Kriptografik Protokol ve Standartlar

Kriptografik Protokol ve Standartlar

Kriptografi pek çok seviyede çalışmaktadır, blok cipher ve açık anahtar kriptosistemleri gibi. Bunları kullanarak protokolleri, ve protokolleri kullanarak da uygulamaları (veya diğer protokoller) elde edersiniz.
Algoritmaların altında yatan güvenlik üzerinde çalışmak yeterli değildir, bir zayıflık belirtisi olarak yüksek-seviyeli protokoller (veya uygulamalar) yaşamsal bilgileri algoritmaların tamir edemeyeceği bir şekilde sızdırabilirler. Basit bir örnek verirsek, iletişim kanalını şifrelemek için kullanılan anahtar hakkındaki bilgi sızdıran protokoller olabilir. Ve sonra algoritmalar ne kadar iyi olursa olsunlar saldırgan bunları atlayarak sadece protokole saldırabilir. Protokollerin analizi genelde zordur, çünkü bu uygulamaları kullanan uygulamalar daha ciddi sorunlara yol açabilir. Böylece, iyi bir protokol yeterli değildir, ama iyi ve sağlam bir uygulamanız da olmalıdır. Aşağıda, iyi bilinen protokol ve standartlar verilmiştir:
Domain Name Server Security (DNSSEC) (Alan Adı Servis Sağlayıcı Güvenliği):
Bu protokol güvenli dağıtılmış isim servisleri içindir.
http://www.ietf.org/ids.by.wg/dnssec.html
Generic Security Services API (GSSAPI)
GSSAPI, farklı kriptografik sistem ve algoritmalar için onaylama, anahtar değiş-tokuşu ve şifreleme arabirimi sağlar.
ftp://ftp.uni-siegen.de/pub/rfc/rfc1508.txt
Secure Socket Layer (SSL)
SSL, güvenli WWW bağlantıları için kullanılan iki protokolden biridir (diğeri SHTTP dir). WWW güvenliği kredi kartı numaraları gibi hassas bilgilerin internet üzerinden transferi arttıkça önemli bir konuma gelmiştir. SSL ilk olarak www.netscape.com tarafından 'açık protokol standardı' olarak geliştirilmiştir. www.openssl.org adresinde belgeler ve açık kaynak uygulamaları bulunabilir.
Secure Hypertext Transfer Protocol (SHTTP)
Bu da WWW işlemleri için daha fazla güvenlik sağlayan başka bir protokoldür. Pek çok bakımdan SSL'den daha esnektir, ama Netscape'in piyasadaki egemenliğine bağlı olarak SSL daha güçlü bir pozisyondadır.
ftp://ftp.uni-siegen.de/pub/rfc/rfc1508.txt
E_Mail Security and Related Service (E-Mail Güvenliği ve İlgili Siteler)
OpenPGP, Phil Zimmermann'ın PGP'sinin yıllardır yaptıklarının bir standardlaştırılmasıdır. Ancak, şimdi ayrı bir ayrı bir standarttır, (http://www.pgpi.org) farklı uygulamalar geliştirilmektedir.
Secure-MIME (S-MIME)
(http://www.ietf.org) tarafından desteklenen S/MIME, OpenPGP standardı için bir alternatiftir.
http://www.ietf.org/html.charters/smine-charter.html
Publius Censor-Resistent Publishing Protocol
Bu çok gelişmiş bir sistemdir. Yazar ve okuyucuların ağ makinelerinde belgeleri paylaşmasına olanak tanır öyleki:
(1) ne yazar nede okuyucu kimliğini açıklamak zorunda değildir,
(2) belgelerin belirli bir (takma adlı) yazar tarafından gelmeleri için sertifiklandırılır,
(3) mevcut ağ makineleri arasında bir uzlaşma olmadıkça belgeler silinemez veya düzenlenemez (sansürlanemez).
Teknik raporlar, yazılımlar ve ilgili projelere bağlantılar http://cs1.cs.nyu.edu/waldman/publius adresinden temin edilebilir.
Public Key Encryption Standarts (PKCS) (Açık Anahtar Şifreleme Standartları)
Bu standartlar RSA Veri Güveliği tarafından geliştirilmişlerdir ve RSA'nın güvenli kullanımı için yollar tanımlanmaktadır. RSA Laboratories tarafından yayınlanan bazı belgeler ftp://ftp.rsa.com/pub/pkcs adresinden temin edilebilir.
IEEE P1363: Standart Specifications for Public-Key Cryptography (Açık-Anahtar Kriptografisi için Standart Şartnameler)
Şifreleme ve dijital imzalar için pek çok açık anahtar algoritması içermektedir. Gerekli tüm uygulama ayrıntılarını içeren oldukça geniş bir eki vardır. Daha fazlası için
http://manta.ieee.org/groups/1363
SSH2 Protocol
SSH2 (http://www.ietf.org) çalışma grubu tarafından geliştirilmiştir. Bu protokol internetin ihtiyaçları için çok yönlü bir protokoldür ve şu anda (http://www.ssh.com) da kullanılmaktadır. Bu protokol, terminal oturumlarını ve keyfi TCP bağlantılarını güvene almak için kullanılır. SSH2, Tatu Ylvnen tarafından geliştirilen SSH1 üzerine kuruludur. Protokol şartnameleri http://www.ietf.org/html.charters/secsh-charter.html adresinde bulunabilir.
IPSec (IP Güvenliği)
Yukarıda verilen tüm protokoller internetin uygulama tabakasında belirli programların, doğası icabı güvensiz olan

ağlarda güvenli bir kanal üzerinde iletişimine olanak tanırken, IPSec internetin özü olan “internet protocol-IP” yi güvenli kılmayı çalışmaktadır. RFClerin bir listesi ve geniş ölçekli uygulamalar http://www.ssh.com adresinde bulunabilir.