Smarta kort i Linux

Hur svårt kan det vara?

The magic code

```
if (exponent[0] & 0x80){
  SAFEALIGN_SET_UINT32(&buf[c], htobe32(exponent_len+1), &c);
  SAFEALIGN_SETMEM_VALUE(&buf[c], '\0', unsigned char, &c);
} else {
  SAFEALIGN_SET_UINT32(&buf[c], htobe32(exponent_len), &c);
}
```

Och några hundra rader testkod för att verifiera…….

Varför du inte ska använda lösenord

Är ditt lösenord slumpmässigt?

Minst 25 tecken

Aldrig återanvänt

Datorn aldrig obevakad.

Alltid låst.

Fjärrstyrs din dator?

Om du aldrig gör misstag, är dina kollegor lika felfria?

Flerfaktor

App

Usbdongel(typ ybikey, många olika varianter)

Rsatoken

Otp

Bankdosa

Smart card

A smart card is **a physical card that has an embedded integrated chip that acts as a security token**.


mascot
battery eliminator
Type 8511
Out: 12V DC
KORTTERMINAL
COMEX 9080
F1
F2
F3
F4
CLR
OK
För att radera signalskyddsnycklar - Tryck F1
SECTRA

IDP(Molnet)

Azure

Google

Jumpcloud

Okta

Onelogin

Duo(inte svt:s app)

Svenska leverantörer?

Spårbarhet

Vilka tjänster kan användas med certifikat på kort?

Webben, använd IDP, bygg ALDRIG något själv och kör bara chrome!

Windows, växlas till en kerberosbiljett.

Linux kerberos authentication indicators.

Feta klienter.

Generisk TLS, men vilka klienter och vilka TLSversioner?

Signering, epost.

ssh?

SSH!

Busenkelt, jag har hört att ssh har stöd för certifikat…..

Använd bara openssh med PKCS#11 stöd, även på windows 10(20H1).

Exotiska kortleverantörer kräver exotiska drivrutiner.

Department of Defense

Extrahera publika nyckeln ur kortet.

Hur kör man då ssh med certifikat när ssh bara kan privat/publik nyckel?

ssh->sshd->sssd(och lite PAM)

- ssh->sshd “Jag är kalle, ge mig en publik sshnyckel”
- sshd triggar /usr/sbin/sss_sshd_authorizedkeys
- sssd hämtar en kopia av ditt certifikat från katalogtjänst, verifierar och bygger en publik sshnyckel från certifikatet. Precis som .ssh/authorized_keys hade gjort.
- Användaren knappar in pinkoden för kortet, det känns verkligen som en “äkta certifkatautentisering” för användaren.
- Autentisering klar, välkommen kalle.

What could possibly go wrong?

What could possibly go wrong?

Var är min kerberosbiljett?

Vart är mitt kort för att hämta en kerberosbiljett?

exponenten(e) ska vara ett primtal 3 eller större, 65537 kanske?
Tror du en kryptolog utformar testfallen?

p11-kit kan tunnla pkcs#11 via socket över ssh, komplicerat.

VDI(vmware, citrix) kräver pcsd och kompilering mot okända binärblobbar.

Får du någon inloggning alls?

ssh-agenten!

Det enda vi kan lita på i en okänd miljö.

Vi kan hoppa vidare så länge ssh-konf tillåter.

Pam via pam_ssh_agent_auth ger oss sudo.

Vi behöver aldrig några lösenord för sudo längre och inga lokala konton!!

Inga lokala konton längre!

Alla problem är lösta, eller?

Ssh-agenten, inte alltid svaret

Allt som kör ssh är inte openssh och sssd

Paramiko(python, ansible)

net-ssh(ruby, puppet-bolt)

jenkins

Git och andra ssh-servrar hanterar de publika nycklarna själv.

Openssh8.8 kan nu hantera giltighetstid på sshnyckeln och ersätter pgp för signering i git.

Virtuella miljöer, kan man kan dela på kortet?

windows+openssh+pkcs#11

Wsl 2/Hyperv

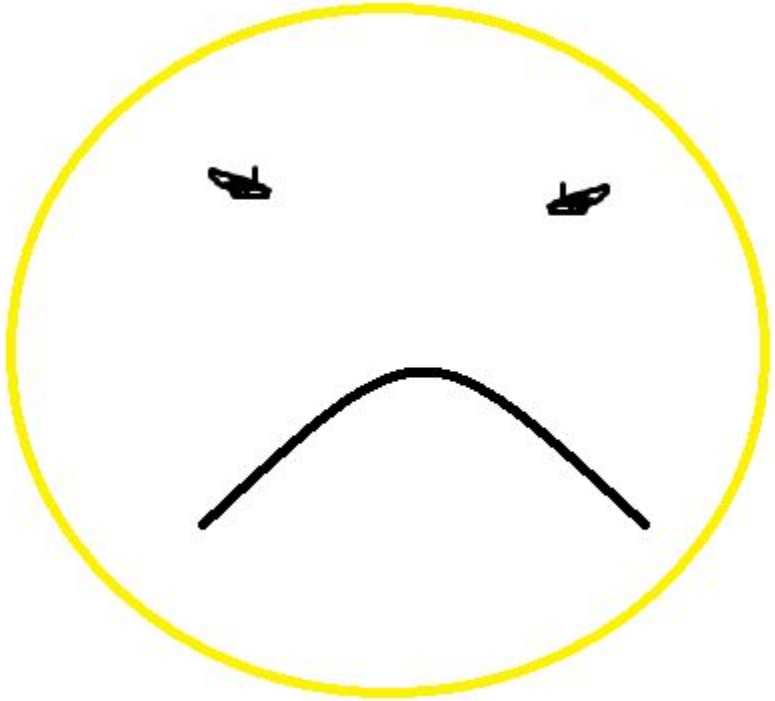
Vmware workstation

Virtualbox

Kvm(linux på linux)

Vdi(citrix/vmware horizon)

macosx?



Gör som de stor grabbarna, använd ssh-certifikat!

Eftersom opensshutvecklarna är purister går x509 bort.

Förenklade certifikat med bara de nödvändiga tilläggen.

Ingen ~/.ssh/authorized_keys att kopiera runt här heller :-)

Din CA/PKI leverantör stödjer väl ssh-certifikat?

Och låter dig signera din publika nyckel genom SSO i webläsaren?

Ssh-keygen har haft stöd i tio år.

Sudo via ssh-agenten(pam-ussh)….

Valet är ditt

Säkerhet

Enkelhet

Stabilitet

Spaning(webauthN/OTP)

Leverantörsberoenden(hur många leverantörer har din teknikstack)

Nss+openssl+gnutls+?

målgrupp

The magic code

```
if (exponent[0] & 0x80){
  SAFEALIGN_SET_UINT32(&buf[c], htobe32(exponent_len+1), &c);
  SAFEALIGN_SETMEM_VALUE(&buf[c], '\0', unsigned char, &c);
} else {
  SAFEALIGN_SET_UINT32(&buf[c], htobe32(exponent_len), &c);
}
```

Och några hundra rader testkod för att verifiera…….

Svåra val om du kör smarta kort:

Nycklar: RSA eller ECC ?

Signeringsalgoritmer: SHA* eller RSASSA-*

Kända problem i historien.

TLS-versioner

Generera nyckel på kort, dator eller annan pkilösning.

Mer info på utsidan av kortet?(porträtt?)

Utskrifter, passersystem, parkering, personalmatsalen eller vad?

Frågor?

peptekmail@gmail.com