



Syncthing

Syncthing, birden fazla cihazda eş zamanlı olarak istenilen dosyaları senkronize etmek için kullanılan açık kaynak kodlu bir yazılımdır. Lokal ve global ağda gerçekleşebilen senkronizasyon işlemi esnasında veriler şifrelenir ve herhangi bir ara sunucu kullanılmadan P2P (Peer-To-Peer) modeline göre çalışılır. Açık kaynak kodlu olma özelliği de buna eklenince uygulama emsallerine göre daha güvenlidir. Ayrıca, bulut tabanlı depolama servislerinde kullanılan alana göre belirli bir ücret ödemek gerekiyken syncthing herhangi bir ara sunucu kullanmadığı için ücretsizdir ve bir dosya boyutu sınırlaması yoktur, istenilen boyuttaki bir dosya sıkıntısız bir şekilde senkronize edilebilir. Son olarak cross-platform olduğunu ve birçok ana işletim sistemini desteklediğini söylemeden geçmeyelim. Yazılım daha detaylı olarak aşağıda başlık başlık incelenecektir.

NE İŞE YARAR?

Örneğin, iş yerindeki bilgisayarınızda bir veritabanınız var ve siz çalışırken bu veritabanını sürekli olarak güncelliyorsunuz. Fakat siz aynı zamanda eve gittiğinizde de bu veritabanı üzerinde birtakım işlemler yapıp onu tekrar güncellemek istiyorsunuz. Peki iş yerinde değiştirmiş olduğunuz veritabanını kendi evinizdeki veritabanıyla nasıl eşlersiniz? Burada iki seçeneğiniz var. Ya işyerindeki veritabanını bir fiziksel belleğe veya bulut tabanlı bir depolama servisine yükler ve eve geldiğinizde o veritabanını kişisel bilgisayarınıza geçirirsiniz ki bu aynı zamanda evde değişiklik yaptığınız zaman onu tekrar aynı yöntemleri uygulayarak işyerinize götürmeniz gerektiği anlamına gelir. Ya da daha mantıklı bir seçenek olarak bir senkronizasyon programı kurar ve tüm işi onun yapmasını sağlarsınız. Syncthing de tam olarak bu amaca hizmet eden bir program. Bir veya daha fazla dosyayı cihazlarınız arasında eş zamanlı bir şekilde senkronize ederek bu dosyalara istediğiniz her yerden ulaşım imkanı sağlar. Syncthing sayesinde paylaşılan dosyalar üzerinde yapılan değişiklik, bu dosyaların herhangi birinin silinmesi veya yeni bir dosya yaratılması gibi işlemler birbirine bağlı tüm cihazlarda bu işlemlerin uygulanmasını sağlar. Tabii ki bahsedilen bu işlemlerin senkronizesi kullanıcının kontrolündedir, seçilecek olan ayarlara bağlı olarak bir dosyanın senkronize işlemi kısıtlanabilir. Bunun dışında syncthing sunduğu güvenlik olanakları ile verilerin gizliliğini ve bütünlüğünü koruma altına alır.

NASIL ÇALIŞIR?

Syncthing dosyaların değiştirilip değiştirilmediğini anlamak için sistemde tarama yapar. Bunlardan ilki belirli aralıklarla yapılan tam taramadır, diğeri ise watcher adı verilen ve dosya üzerinde bir değişim algılandığında kısa süre içerisinde senkronizasyonu başlatan bir özelliktir. Varsayılan olarak tam tarama saatte bir keredir ve watcher özelliği aktiftir. Watcher, dosya üzerinde işlem yapıldıktan sonra bunun işlemin hemen etki etmesini sağlamak içindir fakat watcher ne kadar bir değişim algılandığında bildirim alsada bu değişimi anında senkronize etmez. Yaklaşık 10 saniye boyunca bu değişimleri biriktirir ve bu sürenin ardından uygular, hatta bir dosya silinmişse watcher'ın bunu uygulama süresi yaklaşık 1 dakikadır.

Senkronizasyon işleminde The Block Exchange Protocol (BEP) adı verilen bir protokol kullanılır. Bu protokol tüm cihazları içine alan bir küme oluşturur. Her cihaz metadata ve blok listesi içeren kendi lokal modelini kümedeki diğer cihazlar ile paylaşır. Lokal modellerin birlikte oluşturduğu modele global model adı verilir. Kümedeki her cihaz kendi lokal modelini, global sistemdeki en iyi (genellikle en yeni) modele göre senkronize etmeye çalışır. Bu sayede cihazlar dosyalarını güncel ve birbirlerine eşlenmiş bir şekilde tutarlar.

Syncthing'in dosya sistemi üzerinde nasıl tarama yaptığını ve bu taramalara göre nasıl senkronizasyon yaptığını anladık. Fakat dosyalardaki bu değişimler nasıl algılanıyor? Syncthing, dosyalar belirli uzunluktaki bloklara böler. Ardından her bir bloğun SHA256 hash değeri hesaplar ve bu değeri sırayla blok listesine yazar. Belirli aralıklarla tarama yapılarak blok listesi güncellenir ve kümedeki cihazların blok listeleriyle karşılaştırılır. Eğer blok listelerindeki bir bloğun hash değeri bu bloğun diğer blok listelerindeki hash değerlerinden farklı ise bu o bloğun değiştirildiği anlamına gelir. Syncthing bu bloğu bulunduğu kümedeki başka bir cihazdan indirir ve indirilen bloğun hash değerini bu bloğun global sistemdeki hash değeri ile karşılaştırır. Eğer hash değeri uyuşursa bu bloğu geçici bir dosyaya yazar, uyuşmazsa bu blok silinir ve başka bir cihazdan indirilir. Ardından bu geçici ve güncel olan dosya güncel olmayan dosyayla değiştirilir.

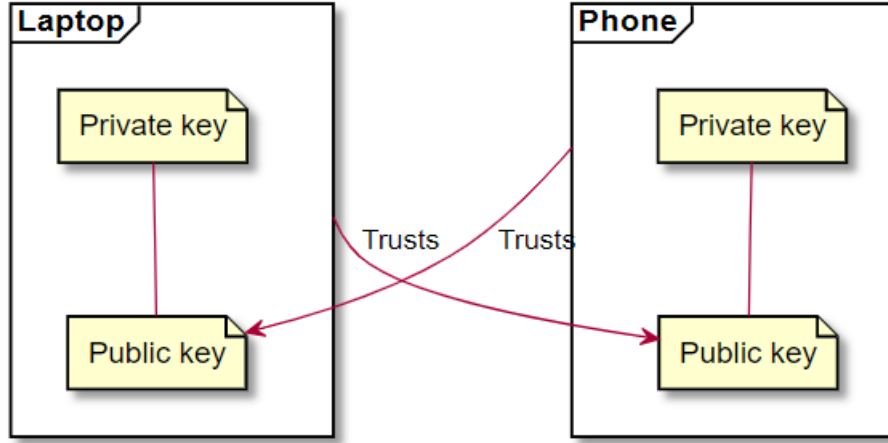
Bunların yanında bir de ID numaraları vardır. Her cihaz kendine özel bir cihaz ID'sine sahiptir. Bu ID; adres çözümlemesi, kimlik doğrulama ve yetkilendirme için kullanılır. Bu ID'yi oluşturmak için syncthing ilk olarak 384 bitlik bir ECDSA anahtar çifti oluşturur. Ardından bu anahtar çiftinden bir tanesi kullanılarak bir x509 sertifikası oluşturur ve bu sertifikanın hash değeri (sha256) elde edilir. Bu hash değeri base32 kullanılarak şifrelenir. Şifreleme sonrası oluşan değer 52 karakterdir. Bu değere 4 adet kontrol biti eklenir ve 8 parçaya ayrılır. Bu değer bizim cihazımızın ID'si olmuş olur. Artık cihazlarımızı lokal ve global ortamda bu ID ile birbirine eşleyebiliriz.

Cihazlarımız için ID değerlerimizi oluşturduk ama bu cihazlar birbirini nasıl bulacak? Syncthing cihazları bulmak için 3 method kullanır.

- 1- Eğer cihazımız statik bir IP adresine sahipse Syncthing direkt olarak bu IP'ye bağlanıp cihazları eşleyebilir.
- 2- Cihazlarımız aynı lokal ağ içerisindeyse belirli aralıklarla kendi ID, adres ve port numaralarını yayınlarlar. Bu sayede aynı ağdaki cihazlar herhangi bir discovery server ile etkileşmeden eşlenebilir.
- 3- Eğer cihazlar statik bir IP'ye sahip değilse ve aynı ağda bulunmuyorlarsa o zaman birbirlerini eşlemeleri için bir discovery server kullanılır. Bu server sadece cihazların birbirini bulması için kullanılır, verilerin senkronizasyonu için kullanılmaz.

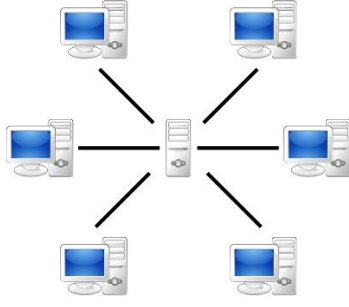
Güvenlik Olanakları

Syncthing'in sağladığı güvenlik olanaklarının başında ID'ler gelir. Cihaz ID'leri ECDSA anahtar çiftinin public key'ini içeren x509 sertifikası kullanılarak üretilir. Cihazlar, ID'leri ile birbirlerine bağlanmak istediklerinde aslında yaptıkları şey birbirlerinin public key'lerine güvenmek olur. Bağlantı sırasında birbirlerine gönderdikleri sertifikalardan karşı tarafın ID'sini üretmeye çalışırlar. Eğer bu işlem başarılı olursa cihazlar birbirlerini eşlemeye bir adım daha yaklaşırlar.

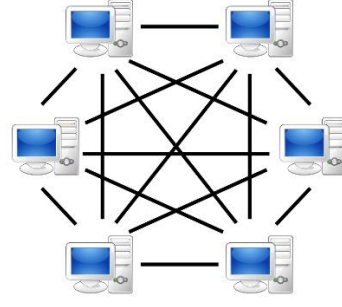


Syncthing trust

Diğer bir güvenlik olanağı ise P2P modeline göre çalışmasıdır. Dosyaların senkronizasyonu için herhangi bir ara sunucu kullanılmadığından bu dosyalara yetkisiz bir erişimin sağlanma olasılığı çok düşüktür. Ayrıca senkronizasyon işlemi şifreli bir şekilde gerçekleştiği için veri sızıntısı olsa dahi veriler güvendedir.



Server-based



P2P-network

Bunların yanında bir de güvenlik açıkları vardır. CVE-2017-1000420 ve CVE-2021-21404 numaralı uygulama açıkları, yazılımın belirli bir sürüm aralığına özel olup yamalanmış açıklardır. Syncthing'in güncel sürümlerinde bulunabilen başka bir güvenlik açığı yoktur.

Kaynakça:

<https://linuxctl.com/2017/04/syncthing---why-you-should-be-using-it/?fbclid=IwAR0BfwByBF-aqbq6stPLq7uWYillmsSyNuFVraT2G0Yyk0EQa6k6t0n91jY#syncthing-the-light-at-the-end-of-the-tunnel>

<https://advancedweb.hu/how-syncthing-provides-secure-file-syncing-without-sharing-your-files-with-a-third-party/>

https://saulalbert.net/blog/how-to-share-large-amounts-of-research-video-data-with-syncthing/?fbclid=IwAR0_E5lDB3sbxcdykVyDTyIQ7HiI8MTyIMaEdWTDvtczj6iM0kSwzEha9nc

HAZIRLAYAN
ALTAY YÜCETAŞ