Sunet-dagarna 2017-10-16 - 19

PGP för nybörjare - Pretty Good Privacy

SUNET/CERT

Maria Edblom Tauson - maria@cert.sunet.se
Arne Nilsson - arne.nilsson@cert.sunet.se

Del 1 E-post och teori bakom PGP

Del 2 Installation och användning av PGP

PGP för nybörjare - Pretty Good Privacy

E-post är en av de viktigaste funktionerna vi har i våra datorer men det finns problem …

- 80-90% av all e-post är SPAM - vanligtvis görs dock filtrering
- Brev levereras i HTML-format – kan försvåra för användaren
- Brev kan innehålla skadliga länkar som kan göra dåliga saker
- Brev kan ha bilagor med skadliga filer ”malware”
- Phishing / Spearphishing (förmå användare att klicka på länkar)
- Varje månad skapas 1.3 miljoner nya sk. phishing sajter – vanligtvis är de endast aktiva några enstaka dagar)

PGP för nybörjare - Pretty Good Privacy

Full-headers är fundamentalt om man vill analysera e-post.

Lär dig att ta fram ”Full-headers” om du vill ha hjälp av din IT-support.

Tyvärr är handgreppen olika i alla e-post klienter men det finns en bra förteckningar för de 29 vanligaste på:

https://mxtoolbox.com/public/content/emailheaders/

Ofta finns det även kortkommandon.

Vanliga tekniker i centrala e-postsystem för att minska de skadliga effekterna är:

- Sender Policy Framework (SPF) – RFC5321
- Sender ID – RFC5322
- Domain Keys Identified Mail (DKIM)
- Domain-based Message Authentication, Reporting and Conformance (DMARC)
- Anti- spam och virus

...

PGP för nybörjare - Pretty Good Privacy

Full-header i Thunderbird görs med kommandot Ctrl U - exempel

```
Return-Path: <ama@chalmers.se>

Received: from mail.cert.sunet.se
          by mail.cert.sunet.se (Dovecot) with LMTP id yiCoOPn3rFlqPwAAeHIycQ
          ; Mon, 04 Sep 2017 06:51:38 +0000
Received: from smtp1.sunet.se (smtp1.sunet.se [192.36.171.214])
          by mail.cert.sunet.se (Postfix) with ESMTPS id 6BE9C20134;
          Mon,  4 Sep 2017 06:51:38 +0000 (UTC)
Received: from e-mailfilter03.sunet.se (e-mailfilter03.sunet.se [IPv6:2001:6b0:8:2::203] (may be forged))
          by smtp1.sunet.se (8.14.9/8.14.9) with ESMTP id v846pZW3000095
          (version=TLSv1/SSLv3 cipher=ECDHE-RSA-AES256-GCM-SHA384 bits=256 verify=FAIL);
          Mon, 4 Sep 2017 06:51:38 GMT
Received: from e-mailfilter03.sunet.se (localhost.localdomain [127.0.0.1])
          by e-mailfilter03.sunet.se (8.14.4/8.14.4/Debian-8+deb8u2) with ESMTP id v846pFa1005129
          (version=TLSv1/SSLv3 cipher=ECDHE-RSA-AES256-GCM-SHA384 bits=256 verify=NO);
          Mon, 4 Sep 2017 08:51:34 +0200
Received: (from defang@localhost)
          by e-mailfilter03.sunet.se (8.14.4/8.14.4/Submit) id v846otIt003798;
          Mon, 4 Sep 2017 08:50:55 +0200
Received: from martell.ita.chalmers.se (martell.ita.chalmers.se [129.16.226.134])
by e-mailfilter03.sunet.se (envelope-sender <ama@chalmers.se>) (CanIt-Domain-PRO/Pre-stream) with ESMTP id v846oscP003765; Mon, 4 Sep 20
17 08:50:55 +0200

Received: from [129.16.140.63] (129.16.10.245) by martell.ita.chalmers.se
(129.16.226.134) with Microsoft SMTP Server (version=TLS1_2,
cipher=TLS_ECDHE_RSA_WITH_AES_256_CBC_SHA384_P256) id 15.1.845.34; Mon, 4 Sep
2017 08:50:54 +0200
To: Arne Nilsson <Arne.Nilsson@cert.sunet.se>,
          Maria Edblom Tauson
          <maria@cert.sunet.se>,
          Patrick Forsberg <fors@cert.sunet.se>
From: Anne-Marie Achrenius <ama@chalmers.se>
Subject: =?UTF-8?Q?L=c3=a4nk_till_anm=c3=a4lningsdata?=
Message-ID: <997ac529-5e4d-904b-1a36-6e09b3add658@chalmers.se>
Date: Mon, 4 Sep 2017 08:50:54 +0200
User-Agent: Mozilla/5.0 (Windows NT 6.1; WOW64; rv:45.0) Gecko/20100101
Thunderbird/45.8.0
MIME-Version: 1.0
Content-Type: multipart/encrypted; protocol="application/pgp-encrypted";
          boundary="4Qe8THRnCNe6xpPlRBLpxuMvTHGJS4jwI"
X-Originating-IP: [129.16.10.245]
X-ClientProxiedBy: targaryen.ita.chalmers.se (129.16.226.133) To
martell.ita.chalmers.se (129.16.226.134)
X-Bayes-Prob: 0.9252 (Score 4, tokens from: cert-sunet-se:default, sunet-se:default, base:default, @@RPTN)
X-Spam-Score: 4.00 (****) [Tag at 5.00] TVD_SPACE_RATIO:0.001,SPF(none:0),DKIM(none:0),Bayes(0.9252:4.0)
X-p0f-Info: os=Windows 7 or 8, link=Ethernet or modem
X-CanIt-Geo: =?UTF-8?Q?
ip=3D129.16.226.134;_country=3DSE;_region=3DV=C3=A4stra_G=C3=B6taland;_city=3DGothenburg;_latitude=3D57.7167;_longitude=3
D11.9667;_http://maps.google.com/maps=3Fq=3D57.7167,11.9667&z=3D6?=
X-CanItPRO-Stream: cert-sunet-se:default (inherits from sunet-se:default,base:default)
X-Canit-Stats-ID: 0bU5iPy6w - ecf51f58cfcf - 20170904
X-Antispam-Training-Forget: https://mailfilter.sunet.se/canit/b.php?c=f&i=0bU5iPy6w&m=ecf51f58cfcf=cert-sunet-se&t=20170904
X-Antispam-Training-Nonspam: https://mailfilter.sunet.se/canit/b.php?c=n&i=0bU5iPy6w&m=ecf51f58cfcf=cert-sunet-se&t=20170904
X-Antispam-Training-Phish: https://mailfilter.sunet.se/canit/b.php?c=p&i=0bU5iPy6w&m=ecf51f58cfcf=cert-sunet-se&t=20170904
X-Antispam-Training-Spam: https://mailfilter.sunet.se/canit/b.php?c=s&i=0bU5iPy6w&m=ecf51f58cfcf=cert-sunet-se&t=20170904
X-CanIt-Archive-Cluster: PfMRe/vJWMiXwM2YIH5BVExnUnw
Received-SPF: none (e-mailfilter03.sunet.se: domain of ama@chalmers.se
          does not designate permitted sender hosts)
          receiver=e-mailfilter03.sunet.se; client-ip=129.16.226.134;
          envelope-from=<ama@chalmers.se>; helo=e-mailfilter03.sunet.se;
          identity=mailfrom
X-Scanned-By: CanIt (www . roaringpenguin . com) on 192.36.171.203

--4Qe8THRnCNe6xpPlRBLpxuMvTHGJS4jwI
Content-Type: application/pgp-encrypted
Content-Description: PGP/MIME version identification

Version: 1

--4Qe8THRnCNe6xpPlRBLpxuMvTHGJS4jwI
Content-Type: application/octet-stream; name="encrypted.asc"
Content-Description: OpenPGP encrypted message
Content-Disposition: inline; filename="encrypted.asc"
```

Läs Receive-raderna bakifrån – i detta fall 129.16.226.134

I ovanstående e-post finns det tyvärr många uppgifter som **kan** förfalskas.

En referens för den som vill fördjupa sig i tolkandet av full-headers i e-post är:

https://www.howtogeek.com/108205/htg-explains-what-can-you-find-in-an-email-header/

En viktig uppgift som det är vanligt att det förfalskas är ”**From:**” -raden

Och därmed kommer vi in på dagens ämne.

PGP för nybörjare - Pretty Good Privacy

Det finns olika tekniker för att förhöja tilltron till att det är korrekt avsändare som skickat e-post brevet.

De dominerande teknikerna för en användare är:

- Secure/Multipurpose Internet Mail Extensions - S/MIME
- Pretty Good Privacy (PGP)

De stora skillnaden är tillitsmodellen.

S/MIME:s tillit utgår från en Certificate Authority (CA) – i Sunet kan vi använda Digicert som CA för att utfärda personliga certifikat.
Personliga certifikat kan utöver e-post även används vid inloggning t.ex superdatorcenter.

PGP:s tillitsmodell är ”nätverksförtroende” (eng. Web of trust) som innebär att man signerar varandras PGP-nyckel. Signering av en PGP-nyckel innebär att man skall verifiera att kopplingen mellan den elektroniska identiteten och PGP-nyckeln är korrekt. Detta kräver att giltig och relevant identitetshandling har granskats innan man signerar någon annans nyckel.
Signering innebär alltså **inte** att man går i god för individen ifråga.

PGP för nybörjare - Pretty Good Privacy

Både S/MIME och PGP är baserat på asymmetrisk kryptering.

Asymmetrisk kryptering består av en privat och publik nyckel. Den kryptografiska grunden baseras på svårigheten i att faktorisera en STORT tal.

Publiceringen gjordes 1977 av Whitfield Diffie Martin Hellman. Men det hade dock upptäckts tidigare av James Ellis på GCHQ.

Det finns ett flertal olika nycklar i PGP såsom: RSA, RSA-E, RSA-S, ELG-E, DSA.

En av de vanligaste nycklarna är RSA efter upphovsmännen (Rivest-Shamir-Adleman) som även används i SSL/TLS.

Nycklarnas längd är av avgörande betydelse och den idag rekommenderade nyckellängden är 2048 bitar och det beräknas vara tillräckligt fram till 2030. Livslängden baseras på ev. kryptografiska landvinningar och allmän teknisk utveckling.

Råd: Välj standard nyckeltyp och längd.

PGP för nybörjare - Pretty Good Privacy

Asymmetrisk kryptering

En asymmetrisk nyckel består av:

- den privata nyckeln som man skall vara VÄLDIGT rädd om. Om den kommer i orätta händer kan nyckeln anses vara förbrukad

- den publika nyckeln däremot skall man sprida helst via en nyckelserver så att andra lätt kan hitta den

När man skickar ett krypterat brev använder man alltså den privata nyckeln.

När man får ett krypterat brev måste man hämta avsändarens publika nyckel för att dekryptera brevet.

När det är korrekt så innebär det att det i programvaran har gjorts en matematiska operation som är specifik för den aktuella nyckeltypen.

Se på detta som ett lås där det behövs två nycklar för att låsa respektiva låsa upp.

PGP för nybörjare - Pretty Good Privacy

PGP-nyckel – publicering / sökning

När man skapat sin PGP-nyckel skall nyckeln publiceras.
Detta gör man till en nyckel-server – vilken nyckelserver
man använder spelar ingen roll eftersom de synkroniserar.

PGP-servrar är vanligtvis organiserade i sk. pooler såsom

```
hkps.pool.sks-keyservers.net
```

som ger ett flertal ip4/6 adresser och domänen ’sks-keyservers.net’
är konfigurerad med DNSSEC.

Kommandot som används är:

```
gpg –export <primary key ID>
```

Söka efter en PGP-nyckel

```
gpg --keyserver hkps.pool.sks-keyservers.net
          --search-keys arneni@kth.se
```

I detta fall går det lika bra med:

```
gpg --keyserver hkps.pool.sks-keyservers.net
          --search-keys arne.nilsson@cert.sunet.se
```

PGP för nybörjare - Pretty Good Privacy

PGP-nyckel – sökning

```
gpg: searching for "arneni@kth.se" from hkp server
          hkps.pool.sks-keyservers.net

(1)  Arne Nilsson <arne@it.su.se>
     Arne Nilsson <arneni@kth.se>
     Arne Nilsson <arneni@irt.kth.se>
     Arne Nilsson <Arne.Nilsson@it.su.se>
     Arne Nilsson <Arne.Nilsson@its.uu.se>
     Arne Nilsson <Arne.Nilsson@cert.sunet.se>
          1024 bit DSA key B7797437, created: 2002-07-10
```

PGP-nyckelns identiteter
Det finns i denna nyckel ett flertal olika identiteter.

```
gpg --list-keys B7797437
pub   1024D/B7797437 2002-07-10

uid                  Arne Nilsson <arneni@irt.kth.se>
uid                  Arne Nilsson <Arne.Nilsson@its.uu.se>
uid                  Arne Nilsson <Arne.Nilsson@cert.sunet.se>
uid                  Arne Nilsson <arne@it.su.se>
uid                  Arne Nilsson <Arne.Nilsson@it.su.se>
uid                  Arne Nilsson <arneni@kth.se>
sub   2048g/387C7D31 2002-07-10
```

Man kan även ha en PGP-nyckel för en funktionsadress t.ex IRT@<hsk>.se

Vid förändringar i funktionsadressens medlemmar kan det vara lämpligt att byta lösenordet. Detta görs med:

```
gpg –edit-key YOURMASTERKEYID passwd
```

Granskning av en PGP-nyckel – vilka signeringar finns det?

Det ger i detta fall en alltför lång lista men några exempel:

```
.
.
.
sig 3       3FB4CCDC 2004-11-03 Torbjorn Wictorin <Torbjorn.Wictorin@its.uu.se>
sig         66D4FEF8 2004-11-04 Patrik Lidehaell <patrik@kth.se>
sig 2       23C956F0 2005-01-03 Enok Söderberg Hanssen <enok@gsix.se>
sig 3       1B3600A9 2004-10-20 Erik Stenvall (AppGate Network Security AB)
            <ess@appgate.com>
sig 3       95047280 2004-11-04 Nenad Cuturic <cnesko@gmail.com>
sig 3       C639B4A5 2004-11-04 Bjorn Mattsson <Bjorn.Mattsson@bth.se>
sig 3       D553F437 2005-01-25 Stefan Andersson (Chalmers IT And Systems
                  Services) <ander@ita.chalmers.se>
sig         C6AB732E 2005-11-01 Ludvig Omholt <ludde@ludde.net>
sig 3       7FD6111E 2005-11-01 David Hansson <David.Hansson@it.su.se>
sig         1E05F3B5 2008-05-09 Thomas Grenman <Thomas.Grenman@ficora.fi>
sig 3       74AD2205 2008-04-28 Kristians Melins <kristians.melins@cert.lv>
sig         D908321F 2008-05-24 Schreck, Thomas; Z001ZXFY Siemens
                  <t.schreck@siemens.com>
sig         14CA9661 2008-05-01 Andrew Cormack - signing only
                  <Andrew.Cormack@ja.net>
sig         BCDB5521 2008-08-19 Thomas Stridh (Uppsala University, Sweden)
                  <thomas.stridh@its.uu.se>
.
.
.
```

När man signerar kan man göra en rankning med värdena 0 – 3.

Värdet ”3” innebär ”extensive verification”. Vad ”extensive” betyder är upp till den som signerar att bestämma.

PGP-nyckel och dess sub-nycklar

Till en PGP-nyckel kan man knyta sub-nycklar så som i ovanstående exempel där alltså sub-nyckeln är:

```
sub   2048g/387C7D31 2002-07-10
```

Det innebär i detta fall att huvudnyckeln används för att signera e-post och sub-nyckeln används för att kryptera e-post.

En sub-nyckel kan revokeras oberoende av huvudnyckeln och även lagras separat från huvudnyckeln.

Sammanfattningsvis kan man alltså säga att en sub-nyckel är som ett separat nyckel-par som är automatiskt knutet till huvudnyckeln.

PGP-nyckelns giltighetstid

När du skapar en PGP-nyckel sätt en giltighetstid

När du skapat en PGP-nyckel skall du passa på att samtidigt skapa ett revokeringscertifikat

Om du glömmer bort det kan du dock göra det i efterhand förutsatt att du har tillgång till nyckeln och kommer ihåg lösenordet/frasen.

Detta finns beskrivet på länken:

http://www.pgp.net/pgpnet/pgp-faq/pgp-faq-key-revocation.html

Några avslutande ord:

- När PGP-nyckeln skapas sätt ett bra lösenord / lösenordsfras
- Signera din egen nyckel
- Ange en giltighetstid – den kan uppdateras i efterhand
- Uppdatera regelbundet din PGP-nyckelring så uppdateringar finns på din maskin
- Kryptera gärna med din PGP-nyckel viktiga filer som du har på din dator, t.ex

```
gpg –encrypt filename
```

  eller skapa en separat PGP-nyckel för detta ändamål

- Skickar du ett krypterat brev med en bilaga se till att även bilagan i så fall blir krypterad
- Ta för vana att signera e-post du skickar