Bir Şifrepunk'ın Bildirisi

Elektronik çağda açık bir toplum için mahremiyet şarttır. Mahremiyet, bir şeyleri gizleyip saklamak demek değildir. Birinin, bütün dünyanın bilmesini istemediği bir şey mahremdir; ancak sakladığımız şeyleri hiç kimsenin bilmesini istemeyiz. Mahremiyet, birinin kendi iradesiyle kendisini dünyaya ifşa etme hakkıdır.

Eğer iki taraf bir şekilde etkileşimde bulunmuşsa, her birinin bu etkileşime dair bir anısı var demektir. Her bir taraf bu etkileşime dair anılarından bahsedebilir; bunu kim engelleyebilir? Birileri buna karşı yasalar çıkarabilir, ancak ifade özgürlüğü, mahremiyetten de önce, açık bir toplumun temelidir; biz ne olursa olsun bir ifadeyi engelleme peşinde değiliz. Eğer pek çok taraf aynı ortamda beraber konuşursa, her biri diğerleriyle konuşabilir, ve birlikte, bireyler ve diğer taraflar hakkında bilgi toplayabilirler. Elektronik iletişimin gücü bu tür takım konuşmalarını olanaklı kılmıştır ve birileri istiyor diye öylece kaybolacak değildir.

Mahremiyeti arzuladığımızdan, bir işlemin taraflarının, yalnızca ama yalnızca o işlem (ing: *transaction*) için doğrudan zorunlu şeyleri bildiğinden emin olmalıyız. Bilgi yayılabildiğinden, kendimizi olabildiğince az ifşa ettiğimizden emin olmalıyız. Pek çok durumda, kişisel kimlik göze çarpmaz. Mağazadan bir dergi satın aldığımda ve parayı tezgahtara uzattığımda, benim kim olduğumu bilmesine gerek yoktur. E-posta sağlayıcımdan, postalarımı gönderip-almasını istediğimde, sağlayıcımın kiminle konuştuğum, ne söylediğim ve başkalarının ne söylediğini bilmesine gerek yoktur; tek bilmesi gereken iletiyi iletmesi gerektiği ve ona olan borcumdur. Eğer kimliğim, işlemin işleyişinden dolayı açığa çıkıyorsa, mahremiyetim yok demektir. Burada kendimi açığa çıkarma özgürlüğüm yoktur; çünkü bunu her zaman yapmak zorundayım.

Bu yüzden, açık bir toplumda mahremiyet, anonim işlem sistemlerine gerek duyar. Şimdiye kadar (ç.n.: Bu yazının aslı 9 Mart 1993'te yazılmıştır), öncelikli olarak bu görevi para üstlenmiştir. Anonim işlem sistemi, gizli bir işlem sistemi değildir. Anonim bir işlem sistemi, bireylere, yalnızca ve yalnızca kendileri istekleri doğrultusunda kendi kimliklerini açığa çıkarma gücünü verir; mahremiyetin özü budur.

Açık bir toplumda mahremiyet için kriptografi de gereklidir. Eğer bir şey söylemişsem, onun yalnızca istediğim kişiler tarafından duyulmasını isterim. Eğer konuşmamın içeriği bütün dünyaya açıksa, mahremiyetim yoktur. Şifrelemek, mahremiyete olan isteği gösterir; ve zayıf kriptografi ile şifrelemek, mahremiyeti çok fazla istemediğiniz anlamına gelir. Dahası, varsayılan anonimlik ise, birinin kimliğini ifşa etmek, kriptografik imza gerektirir.

Hükümetlerin, şirketlerin ya da büyük, kim olduğu belirsiz oluşumların, kendi cömertliklerinden ötürü bize mahremiyet sağlamasını bekleyemeyiz. Bizim hakkımızda konuşmak onların yararınadır ve bunu yapmalarını beklemeliyiz. Konuşmalarını engellemeye çalışmak, bilginin gerçekliğine karşı savaşmaktır. Bilgi özgür olmayı yalnızca istemiyor, özlüyor. Bilgi var olan depolama alanını doldurmak için genişler. Bilgi, Söylenti'nin daha genç, daha güçlü kuzenidir; bilgi çok hızlı yayılır, daha fazla gözü vardır, daha fazla bilir ve Söylenti'den daha az anlar.

Eğer mahremiyet bekliyorsak, mahremiyetimizi savunmalıyız. Bir araya gelmeli ve anonim işlemlerin yapılabileceği sistemler yaratmalıyız. İnsanlar fısıltılar, karanlık, zarflar, kapalı kapılar, gizli el sıkışmalar, ve ulakları kullanarak, mahremiyetlerini yüzyıllardır savunuyorlar. Geçmişin teknolojileri güçlü mahremiyete izin vermiyordu, ancak elektronik teknolojiler veriyor.

Biz Şifrepunklar, kendimizi anonim sistemler oluşturmaya adamış bulunuyoruz. Mahremiyetimizi, kriptografi ile, anonim e-posta iletme sistemleri ile, dijital imzalar ile, ve elektronik para ile koruyoruz.

Şifrepunklar kod yazar. Biliyoruz ki, birisi mahremiyetini korumak için yazılım yazmalıdır, ve hepimiz yapmadıkça mahremiyeti elde edemeyeceğimizden, biz bunu yazacağız. Kodumuzu yayınlarız ki arkadaşlarımız Şifrepunklar onunla oynayıp, ona alışabilsin. Kodumuz, dünya çapında, herkesin kullanımına açıktır. Yazdığımız yazılımları onaylayıp onaylamadığınızı çok da umursamıyoruz. Biliyoruz ki yazılım yok edilemez ve yaygın olarak dağıtılmış bir sistem kapatılamaz.

Şifrepunklar kriptografi üzerindeki düzenlemelere esefle bakar; zira şifreleme temel olarak mahrem bir davranıştır. Şifreleme işi, aslında, bilgiyi kamusal alandan uzaklaştırır. Kriptografi karşıtı kanunlar dahi yalnızca devletin sınırlarına ve şiddetinin uzanabildiği yere kadar etkilidir. Kriptografi, ve onun mümkün kıldığı anonim işlem sistemlerinin, yerküreye yayılması kaçınılmazdır.

Mahremiyetin yaygın olabilmesi için, sosyal sözleşmenin bir parçası olması gerekir. İnsanlar toplanarak, ortak yarar adına bu sistemleri hep beraber yerleştirmelidir. Mahremiyet ancak birinin arkadaşlarının toplumdaki iş birliği kadar yayılır. Biz Şifrepunklar sorularınız ve endişelerinize talibiz ve umuyoruz ki sizin ilginizi çekebiliriz böylece kendimizi kandırmış olmayız. Ancak bazıları bizim hedeflerimize karşı çıkıyor diye yolumuzdan dönecek değiliz.

Şİfrepunklar, ağları mahremiyet açısından daha güvenli kılmaya söz vermişlerdir. Hadi hep birlikte hızlıca harekete geçelim.

İleri.

Eric Hughes.