Richard Komžík
20070515

Trojhlavý pes a iní démoni

IT bezpečnosť na AsÚ SAV

NETnews

DÔVODY, CIELE

- konsolidácia
- rastúci počet užívateľov, počítačov
- príliš veľa kônt, hesiel - **Kerberos**
- príliš veľa rozdrobeného diskového priestoru - **LDAP**
- zjednodušenie administrácie účtov
- bezpečnosť

ZÁKLADNÉ POJMY

- **AAA**
- **autentifikácia - Authentication** - preukázanie, že som ten, za koho sa vyhlasujem
  - čo som - odtlačok prsta, dúhovka, DNA - xerox odtlačku
  - čo mám - HW kľúč - odcudzenie
  - čo viem - heslo - kompromitácia, slovníkový útok
- **autorizácia - Authorization**- preukázanie, že mám oprávnenie vykonávať nejakú činnosť, používať určitú službu
- **účty - Accounting**

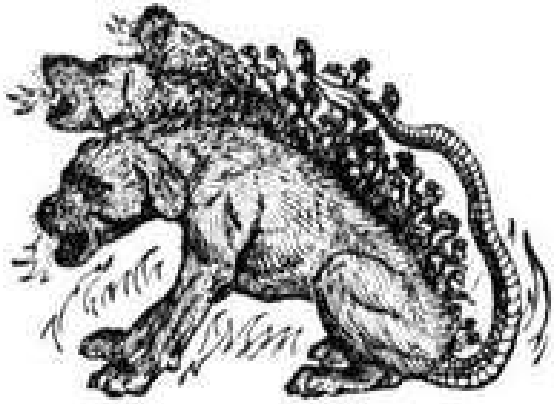
- **šifrovanie**
  - **symetrické**
    - jeden kľúč pre zašifrovanie aj rozšifrovanie
    - problém prenosu kľúča v nedôveryhodnom prostredí
  - **asymetrické**
    - verejný a tajný kľúč
    - fungujú iba v páre: šifruje sa verejným, dešifruje tajným a vice versa
    - hashovacia suma: charakterizuje vstup, jednocestnosť
    - problémy:
      - výpočtovo náročnejšie
      - dôveryhodnosť verejného kľúča – certifikačná autorita
      - kompromitácia MD5, SHA1
  - využitie: šifrovanie, elektronické podpisovanie

Trojhlavý pes a iní démoni

http://en.wikipedia.org/wiki/Cerberus

Κέρβερος

Kerberos

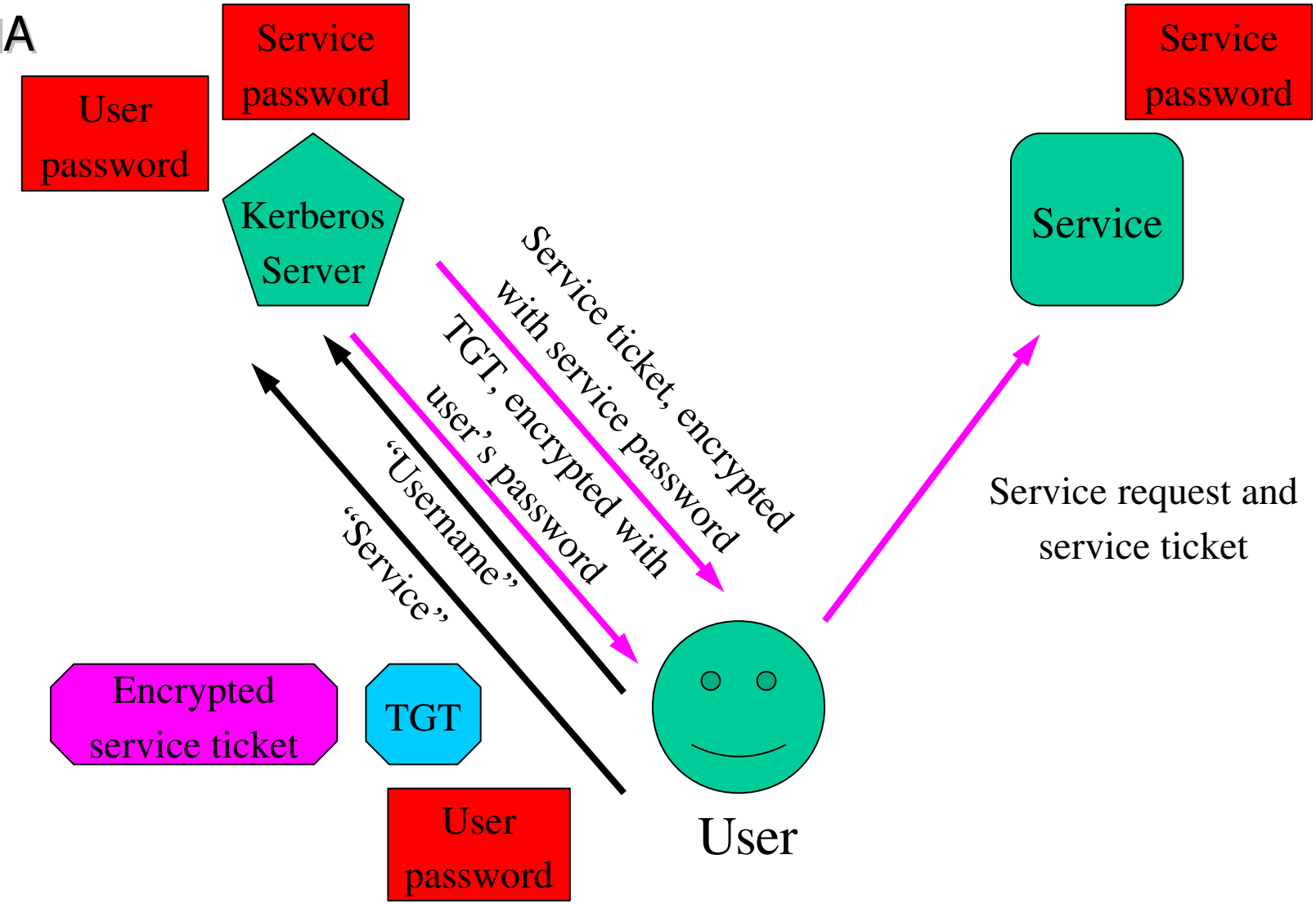


Cerberus

KERBEROS

- autentifikačný protokol (staršie spôsoby NIS/Yellow Pages, NIS+)
- viacero verzií: Heimdal, MIT v.5
- ukladá, spravuje login/password
- symetrické šifrovanie
- dôveryhodná tretia strana/inštancia
- principals pre užívateľov, služby
- vydáva časovo obmedzené lístky: tickets/credentials
- cieľ: 'single-sign-on' system

SCHÉMA


Service password
User password
Kerberos Server
Service password
Service
Service ticket, encrypted with service password
TGT, encrypted with user's password
"Username"
"Service"
Service request and service ticket
Encrypted service ticket
TGT
User password
User

PROBLÉMY/UPOZORNENIA

- nie všetky služby podporujú Kerberos
- potreba dobrej synchronizácie času - NTP
- závislosť na kerberos-servri, ideálne: replikovaný, dedikovaný
- prihlásiť sa môže len ten, kto má platný lokálny účet
- nepoužívať kerberos pre root-a

VÝHODY

- jedno prihlásenie na 8 hodín: ssh, scp, www/w3, ftp, telnet
- heslá nie sú po sieti vôbec prenášané

POUŽITIE

- zadať na kerberos-servri principal pre užívateľa a jeho počítač
- nakonfigurovať počítač užívateľa
  - REALM: TA3.SK
  - kerberos server: auriga.ta3.sk = kerberos.ta3.sk, kerberos2.ta3.sk
  - DNS
- kinit; klist; kpasswd; kdestroy

WINDOWS

- nainštalovať ksetup.exe z \support\tools\support.cab - teda inštalačné CD: \support\tools\setup - zaškrtnúť *complete*
  - *ksetup /setrealm TA3.SK*
  - *ksetup /addkdc TA3.SK kerberos.ta3.sk*
  - *ksetup /addkdc TA3.SK kerberos2.ta3.sk*
  - *ksetup /mapuser * **
- konfigurácia kerberos je uložená v *HKEY_LOCAL_MACHINE\SYSTEM\CurrentControlSet\Control\Lsa\Kerberos*
- M$ si vybral Kerberos ako autentifikačný protokol

LINUX

- /etc/krb5.conf
- /etc/pam.d/system-auth
- *authconfig --enablekrb5 --krb5kdc=kerberos.ta3.sk *
  *--krb5adminserver=kerberos.ta3.sk --krb5realm=TA3.SK *
  --enablekrb5kdcdns --enablekrb5realmdns --update
- kľúč: */etc/krb5.keytab*
- ssh, scp
  - /etc/ssh/sshd_config
    - *KerberosAuthentication yes*
    - *KerberosOrLocalPasswd yes*
    - *GSSAPIAuthentication yes*
  - /etc/ssh/ssh_config
    - *GSSAPIAuthentication yes*

LDAP

- Lightweight Directory Access Protocol, X500
- adresárová služba – menšie súbory, prevažne čítanie
- do adresára sa dajú uložiť rôzne potrebné informácie
- autorizácia – kto smie využívať aké služby
- cieľ: vytvoriť jednotný priestor (diskový priestor, najrôznejšie informácie) pre všetkých užívateľov, nezávisle na ich OS
- výhody: centralizovaná správa, zálohovanie

DROBNOSTI

- programovanie v shelli
  - *for i in `ls *.FITS`; do k=`echo $i | tr A-Z a-z` ; echo $i $k; convert -geometry 30% $i $k ; done*
  - wildcards = žolíkové znaky, regulárne výrazy:
    *ls -l [c-o,x]*1?.fits*
- grafické knižnice pre FORTRAN
  - pgplot http:ww.astro.caltech.edu/~tjp/pgplot/
  - pilib http://sourceforge.net/projects/pilib/
  - dislin http://www.dislin.de

OTÁZKY

- greylisting - antiSPAM nástroj
  - zdržiava, väčšia záťaž pre server

INCIATÍVY

- SANET – pre diakritiku používať UTF-8

VoIP

- natívne IP telefóny v Bratislave, Lomnickom štíte
- Úrad SAV na VoIP/SIP
  - http://www.urad.sav.sk/files/phone_zoznam_new.htm
  - 02/57510???
  - http://auriga.ta3.sk/VoIP/check_enum.php

HARDWARE

- Komisia P SAV pre informačné a komunikačné technológie
- účelovo prideľované prostriedky areálom
- posledné 3 roky po 200 000.-Sk
- VoIP
- obnova servrov, rack chassis
- gemini – NTP server
- indus – log server
- auriga (80 000.-Sk na konci roku 2006)
- racky
- klimatizácia

HARDWARE - BEŽNÉ

- IP telefóny Bratislava
- sieťová laserová tlačiareň na spodnú chodbu
- HUBy vs. switche
- 11 Mbps rádio na Lomnický štít
- optika na Lomnickom štíte

HARDWARE - POTREBNÉ

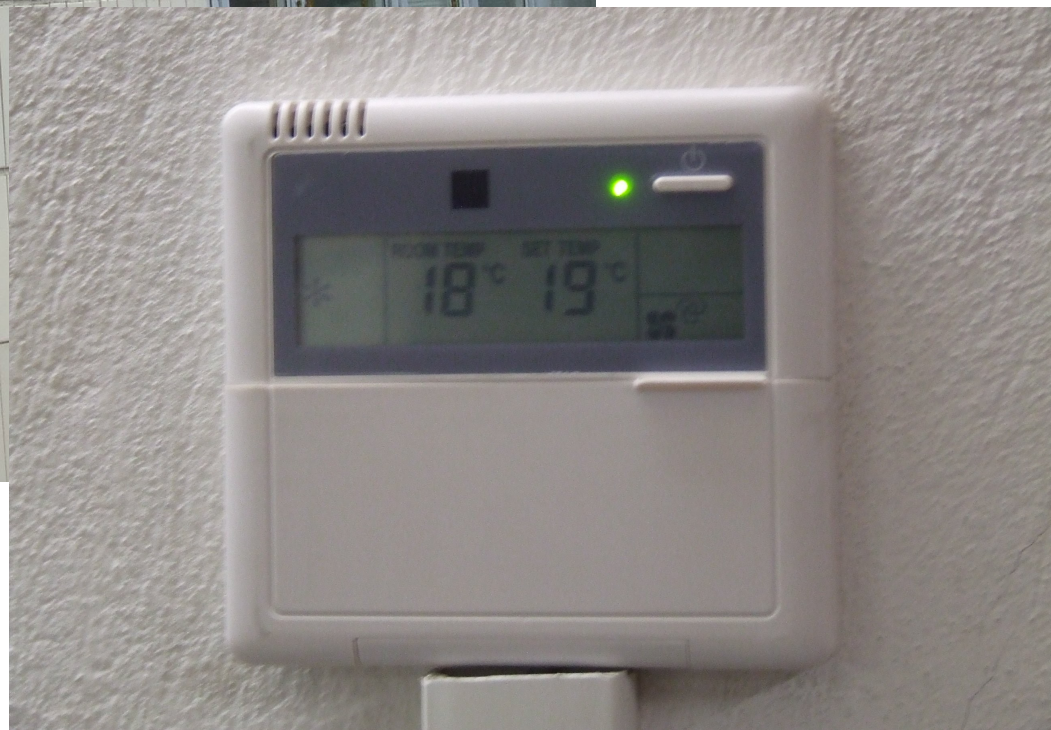
- natívne IP telefóny – paušál ST
- cygnus – WWW

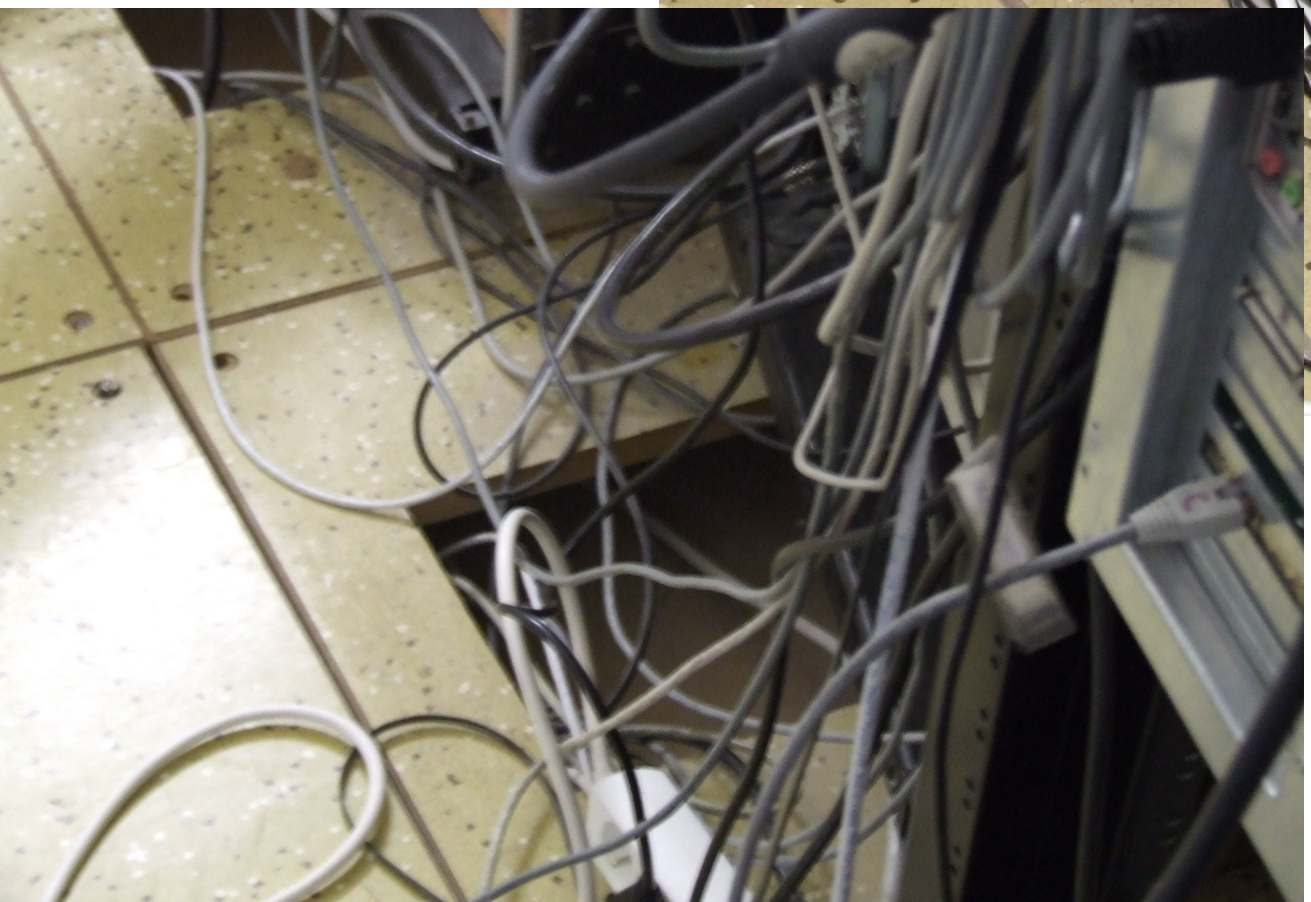

Mercury
Orbis
Nowy Targ

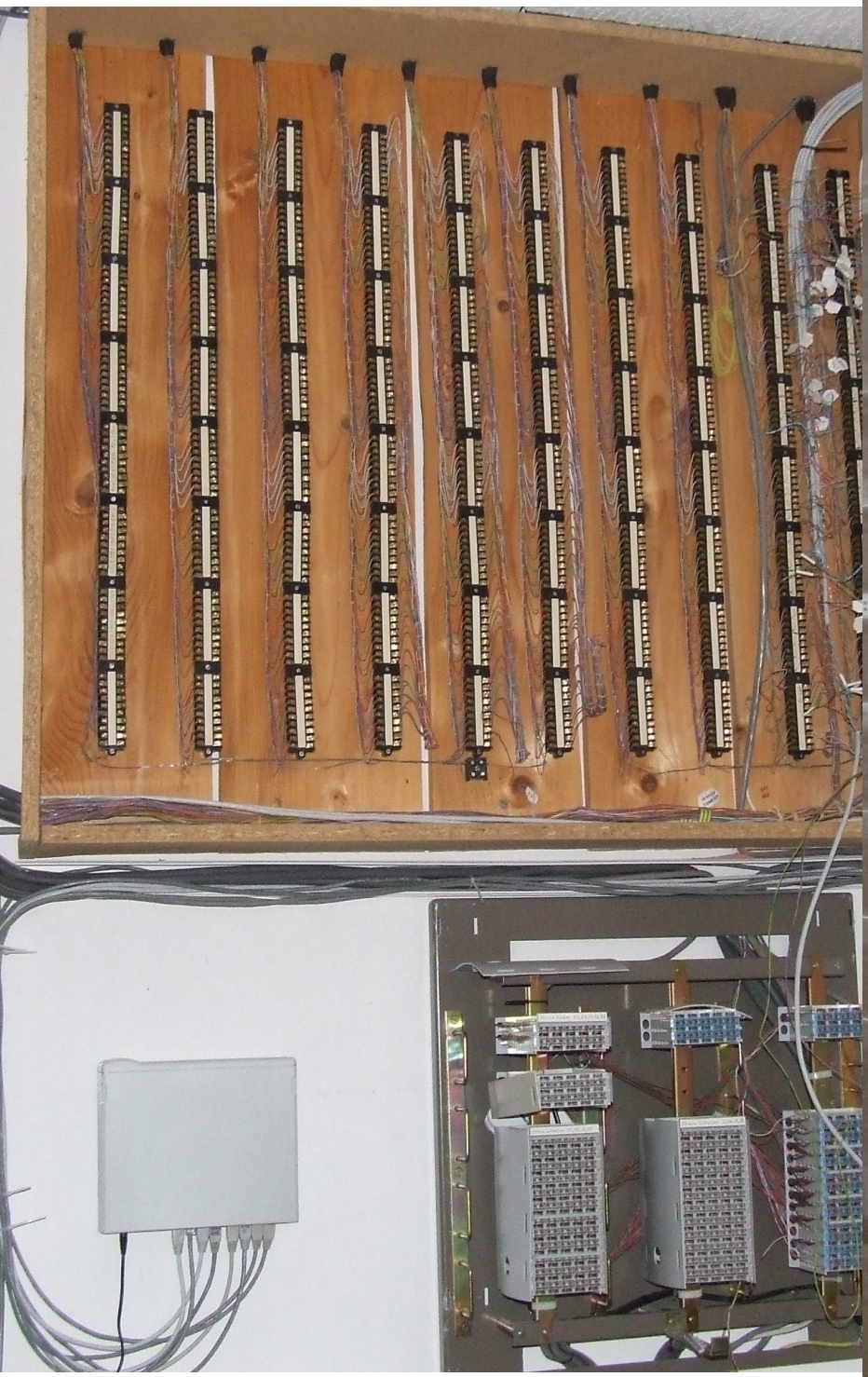

DVD
disc
ID


ROUTER

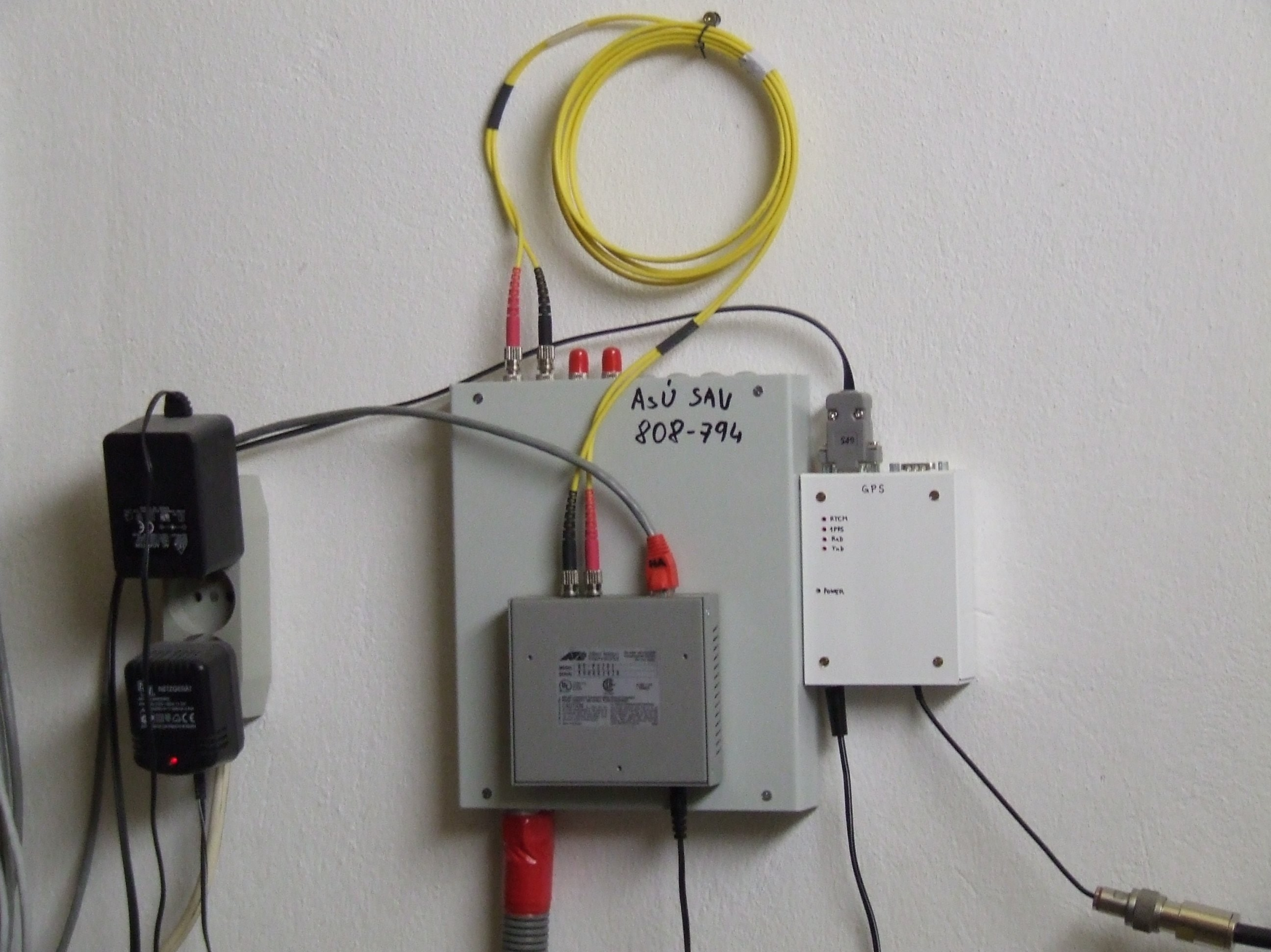

Fujiko
AIR CONDITIONERS


18°C
19°C






Oertel
VoIP Gateway
3com


AsÚ SAV
808-794
GPS
RTCM
1PPS
RxD
TxD
Power

ĎAKUJEM ZA POZORNOSŤ