AKADEMİK BİLİŞİM 2010

Öncül Parola Denetimi Yöntemiyle Parola Seçim Sistemi:

Türkçe Parolalar için Bir Araştırma

İlker Korkmaz, Prof. Dr. Mehmet Emin Dalkılıç

11.02.2010
Muğla

SUNUM TASLAĞI

- Giriş
  - Problemin Tanımı
  - Hedef
- Literatür
  - Öncül Parola Denetimi
- Karar Ağacı Yöntemi ile Öncül Parola Denetimi ve Deneyler
  - Karar Ağaçları
  - Hyppocrates ile Yapılan Deneyler
- Sonuçlar ve Öneriler

GİRİŞ

- Güvenliğin ilk adımı: “ parola ”
- Parola kullanım amacı: “ kimlik doğrulama ”
- Kolay tahmin edilebilen parolalar?

“tehlike”...

Problemin Tanımı

- İlk savunma hattının güvenilirliği neye bağlı?
  - Parola seçimlerinde zayıf ve güçlü parola modelinin belirlenmesi
  - Öncül parola denetimi

Hedef

- Parola güvenliği üzerine araştırma
  - Türkçe kelimeleri ve Türk kullanıcıları dikkate alan öncül parola denetim deneyleri gerçekleştirmek

LİTERATÜR

- Parola güvenliğini arttırmak nasıl olabilir?
  - Kullanıcı eğitimi
  - Otomatik üretilmiş parolaların kullanımı
  - Ardıl (***Reactive***) parola denetimi
  - Öncül (***Proactive***) parola denetimi

Mevcut Çalışmalar

- Öncül parola denetimi
  - Kural tabanlı modeller
    - "*A Proactive Password Checker, Matt Bishop, 1990*"
    - "*Improving System Security via Proactive Password Checking, Matt Bishop, Daniel V. Klein, 1995"*
  - Bloom Filtreleri
    - *"OPUS: Preventing Weak Password Choices, E. H. Spafford, 1992"*
  - Markov modeli
    - "BAPasswd: A New Proactive Password Checker, C. Davies, R. Ganesan, 1993"
  - Karar Ağaçları (***decision trees***)
    - "High Dictionary Compression for Proactive Password Checking, Bergadano et al, 1998"
    - "Hyppocrates: A new Proactive Password Checker, Carlo Blundo et al, 2004"

KARAR AĞACI YÖNTEMİ İLE ÖNCÜL PAROLA DENETİMİ VE TÜRKÇE PAROLALAR ÜZERİNDE DENEYLER

- Şifrelenmiş Türkçe parolaların kırılmaya çalışılması ve şifrelenmemiş açık parolaların karakteristiklerini incelemek üzere yapılan istatistiksel çalışmalar ile zayıf ve güçlü parola adayları belirlenmeye çalışılmıştır.
- Öncül Parola Denetimi yazılımı ile Türkçe parolaların denetlenmesi üzerine deneyler yapılmıştır.

Öncül Parola Denetleme Araçları

- Denetleme:
  - Sözlük ataklarına dayanamayacağı düşünülen,
  - Kolay tahmin edilebileceği düşünülen,
  - Zayıf olarak nitelendirilen

  parola adaylarını kabul etmeme
- Araç:
  - Öncül parola denetleme yöntemlerinden birini/birkaçını uygulayan programlar

Kullanılan Öncül Parola Denetleyiciler

- ProCheck
  - Bergadano et al, “High Dictionary Compression for Proactive Password Checking”, ACM Transactions on Information and System Security, vol. 1, no. 1, Nov. 1998, pp. 3-25
- Hyppocrates
  - Blundo et al., “HYPPOCRATES: A New Proactive Password Checker”, The Journal of Systems and Software, vol. 71, pp. 163-175, 2004

Hyppocrates

- Versiyon 2.0
- GNU lisansı ile açık kaynak kodlu
- C programlama dili ile hazırlanmış
- “gcc” derleyicisi ve kütüphaneleri ile derlenebiliyor
- Bağımlılıklar: XForms ... (önerilen XFormsV0.88 sorun çıkardı; libForms-88 ile derlenebildi.)

Program Mekanizması

- "Hyppocrates" programının işleyiş mekanizması:
  - Verilen bir parola aday sözlüğü ile eğitim safhasında "karar ağacı" yapısı oluşturulur.
  - Bu karar ağacı, bir parolanın kabul edilip edilmeyeceğine karar verir.

Karar Ağacı

- Sınıflandırma yapmak için kullanılan bir yapı
- Ağaç yapısının kök düğümüne verilen bir istek için, en alt yaprağa inildiğinde karar verilmiş olur.
- Karar verme mekanizmasında eğitim safhasındaki önbilgi (parola aday sözlüğü) ve ilgili isteğin nitelikleri (***attribute***) etkilidir.

“Hyppocrates”ın Karar Ağacı

- Milyonlarca kelime içeren sözlük eğitildiğinde karar ağacı büyür.
- Bazı özel kelime grupları için alt dallar çok yer kaplayabilir.
- Budama (***pruning***) taktiği ile o dalın altındaki farklı nitelikteki sözcükler aynı sınıflandırma kararını alırlar. Budama sonucu tahminleme nedeni ile hata olasıdır.

Türkçe Parolalar ile Yapılan Deneyler ve Sonuçları

Eğitim			*Test*	
mod	*zayıf sözlük*	*güçlü sözlük*	*farklı zayıf sözlük*	*farklı güçlü sözlük*
H	klm3map.txt %100	strong1 %100	weakMAP %87	strongMAP %72
H	words %100	strong1 %100	weakMAP %87	strongMAP %71
MH	klm1utf.txt %100	strong1 %99	weakUTF8 %24	strongUTF8 %70
MH	words %99	strong1 %99	weakUTF8 %87	strongUTF8 %69

Türkçe Parolalar ile Yapılan Deneyler ve Sonuçları (devam)

Eğitim		*Test*	
zayıf sözlük	*güçlü sözlük*	*farklı zayıf sözlük*	*farklı güçlü sözlük*
tdkMAP.txt %99	strong1 %100	weakMAP %87	strongMAP %72
		weakMAP.noise %80	strongMAP.1noise: %89 strongMAP.2noise: %91 strongMAP.3noise: %91
words %100	strong1 %100	weakMAP %87	strongMAP %71
		weakMAP.noise %82	strongMAP.1noise: %83 strongMAP.2noise: %90 strongMAP.3noise: %90

Deneyler Sonucunda Genel Değerlendirme

- Türkçe parolalar için uygun model: Hyppocrates programının varsayılan hali ile kullanılıp, zayıf sözlük adayı olarak Türk Dil Kurumu sözlüğünde geçen kelimelerin “ç,ğ,ı,ö,ş,ü” harflerinin dönüştürülmüş hali ile eğitilmesi; test sözlüklerinin de dönüştürülerek kullanılması uygun görülmüştür.
- Terminalden, Hyppocrates programına bağlanan bir program yardımıyla dönüştürme işlemleri yapılabilmektedir.
- Önerilen model için,
  - ağaç boyu: 218 Byte (budanmış hali de aynı) + istisna dosyası: 14 Byte
  - sıkıştırma oranı: 218 B / 596051 B = %0,03 (<%1)
  - hata oranları:
    - eğitim sözlükleri için %0 (istisna dosyası da düşünülerek)
    - farklı sözlükler için:
      - zayıf test sözlüğü (weakMAP) için: %13
      - gürültülü zayıf sözlük için: %20
      - güçlü varsayılan sözlük (strongMAP) için: %28
      - gürültülü güçlü sözlükler için: %11 ~ %9

SONUÇLAR VE ÖNERİLER

- Sonuçlar:
  - Türk kullanıcı parolaları ile etkin öncül parola denetimi testleri yapmak üzere Hyppocrates üzerinde deneyler yapılıp öneriler sunulmuştur.
- Öneriler:
  - Türkçe sözlük için; kitaplarda geçen kelimeler, özel isimler, film, sportif takım, şehir, semt isimleri v.b. derlenerek sözlük genişletilebilir.
  - Hyppocrates kaynak koduna, meta-karakterlere karşı davranışını belirlemek üzere müdahale edilerek, değişiklikler yapılıp Türkçe parola denetim testlerine daha uygun bir model bulabilmek üzere devam edilebilir.

TEŞEKKÜRLER

...