

Cözümler

1. a) ISO tarafından tanımlanmış ağ yönetim alanları hangileridir?

Performance management, fault management, configuration management, accounting management, security management.

b) Ağ yönetim altyapısını oluşturan bileşenleri tanımlayınız.

- **Managing entity:** control the collection, processing, analysis, display of network management information, and is used by the network manager to control the devices in the network.
- **Managed device:** a piece of network equipment that is under the control of the managing entity.
- **Management agent:** a software process running on a managed device that communicated with the managing entity and takes action on the managed device under the control of the managing entity.
- **MIB:** pieces of information associated with all of the managed objects in a device.
- **Network management protocol:** runs between the managing entity of the management agents on the managed devices, allowing the agents to alert the managing entity to potential problems, and allowing the managing entity to send commands to the management agents.

c) SNMP’de *request-response* ile *trap* mesajları arasındaki önemli fark nedir?

The trap message is sent by the management agent to the managing entity (and requires no response from the managing entity). A request-response message is sent by the managing entity, with the response coming back from the management agent.

2. Güvenli bir haberleşmede istenen sırdaşlık (confidentiality), kimlik doğrulama (authentication), mesajın tamlığı (message integrity), kullanılabilirlik ve erişim kontrolü (availability and access control) terimlerini açıklayınız.

Sırdaşlık: Mesajın içeriğini sadece gönderen ve alanın bilebilmesi.

Kimlik doğrulama: Haberleşmede mesajı gönderen ve alanın gerçekten iddia ettikleri kişiler olduklarından emin olunması.

Tamlık: İletim sırasında mesaj içeriğinde değişiklik olup olmadığından emin olunması.

Kullanılabilirlik ve erişim kontrolü: Ağın istenen kişilerce istendiği zaman kullanılabilmesi, kötü kişilerin erişimine kapalı olması.

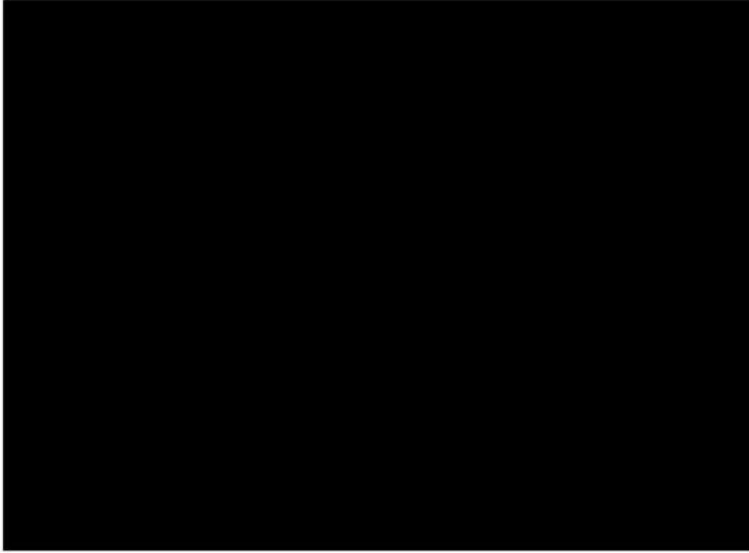
3. N adet kişiden her biri geri kalan N-1 kişi ile haberleşmek istesin. *Simetrik* anahtar şifrelemesi için kaç adet anahtara ihtiyaç vardır? *Kamusal* anahtar şifrelemesi için kaç adet anahtara ihtiyaç vardır?

If each user wants to communicate with N other users, then each pair of users must have a shared symmetric key. There are $N*(N-1)/2$ such pairs and thus there are $N*(N-1)/2$ keys. With a public key system, each user has a public key which is known to all, and a private key (which is secret and only known by the user). There are thus 2N keys in the public key system.

4. Bir davetsiz kullanıcın (intruder) elinde bir mesajın hem şifreli hem de şifresi çözülmüş sürümleri elinde olsun. Bu durumda hangi saldırıyı gerçekleştirebilir?

In this case, a known plaintext attack is performed. If, somehow, the message encrypted by the sender was chosen by the attacker, then this would be a chosen-plaintext attack.

5. Sırdaşlık, mesaj tamlığı ve kimlik doğrulama özelliklerinin bulunduğu güvenli e-mail gönderme nasıl gerçekleştirilir, bütün detayları ile blok diyagram olarak gösteriniz.



6. Kamusal anahtar şifrelemesi, sırdaşlık, mesaj tamlığı ve kimlik doğrulama gibi alanların hepsinde başarı ile kullanılabilmesinin nedenini matematiksel olarak açıklayınız.

$$(m^e)^d \bmod n = (m^d)^e \bmod n$$

7. Poisson sürecine uygun şekilde bir yönlendiriciye paketler ortalama 500 paket/sn hızında gelmektedirler. Yönlendiricinin hizmet süresi üstel dağılmakta ve ortalama 1 milisaniye'dir.

- a) Gelen paketin yönlendiriciyi boş bulma olasılığını bulunuz.
- b) Yönlendiricideki ortalama paket sayısını bulunuz.
- c) Ortalama bekleme süresini bulunuz.
- d) Paketin kuyrukta geçirdiği süreyi bulunuz.

a) $\lambda = 500$, $\mu = 1000$, $\rho = 0.5$

$P_0 = 1 - \rho = 0.5$

b) $E[n] = \rho / (1 - \rho) = 1$ paket

c) $E(T) = E[n] / \lambda = 1 / 500$ saniye

d) $E[w] = E[T] - 1 / \mu = 1 / 500 - 1 / 1000 = 1 \text{ ms}$

8. Bir yönlendirici M/M/1 ile modellenmekte ve paketlerin geliş hızı ortalama 10 paket/msn. Zamanın %99.9'unda yönlendiricide en çok 3 paket olması için hizmet hızı ne olmalıdır?

$$(10/\mu)^3 \leq 0.001$$

$$\mu \geq 100 \text{ paket/ms}$$