Bilgisayar Ağları Örnek Proje

PREY NEDİR? NASIL ÇALIŞIR?

Prey dizüstü bilgisayarlar, akıllı telefonlar ve diğer elektronik cihazlar için bir özgür internet hizmeti ile ayrıca kontrol paneli ile izleme ve görüntüleme sunan ana bilgisayara bağlayan bir açık kaynak ajan yazılımdır. Yani kontrol etmek istediğiniz cihaza bu yazılımı kurduğunuz takdirde başka bir platformdan düşen logları takip ederek cihaz hakkında çeşitli konularda bilgi sahibi olabilirsiniz. Bu yazılım host cihazların geçerli konumu hakkında bilgi ile cevap isteyen casus sinyal verebilir ve diğer çeşitli eylemleri tetikleyebilir. İstemci tarafında kaynak kodunun tamamı GitHub'da yayınlanan yazılım(<https://github.com/prey/>) GNU Genel Kamu Lisansı altında dağıtılmaktadır. Bilindiği gibi Genel Kamu Lisansı yaygın olarak kullanılan Özgür kaynak yazılım lisansıdır. Açık kaynak kodlu sürümü de genel kullanıma açık olmasına rağmen resmi sunucu kodu, tescillidir. Masaüstü Prey, ya bir Wi-Fi şebekesine ya da başka bir ağa bağlandığında nirengi ile konum bilgileri sağlar. Cep telefonlarında bu cihazın dahili GPS izleyicisi kullanılarak yapılır.

NİRENGİ NEDİR?

Nirengi veya üçgenleme, haritacılıkta bilinmeyen bir uzunluğu, yüksekliği veya koordinatı bulmak için bir alanı üçgenlere bölerek yapılan hesap. Nirengi hesabında kullanılan referans cisme nirengi noktası veya kısaca sadece nirengi denir. Bu nedenle nirengi sözcüğü Türkçede zaman zaman "referans" anlamında da kullanılır.

PREY HANGİ PLATFORMLARDA ÇALIŞIR?

Prey; Windows, Mac OS, Linux, Android ve iOS çoğu sürümlerinde çalışır. Mobil karşıtları kendi dillerinde, Java ve Objective-C ile yazılmış iken Prey masaüstü sürümü, öncelikle Bash ile yazılmıştır.

PREY TARZI UYGULAMALAR VE ÇALIŞMA PRENSİBLERİ

Prey ilgili işletim sisteminde kurulduğundan diskteki değişiklik uygulamamızın çalışmamasına yol açabilir. BIOS a yüklenen ve prey gibi özelliklere sahip bir program olsaydı? Adı: Lojack … İlgili bilgi aşağıdaki bağlantıda mevcut.

LoJack : Lojack Sisteminin çalışma mantığı, Bilgisayarın anakartının üzerindeki BIOS çipine yerleştirilip entegre edilir. Bu çipin üzerinde geniş bir radyo frekansı aralığında takip mekanizması vardır. Çalıntı olan bilgisayar açık ve ya kapalı olması farketmez. Tüm bilgiler radyo frekansı arayıcılığı ile Genel Takip Merkezinin veritabanına saniyesi saniyesine kayıt oluşturmaya başlar. Bilgisayar açıldığında ise size BIOS arayıcılığı ile bilgisayarın çalıştığını takip merkezine iletir ve dilerseniz bilgisayarınızı takip merkezinden kilitleyebilir, hırsızların verilerinize erişimini engelleyebilirsiniz.

Bu teknoloji sadece elektronik cihazlarda değil, yeni nesil çoğu otomobillerde birer birer uygulanmaktadır. Çalışma mantığı bilgisayarın ki ile aynıdır radyo frekansı aracılığıyla yer tespit edilir ve dilerseniz aracı durdurabilirsiniz. Bu teknolojiyi çoğu kargo firmaları da kullanmaktadır. Bir yerden kargo bekliyorsanız kargo firmanızın size verdiği takip numarası aslında LoJack numarasıdır. Bu numarayı kargo takip sistemine girdiğinizde kargonuzu taşıyan aracın nerede olduğunu görüyorsanız bu sistem sayesindedir. ABD’ nin yüksek güvenlikli cezaevlerinde, mahkumlara akıllı kelepçe niteliğinde takılan kelepçelerin teknolojileri de LoJack teknolojisiyle çalışmaktadır. Takip merkezinden mahkumlara elektrik akımı yollayarak mahkumların kaçmasına engel olabilirsiniz.

Windows uzaktan masaüstü kontrolü (Remote Desktop Connection): Uzak Masaüstü Bağlantısı (Remote Desktop Connection) aracını kullanarak uzaktaki sistemlere bağlanıp oturum açmak neredeyse tüm Windows sistem yöneticilerinin, hatta artık bireysel kullanıcıların bile tercih ettiği bir yöntem. Uzak Masaüstü Bağlantısı sayesinde, kendi Windows oturumunuzda çalışırken tamamen farklı bir lokasyonda açık olan bir Windows’a oturum açabilir ve sanki yerel masaüstü oturumunuzmuş gibi yönetebilirsiniz. Bu uzak sistem bir Windows istemci işletim sistemi olabileceği gibi bir Windows Server işletim sistemi de olabilir.

Varsayılan RDP portu veya Uzak Masaüstü Portu TCP 3389’dur ve bağlanılacak uzak bilgisayar üzerinde belirlenir. Ancak şunu unutmayın: varsayılan Uzak Masaüstü Portu gerektiğinde değiştirilebilir ve tamamen farklı bir TCP port atanabilir.

Uzak Masaüstü Portu: 3389

Bir Windows işletim sistemine Uzak Masaüstü Bağlantısı yapabilmek için bazı ön koşulların yerine getirilmiş olması gerekir. Bu koşulları özet olarak aşağıda bulabilirsiniz.

Bağlanacağınız uzak bilgisayar üzerinde Uzak Masaüstü (Remote Desktop) özelliği kullanıcıları kabul edecek şekilde ayarlanmış olmalı. Bağlanacağınız uzak bilgisayar üzerinde herhangi bir güvenlik duvarı programı çalışıyorsa, yapılandırılan Uzak Masaüstü Portu için gerekli izinler verilmiş olmalıdır. Buna Windows Güvenlik Duvarı da dahil. Bağlanacağınız uzak bilgisayar bir modem veya router arkasındaysa (ki genelde böyledir) mutlaka gerekli NAT kuralları oluşturulmuş olmalıdır. Eğer bağlanacağınız uzak bilgisayar yerel ağdaysa ve siz de o bilgisayar ile aynı ağdaysanız NAT gerekmez. Eğer sizin bilgisayarınızın bulunduğu ağ önünde bir güvenlik duvarı çalışıyor ise, Uzak Masaüstü Bağlantısı aracını çalıştırabilmek ve varsayılan port 3389’dan dışarı çıkabilmek için gerekli güvenlik duvarı izinleri tanımlı olmalıdır.

Bu tarz programların çalışma prensibi bilgisayar, sunucu ve internet üçlüsüyle ilgili bir etkileşim oluşturmak. Bilgisayara kurulan program yardımıyla veri tabanında belli bilgilerin depolanması ve sunucu yardımı ile o bilgilere farklı bir ortamdan (tarayıcıdan) ulaşabilmek. Kendi cihazımızdan izin vererek uzaktan cihazımız hakkında değişikliklere izin vermek. Vpn teknolojisinden faydalanılarak güvenlik, hız ve performans artırılabilir ancak kimse %100 güvenli olduğundan bahsedemez. Çünkü sizin bilgilerinin ilgili programın sunucularında şifrelenmiş olarak duruyor. Bu bilgilerin loglanıp başkaları tarafından görülmediğinin garantisi yok.