Alberto Cammozzo
tel. +39-49-8274175
mmzz@stat.unipd.it

16 Dicembre 1999

# Sicurezza del PABX Alcatel 4400 nella rete dati del Dipartimento

L'installazione della nuova rete di fonia di Ateneo, in corso di realizzazione, prevede l'utilizzo della rete dati per trasmettere alcuni segnali al fine di conseguire risparmi economici (cfr. lettera CCA 13 dic 99).

In quanto amministratore e responsabile della rete dati ho verificato la rispondenza del nuovo apparecchio ai necessari requisiti di sicurezza informatica.

Purtoppo il nuovo centralino (PABX) Alcatel 4400 (che è un vero e proprio computer Unix) connesso alla rete del Dipartimento non risponde a nessun requisito di sicurezza informatica, tanto che è bastata una mezz'ora di tempo per aggirare i suoi sistemi di sicurezza e guadagnarne l'accesso. Le conseguenze di questa vulnerabilità possono andare dall'interruzione dei servizi telefonici alla manomissione degli archivi contenenti le registrazioni delle telefonate effettuate.

L'evidenza indica che sono soggetti alla medesima vulnerabilità anche altri centralini installalti in Ateneo (S.Canziano, Ognissanti, Bò).

## 1 Profilo in rete: servizi aperti

La scansione dei servizi aperti indica diverse porte aperte, alcune facilmente identificabili (`telnet`, `ftp`) altre probabilmente collegate a programmi che girano sul PABX.

| Port | State | Protocol | Service |
|---|---|---|---|
| 21 | open | tcp | ftp |
| 23 | open | tcp | telnet |
| 513 | open | tcp | login |
| 514 | open | tcp | shell |
| 2533 | open | tcp | unknown |
| 2535 | open | tcp | unknown |
| 2536 | open | tcp | unknown |
| 2539 | open | tcp | unknown |
| 2540 | open | tcp | unknown |
| 2545 | open | tcp | unknown |
| 2554 | open | tcp | unknown |
| 2555 | open | tcp | unknown |
| 2560 | open | tcp | unknown |

```
520     open        udp       route
2556    open        udp       unknown
9743    open        udp       unknown
```

I servizi `telnet` e `ftp` permettono il collegamento remoto e il trasferimento di *file* remoto, rispettivamente. Le porte `login` e `shell` sono analoghe a quella `telnet`, con alcune aggravanti, come risulterà dall'analisi della configurazione della macchina. Il servizio `udp route` permette la trasmissione di informazioni riguardanti l'instradamento del traffico dati. Gli altri servizi rispondono ad un collegamento diretto, ma le funzionalità dei servizi collegati sono ignote da un'analisi di rete; risulteranno chiare solo dopo un'analisi della configurazione del sistema..

Nessuno di questi servizi dovrebbe essere "visibile" da Internet: `telnet` e `ftp` permettono il tentativo sistematico di intrusione con attacchi di tipo "brute force" per indovinare le combinazione *login/password* , `route` può consentire il sovvertimento delle tabelle di instradamento, e le altre porte possono essere soggette ad attacchi di tipo *buffer overflow* e denial of service pur rimanendo ignota la loro funzione.

## 2 Login banali

La consultazione del manuale dell'apparecchiatura ha reso superfluo il tentativo *brute force* sulla porta `telnet`: vi sono indicate una serie di *login* oltre a quella di `root`: `swinst`, `mtch`, `mtcl`, `client`. La *login* `client` ha password nulla, mentre `mtch` e `mtcl` hanno *password* uguale alla *login*.

I profili corrispondenti a `swinst`, `mtch`, `mtcl` consentono interventi sui dati, sulla configurazione del PABX e l'installazione di *software*.

## 3 Analisi della configurazione

All'interno del PABX, il file `/etc/hosts.equiv` contiene il carattere "+", consentendo l'accesso *senza autenticazione* a chi si presenti con un nome di *login* valido.

L'analisi dei file di inizializzazione dei servizi di rete ha permesso l'identificazione dei servizi collegati alle porte aperte e non note al momento dell'analisi del profilo di rete:

```
#
# Alcatel 4400 proprietary services.
# To add a new service, please contact 4400 infrastructure team.
#
netaccess       2533/tcp                        # CMISD/ABCA network access
pad             2534/tcp                        # PAD X.25
cmisd           2535/tcp                        # CMISD serveur
saverest        2536/tcp                        # Save/restore appli

acd             2538/tcp                        # ACD v2
builddistant    2539/tcp                        # Audit : Build-distant
```

```
loaddistant     2540/tcp                        # Audit : Load-distant
auditres1       2541/tcp                        # Audit : reserved
auditres2       2542/tcp                        # Audit : reserved
acdccs          2543/tcp                        # ACD terminal server
acdpcag         2544/tcp                        # ACD PC agent
suprout         2545/tcp                        # Suproutage
alb             2546/tcp                        # ACD Agent List Builder

rtest           2554/tcp
rcsta           2555/tcp                        # ASN-1 DHS3 CSTA acces server
hybrid-vpn      2556/udp                        # Hybrid VPN over UDP
notif-gsm       2557/udp                        # GSM notification server
redundancy      2558/tcp                        # CPU redundancy on ethernet
rsl             2559/udp                        # RSL socket port
rlis            2560/tcp                        # LIS server
ahltcp          2561/tcp                        # AHL on ethernet

securid         5500/udp                        # ACE/server
securidprop     5510/tcp                        # ACE/server
sdlog           5520/tcp                        # ACE/server
sdserv          5530/tcp                        # ACE/server
```

# 4 Analisi delle *password*

Il file di *password* contiene altri utenti con password banali. L'analisi completa (*cracking*) delle *password* è ancora in corso ma sono già state evidenziate le seguenti coppie:

```
adfexc [adfexc]
kermit [kermit]
mtch [mtch]
mtcl [mtcl]
ppp [ppp]
halt [tlah]
install [llatsni]
```

# 5 Conclusioni

L'attuale profilo di sicurezza della macchina è minimo: chiunque con una conoscenza anche approssimativa del sistema è in grado di tentare l'intrusione attraverso i servizi `telnet`, `ftp`, `login`, `shell`. Identificare le *login* è questione di tempo e determinazione, anche senza avere a disposizione il manuale; inoltre non vi è nessun bisogno di indovinare le *password*, grazie al "+" nel file `/etc/hosts.equiv`.

A titolo di esempio, per *spegnere* il centralino dovrebbe essere sufficente da una qualsiasi macchina unix/linux *in tutto Internet* digitare il comando "`rlogin PABX`" come utente "`halt`".

Un utente più malizioso potrebbe cancellare e alterare dati, e con le necessarie conoscenze sovvertire le comunicazioni telefoniche o generarle artatamente.