Yer altındaki Internet : DarkNET

Bil. Y. Müh. Çağatay YÜCEL
Yaşar Üniversitesi

17.04.2014

DARKNET

Her gün kullandığımız internetin hiç görmediğimiz köşesine yakından bakalım.

DarkNet Nedir?

- Internetin suçlulara ve suç unsuru sayılabilecek aktivitelere ev sahipliği yaptığı köşesidir.

- Arama motorlarının ve standart bir ev kullanıcısının erişimine izin vermeyen çeşitli yazılımlar aracılığıyla gizlenmiş suç faaliyetleri içeren bir ağdır.

  - **Yeraltındaki internet**
  - **Dark Net - Karanlık Web**
  - **Derin Web – Deep Web** olarak da adlandırılmaktadır.

DarkNet'in Tarihçesi – İlk Mesajlaşma

- Her suç aktivitesinde olduğu gibi, Darknetler aslında Internet ile hemen hemen aynı zamanda varolmaya başladılar.

- Ek bilgi: Arpanet, dünya üzerinde ilk packet-switching teknolojisi ile TCP/IP üzerinde kurulan ağıdır. Bu ağ üzerindeki ilk mesajlaşma Kaliforniya Üniversitesinden Doktora öğrencisi Charley Kline tarafından gerçekleştirilmiştir. **Bu an itibari ile bir kaç yıl içerisinde internet üzerinde gizli ağlar kurulmaya başlanmıştır.**

DarkNet'in Tarihçesi – Bilgi Barınakları

- 1980'lerin başlarında Karayiplerde hassas ve çoğunlukla illegal bilgilerin paylaşılması ihtiyacı üzerine "Data Haven" olarak adlandırılan veri barınakları kurulmuştur.

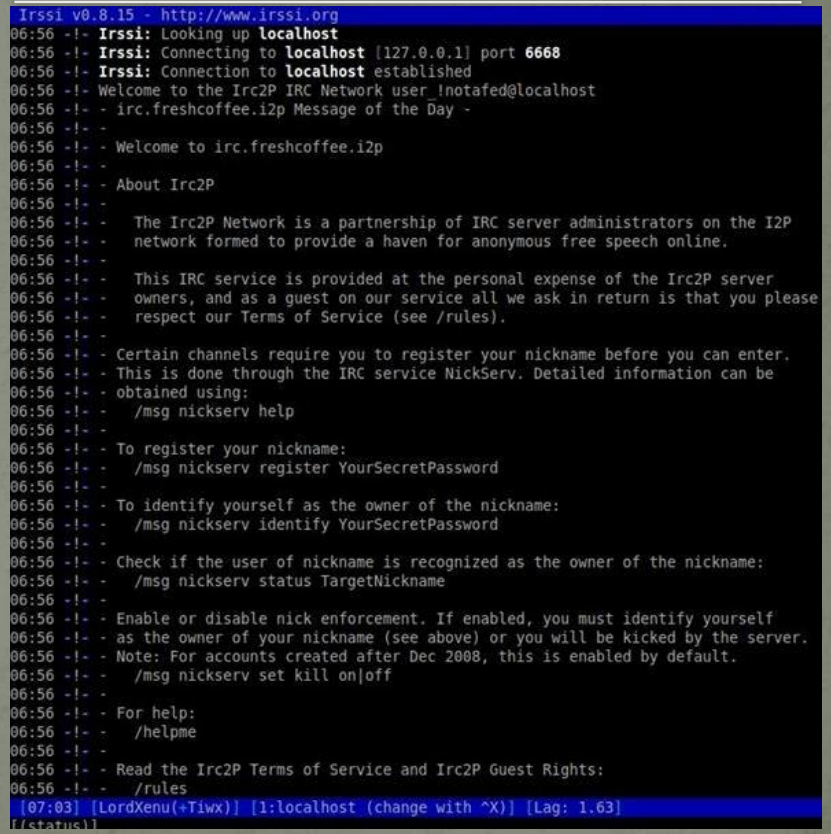
- Bu barınaklarda çoğunlukla serbest politik konuşmalar, kumar ve illegal pornografi ağırlıklı veriler saklanmış ve paylaşılmıştır.

DarkNet'in Tarihçesi - IRC

IRC – Internet Relay Chat protokolü

- 1988'de Jarkko Oikarinen adlı kişi tarafından Finlandiyada çoklu mesajlaşma programı olarak tasarlanan bu protokol, 1990'ların başında yaygın olarak kullanılmaya başlandı.

IRC Sohbet Odası



DarkNet'in Tarihçesi – P2P Ağlar ve Napster Ağı

P2P Mimarisi

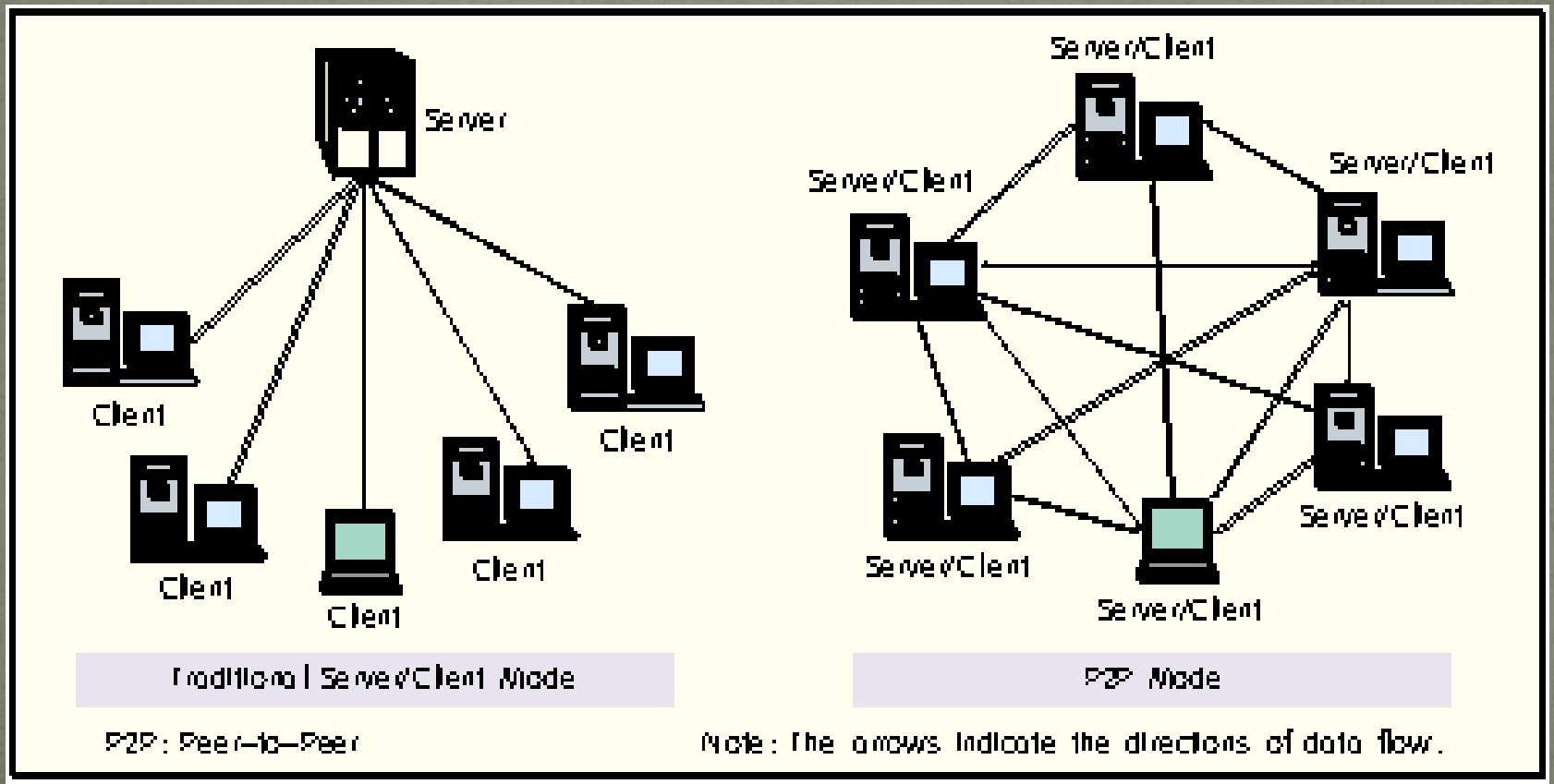


Figure 1. Comparison between P2P and C/S modes.

DarkNet'in Tarihçesi – **HavenCo**

- HavenCO, 2000 yılında Sealand Prensliğinde kurulmuş olan bir veri barınağıdır.

- Hedefi illegal pornografi ve terrör faaliyetleri haricinde her türlü verinin telif haklarından bağımsızca barındırıldığı bir veri kalesi oluşturmaktı.

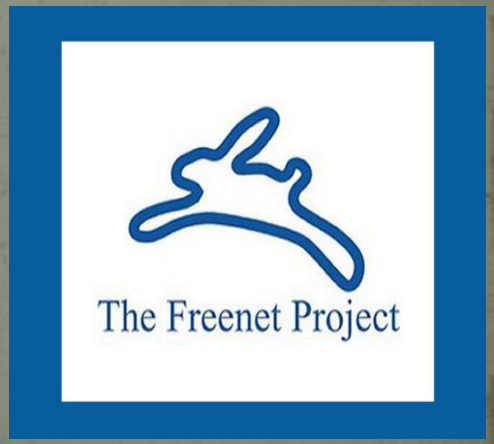
DarkNet'in Tarihçesi – **HavenCo**

- 2008de kapatılan bu şirket telif hakları konusunda düzenlemeler yaptıktan sonra tekrardan açılmıştır.
- İngilterenin kuzeyinde olan bu küçük prenslikte faaliyet sürdüren bu şirket halen daha kullanıcılarına hizmet vermektedir.

DarkNet'in Tarihçesi –**Freenet**

- 2000 yılında aynı zamanda bir yüksek lisans tezi olarak İrlandalı Ian Clarke tarafından Dağıtık Merkezsiz Dosya Depolama ve Paylaşma Teknolojisi doğmuştur.

- Daha sonradan geliştirilen bu sistem ile beraber Freenet sisteminin doğuşu
  - Dosya Depolama ve Paylaşma
  - Anonim olarak forumlarda konuşabilme
  - Anonim online chat
  - Anonim web surfing



DarkNet'in Tarihçesi

- Bu tarihsel gelişimlerin sonucunda türeyen Tor, Freenet, Gnutella, IRC, Waste ve benzeri programların genel adına **DarkNet** denmektedir.

- DarkNet tanımı kullanıldığında farklı bir internet yapısından söz edilmemekte, sadece anonimitenin sağlandığı ve bu bahsi geçen internet üzerinden haberleşen özel yazılımlarla erişimin sağlanabildiği bir alt mimariden bahsedilmektedir.

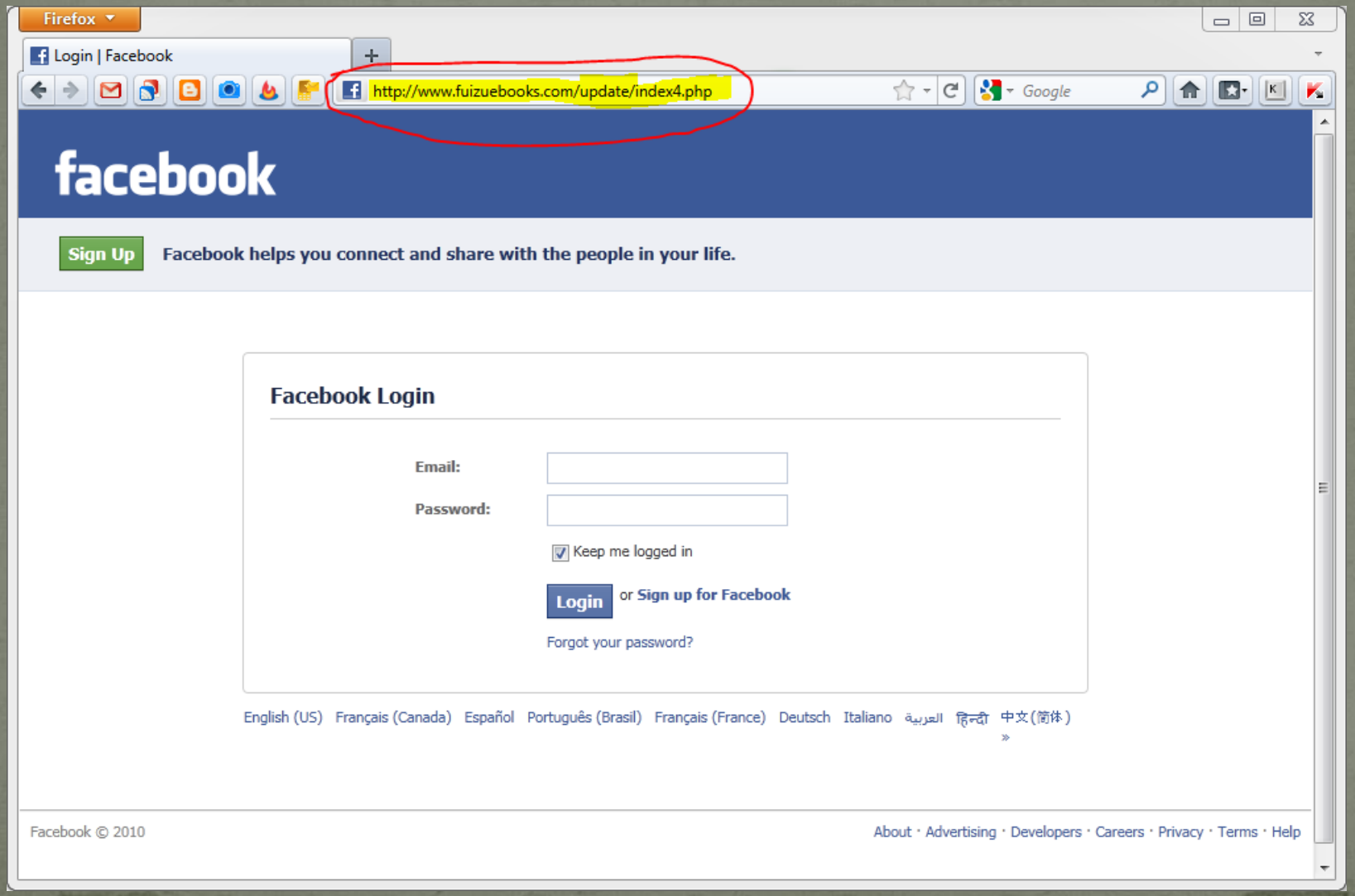
Kimler Kullanır?

Kimler Kullanır?

- İllegal her türlü veriyi kullanan, saklayan ve satan her türlü suçlu
- Politik propaganda yapan kimseler, Aktivistler
- Spam ve Phishing saldırısı gerçekleştirenler.
- Mahremiyetine özen gösteren kimseler.

Spam Saldırıları

Phishing Saldırıları



Phishing Saldırıları

Dear valued customer of TrustedBank,

We have recieved notice that you have recently attempted to withdraw the following amount from your checking account while in another country: $135.25.

If this information is not correct, someone unknown may have access to your account. As a safety measure, please visit our website via the link below to verify your personal information:

http://www.trustedbank.com/general/custverifyinfo.asp

Once you have done this, our fraud department will work to resolve this discrepency. We are happy you have chosen us to do business with.

Thank you,
TrustedBank

Member FDIC © 2005 TrustedBank, Inc.

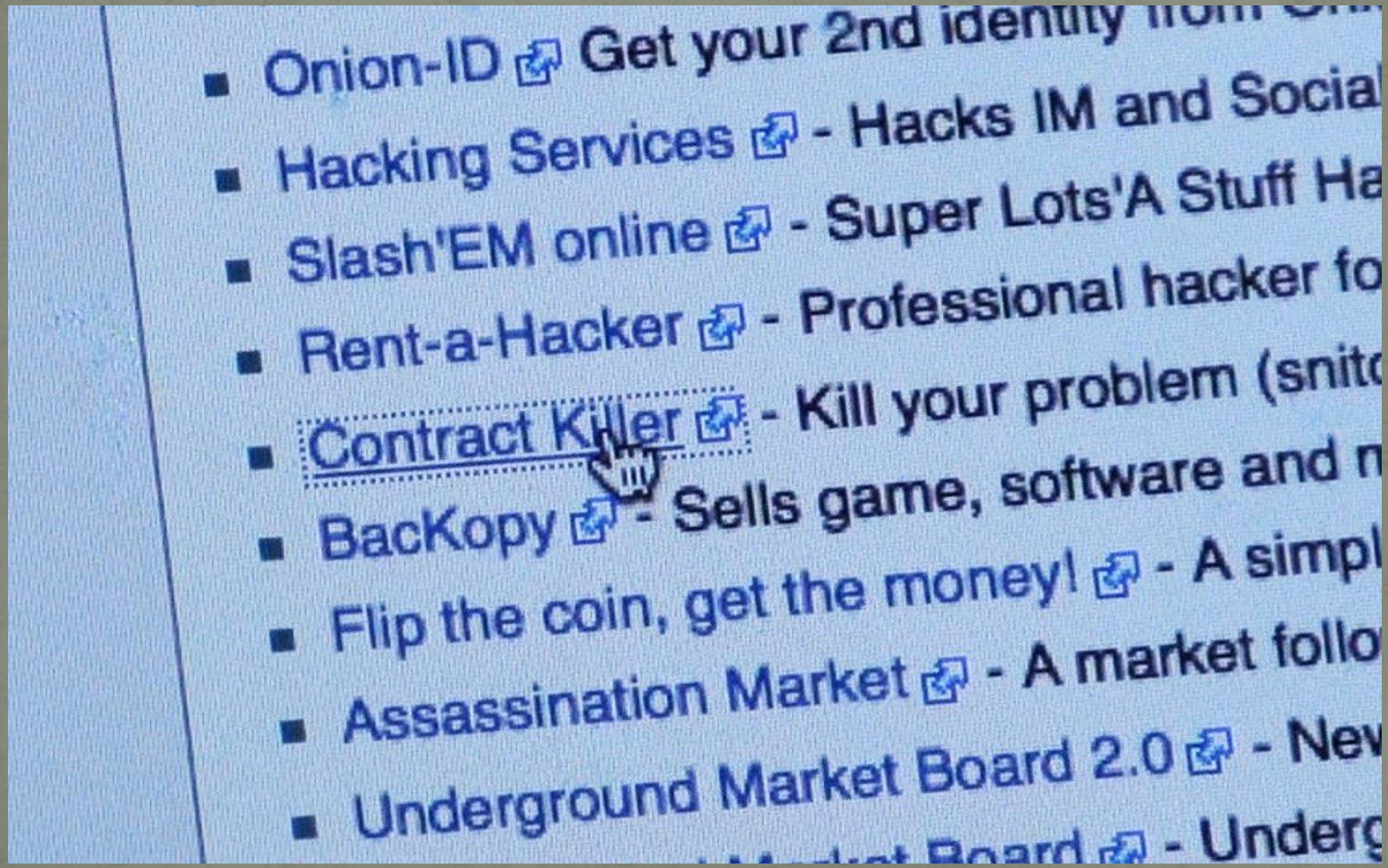
İllegal Alışveriş Siteleri

Walther PPK, Kal.7,65

New and unused!

Product	Price	Quantity
Walther PPK, Kal.7,65	600 EUR = 7.578 ฿	1 X Buy now
Ammo, 50 Rounds	40 EUR = 0.505 ฿	1 X Buy now

İllegal Alışveriş Siteleri



Online Dolandırıcılar – 419 scam

- Subject : MR SULEMAN BELLO

  FROM THE OFFICE MR SULEMAN BELLO
  AFRICAN DEVELOPMENT BANK (ADB).
  OUAGADOUGOU BURKINA FASO.
  WEST AFRICA.

  TRANSFER OF ($ 25,200.000.00) TWENTY FIVE MILLION, TWO HUNDREN THOUSAND DOLLARS.

  I AM SULEMAN BELLO, THE AUDITOR GENERAL OF AFRICAN DEVELOPMENT BANK HERE IN BURKINA FASO. DURING THE COURSE OF OUR AUDITING, I DISCOVERED A FLOATING FUND IN AN ACCOUNT OPENED IN THE BANK BY MR JOHN KOROVO AND AFTER GOING THROUGH SOME OLD FILES IN THE RECORDS I DISCOVERED THAT THE OWNER OF THE ACCOUNT DIED IN THE (BEIRUT-BOUND CHARTER JET) PLANE CRASH ON THE 25TH DECEMBER 2003 IN COTONOU (REPUBLIC OF BENIN). INTO A FOREIGN ACCOUNT.

  I NEED YOUR STRONG ASSURANCE THAT YOU WILL NEVER, NEVER CHEAT ME AS SOON AS THIS FUND HIT INTO YOUR ACCOUNT. WITH MY INFLUENCE AND THE POSITION OF THE BANK OFFICIAL WE CAN TRANSFER THIS MONEY TO ANY FOREIGNER'S RELIABLE ACCOUNT WHICH YOU CAN PROVIDE WITH ASSURANCE THAT THIS MONEY WILL BE INTACT PENDING OUR PHYSICAL ARRIVAL IN YOUR COUNTRY FOR SHARING. THE BANK OFFICIAL WILL PROVE ALL DOCUMENTS OF TRANSACTION IMMEDIATELY FOR YOU TO RECEIVE THIS FUND LEAVING NO TRACE TO ANY PLACE AND TO BUILD CONFIDENCE.

  ON THE CONCLUSION OF THIS TRANSACTION YOU WILL BE ENTITLED TO 30% OF THE TOTAL SUM AS GRATIFICATION, WHILE 10% WILL BE SET ASIDE TO TAKE CARE OF THEEXPENSES THAT MAY ARISE DURING THE TIME OF TRANSFER AND ALSO TELEPHONE BILLS, WHILE 60% WILL BE FOR ME.

  SO ON THE INDICATION OF YOUR WILLINGNESS I WANT YOU TO FORWARD TO ME YOUR :FULL NAME: SEX: COMPANY: IF ANY FULL CONTACT ADDRESS: PHONE: CELL: FAX: CITY: STATE:ZIP CODE COUNTRY: OCCUPATION AND ALL THE NECESSARYINFORMATION WILL BE SENT TO YOU ON THE ACCEPTANCE TO CHAMPION THIS TRANSACTION WITH ME.

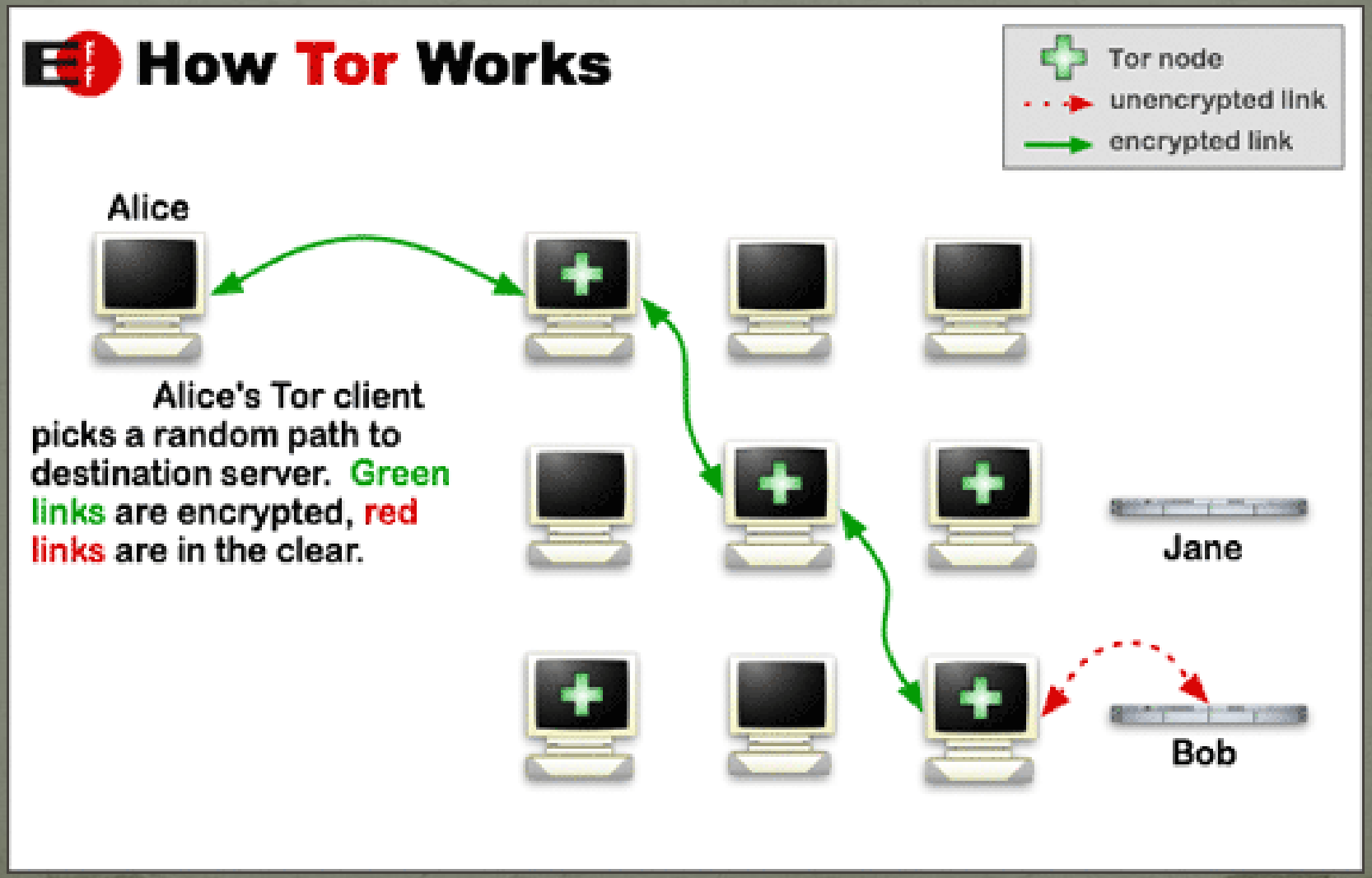
  THANKS
  YOURS TRULY
  SULEMAN BELLO

Nasıl Çalışır ? – TOR

- İlk etapta A.B.D. Denizcilik Araştırma Enstitüsünde geliştirilmiştir.

- Onion Routing tekniği kullanılmaktadır. Bu teknik;
  - Her katmanda şifreleme ve
  - Paketin rotasındaki her düğümde deşifreleme ve yeni rotanın belirlenmesi ile oluşturulmaktadır.

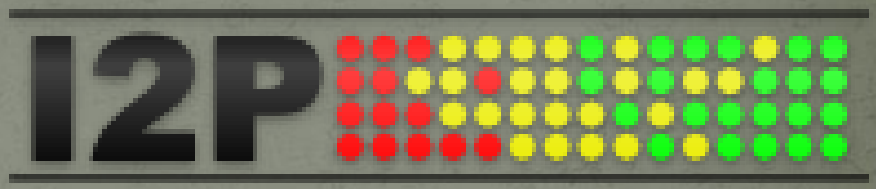
Nasıl Erişilir? – TOR (The Onion Router)



TOR

- Bir Tor uygulaması…

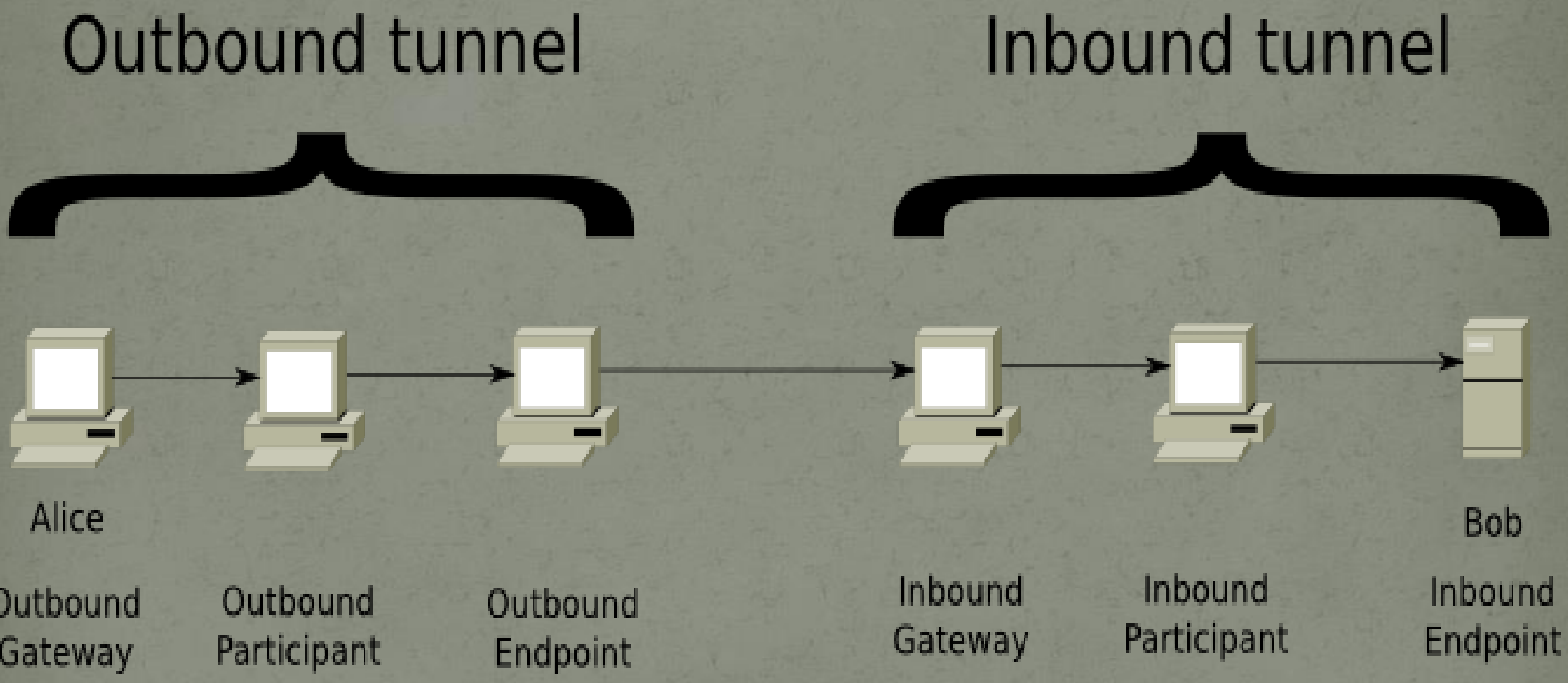
I2P – Invisible Internet Project



- Benzer bir altyapıya sahip bu networkte farklı tünel yapıları kullanılmaktadır.

- Sadece belirgin bir süre zarfı için geçerli olan bu tüneller, TOR'a ek olarak sisteme zaman parametresini de eklemektedir.

I2P – Invisible Internet Project



I2P – Invisible Internet Project

- I2P uygulaması…

Sorularınız ve Görüşleriniz

Dinlediğiniz için teşekkür ederim..