



FINDIK – Herkese Açık Filtre

18.04.2009

FINDIK Ekibi <findik@findikproject.org>





Sunum Planı

- Neden içerik filtreleme?
- Peki neden FINDIK?
- FINDIK nasıl kullanılır?
- FINDIK uygulama tasarımı
- FINDIK nasıl geliştirilir?
- Gelecek adımlar
- Sorular





Neden İçerik Filtreleme

- Hukuki sorumluluklar
 - Korsan içerik.
 - Saldırılar
 - Dışarıdan içeriye
 - İçeriden dışarıya
 - 5651





Neden İçerik Filtreleme

- Türkiye’de meşhur 5651 s.k. ile toplu internet kullanımı sağlayan yerlere getirilen yükümlülükler ve erişimden sorumlu tutulmaları sonucu oluşabilecek problemlerin önüne geçmek.





Neden İçerik Filtreleme

- Kullanıcı politikaları
 - Firmalar
 - Farklı birimler için farklı profiller.
 - Internet hizmeti sağlayanlar
 - Amaç için kullanıldığından emin olmak.





Neden İçerik Filtreleme

- Bant genişliği tasarrufu
 - Dosya indirme için özelleşmiş sistemler.
 - Erişilmek istenen içerik ile beraber gelen reklamlar.





FINDIK nedir?

- İçerik filtreleme yeteneğine sahip bir yazılımdır.
 - Web içerik filtreleme yazılımından beklenen standart özelliklerin tümüne sahip.





FINDIK nedir?

- Sadece içerik filtreleme yazılımı değildir.
 - Uygulama çatısıdır.
 - İçerik analiz için kolay kullanılabilir ve yetenekli bir arayüz sunar. (Geliştiriciye)





FINDIK nedir?

- Uygulama çatısıdır.
 - Antivirüs filtresi, her protokol için uygulanabilir.
 - Bir protokolün SSL uygulması için ek çaba harcamaya gerek yoktur. (HTTP / HTTPS)





FINDIK nedir?

- Geliştirici dostu bir arayüz sunar.
 - Geliştirici sadece içerik analizine ya da destek vermek istediği protokole özel konulara odaklanır.
 - Ya da bambaşka bir altsistemi/servisi FINDIK'a ekler.





Neden FINDIK?

- Neden böyle bir projeye başladık?
 - Bu alanda fazla “özgür” yazılım yok.
 - Mevcut yazılımlar beklentileri karşılamıyor.
 - Çoğu kolay genişletilebilir değil.





Neden FINDIK?

- FINDIK'ı tasarlarken/geliştirirken güvenlik, genişletilebilirlik, kullanılabilirlik ve performans kavramlarını en yüksek önem ile ele aldık.





FINDIK nasıl kullanılır?

Minik bir demo.





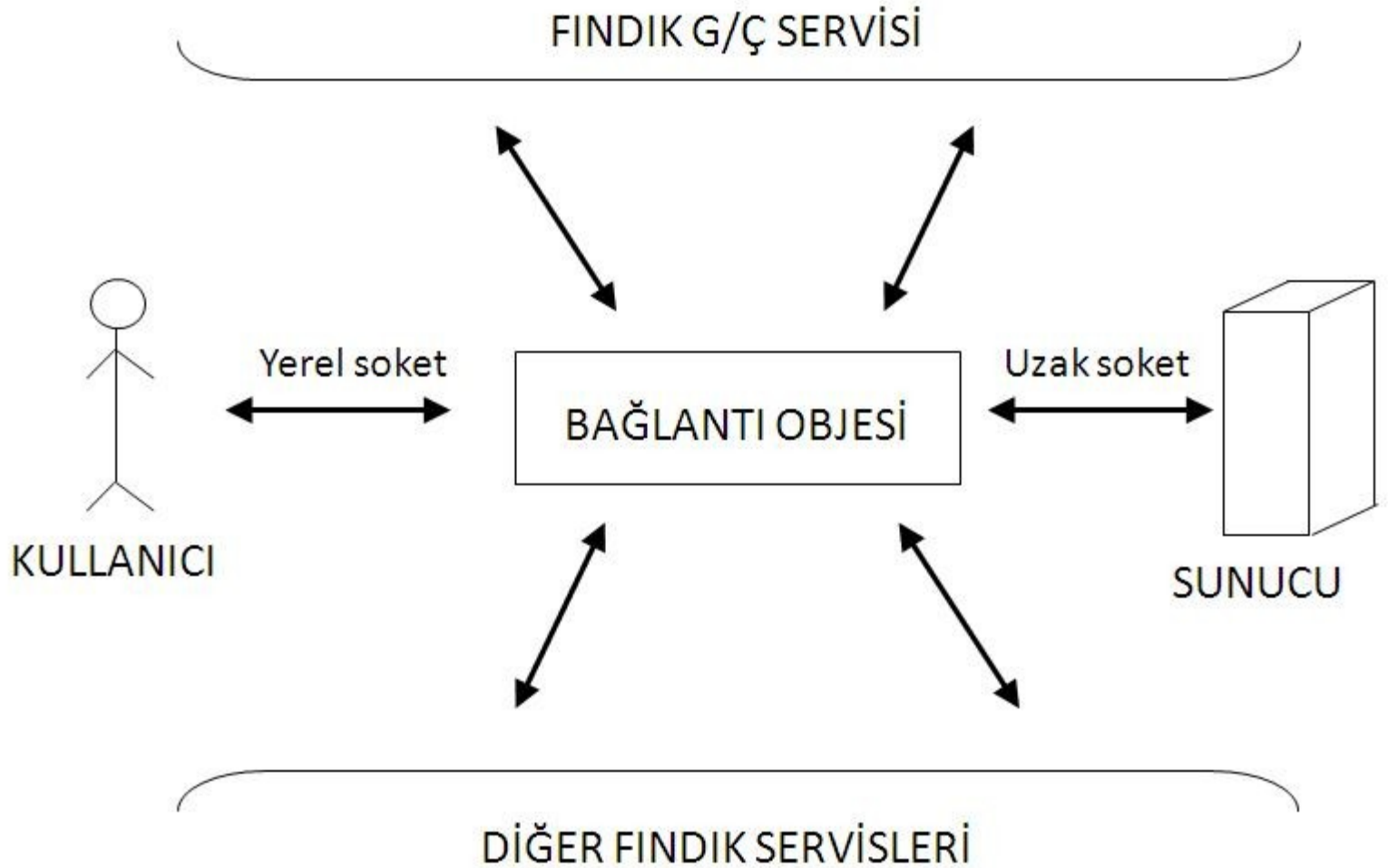
FINDIK Uygulama Tasarımı

- Altsistemlerden hizmet alan/isteyen bağlantı nesnesi.
 - Her bir TCP bağlantısı için bir bağlantı nesnesi.
 - TCP bağlantısının ortasında. Yerel ve uzak uçlar için birer soket.





FINDIK Uygulama Tasarımı



FINDIK



FINDIK Uygulama Tasarımı

- Boost API.
 - Boost ASIO kütüphanesinin `io_service` sınıfı, FINDIK bağlantı nesnesinin kullandığı en önemli servis.
 - Tüm döngüyü yönetiyor.
 - Eşzamansız (asynchronous)





FINDIK Uygulama Tasarımı

- Erişim kontrol listelerinin ve kara listelerin veritabanında saklanması.
 - Sık değişen, sık erişilen, büyük veri.
 - Performans sorunları
 - MySQL
 - Sorgu önbelleği.





FINDIK Uygulama Tasarımı

- log4j destekli kayıt tutma
 - Veritabanı
 - NT Event Logger
 - Syslog
 - Dosya





FINDIK Özellikleri

- HTTP protokolünü destekliyor.
 - Dolayısıyla HTTPS de destekleniyor.
 - Kerberos ya da LDAP ile yetkilendirme.
 - Alan adı, URL ve içeriğe göre filtreleme.
 - İçerik tipi (uzantı, dosya türü)
 - Virüs





FINDIK Özellikleri

- SSL içerik filtreleme mi? Nasıl?
 - Ortadaki FINDIK (FINDIK in the middle)
 - Güvenlik
 - Sertifika kontrolleri
 - Kullanılabilirlik





FINDIK Nasıl Geliştirilir?

- FINDIK geliştirici dostu bir arayüz sunar.
- FINDIK servisleri modülerdir.
 - Filter service
 - Parser service
 - Auth service
 - Reply service





FINDIK Nasıl Geliştirilir?

```
class sample_filter:
    public boost::enable_shared_from_this<sample_filter>,
    public findik::filter::abstract_filter
{
public:
    boost::tuple<bool, filter_reason_ptr> filter(connection_ptr
    connection_, unsigned int param = 0)
    {
        if (connection_->current_data()->content_size() > 1024)
            return boost::make_tuple(false, create_reason("", ""));

        filter_reason_ptr frp_;
        return boost::make_tuple(true, frp_);
    }

    bool is_applicable(findik::io::connection_ptr connection_)
    {
        return connection_->current_data()->has_content();
    }
};
```





Gelecek adımlar

- Diğer protokoller
 - SMTP
 - POP3
 - IMAP
 - IM





Gelecek adımlar

- Uygulama seviyesi saldırı önleme
- Akıllı algoritmalar ile deneysel video, audio filtreleme
- TPM ile güvenilir zaman damgalama
- Yönetim arabiriminin geliştirilmesi





FINDIK Seni İstiyor!

- Geliştirilecek ve test edilecek çok konu var.
- Yeni fikirler, büyük farklar
- Bazen de sadece eğlence





Sorular

