Säkerhet

Daniel Bosk

Institutionen för informationsteknologi och medier (ITM),
Mittuniversitetet, Sundsvall.

security.tex 328 2012-10-10 11:53:27Z danbos

Mittuniversitetet
MID SWEDEN UNIVERSITY

Översikt

1. Kommunikation och datasäkerhet
   - En säker anslutning
   - Några exempel från applikationslagret
   - Säkerheten hos SSL
2. Malware och hot på World Wide Web
   - Malware
   - Hot på World Wide Web
3. Hashfunktioner
   - Allmänt om hashfunktioner
   - Några olika hashfunktioner
   - Exempel från terminalen

Mittuniversitetet
MID SWEDEN UNIVERSITY

En säker anslutning

Trådbundet och trådlöst nätverk

- Hur fungerar trådbundet och trådlöst nätverk?
- Vad är skillnaderna ur ett säkerhetsperspektiv?

TCP/IP-modellen

Applikationslagret Kommunikation till och från program. Exempel på protokoll: HyperText Transfer Protocol (HTTP), HTTPS, File Transfer Protocol (FTP), Secure SHell (SSH).

Transportlagret Förbindelsen mellan sändare och mottagare. Data delas upp i paket. Exempel på protokoll: Transport Control Protocol (TCP), User Datagram Protocol (UDP).

Nätverkslagret Kopplar ihop noder till ett nätverk. Exempel på protokoll: Internet Protocol (IP).

Länklagret Datorns kommunikation med närliggande enheter i resten av nätverket. Exempel på protokoll: Ethernet, IEEE 802.11{a,b,g,n}.

Mittuniversitetet
MID SWEDEN UNIVERSITY

Hur fungerar trådbundet och trådlöst nätverk?

Skillnaden ligger i länklagret.

Trådbundet Vid stjärnnät skickas allt via den centrala hubben som sedan skickar vidare till mottagare eller annan hubb.

Trådlöst Data skickas genom luften till accesspunkten.

Vad är skillnaden ur ett säkerhetsperspektiv?

Skillnaden är vilka som är mottagare.

Trådbundet Data skickas okrypterat genom kabeln. Den som har tillgång till kablarna kan avlyssna.

Trådlöst Data skickas genom luften. Utan kryptering kan alla inom $50 - 100\ \mathrm{m}$ ta emot data. Med kryptering kan alla som har krypteringsnyckeln ta emot[1].

[1] Och även alla som har tillräcklig datorkraft för att knäcka kryptonyckeln.

HTTP vs HTTPS

Applikationslagret

HTTP

- När en webbläsare begär innehåll från en webbserver görs detta via HTTP-protokollet.
- Exempel på begäran: `GET /path/to/file/index.html HTTP/1.0`
- Exempel på svar: `HTTP/1.0 404 Not found`. Därefter följer HTML-kod för en felsida.

HTTPS är HTTP med TLS/SSL

- Servern för över sitt certifikat.
- Klienten krypterar ett slumptal med serverns publika nyckel. Bara den som har den motsvarande privata nyckeln kan avkryptera.
- Slumptalet används för att kryptera kommunikationen.
- Samma som för HTTP.

Mittuniversitetet
MID SWEDEN UNIVERSITY

SSH och SFTP

Applikationslagret

Secure SHell (SSH) Upprättar en krypterad anslutning till en server, likt den för HTTPS. Låter därefter användaren logga in och startar därefter en terminal på servern.

SFTP Upprättar en SSH-anslutning till servern. Låter användaren logga in och startar därefter (i princip) en FTP-server istället för en terminal.

Säkerheten hos SSL

Säkerhetsstruktur och *trust model*

1. (Regeringen för CAs land)
2. Certificate Authority (CA)
3. Middle CA ...
4. (Server, företag och administratör)

Det finns uppskattningsvis strax över 600 CAs i världen.

Två CAs: Comodo och DigiNotar

- Comodo är en av världens största CAs.
- DigiNotar *var* den störta CA i Nederländerna.
- Dessa två blev hackade. Comodo i mars 2011. DigiNotar ungefär i juni, det avslöjades i början av september. DigiNotar ansökte om konkurs den 21 september.
- Förövarna genererade och signerade ungeför 500 falska certifikat för bland andra domänerna `google.com`, `gmail.com` och `facebook.com`.
- Certifikaten användes troligtvis av den Iranska regeringen för att övervaka medborgare i Iran.

Mittuniversitetet
MID SWEDEN UNIVERSITY

Alternativ till Certificate Authorities

- I augusti på BlackHat USA 2011 presenterades Convergence [Con11].
- Bygger på att du själv väljer vem du litar på.
- Systemet har *notaries* som sitter på andra nät och laddar hem certifikaten för samma servrar som du och det verifieras att alla fick samma resultat.

SSH har inte samma *trust model*

SSH kräver att du vet vilka nyckel-ID som en viss server ska ha.

Malware

Virus Ett program som infekterar andra program genom att kopiera sin egen kod in i dem.

Worm En mask (engelskans *worm*) är ett program som förflyttar sig själv från dator till dator.

Trojan Ett program som ger sken av att vara någonting annant men öppnar egentligen en bakdörr in i systemet.

Hot på World Wide Web

- Virus, worms och trojaner sprids via internet.
- Kräver (i princip) att du laddar hem dem och kör dem. Detta inkluderar att bli lurad att ladda hem och köra dem, exempelvis bilagor till e-post.
- Se Open Web Application Security Project [The10].

OWASP Top Ten för nätverksdrift

Från [The10]:

- A3 Broken Authentication and Session Management
- A6 Security Misconfiguration
- A7 Insecure Cryptographic Storage
- A9 Insufficient Transport Layer Protection

Hashfunktioner

- En funktion $H\colon S \to T$ från mängden av alla strängar S till en delmängd T med strängar av en given längd.
- Ska vara en envägsfunktion, svårt att finna krockar.

MD4 och MD5

MD4 Av Ronald Rivest från 1990. 128-bitars hashvärde, 3 rundor. Används för Windows lösenordshashvärden.

MD5 Av Ronald Rivest från 1992. 128-bitars hashvärde, 4 rundor. Inte kollisionsresistent. Bygger på Merkle-Damgård-konstruktion.

MD5 kollision

Julius. Caesar
Via Appia 1
Rome, The Roman Empire

May, 22, 2005

To Whom it May Concern:

Alice Falbala fulfilled all the requirements of the Roman Empire intern position. She was excellent at translating roman into her gaul native language, learned very rapidly, and worked with considerable independence and confidence.

Her basic work habits such as punctuality, interpersonal deportment, communication skills, and completing assigned and self-determined goals were all excellent.

I recommend Alice for challenging positions in which creativity, reliability, and language skills are required.

I highly recommend hiring her. If you'd like to discuss her attributes in more detail, please don't hesitate to contact me.

Sincerely,

Julius Caesar

(a) Rekommendationsbrev

Julius. Caesar
Via Appia 1
Rome, The Roman Empire

May, 22, 2005

Order:

Alice Falbala is given full access to all confidential and secret information about GAUL.

Sincerely,

Julius Caesar

(b) Order

Figur: Två brev i PostScript med MD5 hashvärdet a25f7f0b 29ee0b39 68c86073 8533a4b9 [DL].

Mittuniversitetet
MID SWEDEN UNIVERSITY

SHA-familjen

SHA-1 Av National Security Agency (NSA) från 1995. 160-bitars hashvärde, 80 rundor. Bygger på Merkle-Damgård-konstruktion.

SHA-2 Av National Security Agency (NSA) från 2001. 224/256- eller 384/512-bitars hashvärden, 64 respektive 80 rundor. Bygger på Merkle-Damgård-konstruktion.

SHA-3 Av Bertoni, Daemen, Peeters och Van Assche från 2007-2012. Kan ge godtyckligt stort hashvärde. Bygger på sponge-funktioner.

Exempel från terminalen

```
1 (0):danbos@ID20809793:security$ sha256sum
2 jag testar med en mening
3 1a558689ccc4ff988b5f8c3f1bc2bf5f48b116c890077a6ff10a1718429e579b  -
4 (0):danbos@ID20809793:security$ sha256sum
5 jag testar med en annan mening
6 829eb0677df411ee0d821bdd87c0ceb7b4d0db1996c0f312b2cbbd5aaf2e42af  -
7 (0):danbos@ID20809793:security$ sha256sum security.tex
8 c535894cb08c14564eb3d08e32fd4d40b80354f9d8e2b1e8b28028c28f6455ae  security.tex
9 (0):danbos@ID20809793:security$
```

Mittuniversitetet
MID SWEDEN UNIVERSITY

Referenser

[Con11] Convergence, oct 2011.

[DL] Magnus Daum och Stefan Lucks. Hash collisions (the poisoned mesage attack): ”the story of Alice and her boss”.

[The10] The Open Web Application Security Project. OWASP Top 10 – 2010 : The ten most critical web application security risks, apr 2010.