtarlar sunar);
- IV başlatma vektörünün yetersiz bit boyutu (WEP standardı, yetersiz olduğu ortaya çıkan 24 bitlik bir başlatma vektörü sunar ve az sayıda alınan paketle nispeten yüksek çarpışma olasılığı nedeniyle, WEP anahtarının değerini elde etmek için bir kriptografik saldırı);
- CRC-32 lineer işlevine dayalı zayıf ICV sağlama toplamı (ağda gönderilen bilgilerde fark edilmeyen değişiklik olasılığı vardır);
- Zayıf RC4 bilgi şifreleme algoritması (ağ anahtarı ile bilgi şifrelemenin sonucu arasında çok fazla bağımlılık vardır);
- Yetersiz kullanıcı kimlik doğrulama sistemi (kimlik doğrulama mesajlarını taklit etme olasılığı vardır).
- WEP algoritmasının sunulan zayıflıklarına dayanarak, WLAN ağlarının güvenlik seviyesini test eden saldırılar yapmak için birçok araç oluşturulmuştur. WEP'e karşı en popüler saldırılar şunları içerir:
- FMS saldırısı - WEP şifreleme standardında kullanılan RC4 algoritmasına istatistiksel bir saldırı (Fluhrer, Mantin ve Shamir tarafından geliştirildi);
- KoreK saldırısı - RC4 algoritması şifreleme işleminin birkaç daha fazla bağımlılığını (FMS saldırısına kıyasla) kullanan istatistiksel bir saldırı (KoreK lakaplı bir kişi tarafından geliştirildi);
- Chopchop saldırısı - alınan paketlerden birinin şifresini kademeli olarak çözerek ağa erişim sağlama yönünde gerçekleştirilen etkileşimli bir saldırı;
- PTW saldırısı - RC4 algoritması üzerine istatistiksel bir saldırıdır (Pyshkin , Tews ve Weinmann tarafından geliştirilmiştir) ve veri şifreleme sürecinin ardışık bağımlılıkları sayesinde, nispeten az sayıda anahtar değeri ile anahtar değerini elde etme olasılığını önemli ölçüde artırır. Alınan Paketler.

Sık kullanılan bir diğer saldırı türü ise Sözlük saldırısıdır. Kablosuz bilgisayar ağlarında örneğin

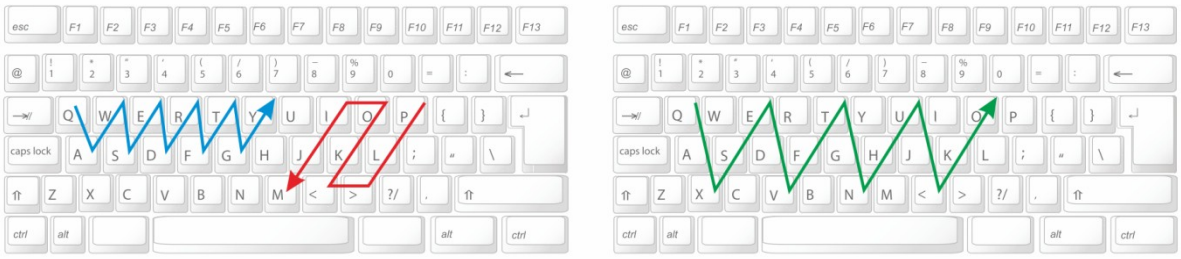
Funded by the European Union. Views and opinions expressed are however those of the author(s) only and do not necessarily reflect those of the European Union or the European Education and Culture Executive Agency (EACEA). Neither the European Union nor EACEA can be held responsible for them.

Co-funded by the Erasmus+ Programme of the European Union

kriptografik anahtar değerleri elde etmenin kaba kuvvet yöntemlerinden biridir. WPA/WPA2 anahtar değerlerini elde etmek için yöntem, tek yönlü şifrelemeye ve sözlükteki girişleri yakalanan 4 yönlü el sıkışma dizisindeki bilgilerle karşılaştırmaya dayanır. Sözlük saldırıları, kaba kuvvet yöntemine kıyasla anahtar değerleri elde etme süresini azaltmak amacıyla gerçekleştirilir. Anahtar değerini alma işlemi, olumlu bir sonuç elde edilene kadar (yani, sözlükteki girişin geçerli bir anahtar değer olduğu ortaya çıktığında) veya sözlükteki tüm girişler olumsuz sonuçla karşılaştırılıncaya kadar devam eder. Negatif bir sonuç, anahtar değerin yüksek düzeyde karmaşıklığını ve kaba kuvvet yöntemini kullanma ihtiyacını gösterebilir[3].

Bu saldırının başarısı, uygun bir sözlüğün seçilmesidir. Sözlük, örneğin kriptografik anahtar değerleri elde etmek için sözlük saldırıları durumunda kullanılan bir metin dosyasıdır. Aranan anahtar değeri oluşturabilecek uygun şekilde hazırlanmış öğelerin bir listesini içerir. Kuvvet saldırıları durumunda sözlüklerin kullanılması, incelenen değerler kümesinin önemli ölçüde azaltılmasına olanak tanır, bu da kriptografik anahtar değerini edinme sürecinin hızlandırılmasına neden olabilir. Sözlüklerin içeriği, örneğin sunulan öğeler temelinde oluşturulur[3]:

- yerli ve yabancı sözlüklerde geçen kelimelerin bir listesi;
- büyük ve küçük harfli kelime kombinasyonları, ters yazılmış kelimeler (yani palindromlar);
- kesik sesli harfler veya ünsüzler ile sözlük girişlerinin kombinasyonları;
- seçilen adların, soyadların, sözlük girişlerinin çoklu tekrarlarının kombinasyonları;
- sayısal değerler, özel karakterler vb. içeren sözcük kombinasyonları;
- kullanıcılar tarafından en sık kullanılan parolaların ve oturum açma bilgilerinin bir listesi;
- popüler şirketlerin, kuruluşların, teknik terimlerin, özel adların vb. listesi;
- çeşitli internet portallarından bilgi sızıntıları (yani oturum açma bilgileri, takma adlar, şifreler);
- seçilen desenler için bitişik klavye karakterlerinin kombinasyonları (Şekil 1).



Şekil 1 . Ağ anahtarı oluşturma modellerinin örneklerini gösteren şema

Ağ anahtarı, ağ esnekliği çalışmasında önemli bir rol oynar. Kimlik doğrulama sürecinde ağ kullanıcıları tarafından kullanılan bir dizi karakterdir. Kimlik doğrulama işlemi, paylaşılan hizmetlere ve ağ kaynaklarına erişimi yetkisiz kullanıcılardan korumada önemli bir adımdır. Ağ anahtarları genellikle ağ yöneticileri tarafından oluşturulur ve yönetilir ve bir bilgisayar ağının güvenliğindeki en zayıf halkayı oluşturabilir. Göreceli olarak zaman alan veya kaba kuvvet

Funded by the European Union. Views and opinions expressed are however those of the author(s) only and do not necessarily reflect those of the European Union or the European Education and Culture Executive Agency (EACEA). Neither the European Union nor EACEA can be held responsible for them.

yöntemleri kullanılarak gerçekçi zamanda kırılması imkansız olan anahtar değerler, örneğin sunulan kurallara dayalı olarak oluşturulmalıdır [3]:

- Yönetici tarafından yönetilen her kablosuz ağ, farklı bir ağ anahtarı kullanılarak güvence altına alınmalıdır;
- Her ağ kullanıcısı ayrı bir ağ anahtarı kullanmalıdır;
- Ağ anahtarları yeterli sayıda karakter üzerine kurulmalıdır;
- Anahtarların oluşturulması, kullanılabilir maksimum karakter alanına dayalı olmalıdır;
- Anahtarlar, kurumsal ve kişisel bilgiler kullanılarak oluşturulmamalıdır;
- Anahtar oluşturma, herkese açık sözlüklerdeki bir öğe listesine dayanmamalıdır;
- Ağ anahtarları, rastgele karakter dizileri temelinde oluşturulmalıdır;
- Ağ anahtarları periyodik olarak güncellenmelidir;
- Halihazırda kullanılan anahtar değerler, artık kullanılmayan anahtar değerlerle ilişkilendirilmemelidir.

2. Sanal VPN tünelleri. Teorik temel: türleri, mimarisi, çalışma prensibi, şifreleme protokolleri. Open VPN programının kurulumu (konfigürasyon, adresleme, parametre seçimi, anahtar oluşturma).

Sanal Özel Ağ, özel ağ trafiğinin bir genel ağ üzerinden gönderici ve alıcı arasında aktığı bir tüneldir. VPN, 'Sanal Özel Ağ' anlamına gelir. Bir VPN ağı, internetteki tüm etkinlikleri şifreler, IP adresini gizleyerek ağ kullanıcısının kimliğini korur. Bir VPN bağlantısı, dünyanın her yerinden uygulamalara, web sitelerine ve eğlence platformlarına güvenli erişim sağlar. Daha iyi kalite veya daha yüksek düzeyde güvenlik sağlamak için iletilen verileri isteğe bağlı olarak sıkıştırmak veya şifrelemek, böylece ağ içindeki gizliliği korumak mümkündür [4].

Önce istemcinin VPN sunucusuyla kimliği doğrulanarak güvenli bir tünel oluşturulur. Sunucu daha sonra gönderilen ve alınan tüm verilere bir şifreleme protokolü uygular. Her veri paketinin güvenliğini sağlamak için VPN, onu daha sonra kapsülleme ile şifrelenen harici bir pakete yerleştirir. İletim sırasında verilerin güvenliğini sağlar ve VPN tünelinin temel bir bileşenidir. Veriler sunucuya ulaştıktan sonra şifre çözme işleminde harici paketler kaldırılır [4] .

VPN'ler iki ana kategoriye ayrılabilir [5] :

- Kullanıcıların genellikle özel yazılım aracılığıyla uzak bir ağa bağlanmasına izin veren bir uzaktan erişim VPN'i.
- Şirketler, özellikle büyük şirketler tarafından kullanılan siteden siteye VPN'ler. Seçilen konumlardaki kullanıcıların diğer kullanıcıların ağlarına güvenli bir şekilde erişmesine izin verir.

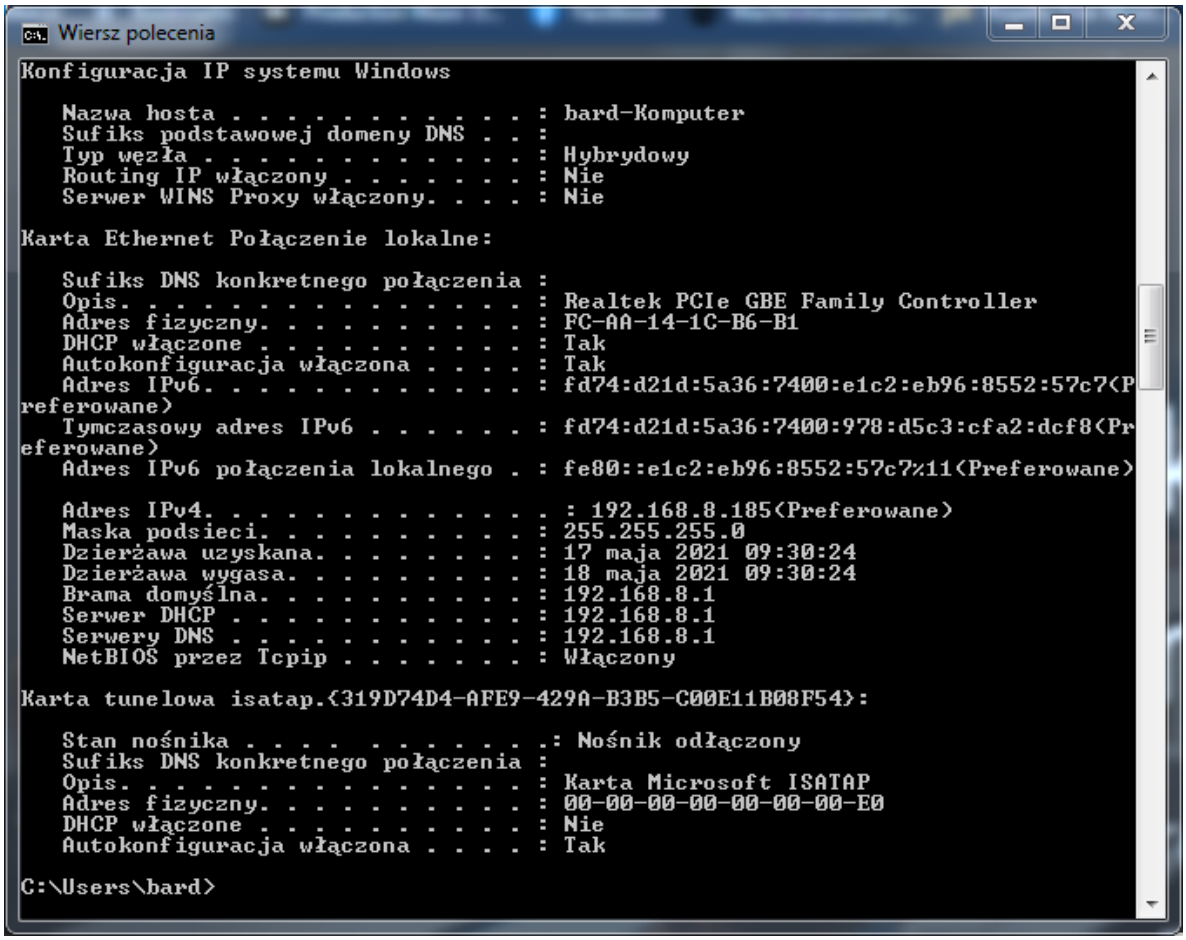
Özel bir VPN geliştirme yazılımına örnek olarak *RadminVPN verilebilir* . Çoğu durumda, bir VPN tüneli kurmak için yerel ağınızda statik bir IP adresine sahip olmak gerekli değildir. Uygun yazılımı indirdikten sonra , bilgisayarınızın statik adresi ile uygun bir ağ oluşturacaktır. [6] .

Radmin VPN iki farklı ağdaki iki bilgisayara bağlanmanızı sağlar. Aşağıda bir yapılandırma

Funded by the European Union. Views and opinions expressed are however those of the author(s) only and do not necessarily reflect those of the European Union or the European Education and Culture Executive Agency (EACEA). Neither the European Union nor EACEA can be held responsible for them.

Co-funded by the Erasmus+ Programme of the European Union

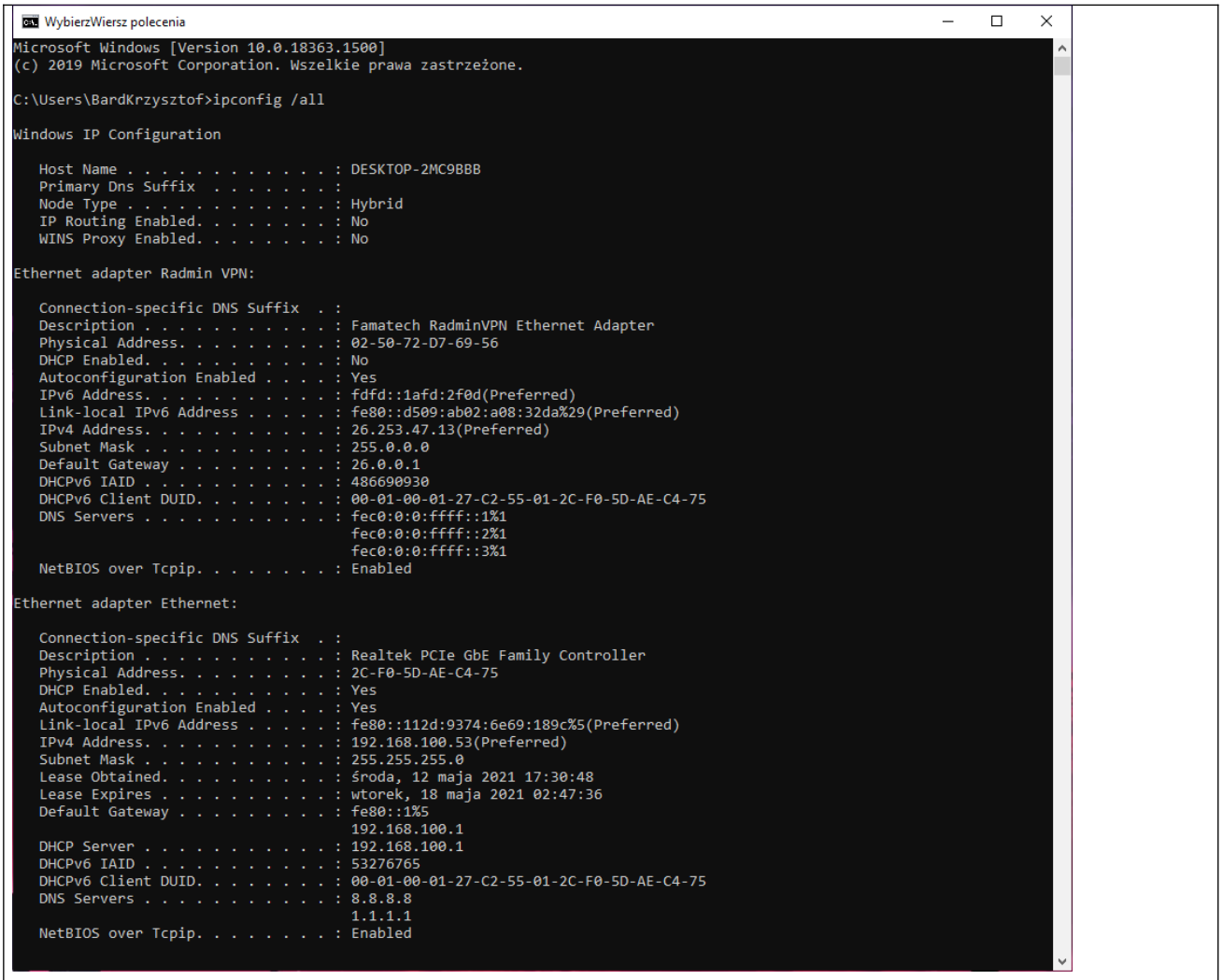
örneği gösterilmektedir. VPN kanalının çalışmasının daha kolay anlaşılması için Şekil 2 ve 3, aralarında güvenli bir kanalın oluşturulacağı bilgisayarların ilk yapılandırmasını göstermektedir.



Şekil 2. Bilgisayarların ilk yapılandırması

Funded by the European Union. Views and opinions expressed are however those of the author(s) only and do not necessarily reflect those of the European Union or the European Education and Culture Executive Agency (EACEA). Neither the European Union nor EACEA can be held responsible for them.

Co-funded by the Erasmus+ Programme of the European Union

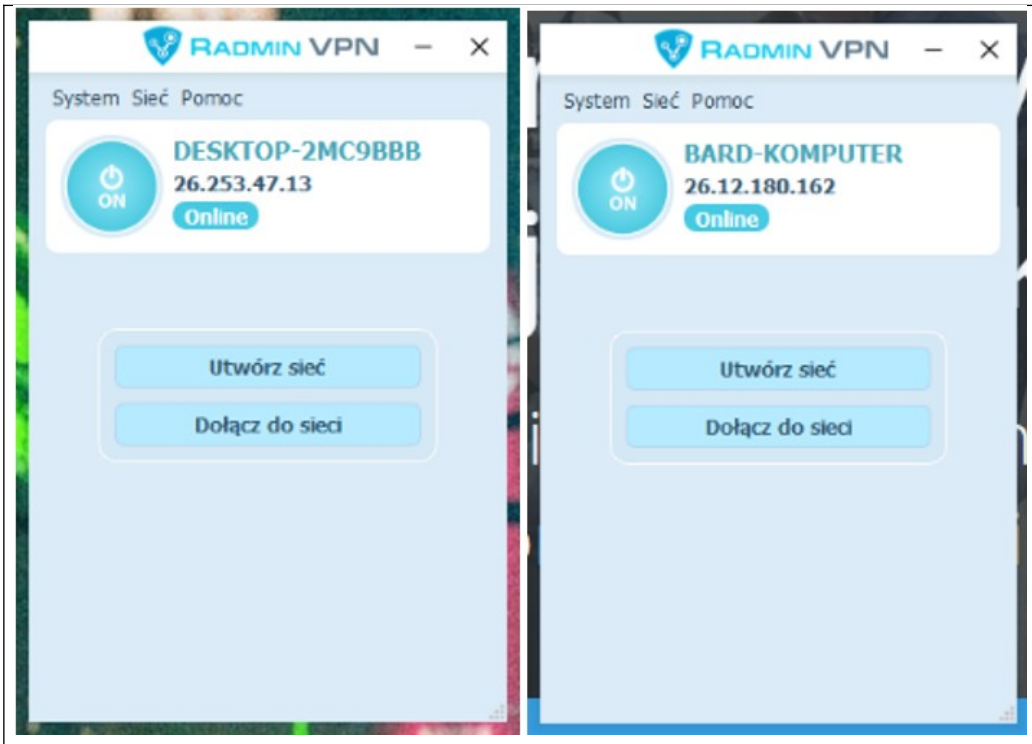


Şekil 3. Bilgisayarların ilk yapılandırması

Gördüğünüz gibi, ağ geçidi adresleri tamamen farklıdır, bu nedenle bilgisayarların birbirleriyle fiziksel veya mantıksal bir bağlantısı yoktur. Bir kanal oluşturmak için her iki bilgisayara da RadminVPN yükleyin. Bunlardan birinde kendi ağınızı oluşturarak başlamanız gerekir.

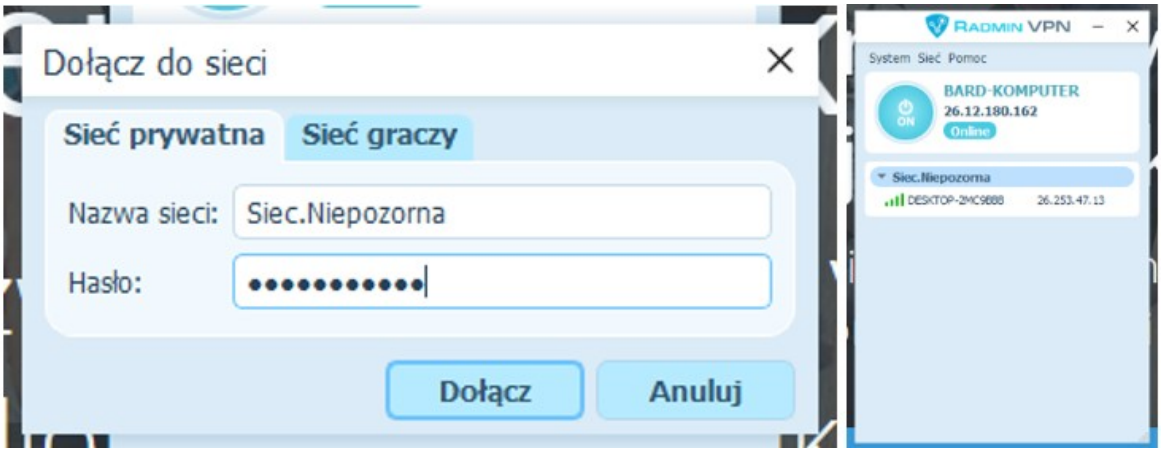
Funded by the European Union. Views and opinions expressed are however those of the author(s) only and do not necessarily reflect those of the European Union or the European Education and Culture Executive Agency (EACEA). Neither the European Union nor EACEA can be held responsible for them.

Co-funded by the Erasmus+ Programme of the European Union



Şekil 4. Uygulama ana ekranının görünümü (soldaki resim - bilgisayar 1'in konfigürasyonu, sağdaki resim - bilgisayar 2).

Bir ağ oluşturmak için , uygulama penceresinde **Ağ oluştur'u seçin, ağ** için bir ad ve şifre girin ve Oluştur düğmesiyle onaylayın. İkinci bilgisayarda bu şekilde oluşturulan ağ, Join the network butonuna tıklanarak yeni oluşturulan ağın adı ve şifresi girilerek eklenmelidir.

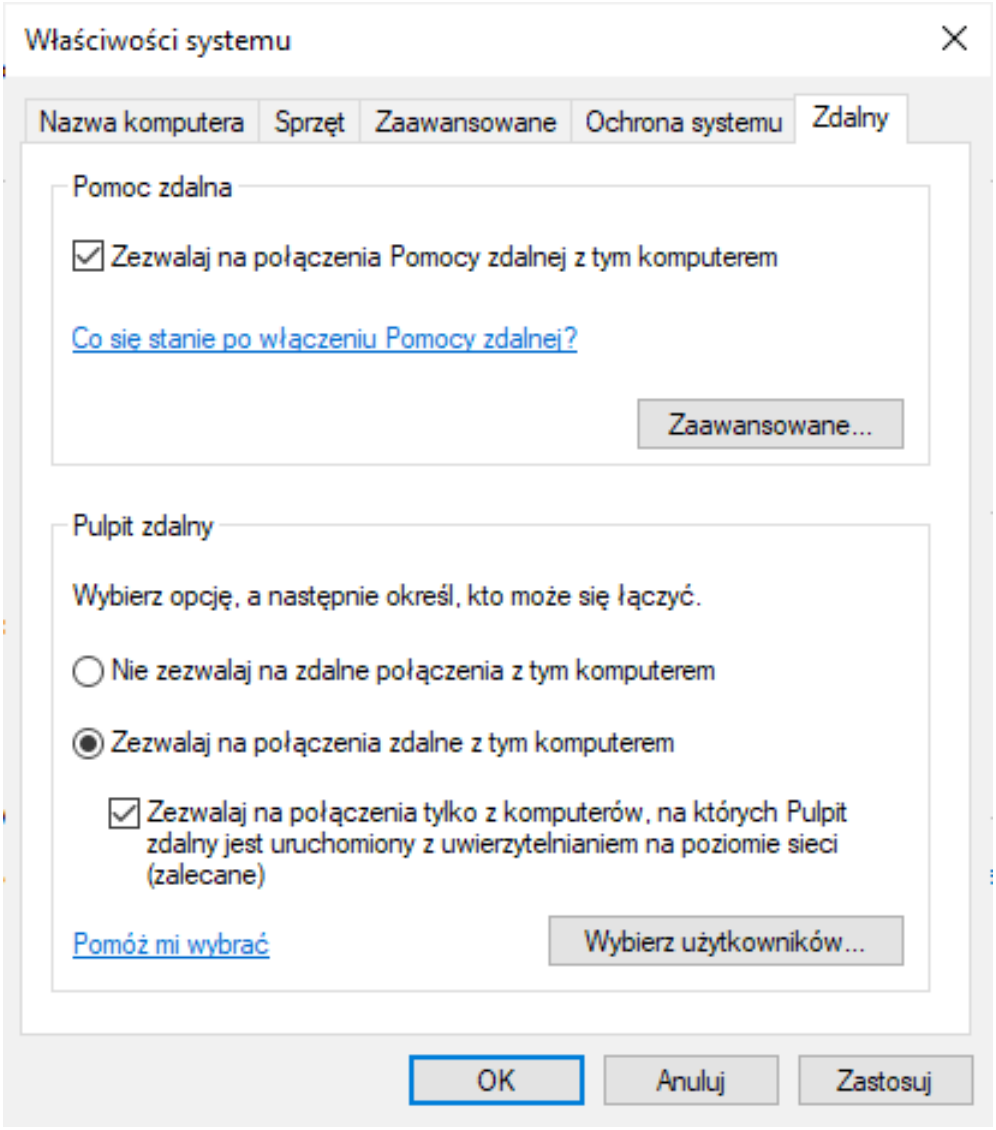


Şekil 5. a) Ağ bağlantısı penceresinin görünümü; b) bağlantı durumu.

Ağa başarılı bir şekilde katıldıktan sonra, her iki bilgisayar da ağ bağlantısı görünümünde olmalıdır (Şekil 5b'de gösterildiği gibi). Bu durumda tünelin diğer tarafında bilgisayarın adını ve adresini görebilirsiniz . İkinci bilgisayarda da aynı olacak. Sistem çalışması için Radmin Server gerekli

Funded by the European Union. Views and opinions expressed are however those of the author(s) only and do not necessarily reflect those of the European Union or the European Education and Culture Executive Agency (EACEA). Neither the European Union nor EACEA can be held responsible for them.

olduğundan , bu aşamadaki bağlantı girişimi başarısız olacaktır . Kurulumla ilgili bilgiler uygulamada görünecek ve her iki bilgisayarda da yapılmalı ve yeniden başlatılmalıdır. Tüm kurulum işlemi tamamlandıktan sonra bilgisayarlar iletişim kurabilecek ancak birinin diğerini kontrol etmesi mümkün olmayacaktır. Birbirinizi kontrol edebilmek için Windows'ta sistem uzak masaüstünü yapılandırmanız gerekir (Denetim Masası->Sistem ve sağ tarafta Gelişmiş Sistem Ayarları'nı seçin).



Şekil 6. Uzak Masaüstü bölümünün ayarları

Sistem Özellikleri penceresi görünür. Ardından, Bu bilgisayara uzak bağlantılara izin ver'i seçerek Uzak sekmesini ve Uzak Masaüstü bölümünü seçin (Şek. 6). Değişiklikleri her iki bilgisayarda da onayladıktan sonra, verilen erişim haklarına sahip bir kullanıcı oluşturun. Bunu yapmak için RadminServer'ı çalıştırın ve sağdaki alanlardan İzinler'i ve ardından İzinler seçeneğini seçin. İzinler penceresinde Tam erişim seçeneğini işaretleyin ve bir kullanıcı oluşturun (ona bir isim ve şifre

Funded by the European Union. Views and opinions expressed are however those of the author(s) only and do not necessarily reflect those of the European Union or the European Education and Culture Executive Agency (EACEA). Neither the European Union nor EACEA can be held responsible for them.

vermeniz gerekir). Bu, VPN kanalı yapılandırma sürecini tamamlar. Oluşturulan tünel çift yönlüdür ve bilgisayarları her iki taraftan da kontrol etmek için kolaylıkla kullanılabilir.

3. E-posta şifreleme. Teorik temel: şifreleme türleri (simetrik ve asimetrik), güvenlik, protokoller, anahtarlar. OpenPGP'nin kurulumu ve konfigürasyonu. Bir e-posta istemcisinin kurulumu ve yapılandırılması.

En yaygın kullanılan iletişim kanallarından biri, giderek artan bir şekilde bilgisayar korsanlığı saldırılarının hedefi haline gelen elektronik postadır (e-posta). Bu unsuru korumak, bir siber güvenlik çözüm paketinin önemli bir parçasıdır. E-postayı korumak ve ekleri şifrelemek çok önemli iki çevrimiçi güvenlik sorunudur. E-posta şifrelemesi, yalnızca gizli verilerin sızması riskini en aza indirmekle kalmaz, aynı zamanda yetkisiz müdahaleyi de önler. E-posta ve ekleri, varsayılan olarak SSL ve TLS protokolleri ile güvenli değildir ve tüm mesajlar düz metin olarak gönderilir [8] .

Şifreleme algoritmaları, kriptografi gibi iki kategoriye ayrılır:

- simetrik şifreleme algoritmaları;
- asimetrik şifreleme algoritmaları;

İki şifreleme yöntemi arasındaki temel fark, kullanılan anahtar sayısıdır. Simetrik şifrelemede tek bir anahtar kullanılırken asimetrik şifrelemede iki farklı ancak ilişkili anahtar kullanılır. Anahtarlardan biri özel anahtar, diğeri ise genel anahtardır. Simetrik şifreleme algoritmaları, hem şifreleme hem de şifre çözme işlevlerini gerçekleştirmek için aynı anahtarı kullanır. Asimetrik şifreleme algoritması, verileri şifrelemek için bir anahtar ve şifresini çözmek için başka bir anahtar kullanır. Bu, birisine şifreli bir mesaj göndermek istersek, onu alıcının açık anahtarıyla şifrelediğimiz ve alıcının şifresini çözmek için kendi özel anahtarını kullandığı anlamına gelir.

Şifrelemeyi bölmek için başka bir kriter de anahtar uzunluğudur. Anahtarın uzunluğu, kriptografik algoritmaların her biri tarafından sağlanan güvenlik düzeyi ile doğrudan ilişkilidir. Anahtar ne kadar uzun olursa, veriler o kadar güvenli olur. Simetrik algoritmalarda, anahtarlar rastgele seçilir ve uzunlukları gerekli güvenlik düzeyine bağlı olarak tipik olarak 128 veya 256 bittir. Asimetrik şifreleme durumunda, şifreleme ve şifre çözmenin gerçekleşmesi için, genel ve özel anahtarlar arasında (bazı benzersiz matematiksel formüller şeklinde) matematiksel bir ilişki olmalıdır.

Daha yüksek hızı nedeniyle, simetrik şifreleme, ABD hükümeti tarafından gizli ve gizli bilgileri şifrelemek için kullanılan Gelişmiş Şifreleme Standardı (AES) gibi birçok modern bilgisayar sisteminde bilgileri korumak için yaygın olarak kullanılmaktadır. AES, önceki veri şifreleme standardının (DES) yerini almıştır.

Asimetrik şifreleme, birden çok kullanıcının bir mesajı veya veri kümesini hem şifrelemek hem de şifresini çözmek için erişim gerektirebileceği sistemlerde kullanılır. Bir örnek, mesajı şifrelemek için genel anahtarın ve şifresini çözmek için özel anahtarın kullanılabileceği e-posta şifrelemesi olabilir.

Funded by the European Union. Views and opinions expressed are however those of the author(s) only and do not necessarily reflect those of the European Union or the European Education and Culture Executive Agency (EACEA). Neither the European Union nor EACEA can be held responsible for them.

Co-funded by the Erasmus+ Programme of the European Union

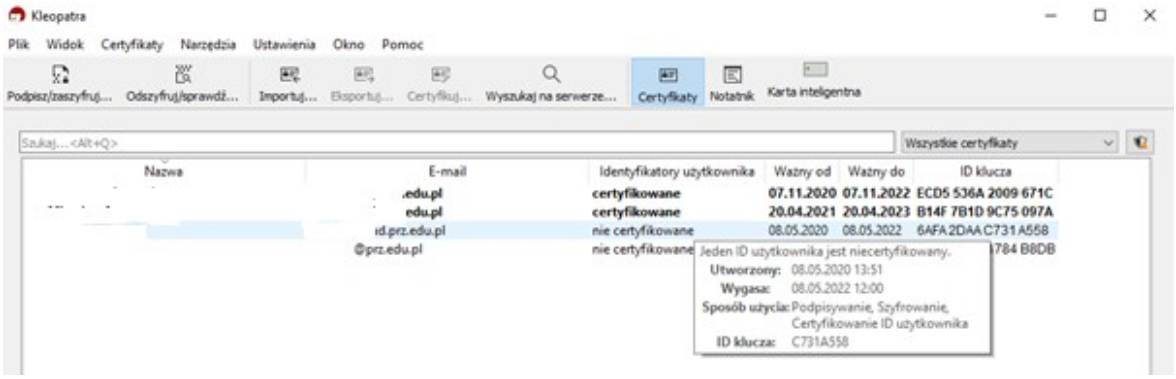
Bir çözüm, OpenPGP standardıdır. Şifreli e-posta uzantılarını tanımlar - şifreleme ve dijital imzalar. Standart, mevcut PGP programına dayanıyordu . Şu anda, birçok farklı uygulama var. Standart, RFC 4880'de tanımlanmıştır. Kullanıcılar genellikle e-posta gönderme sürecinde Thunderbird e-posta istemcisini kullanır. Bu istemci, OpenPGP standardını kullanarak şifrelenmiş ve dijital olarak imzalanmış e-postalar göndermenize ve almanıza olanak tanır. Bu özellik genellikle uçtan uca (e2ee) şifreleme olarak bilinir ve iletişimi daha güvenli hale getirir ve üçüncü şahıslar tarafından gözetlenme olasılığını azaltır. Thunderbird 78, OpenPGP ve S/MIME olmak üzere iki şifreleme standardı için yerleşik desteğe sahiptir.

Thunderbird'ün önceki sürümlerinde (v68 ve önceki sürümler) yerleşik S/MIME desteği vardı ve Enigmail eklentisini ve GnuPG yazılımını kullanarak OpenPGP desteği ekleyebilirsiniz. Enigmail eklentisi , eski kullanıcılarının Thunderbird 78'de OpenPGP'ye geçişine yardımcı olmak veya Enigmail'den 'Junior Mode' kurallarını nasıl geri yükleyecekleri konusunda rehberlik almak dışında Thunderbird 78 için artık mevcut değil . Thunderbird ayarlarınızı daha eski bir sürümden (örn. 68.x) 78.x sürümüne yükseltebilirsiniz. Ancak Thunderbird 78'i ilk kez kullanmadan önce Thunderbird profilinizi yedeklemeniz önerilir, çünkü yükseltmeden sonra profil artık Thunderbird 68 ile kullanılamaz.

Enigmail , tüm anahtarları ve güvenilir ayarları depolamak ve yönetmek için GnuPG'yi kullandı. Geçiş yapabilirsiniz ve Enigmail eski anahtarları GnuPG'den okuyacak ve içe aktaracaktır. Thunderbird 78, Enigmail'den farklı ayarlar kullanır . Enigmail ile bir e-posta hesabı için OpenPGP'yi etkinleştirmek mümkündü, ancak hangi anahtarın kullanılacağını otomatik olarak seçmesine izin verdi. Thunderbird 78 bu ayarları birleştirir. Bir e-posta hesabı için OpenPGP'yi etkinleştirmek için hangi anahtarın kullanılacağını açıkça belirtmelisiniz.

Şifreleme için GPG4win yazılımı kullanılacaktır. Bir dizi gelişmiş veri şifreleme aracıdır. Yalnızca e-postaya değil, dosya ve klasörlere de yetkisiz erişime karşı koruma sağlar . Gpg4win ile çalışmak asimetrik şifrelemeye, yani iki anahtara dayalıdır - özel ve genel. Birincisi verileri şifrelemek için kullanılır, ikincisi ise mesajın erişebilen alıcılarına ulaşmalıdır. Özel anahtarı güvenli bir yerde saklayın.

Paket, GnuPG şifreleme aracı, Kleopatra sertifika yöneticisi (Şekil 7), alternatif GPA sertifika yöneticisi, Claws Mail e-posta istemcisi gibi öğelerin yanı sıra Microsoft Outlook ile entegrasyona izin veren iki eklenti (2003, 2007, 2010 ve sürümlerinde) içerir. 2013) ve Windows Gezgini.



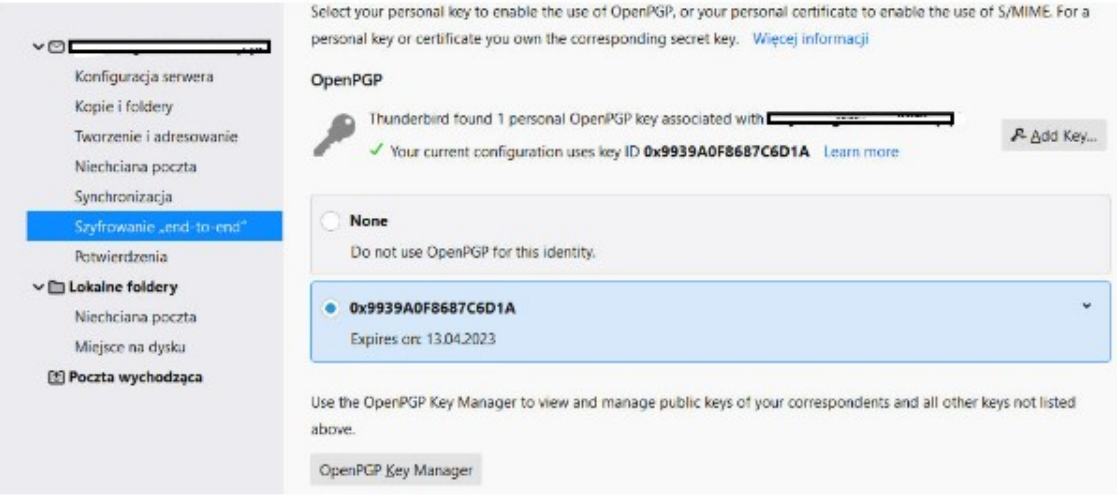
Funded by the European Union. Views and opinions expressed are however those of the author(s) only and do not necessarily reflect those of the European Union or the European Education and Culture Executive Agency (EACEA). Neither the European Union nor EACEA can be held responsible for them.

Şekil 7. Sertifika yöneticisi - Kleopatra.

Gpg4win, OpenPGP ve S/MIME (X.509) standartlarını destekler ve varsayılan olarak 2048 bit anahtarlar kullanarak sertifikalar oluşturur. RSA, standart şifreleme ve imzalama algoritmasıdır. Ayrıca paket, SHA1, SHA256 ve MD5 sağlama toplamlarının oluşturulmasına ve doğrulanmasına da izin verir.

Mesaj şifreleme ortamının yapılandırılması.

programına e-posta hesapları atadıktan sonra bir çift anahtar oluşturulmalıdır. Bir çift anahtar, bir özel anahtar ve bir genel anahtardan oluşur. Özel anahtar belirli bir hesaba atanır. Bu hesaba şifreli mesaj göndermek isteyen kişi, alıcının açık anahtarına sahip olmalıdır.



Şekil 8. Uzak Masaüstü bölümünün ayarları

program kullanmadan şifreli mesajlar göndermek ve almak için doğrudan Thunderbird'ü kullanabilirsiniz . Yeni bir alıcıya ilk mesajınızı gönderirken ortak anahtarınızı göndermeyi unutmayın (Şek. 8). Şifreli bir mesaj örneği Şekil 9'da gösterilmektedir.

Funded by the European Union. Views and opinions expressed are however those of the author(s) only and do not necessarily reflect those of the European Union or the European Education and Culture Executive Agency (EACEA). Neither the European Union nor EACEA can be held responsible for them.

Co-funded by the Erasmus+ Programme of the European Union

```
-----BEGIN PGP MESSAGE-----

wcDMA0r5u59RHK/uAQv/cvK0XliobGKfmQ25IcGe4kxtcXan9oDhQ0HODeAQyLSfpPFYOitt4LpF
Kc2aae3ayqRN+0bhTESVFaxttCw76E5wszkM9cK8UdxYzrX9PuaujtzYj8kSx3m0skfXrdglYnM8
llIYNETSgTnFSZ4jHKQLVIHVw9ZMztoo/ibLVJY3TTd7aKn7+cYyepNasrPPzoxcSGjJ1pQCkJ6t
SGtm8HDBfekKbK6qTKefYdGrCDBS4sAsuszwaX5QtSn50LAE2FkXCiKzTh6DkdFxQQ7yk/rUTs93
MkRwRtjteDqO7KC1yNPBim+KVLVG20EibD1FrdFIsbaEaPIl3Y06LhmjBMrUOUaMhPJpYDM1Ki8u
gqGHOQmqISQU1y6/poyGDmOfSPOFchWaTB+9fjzpmEb32mK10D1JOM2llut5AtmZH8W1lKpy4cdC
XygSXMkJ4as+p9/MtICdESyFkDXamESbtI04Ay5Xj+YrBnQ+Wk0lHOeLfSFg+cj7fwUuasRvEIe0
wcDMA3pKlfoZRRoWAQv/UVilR5h++k8Tq8uk/IeUchC3Si832Li8Ro++dGxy65Gomjlzg+oxbOoj
0u1kZGs5QbCywv5+vlo7CxpGSeMcBbj1T5jV/cKk1An9bdCjADXFLw4sEWCtqTR47OFqArvqi2gm
2iOW4g6Zcnd2lcfGe5kmeyRKt8OmHL6LDaZXSnJCJkhNRwr3GKHh8gJeT00bn+72M9TbBKXxLe3T
bnGw2ypPIQJ55k2x+ZbgkjDnQQDogsHpB1ip7K5yYArf+rI4uPqbYQgSU3NYYAUsmOtI2yesouvV
gFic/0TE9xq0qhciE2bTWPxH5ikxCMwLQa33E8+hngsSDfoyoRdolSEwjhI8KHthzddXzPNSkdgn
Q4pdGUljFaDivtLc7cNs3SFKoZBiZcQaHRTABVNDMQgRqgoG6F0Ditu03vXCh5aR8/zUVS6moGT8
2sh/VWvryEAHKLSUPZulgwaZlD5hxosUMuwzGibLzaCApbilNdzm4zaDz2KdGBwmvyGkC7oT4lvj
0sMwAbnd2f3Hz+AuXFajZ6uO8m6ibKMtJRM3EXggkNhue0rIU4KLchp9U9jLAt6GMQjPFKmgGqEj
U7/QPiVbJ8DjbmhYH90JwYH8hJCx1rq4AtXOxJgz8w0B+MOe6maKxDaDqS9gQj/n9N/Hvj8btZKz
turb54Y8MxZXXXoNxLAVZr1HHcbQoweHIx0EXanoMsxEwT3ugAiQetwBzXnR9DOzxTkzeOMK1ooS
6jnVTQy454q1+w6fNWAfBbpYY73Lt1NifD7mHoqe1G3oWhgzj/uUs67TJlDjLfqzhxqw0TnfXyNM
+457fZCj+iYwdV8DhfDb4dyfYmDjA8LLP8Uw7gLtkFxDldsaLf7/xQ5g98eKhz/4INI0xL+5Znno
x4SnkX++hy4z/nRKBNQcIupW7KuG1SOABTIhQWx3mtxyte0mxBRxiApfC5HfNzQM+vtmhJK8mlHK
Osc3kVw6kTodafSTi/qLghcOh2R7h8hL7qRc56ig7i4nPY5bnsPpfyyPYAuUDJQUz5z4tFrdEX/+
gw/gH3O8hTS17VSfgya0BUwJvMnlbS1+VZ7zomF405ne8hrFsT5j/dnjP7NgGS3CVMDLyEDtQA7k
Vbru0EN4JTsCu3T7rMnRrGtX1kfsTXBLayhcpbaMyHojMKw60p41o2gvTn5fw/+GJHGQdsZ3HJ+g
fr9EWKLQzQX6PSLsJ5OexLRkMtHXV4jBoSRyTzFTwprBkNNKZu2aRYa17BBFuVc5RTf8rSVWq7Eq
rKrXGOP+GgqGGTxoD8zfFtp0YJ+mP28L0DtuPnmG9IzxdbXO/JG6sT6hzPEA6MIlaW6Y++94Jpg2
XEKsGOdW9IHx9613FwjPtj6HKC8GtN5s8dgSAm3tw5KUWfchtKIOZYiynxuRnwIMN0UM0G2QFKYr
pU+50ba8rdui9D2YFzEcbw9a3meaWksO3Zvd8obQfwGFMX9DwV5VPEcmASHEUMULGBUO3KIUtaxU
Sdg9qmehxPMkkH3bB3x+G79WmV0ss0G9r+uVk/XhzxckqUI0w++q2PmWsXAIP2NsyX7W1BHyZ5J0
HhUwUllGtpl3gv/WwOxTyoEz2oeQucK5Eq91vEwaudCnip7STqK2WpboGvAQ54ZIZRFbm/4sOd/W
4kH6xyeYBTsIf3ft7LyvoB6Xq9lA1xOFe94CcAqty90FynvF26Da7QRsNQalhfhfB1bnaEQIgf+7
J9fpMYQEcC4tT8RW9vtozQurNpgZnZS9sjWjke6/j3XV7paxOW7OG8nc+1r09LQMMtVjvI5Zd1FV
JyAtr1EsoF/9MzFfofn6eCtU8VvXiS8+cIDjTqrb2EKS68Rpu9Z8LCgz
=MjYk
-----END PGP MESSAGE-----
```

Şekil 9. Şifreli mesaj örneği.

Thunderbird, onlarla birlikte gönderilen iletilerin ve eklerin şifresini otomatik olarak çözer. Şifreli yazışmaları göndermeden önce alıcıların genel anahtarlarını bilmeniz gerektiğini unutmayın. GPG eklentisi ile şifreleme, yalnızca içeriği değil, ekleri de korur. Alıcının anahtarını bilmeden şifreli bir mesaj gönderemeyiz. Ek olarak Thunderbird, birkaç e-posta hesabını senkronize etmenize olanak tanır.

Sorular :

Sorular Tartışma Forumu kısa bir açıklama ile cevaplanacak. Cevaplar, mentorluk oturumları sırasında mentor ile tartışılacaktır.

1. VPN nedir?
2. VPN çözümünü nasıl kullanabilirsiniz?
3. PGP e-posta şifrelemesi için özel anahtarınızı birine gönderebilir misiniz?

Funded by the European Union. Views and opinions expressed are however those of the author(s) only and do not necessarily reflect those of the European Union or the European Education and Culture Executive Agency (EACEA). Neither the European Union nor EACEA can be held responsible for them.

Co-funded by the Erasmus+ Programme of the European Union

Öz değerlendirme soruları . Cevap verdikten sonra, öğrenci sonuçları görebilir ve platformda kayıtlı olanlarla karşılaştırabilir.

1. Verilerinize uzaktan erişimden güvenli erişim yöntemi
2. E-posta görüşmenizi güvence altına alma yöntemleri

Ekler:

1. Sunum
2. Video filmler

Referanslar:

1. Rana, Muhammed Ehsan & Abdulla, Mohamed & Arun, Kuruvikulam . (2021). Kablosuz Ağlar için Ortak Güvenlik Protokolleri: Karşılaştırmalı Bir Analiz. 10.2991/ahis.k.210913.080.
2. Habibi Lashkari, Arash & Sendón Varela, Juan & Samadi, Behrang. (2009). Kablosuz güvenlik protokolleri (WEP, WPA ve WPA2/802.11i) üzerine bir anket. 10.1109/ICCSIT.2009.5234856.
3. Kumkar , Vishal & Tiwari, Akhil & Tiwari, Pawan & Gupta, Ashish & Shrawne , Seema. (2012). Kablosuz Güvenlik protokollerinin (WEP ve WPA2) açıkları. Uluslararası Bilgisayar Mühendisliği ve Teknolojisinde İleri Araştırmalar Dergisi. 1.
4. Costa, Luís & Fdida , Serge & MB Duarte, Otto Carlos. (2000). Sanal Özel Ağlara Giriş: D-VPN'lere Doğru.
5. https://www.vpnmentor.com/blog/ Different-types-of-vpns-and-When-to-use-them/
6. https://www.radmin-vpn.com
7. https://www.fortinet.com/resources/cyberglossary/pgp-encryption

Funded by the European Union. Views and opinions expressed are however those of the author(s) only and do not necessarily reflect those of the European Union or the European Education and Culture Executive Agency (EACEA). Neither the European Union nor EACEA can be held responsible for them.