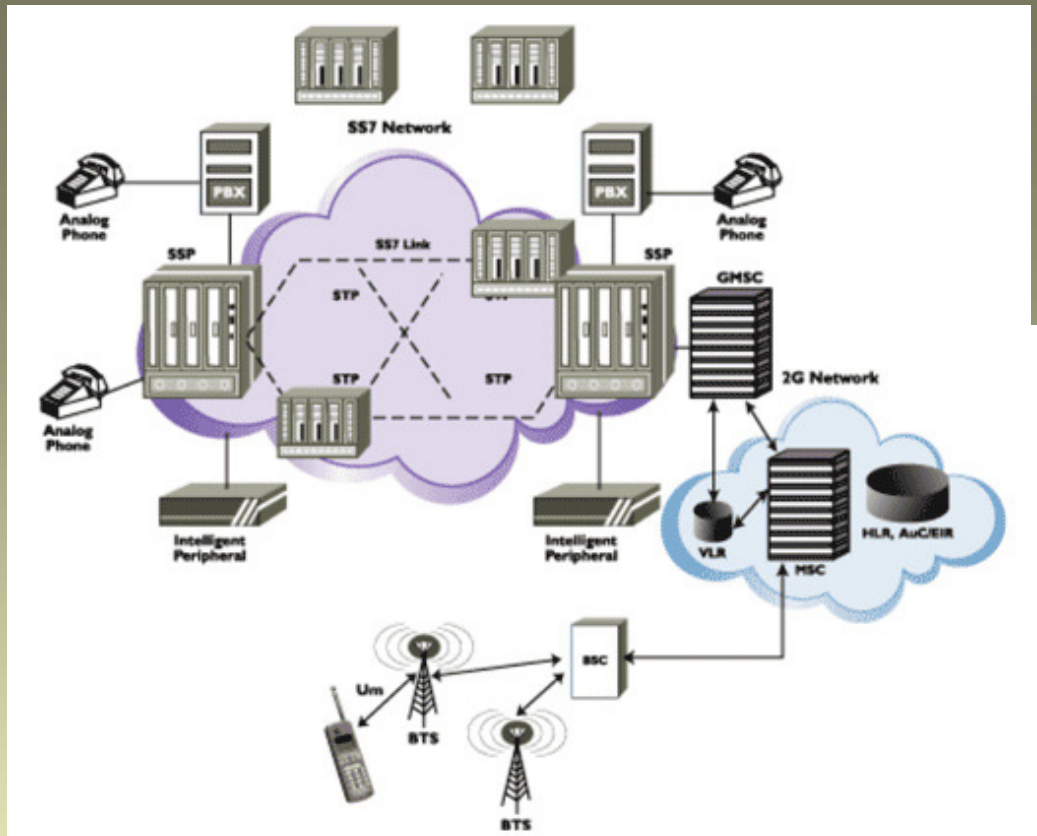


Sistemul de semnalizare SS7

Petre Ogruțan, ianuarie 2015

Protocoale în telecomunicații

În telecomunicații un protocol este un ansamblu de reguli dedicat schimbului de date între sisteme de calcul.

Un protocol defineşte sintaxa, semantica şi sincronizarea comunicației de date digitale cu scopul ca un mesaj trimis să fie interpretat corect şi să genereze un răspuns corespunzător. Un protocol trebuie să asigure un comportament specific, indiferent de modul de implementare. Protocolul poate fi implementat hardware, software sau mixt, este descris în standarde şi trebuie să fie agreat de producătorii echipamentelor de comunicații.

Sinteza caracteristicilor şi funcţiile principale a protocoalelor pentru comunicaţii

1. Transmisia este serială sincronă cu şiruri de biţi (bitstring) sau altfel spus cu blocuri de date (pachete). Şirul de biţi al unui mesaj este împărţit în câmpuri şi fiecare câmp conţine informaţii relevante în cadrul protocolului. Şirul de biţi este format din două părţi, una care conţine antetul (header) şi una care conţine datele. Informaţii mai importante legate de protocol se află în antet. Şirurile de biţi mai lungi decât MTU (Maximum Transmission Unit) sunt divizate.
2. Mesajul este precedat de un anumit număr de tranziţii generate de transmiţător care permit buclei PLL de la receptor să se sincronizeze, transmisiile moderne asigurând refacerea tactului de recepţie din datele transmise.
3. Antetul conţine adresa expeditorului şi adresa destinatarului. Adresa permite localizarea receptorului şi este analizată de receptor care ignoră sau procesează mesajul. Conexiunea între un transmiţător şi un receptor este caracterizată de perechea de adrese corespunzătoare. Unele adrese sunt speciale, de exemplu cea care permite adresarea tuturor receptorilor (adresa de broadcasting). Regulile care descriu adresarea formează schema de adresare.

Sinteza caracteristicilor şi funcţiile principale a protocoalelor pentru comunicaţii

4. Uneori protocoalele solicită realizarea corespondenței între adrese din scheme de adresare diferite, (maparea adreselor). Un exemplu este realizarea corespondenței între adresa IP şi adresa MAC la transmisia Ethernet.
5. Dacă sistemele de calcul nu sunt conectate direct se inserează dispozitive care retransmit mesajul. Un exemplu la rețeaua Ethernet este router-ul.
6. Verificarea corectitudinii mesajului transmis se face adăugând la sfârşitul mesajului o informaţie redundantă. În funcție de algoritmul utilizat se poate asigura detectarea şi eventual corectarea unui anumit număr de erori.
7. La anumite protocoale este nevoie de confirmarea recepționării mesajului. Receptorul transmite un mesaj de confirmare cu o anumită structură către transmițător. Strategia în cazul deconectării temporare sau definitive a transmițătorului de receptor este necesară dacă nu este primită confirmarea recepției. De regulă mesajul este retransmis de mai multe ori, o condiție de eroare fiind setată dacă nu se primeşte confirmarea recepției după un anumit număr de încercări.

Sinteza caracteristicilor şi funcţiile principale a protocoalelor pentru comunicaţii

8. Gestionarea coliziunilor este necesară în cazul în care două sisteme de calcul încep transmisia în acelaşi timp. Gestionarea sensului transferului este necesară pe liniile half duplex. Aceste sarcini sunt rezolvate de un modul Media Access Control conform unei strategii corespunzătoare protocolului utilizat.
9. Sincronizarea vitezei de transfer este necesară când transmiţătorul (sau dispozitivul de retransmisie) transmite mai repede decât poate recepţiona receptorul. Sincronizarea se realizează cu mesaje transmise de receptor către transmiţător.
10. Stiva de protocoale OSI (Open Systems Interconnection) arată organizarea pe nivele ierarhice a protocoalelor de comunicaţii şi conţine nivelele: fizic, legături de date, reţea, transport, sesiune, prezentare şi aplicaţie.

Sistemul de semnalizare SS7

SS7 (Sistemul de semnalizare 7) este un set de protocoale de telefonie dezvoltate pentru prima dată în 1975 pentru rețelele PSTN (Public Switched Telephone Network). Acest set de protocoale este definit de standardul ITU-T Q700 (1988) şi stabileşte printre altele modul de programare, portabilitatea numerelor, facturare, gestionarea numerelor gratuite şi cu suprataxă, servicii SMS (Short Message Service) etc.

Termenul de semnalizare folosit în telefonie se referă la transmisia semnalelor de control asociate unei comunicaţii telefonice. La început semnalizarea era asociată circuitului care realizează convorbirea telefonică (PBX, Private Branch eXchange) cu denumirea Channel Associated Signaling. SS7 este o semnalizare separată şi distinctă față de canalul / circuitul care realizează convorbirea telefonică (Common Channel Signaling).

Setul de protocoale SS7 asigură prin comunicaţia serială sincronă cu blocuri de date un debit important de date, configurând funcţii ca apel în aşteptare, redirecţionare apel, identificare şi afişare număr apel, conferință, căsuță vocală, etc.

Mesajele SS7 utilizează canale de date bidirecţionale dedicate de 56kbps, 64kbps, 2048kbps. Avantajele utilizării canalelor dedicate sunt mărirea vitezei de formare a numărului față de sistemul MF (Multi-Frequency), eficiența mărită a canalelor de voce, posibilitatea de utilizare a serviciilor IN (Intelligent Network) fără canale de voce, îmbunătățirea controlului antifraudă.

Punctele SS7

Fiecare punct din rețeaua SS7 care poate folosi protocolul se numeşte punct de semnalizare şi are ataşat un cod (adresă). Sunt trei tipuri de puncte de semnalizare:

1. **SSP Service Switching Point**
2. **STP Signal Transfer Point**
3. **SCP Service Control Point**

Punctele SSP inițiază, gestionează şi închid o legătură de voce. Un punct SSP poate trimite un mesaj de interogare către un punct SCP (o bază de date) pentru a primi date de rutare. Un punct STP este un comutator care rutează un mesaj în funcție de datele din mesaj.

Conexiunile între punctele de semnalizare

A, conexiunea între două puncte SSP (sau un SSP la un SCP) prin intermediul comutatorului STP, mesajele circulă doar între expeditor şi destinatar;

B, conexiunea între două puncte de comutare STP, de exemplu din două rețele diferite;

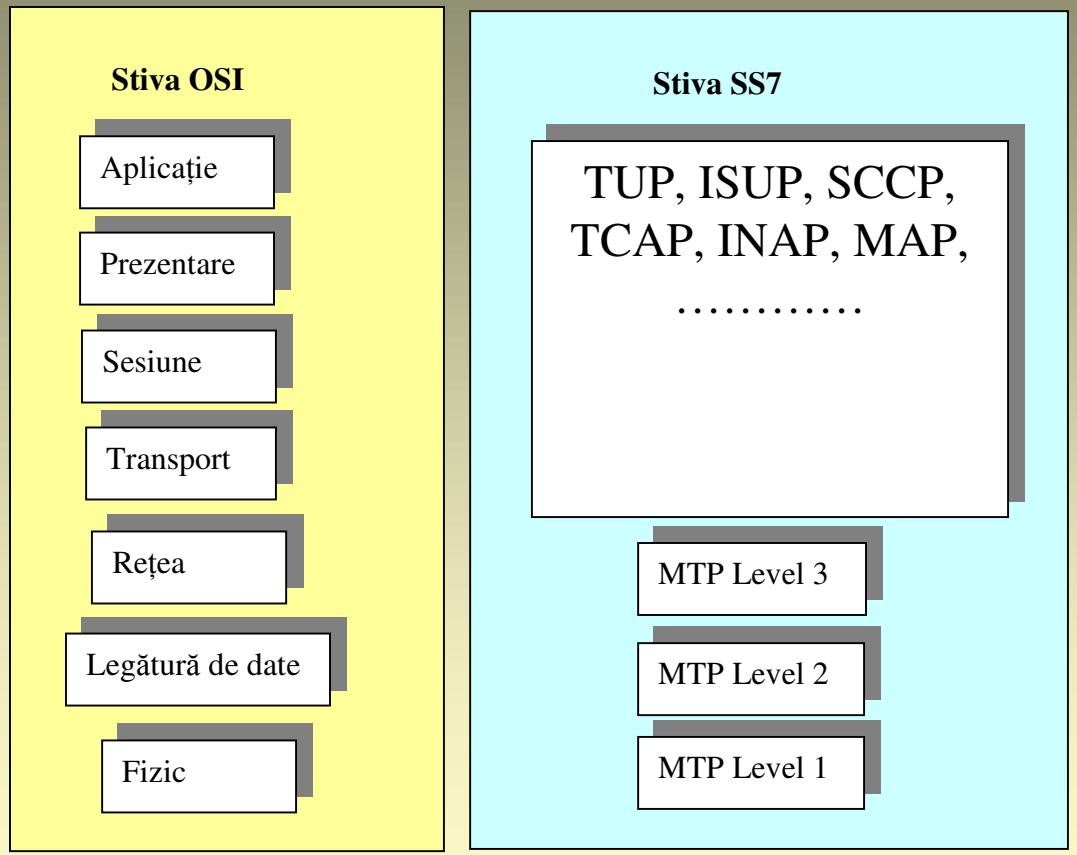
C, conexiunea între două puncte de comutare STP cu aceeaşi funcție pentru mărirea fiabilității;

D, conexiunea între două puncte de comutare STP dintr-o rețea principală şi una secundară. Diferența față de conexiunea B este mică, aşa încât se utilizează şi denumirea de conexiune B/D;

E, conexiunea unui punct SSP prin două puncte STP pentru a asigura o cale alternativă pentru mărirea fiabilității;

F, conexiunea directă între puncte SSP (sau un SSP la un SCP) în rețele fără puncte STP.

Nivelele ierarhice SS7



MTP Level 1 (Message Transfer Part) este nivelul fizic care stabileşte vitezele de transfer în telefonie şi modul de transfer folosind în semnalizare un slot de timp în E-carrier. MTP Level 2 asigură sincronizarea datelor, detecția de erori, retransmisia blocurilor fără confirmare de recepție etc.

MTP Level 3 asigură funcționalități de rutare până la destinație. Nivelele din partea superioară a stivei OSI constau în aplicații, atât în domeniul telefoniei fixe cât şi în cel al telefoniei mobile

Nivelele ierarhice SS7

TUP (Telephone User Part), pentru gestionarea telefoniei analogice;

ISUP (ISDN User Part), pentru gestionarea telefoniei digitale de voce şi date, ISDN şi non ISDN;

SCCP (Signaling Connection Control Part) asigură corespondența între numerele de telefon şi coduri (adrese) ale punctelor SS7;

TCAP (Transaction Capabilities Application Part) gestionează transferul de mesaje între SSP şi SCP. O cerere a SSP către SCP de rutare pentru un anumit număr este analizată de TCAP. TCAP este utilizat atât în telefonia fixă cât şi în cea mobilă;

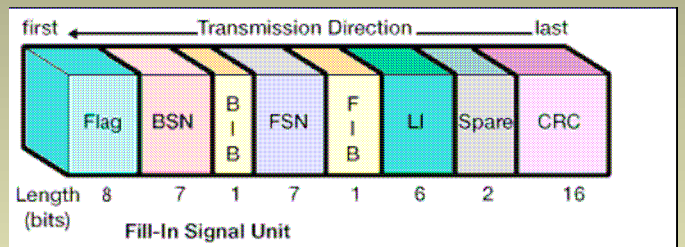
INAP (Intelligent Network Application Part);

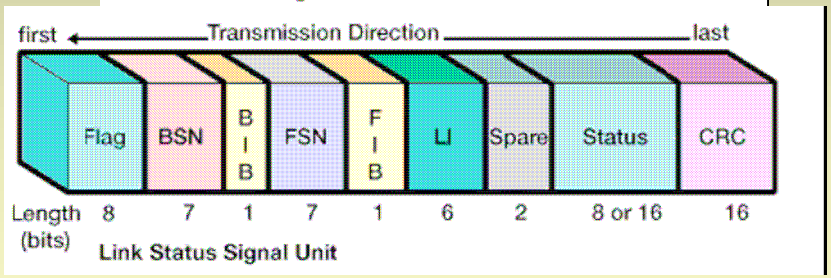
MAP (Mobile Application Part).

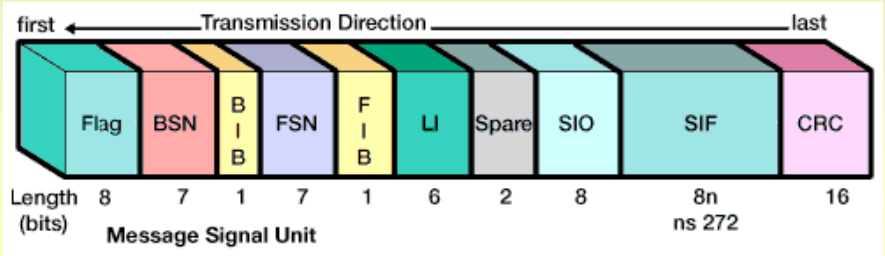
Unități de semnalizare

Pentru transfer se folosesc blocuri de date numite unități de semnalizare (signal units).

Există trei tipuri de unități de semnalizare: Fill-in Signal Unit (FISU), Link Status Signal Unit (LSSU), Message Signal Unit (MSU)







1. FISU sunt transmise continuu cu excepția momentelor când se transmit MSU sau LSSU. Recepția unităților FISU este confirmată spre transmițător, iar verificarea continuă a CRC la transmisie dă o imagine a calității transmisiei;
2. LSSU conține informații despre starea legăturii şi a punctelor de semnalizare;
3. MSU conține datele de control ale legăturii şi gestionarea rețelei în câmpul SIF (Signaling Information Field).

Unități de semnalizare

Câmpul LI (Length Indicator) indică tipul de unitate de semnalizare şi lungimea mesajului (între câmpul LI şi CRC). Dacă numărul de octeți între câmpul LI şi CRC este mai mare decât 63 (maximum 273) în LI se scrie 63. Dacă numărul de octeți între câmpul LI şi CRC este mai mic decât 63 în LI se scrie numărul de octeți. Dacă LI este 0 unitatea este FISU, dacă LI este 1 sau 2 unitatea este LSSU iar dacă LI este între 3 şi 63 unitatea este MSU.

Câmpul FSN (Forward Sequence Number) conține numărul secvenței unității de semnalizare (0-127). Când o unitate de semnalizare este gata de a fi transmisă, punctul de semnalizare incrementează FSN, apoi este calculată informația **CRC** (Cyclic Redundancy Check). După recepția acestei unități punctul de semnalizare receptor verifică CRC-ul şi copiază valoarea FSN în **câmpul BSN** (Backward Sequence Number) al unui mesaj de confirmare pe care receptorul îl trimite înapoi la transmițător. Dacă CRC-ul nu este corect mesajul de confirmare se trimite cu **bitul BIB** (Backward Indicator Bit) setat. Transmițătorul repetă transmiterea unității eronate cu **bitul FIB** (Forward Indicator Bit) setat.

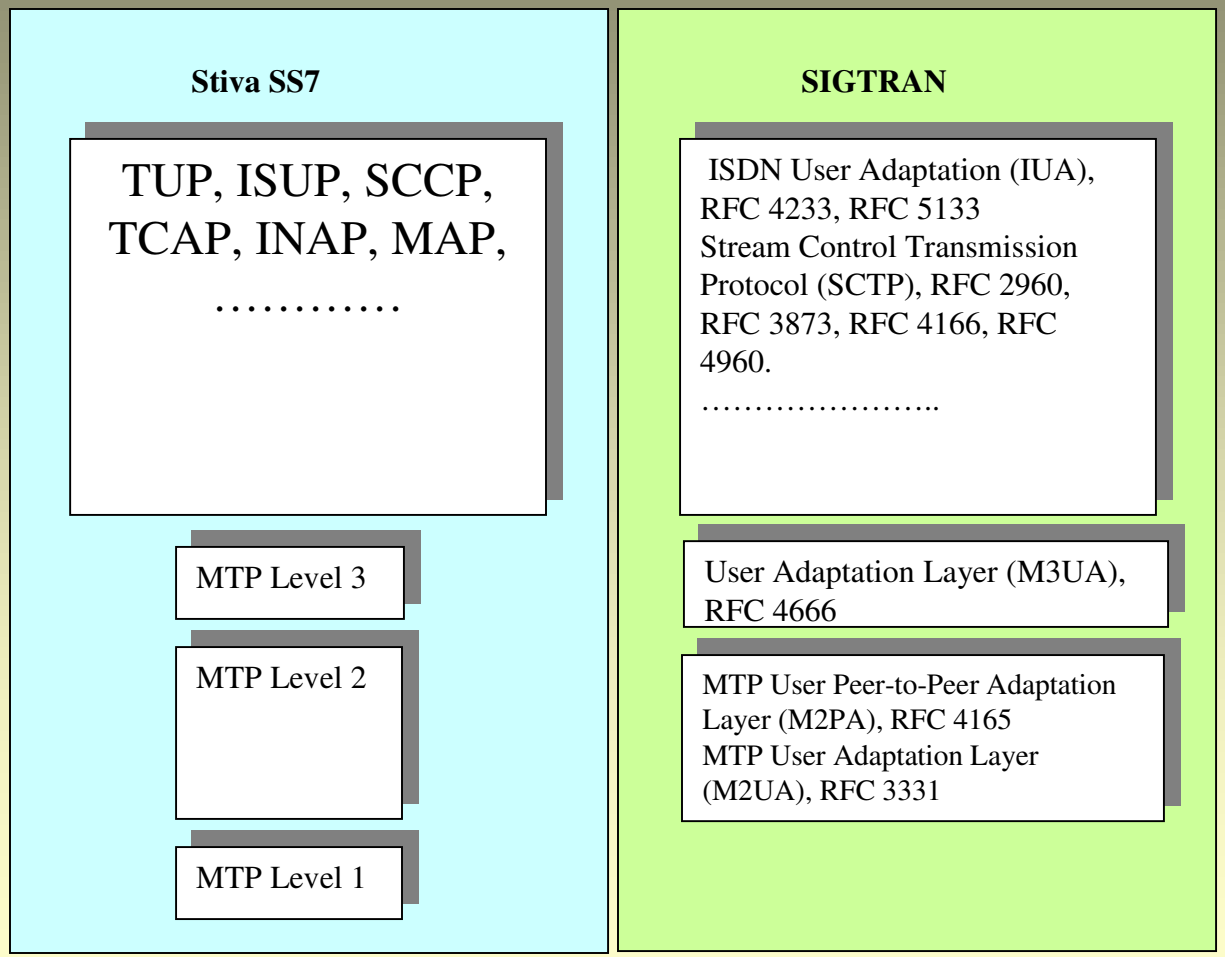
Câmpul SIO (Service Information Octet) din MSU conține un indicator al serviciului şi un indicator al subserviciului, de exemplu dacă apelul este național sau internațional, prioritatea apelului (între 1 şi 3) etc.

Câmpul SIF (Signaling Information Field) din MSU conține tabela de rutare şi datele pentru SCCP, TCAP şi ISUP.

Semnalizări în VoIP

Grupul de lucru Internet Engineering Task Force s-a transformat în SIGTRAN (Signaling Transport) având preocupări în domeniul protocoalelor şi adaptării sistemului SS7 la protocolul Internet (IP). În Framework Architecture for Signaling Transport. (RFC 2719) se introduce noțiunea de gateway de semnalizare cu rolul de a converti mesajele Common Channel Signaling (CCS) din SS7. O contribuție importantă este SCTP (Stream Control Transmission Protocol), utilizat pentru a adapta semnalizările telefoniei PSTN (public switched telephone network).

Nivelele ierarhice SIGTRAN



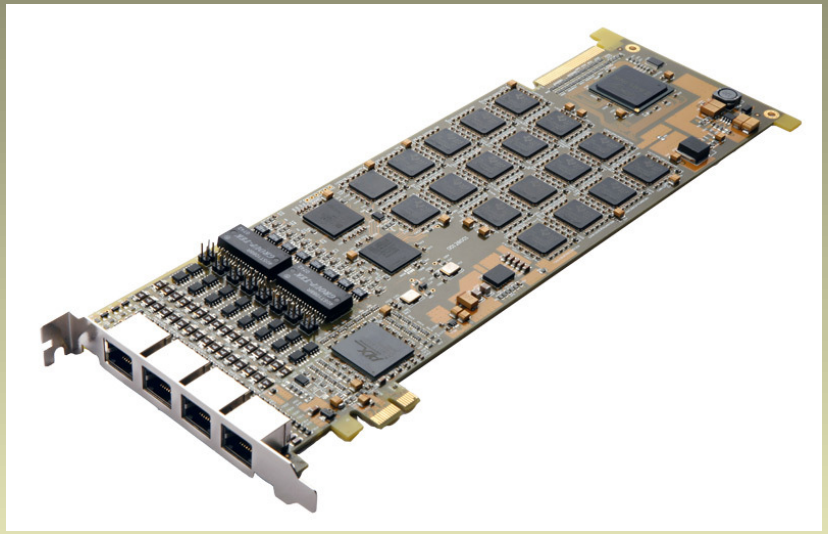
Confidențialitatea apelurilor telefonice

Un articol apărut in Washington Post în 2014 atrage atenția asupra vulnerabilității sistemului de semnalizare SS7. Semnatarul articolului, Tobias Engel susține că "It's like you secure the front door of the house, but the back door is wide open,". Companiile de telefoane cheltuie sume importante pentru criptarea convorbirilor dar interceptarea unităților de semnalizare în sistemul GSM permite localizarea telefoanelor, citirea mesajelor SMS, etc.

În articol se afirmă că este posibil ca serviciile secrete să fi utilizat de mult timp această vulnerabilitate: "Many of the big intelligence agencies probably have teams that do nothing but SS7 research and exploitation,".

O primă metodă de interceptare care poate fi utilizată este programarea în telefon a funcției de call forwarding şi prin aceasta toate apelurile ajung la cel care supraveghează convorbirile. O altă metodă necesită interceptarea în proximitate a unităților de semnalizare SS7 cu o antenă şi decriptarea lor. Un senator din Germania a acceptat să participe la teste şi concluziile celui care a interceptat au fost: "It would strike me as a perfect spying capability, to record and decrypt pretty much any network… Any network we have tested, it works."

Placă SS7



O placă cu interfață PCIe care realizează funcțiile de semnalizare SS7 este placa Synway. Placa are integrate funcțiile nivelelor de protocoale MTP1, MTP2, MTP3, ISUP, TUP, SCCP, şi TCAP, inclusiv suport pentru aplicații multimedia. Cu această placă pot fi implementate aplicații diverse de telefonie care includ apeluri, monitorizare SS7, mesaje SMS, Call center etc.

http://www.synway.net/prds.asp?id=291

Bibliografie

1. http://en.wikipedia.org/wiki/Communications_protocol
2. http://ro.wikipedia.org/wiki/Modelul_OSI
3. http://en.wikipedia.org/wiki/Signalling_System_No._7
4. http://docstore.mik.ua/univercd/cc/td/doc/product/tel_pswt/vco_prod/ss7_fund/ss7fun04.pdf
5. http://www.eurecom.fr/~dacier/Teaching/Eurecom/Intro_computer_nets/Recommended/ss7.pdf
6. http://en.wikipedia.org/wiki/SIGTRAN
7. Craig Timberg, German researchers discover a flaw that could let anyone listen to your cell calls, http://www.washingtonpost.com/blogs/the-switch/wp/2014/12/18/german-researchers-discover-a-flaw-that-could-let-anyone-listen-to-your-cell-calls-and-read-your-texts/