Telecommunications Infrastructure Security

Attacking SS7 applications: SCCP hacking and mapping the phone system.

Philippe Langlois, P1 Security Inc.
phil@p1sec.com

Agenda

- SS7 Basics
- SS7 and IP: the SIGTRAN evolution and problems
- Example of SS7 protocol (ISUP) and related attacks
- A practical SS7 attack: Disabling incoming calls to any subscriber
- New attack perimeters: Femto cell attacks
- Getting secure

SS7 Basics

Introduction to SS7 in the PSTN

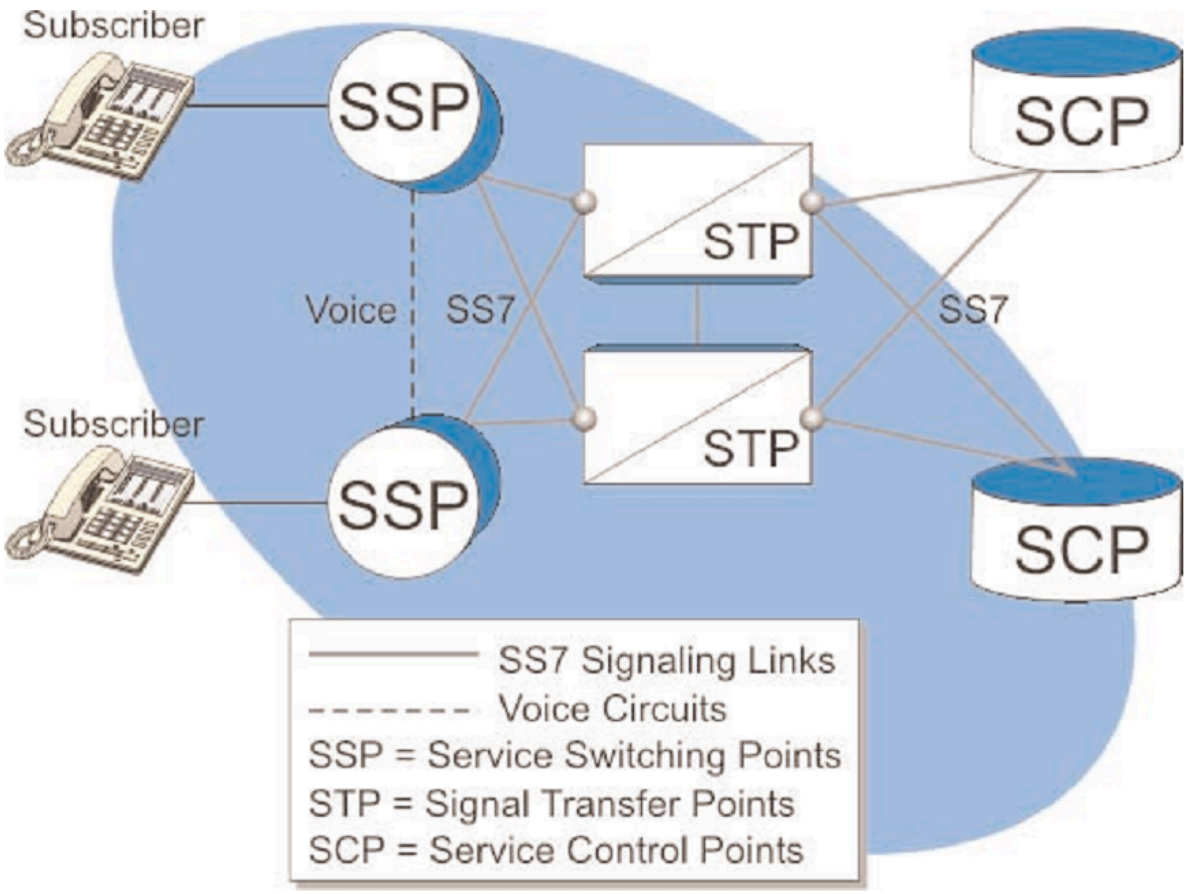
P1 Security Inc, http://www.p1security.com

Why do we have SS7?

Steve Jobs and Steve Wozniak in 1975 with a bluebox

- CCITT#5 in-band signalling sends control messages over the speech channel, allowing trunks to be controlled
- Seize trunk (2600) / KP1 or KP2 / destination / ST
- Started in mid-60's, became popular after Esquire 1971
- Sounds produced by whistles, electronics dialers, computer programs, recorded tones

SS7 basic architecture

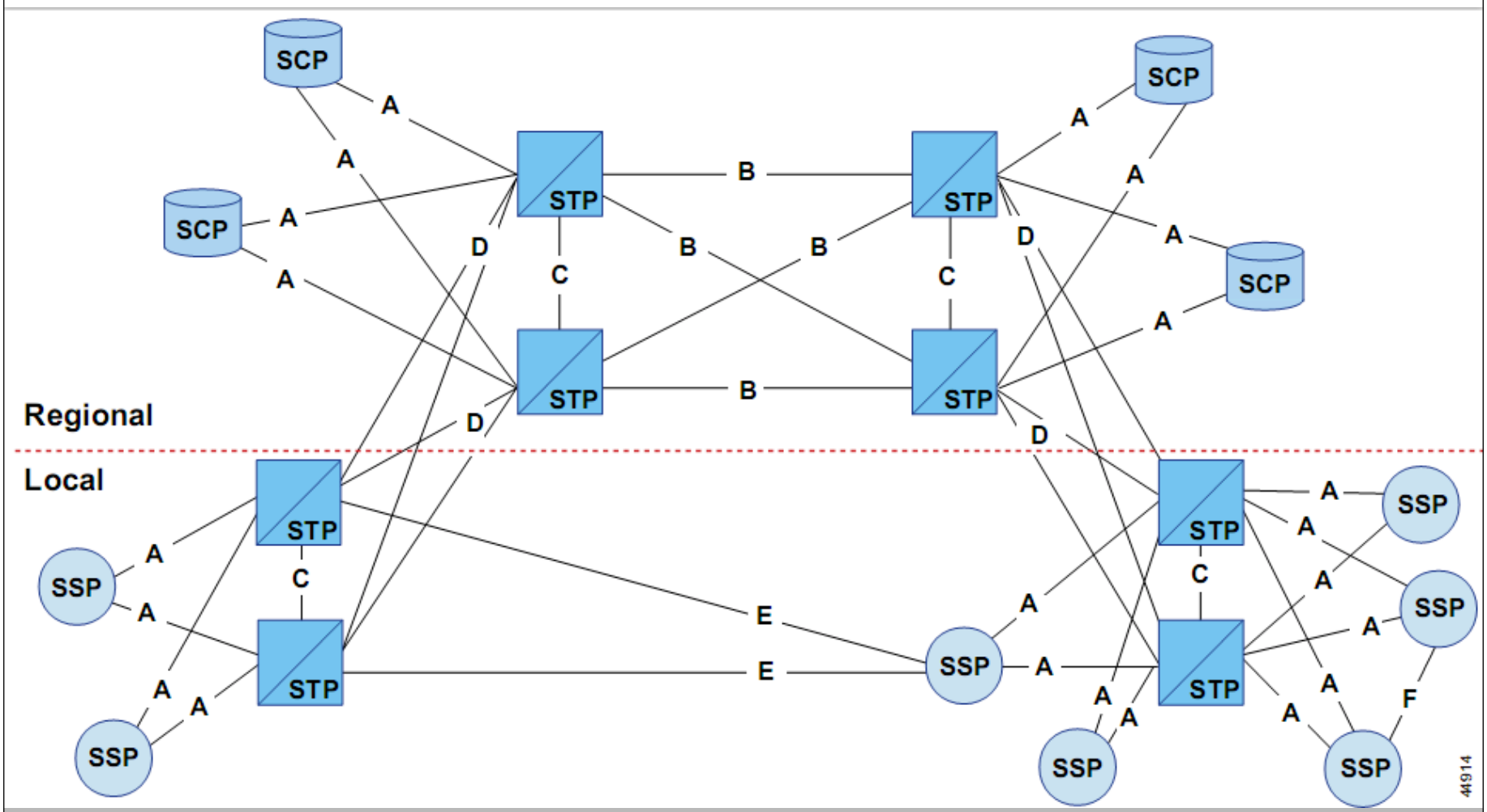


P1 Security Inc, http://www.p1security.com

Basic SS7 network

- **Service Switching Points** (SSP) are the telephone "switches" that are interconnected to each other by SS7 links. The SSPs perform call processing on calls that originate, tandem, or terminate at that site.
- **Signal Transfer Points** (STP) are "routers" that relay messages between network switches and databases. Their main function is to route SS7 messages to the correct outgoing signaling link, based on information contained in the SS7 message address fields.
- **Service Control Points** (SCP) contains centralized network databases for providing enhanced services. Examples of services include toll-free numbers and prepaid subscriptions.

SS7 network



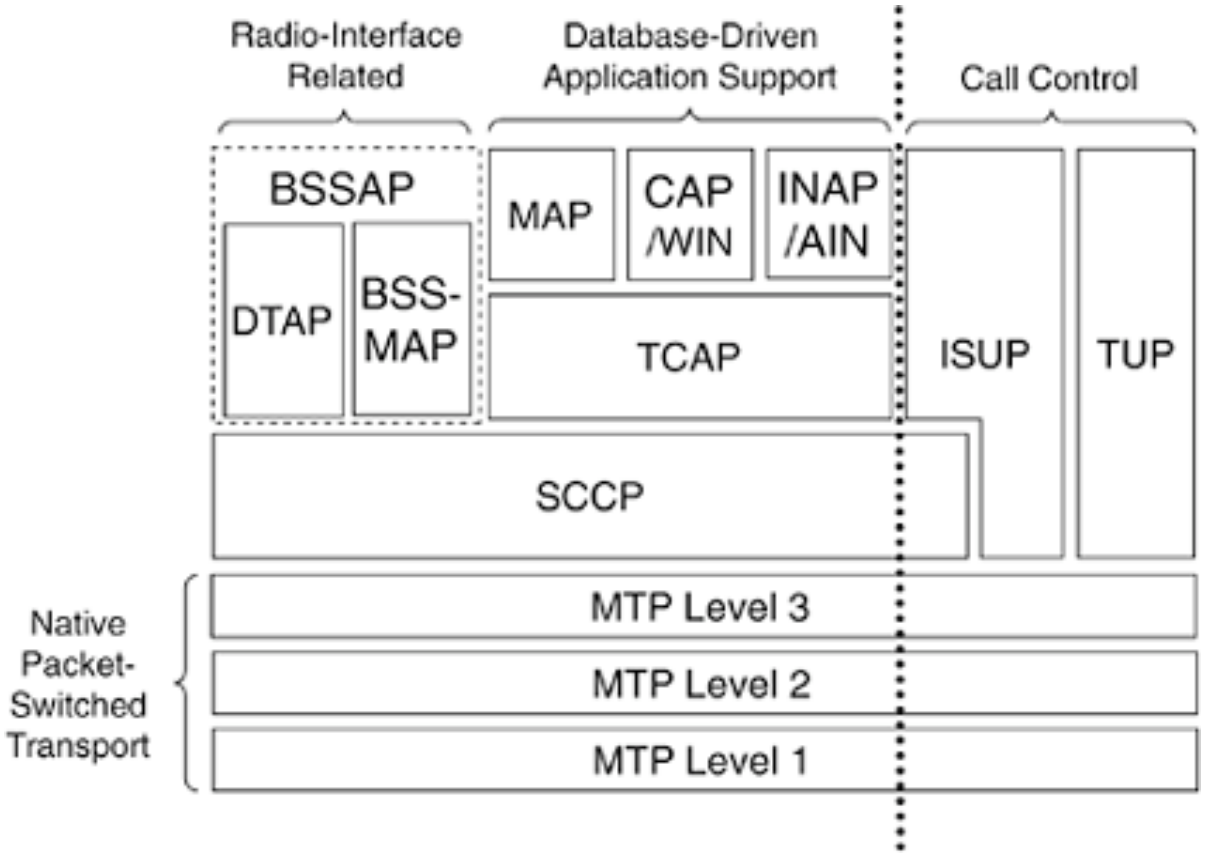
P1 Security Inc, http://www.p1security.com

SS7 reliability

To meet the stringent reliability requirements of public telecommunications networks, a number of safeguards are built into the SS7 protocol:

- STPs and SCPs are normally provisioned in **mated pairs**. On the failure of individual components, this duplication allows signaling traffic to be automatically diverted to an alternate resource, minimizing the impact on service.
- Signaling links are provisioned with some level of **redundancy**. Signaling traffic is automatically diverted to alternate links in the case of link failures.
- The SS7 protocol has built-in **error recovery** mechanisms to ensure reliable transfer of signaling messages in the event of a network failure.
- Management messages (Link Status Signal Units) are constantly sent over the links to **monitor** its status.

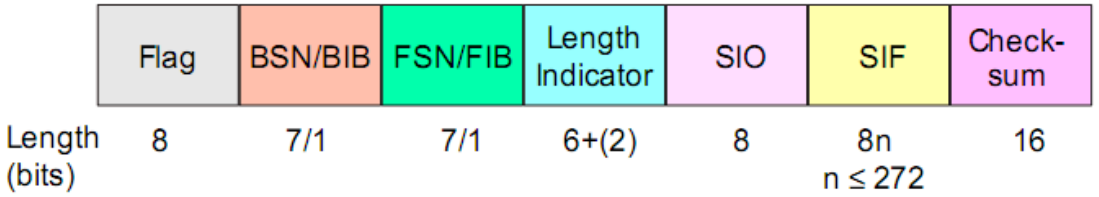
SS7 stack



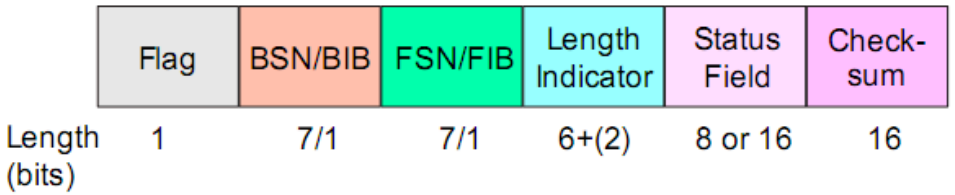
P1 Security Inc, http://www.p1security.com

MTP carrier: MTP Signal Units

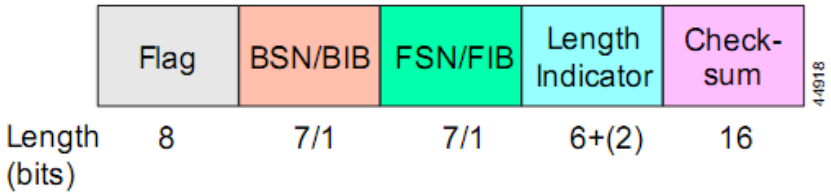
Message Signal Unit



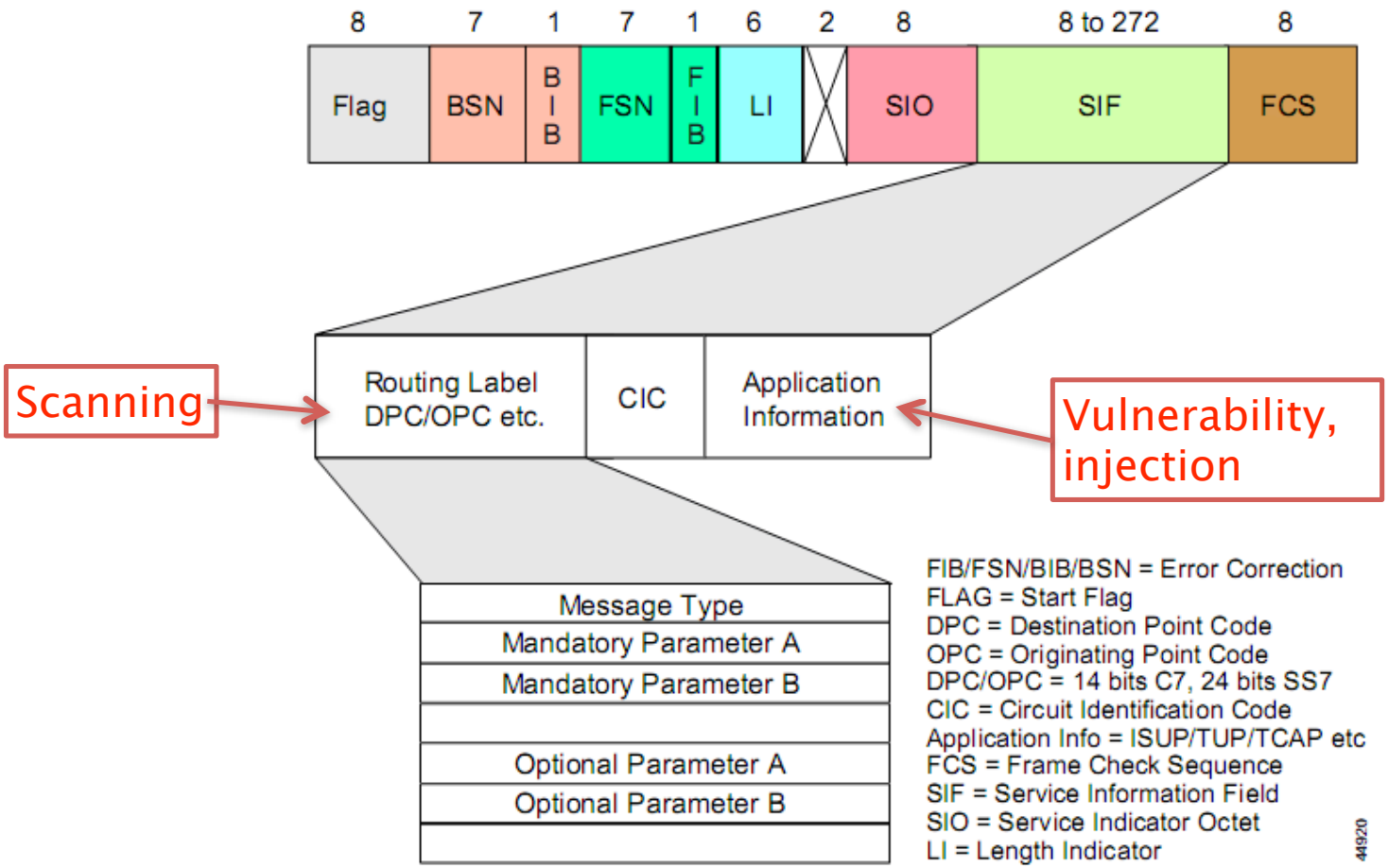
Link Status Signal Unit



Fill-In Signal Unit



Message Signal Unit SIF



Important SS7 protocols

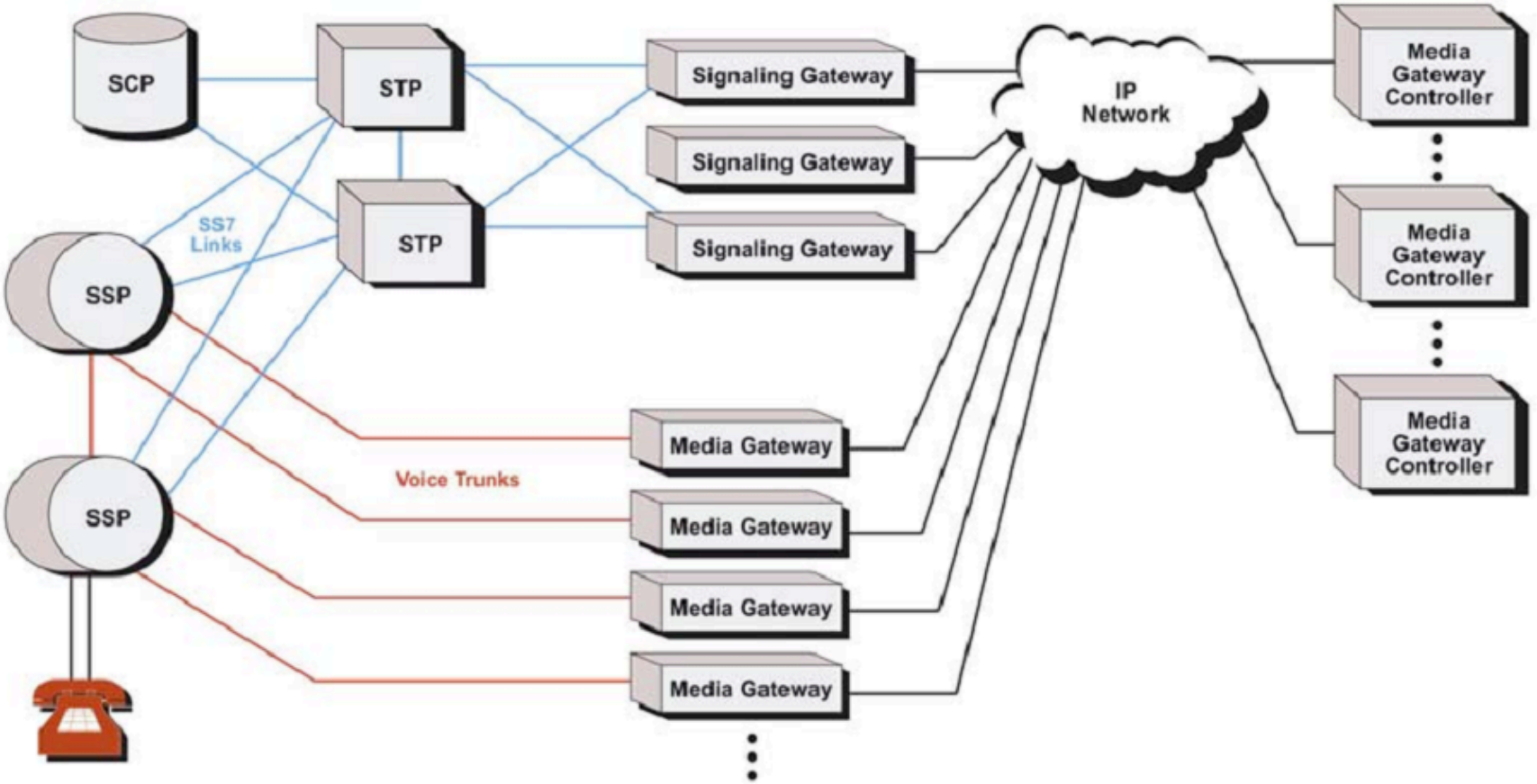
- **MTP** (Message Transfer Part) Layers 1-3: lower level functionality at the Physical, Data Link and Network Level. They serve as a signaling transfer point, and support multiple congestion priority, message discrimination, distribution and routing.
- **ISUP** (Integrated Services Digital Network User Part): network side protocol for the signaling functions required to support voice, data, text and video services in ISDN. ISUP supports the call control function for the control of analog or digital circuit switched network connections carrying voice or data traffic.
- **SCCP** (Signaling Control Connection Part): supports higher protocol layers such as TCAP with an array of data transfer services including connection-less and connection oriented services. SCCP supports global title translation (routing based on directory number or application title rather than point codes), and ensures reliable data transfer independent of the underlying hardware.
- **TCAP** (Transaction Capabilities Application Part): provides the signaling function for communication with network databases. TCAP provides non-circuit transaction based information exchange between network entities.
- **MAP** (Mobile Application Part): provides inter-system connectivity between wireless systems, and was specifically developed as part of the GSM standard.
- **INAP** (Intelligent Network Application Part): runs on top of TCAP and provides high-level services interacting with SSP, SCP and SDP in an SS7 network.

SS7 and IP: the SIGTRAN evolution and problems

Basics of IP telephony
SIGTRAN protocols & SCTP scanning

P1 Security Inc, http://www.p1security.com

SIGTRAN network



P1 Security Inc, http://www.p1security.com

IP Telephony Networks

- **Media Gateway** (MGW) terminates voice calls on inter-switch trunks from the PSTN, compresses and packetizes the voice data, and delivers voice packets to the IP network. For ISDN calls from the PSTN, Q.931 signaling information is transported from the MGW to the media gateway controller for call processing.
- **Media Gateway Controller** (MGC) handles the registration and management of resources at the media gateways. An MGC exchanges ISUP messages with CO switches via a signaling gateway. Sometimes called a softswitch.
- **Signaling Gateway** (SGW) provides transparent interworking of signaling between switched circuit and IP networks. The SGW may terminate SS7 signaling or translate and relay messages over an IP network to an MGC or another SGW.

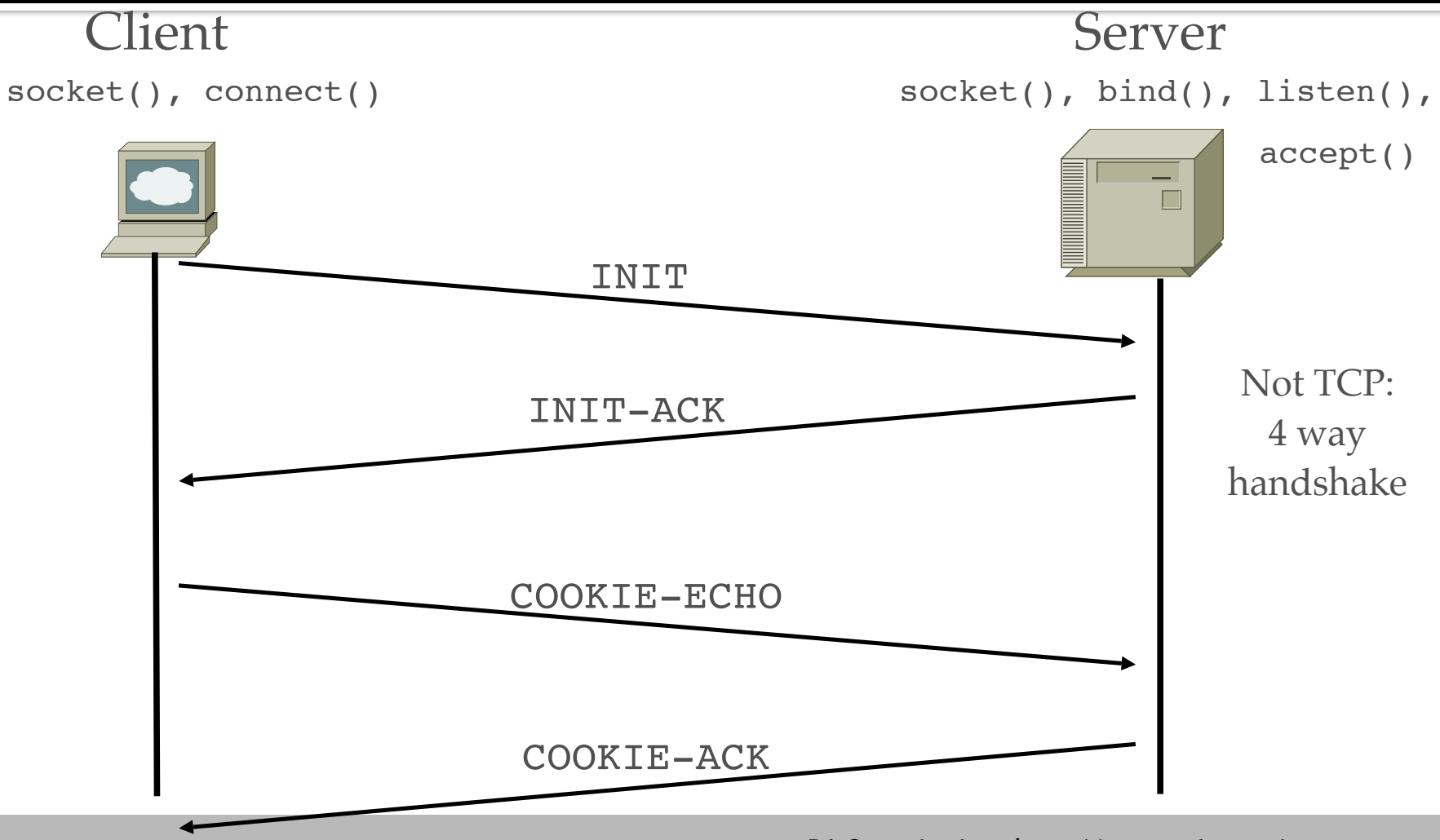
SIGTRAN evolution

- The **SIGTRAN protocols** specify the means by which SS7 messages can be reliably transported over IP networks (thanks SCTP).
- The architecture identifies two components: a **common transport protocol** for the SS7 protocol layer being carried and an **adaptation module** to emulate lower layers of the protocol. For example:
  - If the native protocol is MTP (Message Transport Layer) Level 3, the SIGTRAN protocols provide the equivalent functionality of MTP Level 2.
  - If the native protocol is ISUP or SCCP, the SIGTRAN protocols provide the same functionality as MTP Levels 2 and 3.
  - If the native protocol is TCAP, the SIGTRAN protocols provide the functionality of SCCP (connectionless classes) and MTP Levels 2 and 3.

SCTP Specs & Advantages

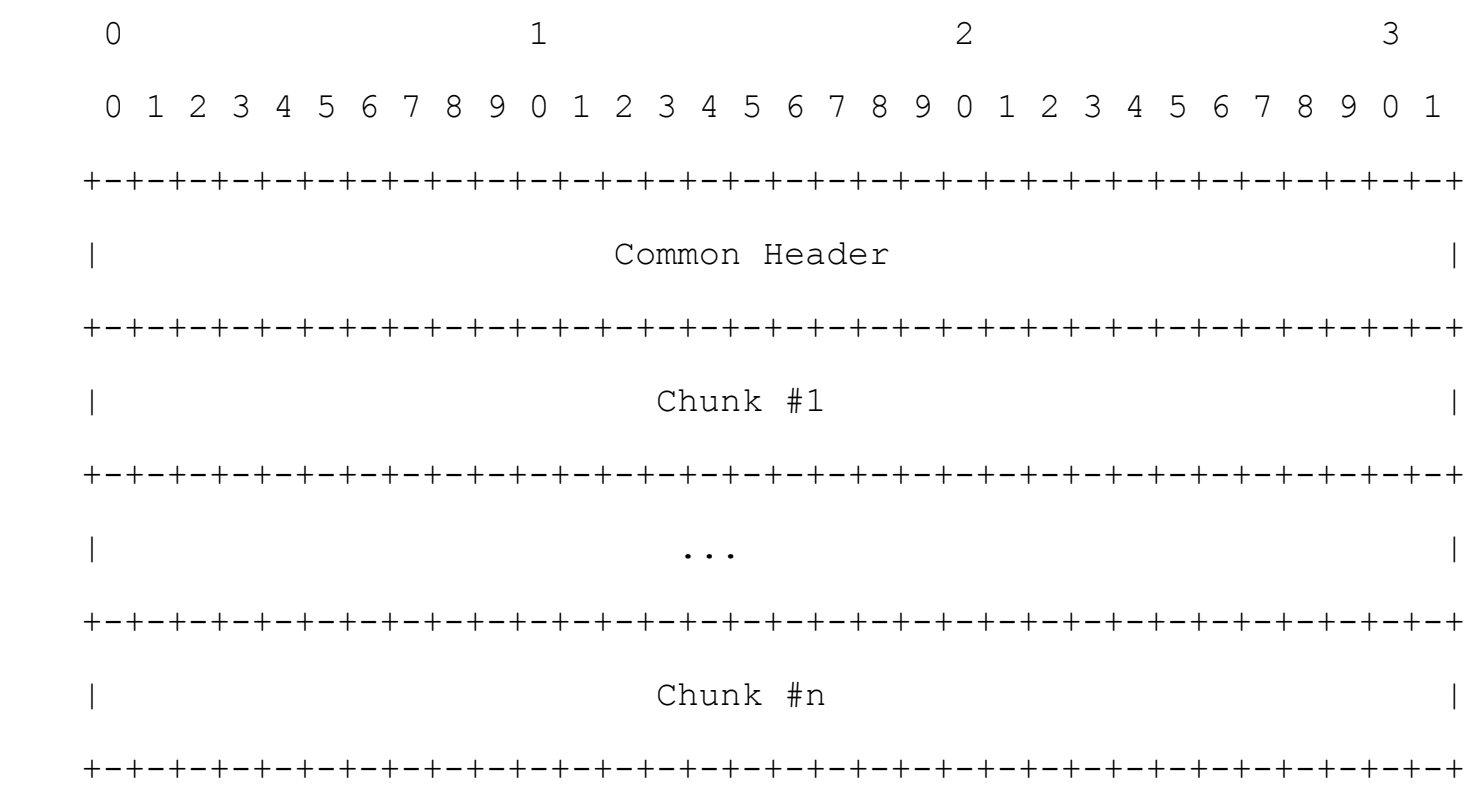
- RFC2960
  - SCTP: Stream Control Transmission Protocol
- Advantages
  - Multi-homing
  - DoS resilient (4-way handshake, cookie)
  - Multi-stream
  - Reliable datagram mode
  - Some of TCP & UDP, improved

SCTP scanning method



SCTP Packets

SCTP packet Format (ascii art straight from RFC2960)

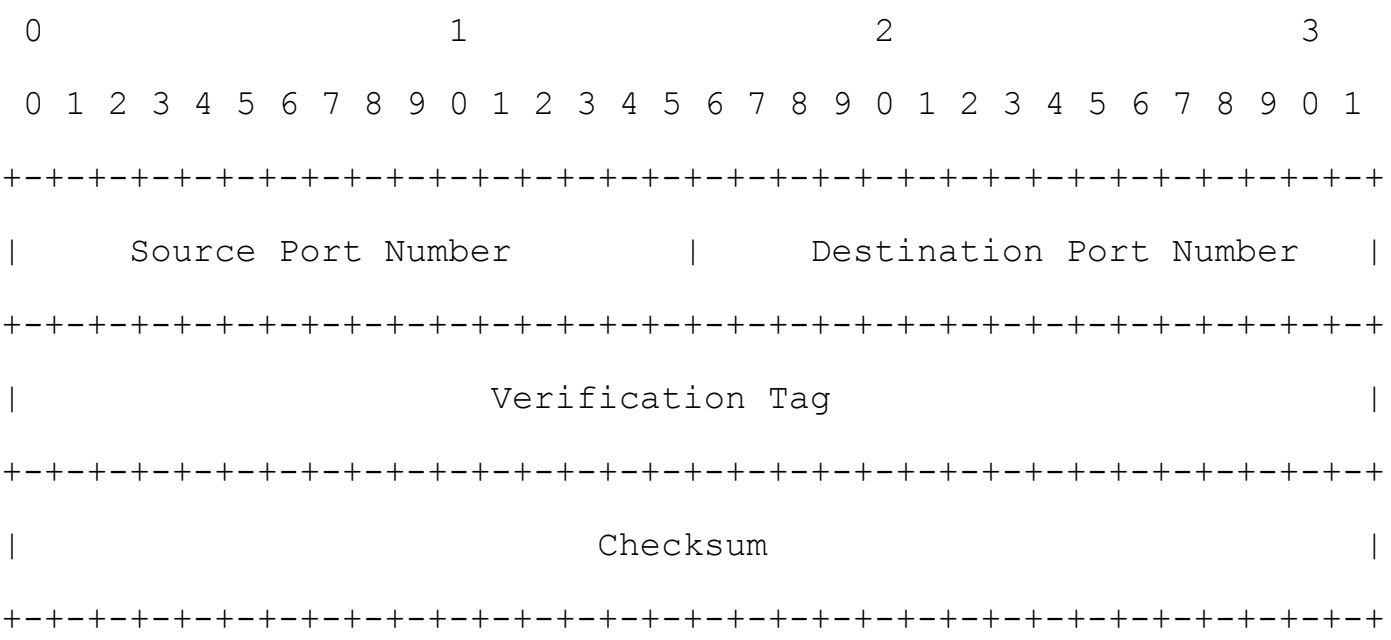


SCTP Chunk types

ID Value	Chunk Type
0	- Payload Data (DATA)
1	**- Initiation (INIT)**
2	**- Initiation Acknowledgement (INIT ACK)**
3	- Selective Acknowledgement (SACK)
4	- Heartbeat Request (HEARTBEAT)
5	- Heartbeat Acknowledgement (HEARTBEAT ACK)
6	**- Abort (ABORT)**
7	- Shutdown (SHUTDOWN)
8	**- Shutdown Acknowledgement (SHUTDOWN ACK)**
9	- Operation Error (ERROR)
10	- State Cookie (COOKIE ECHO)
11	- Cookie Acknowledgement (COOKIE ACK)
12	- Reserved for Explicit Congestion Notification Echo (ECNE)
13	- Reserved for Congestion Window Reduced (CWR)
14	- Shutdown Complete (SHUTDOWN COMPLETE)

SCTP Header

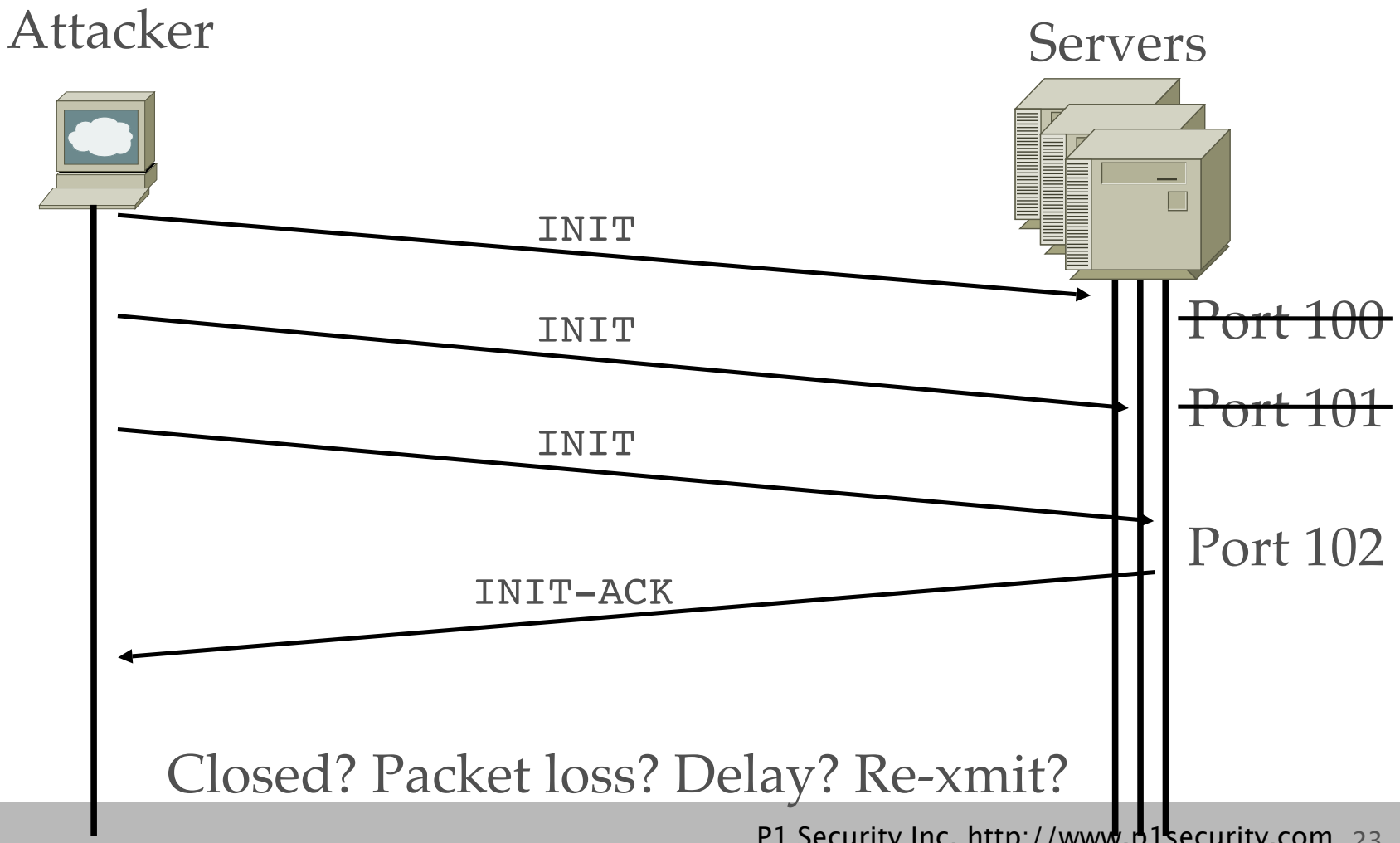
- **SCTP Common Header Format**



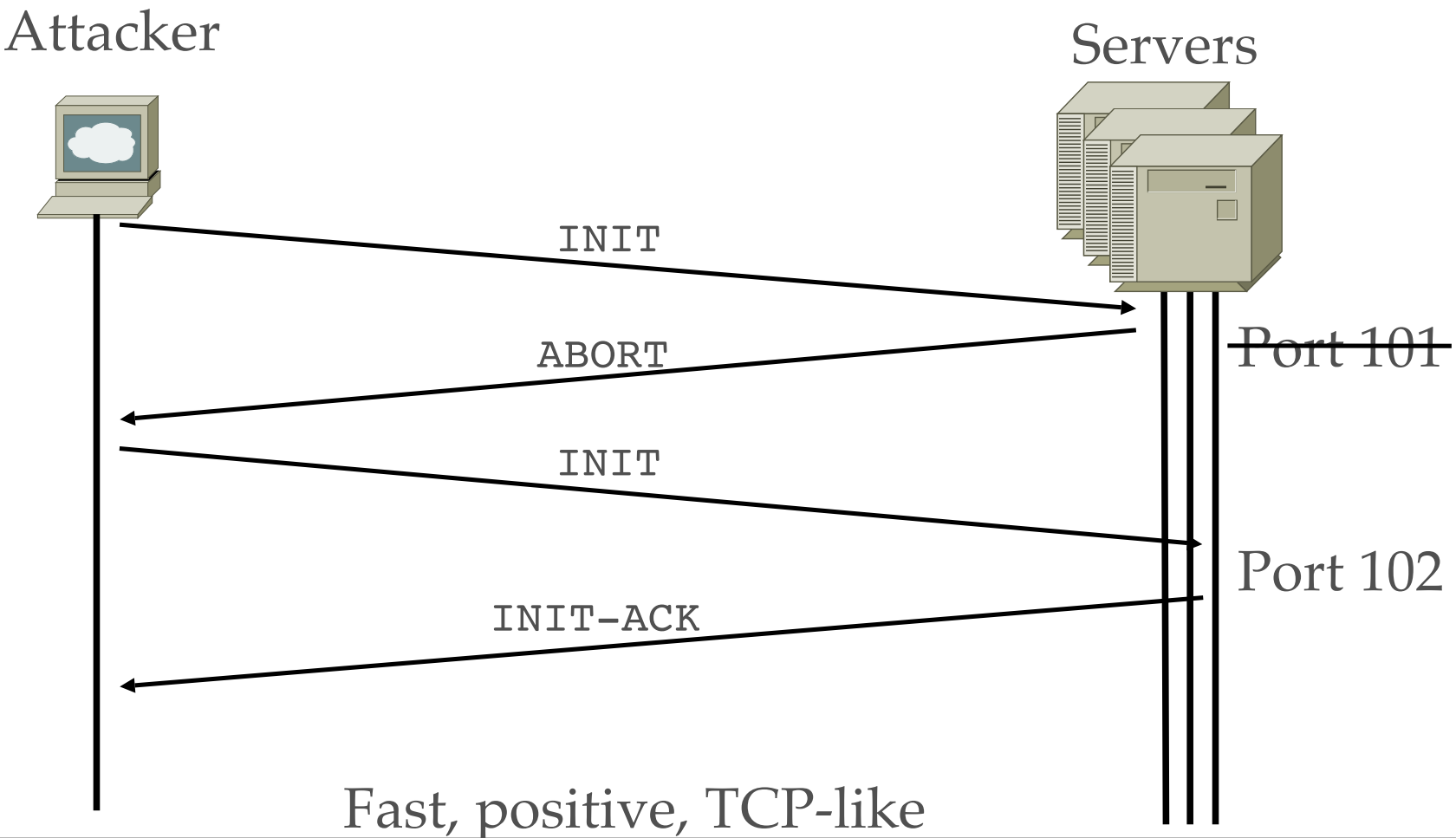
SCTPscan: Mapping SIGTRAN

- SCTPscan
  - Linux, BSD, MacOS X, Solaris, ...
  - IP scan, portscan, fuzzing, dummy server, bridge
  - Included in BackTrack, demo
- SCTP Tricks: port mirroring, instreams connections
  - NMAP new SCTP support (-Y), lacks tricks
- SIGTRAN usually requires peer config
  - This is not the average TCP/IP app

From RFC...


Attacker
Servers
INIT
INIT
INIT
INIT-ACK
Port 100
Port 101
Port 102
Closed? Packet loss? Delay? Re-xmit?

SCTP stealth scan

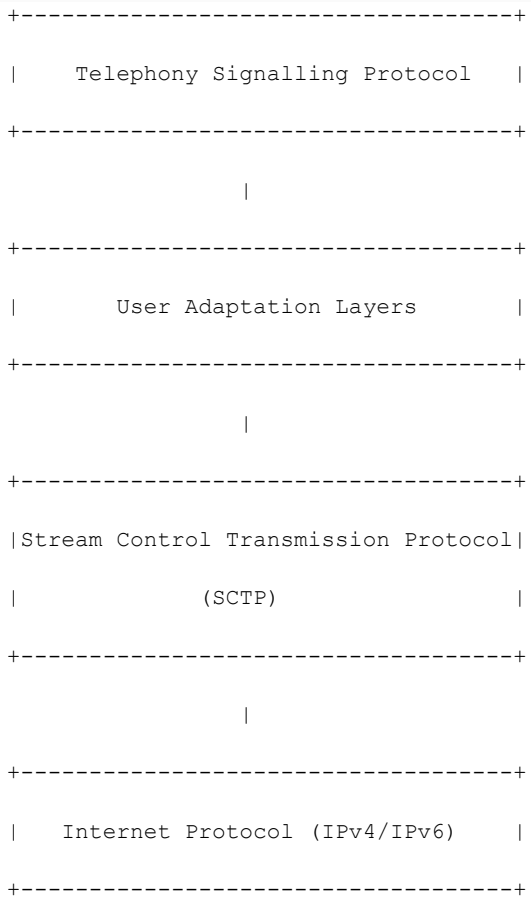


SCTPscan Usage

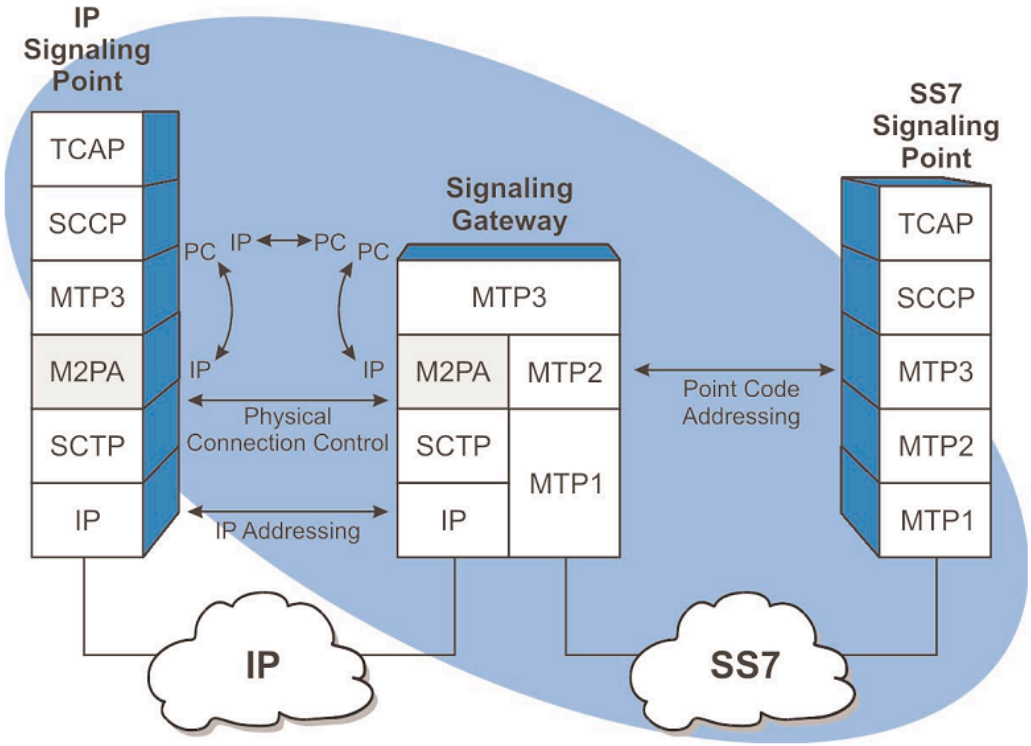
```
root@gate:~/sctp# ./sctpscan --scan --autoportscan
-r 203.151.1
Netscanning with Crc32 checksumed packet
203.151.1.4 SCTP present on port 2905
203.151.1.4 SCTP present on port 7551
203.151.1.4 SCTP present on port 7701
203.151.1.4 SCTP present on port 8001
203.151.1.4 SCTP present on port 2905
root@gate:~/sctp#
```

- Demo...

What goes over SCTP?

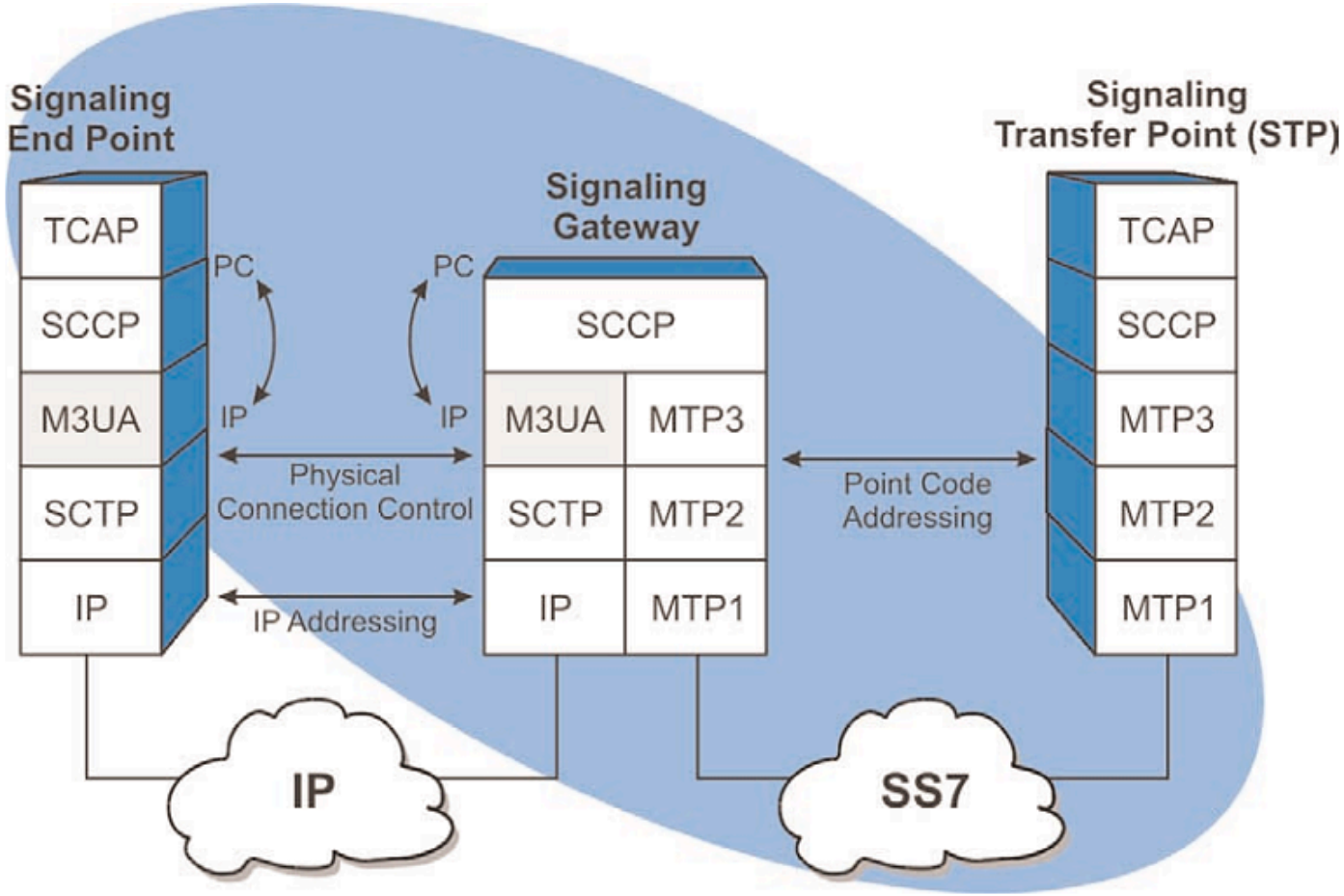


User Adapation example: M2PA

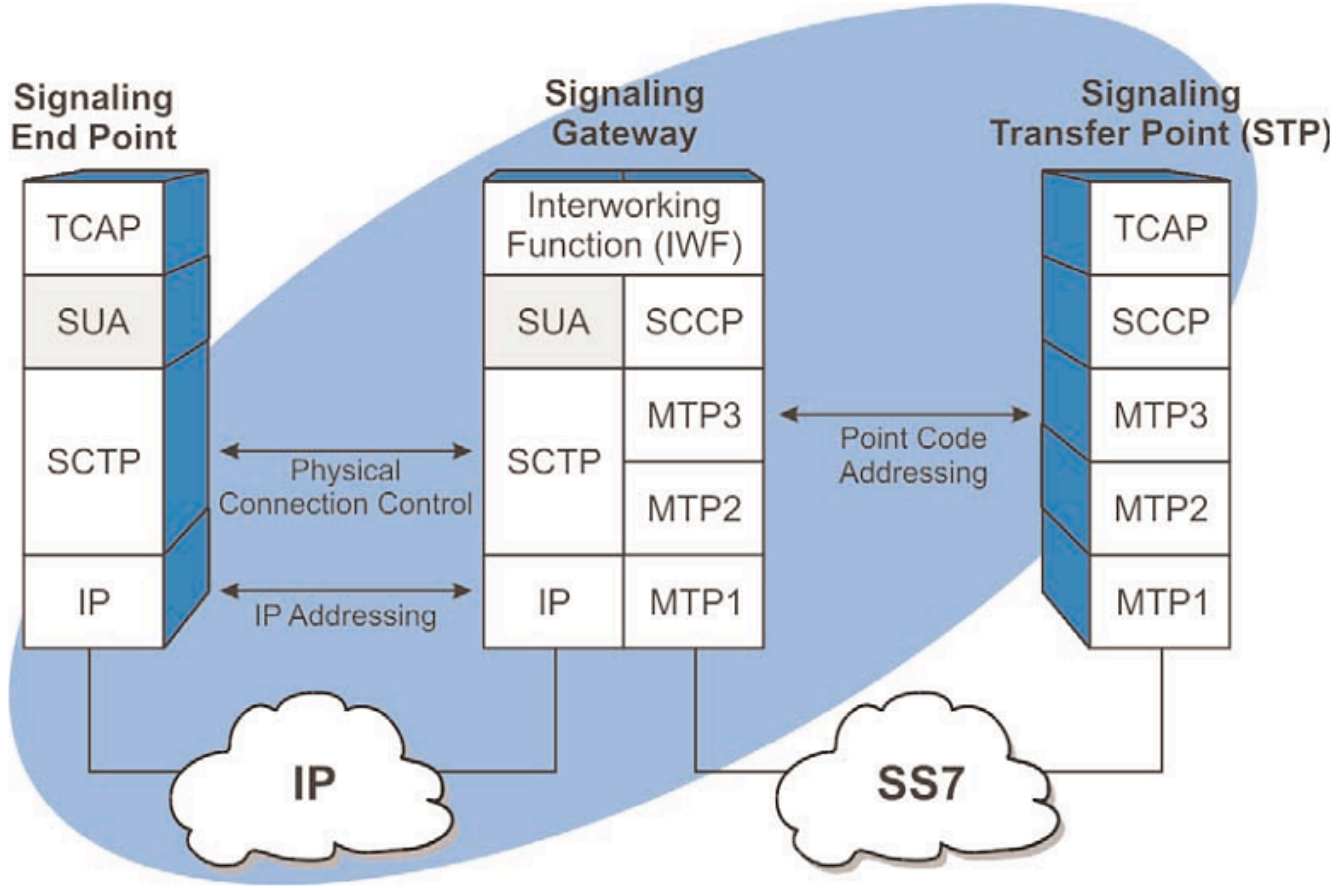


From RFC 4166

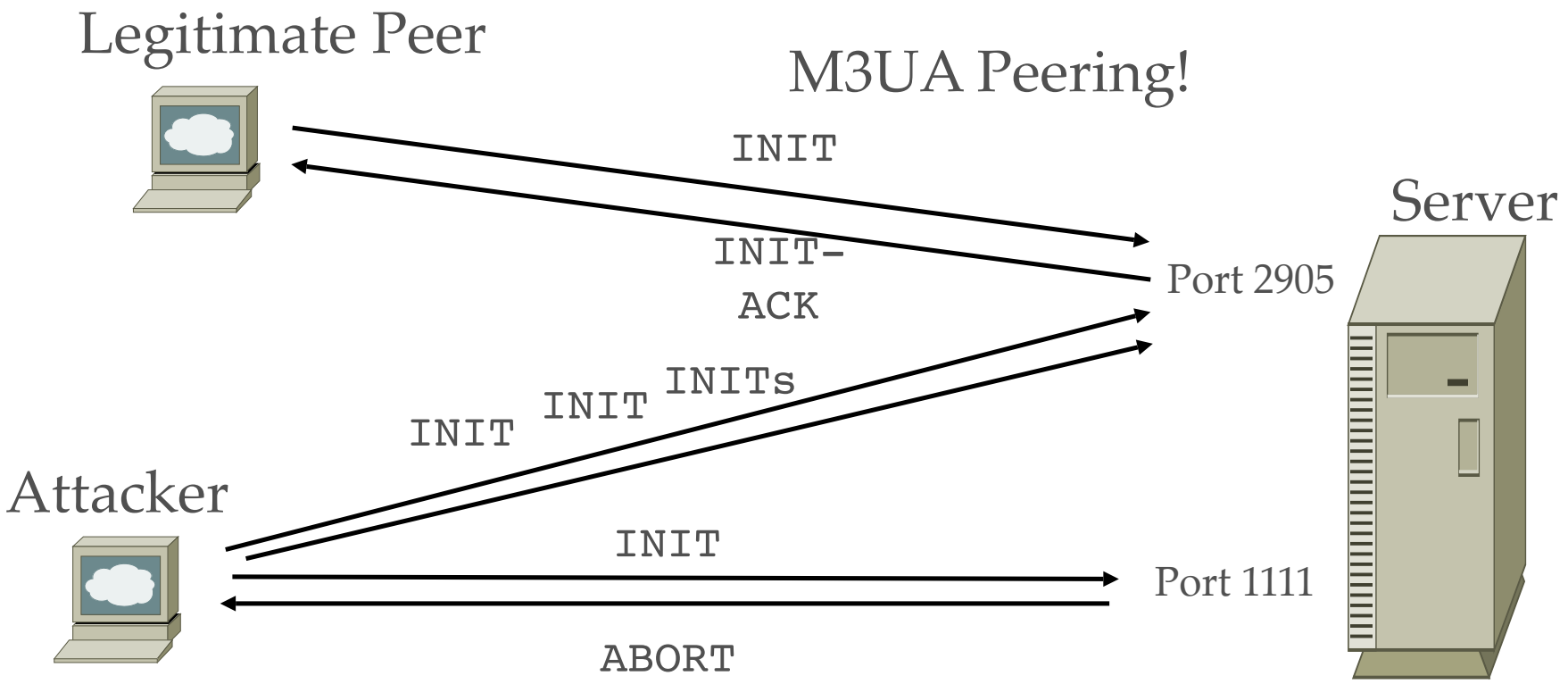
M3UA Protocol Adaptation Layer



SCCP User Adaptation (SUA) Layer



SS7 Peering: attacker enemy



No answer on actual peering port: How rude!

On SS7 application attacks: hackers loose

Connecting to 7bone:

Playground & Research SS7 Network

P1 Security Inc, http://www.p1security.com

OpenSS7 stack

- OpenSS7 is a SS7 and SIGTRAN protocol stack which provides GPL'ed and LGPL'ed source.
- Open source implementation of the SS7 stack as specified by ITU-T, ETSI, ANSI, and other standards bodies. It derives primarily from an implementation of the ITU-T Q.700-Series Recommendations
- ISUP and TCAP support
- Supports a variety of E1/T1 boards. Runs on Kernel 2.4 and 2.6 (specific kernel versions!)
- Project not yet suitable for carrier-grade implementations.

Dialogic / Intel stack

- Mature commercial SS7 stack implementing most protocols
- Supports Wintel, Linux and Solaris environments. Standalone, virtually no dependencies
- Can handle a variety of hardware interfaces
- Can be freely downloaded and run in “trial mode” (stack resets after 10 hours of use)
- Fully documented APIs and numerous code examples, test programs and scripts
- Ideal for testbed development, with the ability to scale up to carrier environments
- Actively maintained

Other implementations

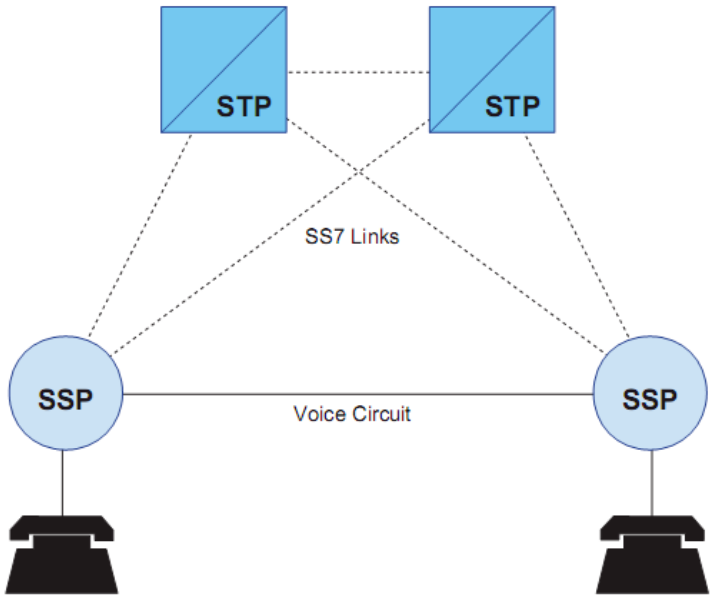
- SCTPscan includes its own SCTP spoof & sniff implementation, can be used to build custom SCTP queries and security tools
- The sctplib library is a fairly complete userland implementation of the SCTP stack, open source and actively maintained.
- HP OpenCall SS7. Used in several carrier deployments, provides a well documented API but cannot operate in trial mode.
- Telesys MACH-SS7 stack. Robust, well documented commercial stack.
- Proprietary stacks (NSN, Alcatel, Huawei, …)

- Attack: several closed source implementations, room for vulnerabilities

Example of SS7 protocol: ISUP & related attacks

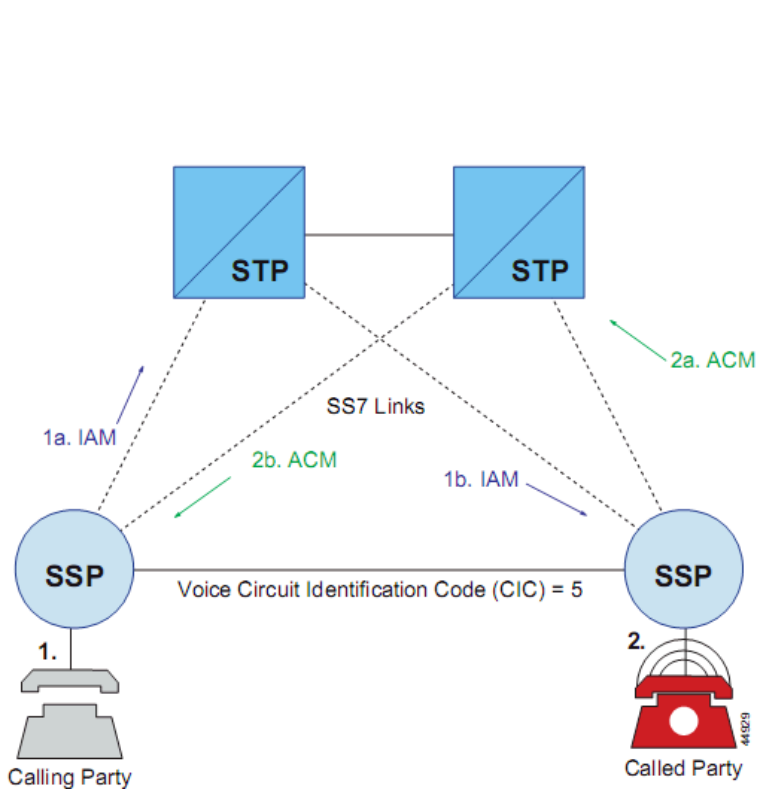
ISUP message types
ISUP call flows

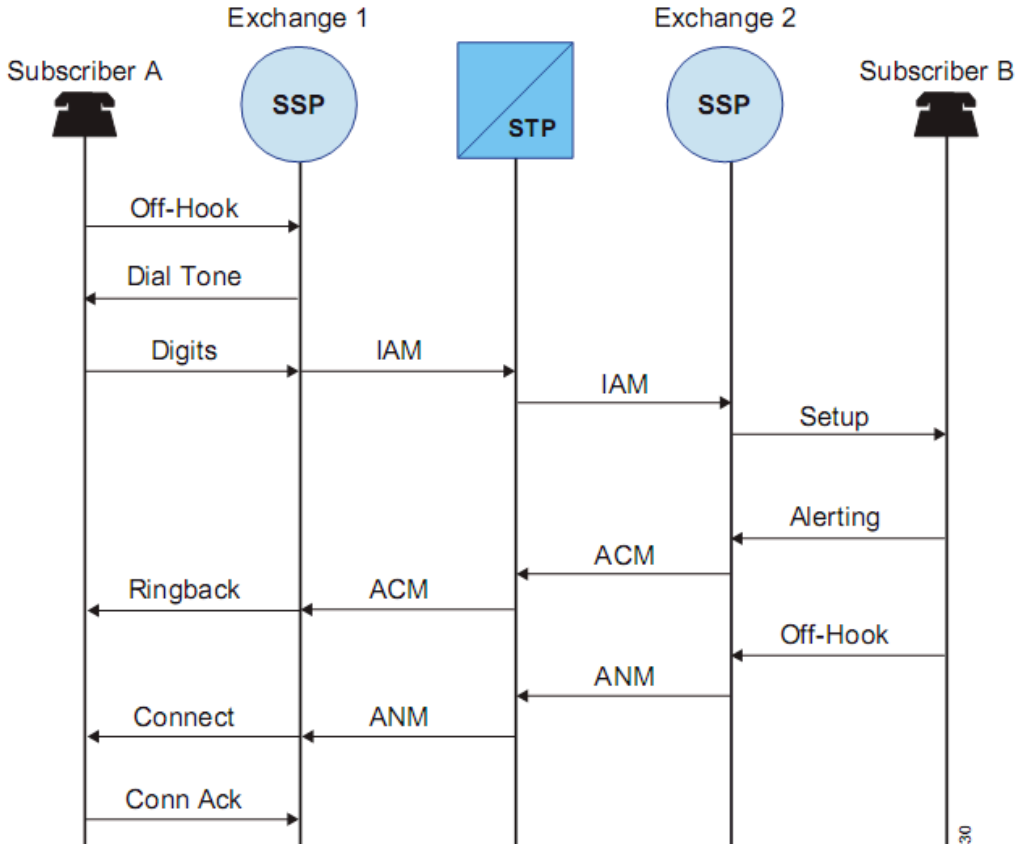
ISUP message (ITU-T)



Subservice Field	Service Indicator
DPC Low-Order Octet	
OPC Low-Order 2 bits	DPC High-Order 6-bits
OPC Middle-Order Octet	
4-bit SLS/SLC	OPC High-Order 4-bits
CIC Low-Order Octet	
4-bit SLS/SLC	CIC High-Order 4-bits
Message Type	
Interpretation varies according to Message Type variable	

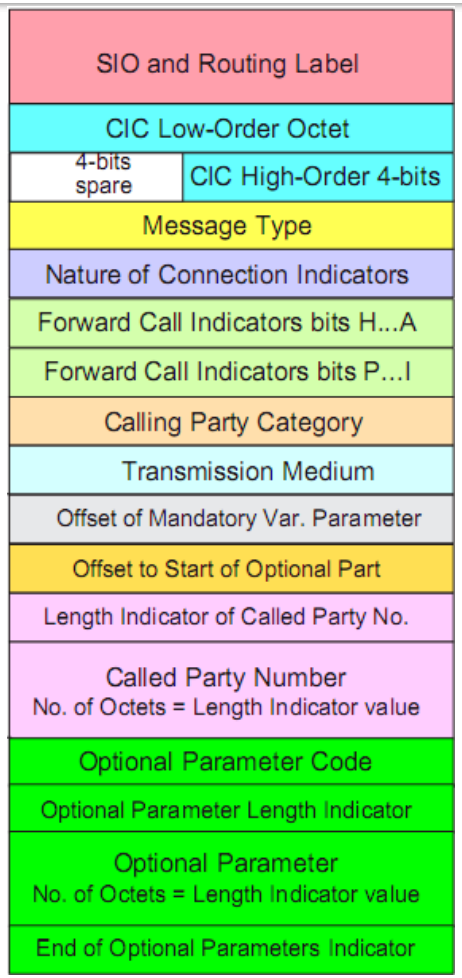
ISUP Call Initiation Flow





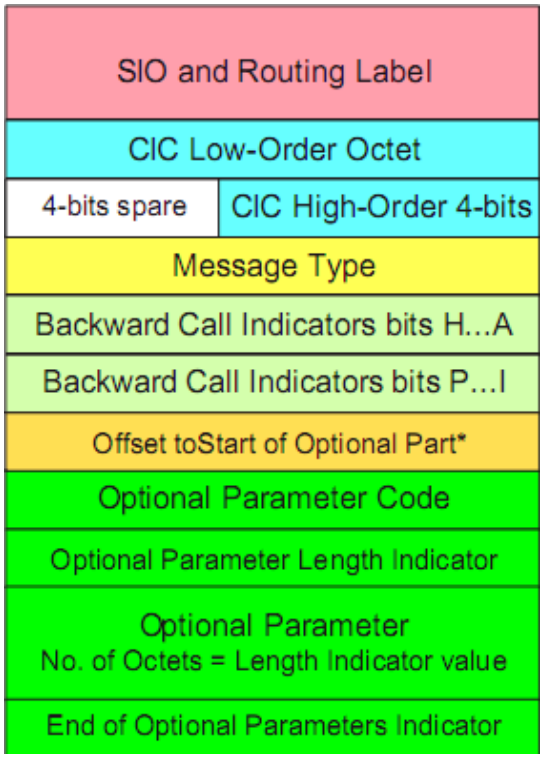
ISUP AIM

- An **initial address message** (IAM) is sent in the "forward" direction by each switch in the circuit between the calling party and the destination switch of the called party.
- An IAM contains the **called party number** in the mandatory variable part and may contain the **calling party name** and number in the optional part.
- **Attack: Capacity DoS**

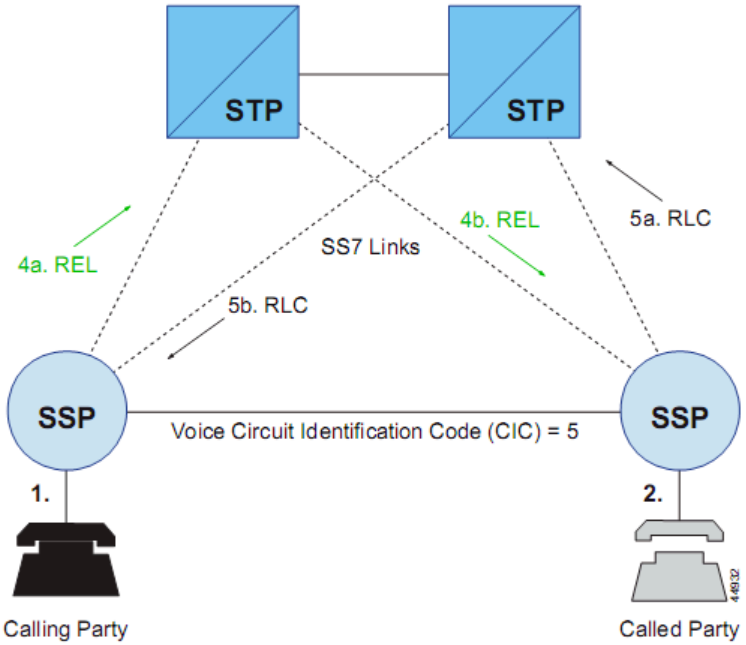


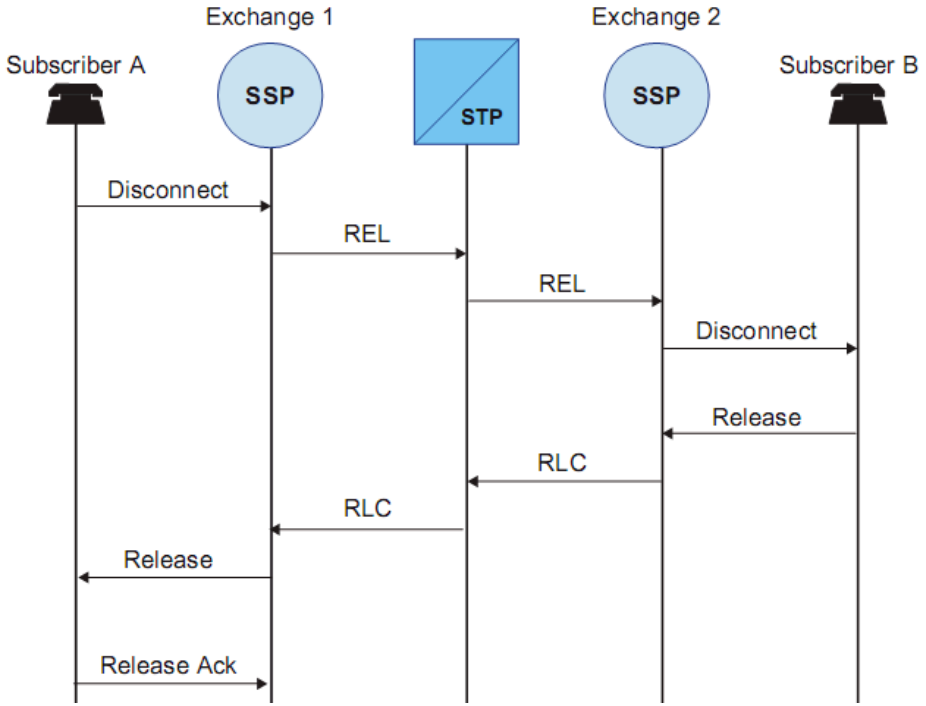
ISUP ACM

- An **address complete message** (ACM) is sent in the "backward" direction to indicate that the remote end of a trunk circuit has been reserved.
- The originating switch responds to an ACM message by connecting the calling party's line to the trunk to complete the voice circuit from the calling party to the called party.
- The calling party hears ringing on the voice trunk.



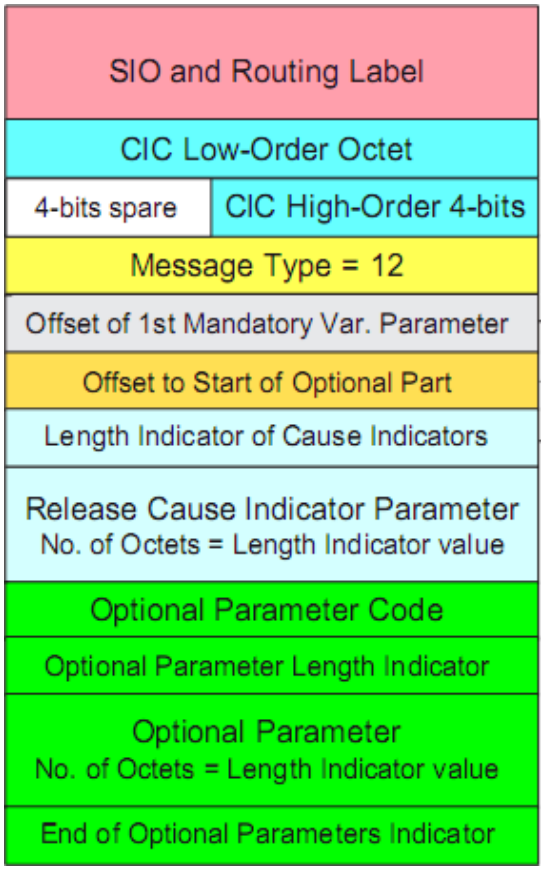
ISUP Call Release Flow





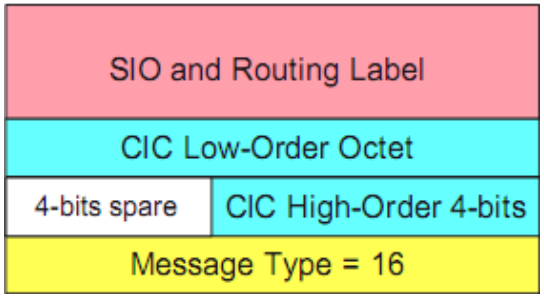
ISUP REL

- A **release message** (REL) is sent in either direction indicating that the circuit is being released due to a specified cause indicator.
- An REL is sent when either calling or called party **hangs up** the call (cause = 16).
- An REL is also sent back to the calling party if the called party is **busy** (cause = 17).
- **Attack: Selective DoS**

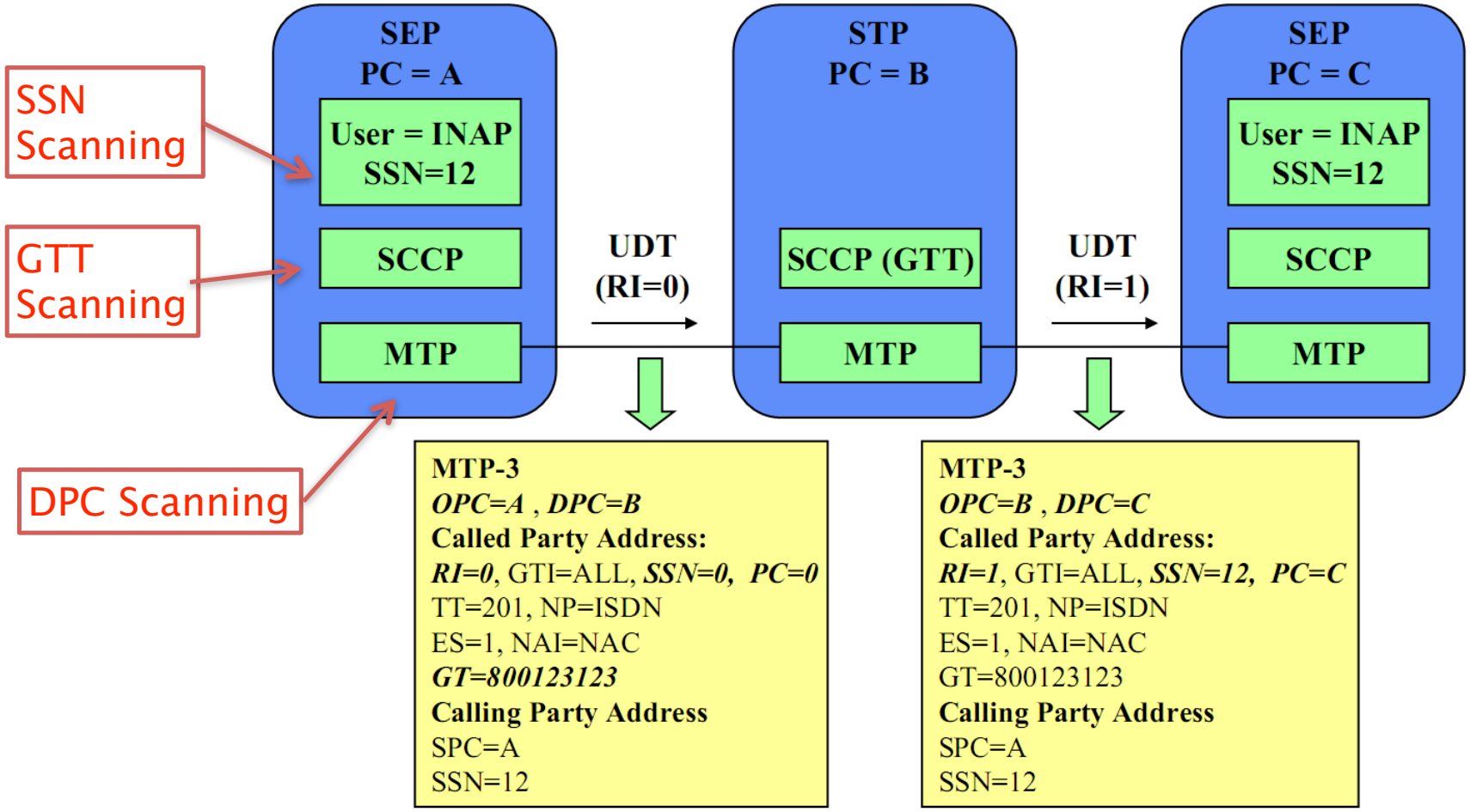


ISUP RLC

- A **release complete message** (RLC) is sent in the opposite direction of an REL to acknowledge the release of the remote end of a trunk circuit and to end the billing cycle, if appropriate.



GTT example


SSN Scanning
GTT Scanning
DPC Scanning
SEP
PC = A
User = INAP
SSN=12
SCCP
MTP
UDT
(RI=0)
STP
PC = B
SCCP (GTT)
MTP
UDT
(RI=1)
SEP
PC = C
User = INAP
SSN=12
SCCP
MTP
MTP-3
OPC=A , DPC=B
Called Party Address:
RI=0, GTI=ALL, SSN=0, PC=0
TT=201, NP=ISDN
ES=1, NAI=NAC
GT=800123123
Calling Party Address
SPC=A
SSN=12
MTP-3
OPC=B , DPC=C
Called Party Address:
RI=1, GTI=ALL, SSN=12, PC=C
TT=201, NP=ISDN
ES=1, NAI=NAC
GT=800123123
Calling Party Address
SPC=A
SSN=12

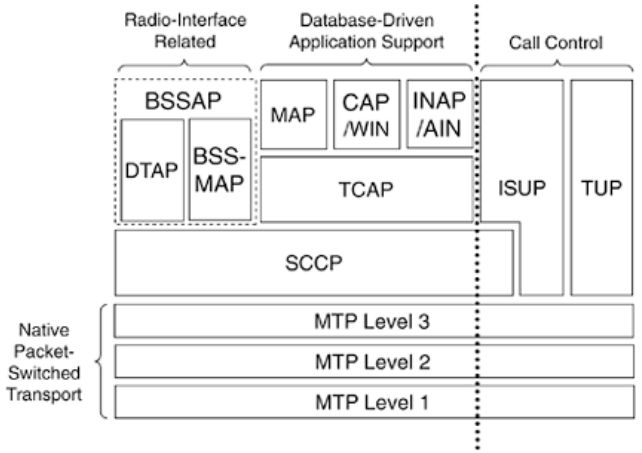
A Practical SS7 Information Gathering

Send Routing Info or monitoring anyone with a phone, anywhere...

P1 Security Inc, http://www.p1security.com

Geolocation & Information Gathering

- SS7 MAP message: SendRoutingInfo (SRI)
- Sends back the **MSC in charge**. Correlates to country.
- Nobody knows i'm not an HLR.



- **Real world usage: Identification for SPAM, 150 EUR for 10k, HTTP APIs & GW**
- **Attack: Global tracking and geolocation of any phone**

A practical SS7 attack

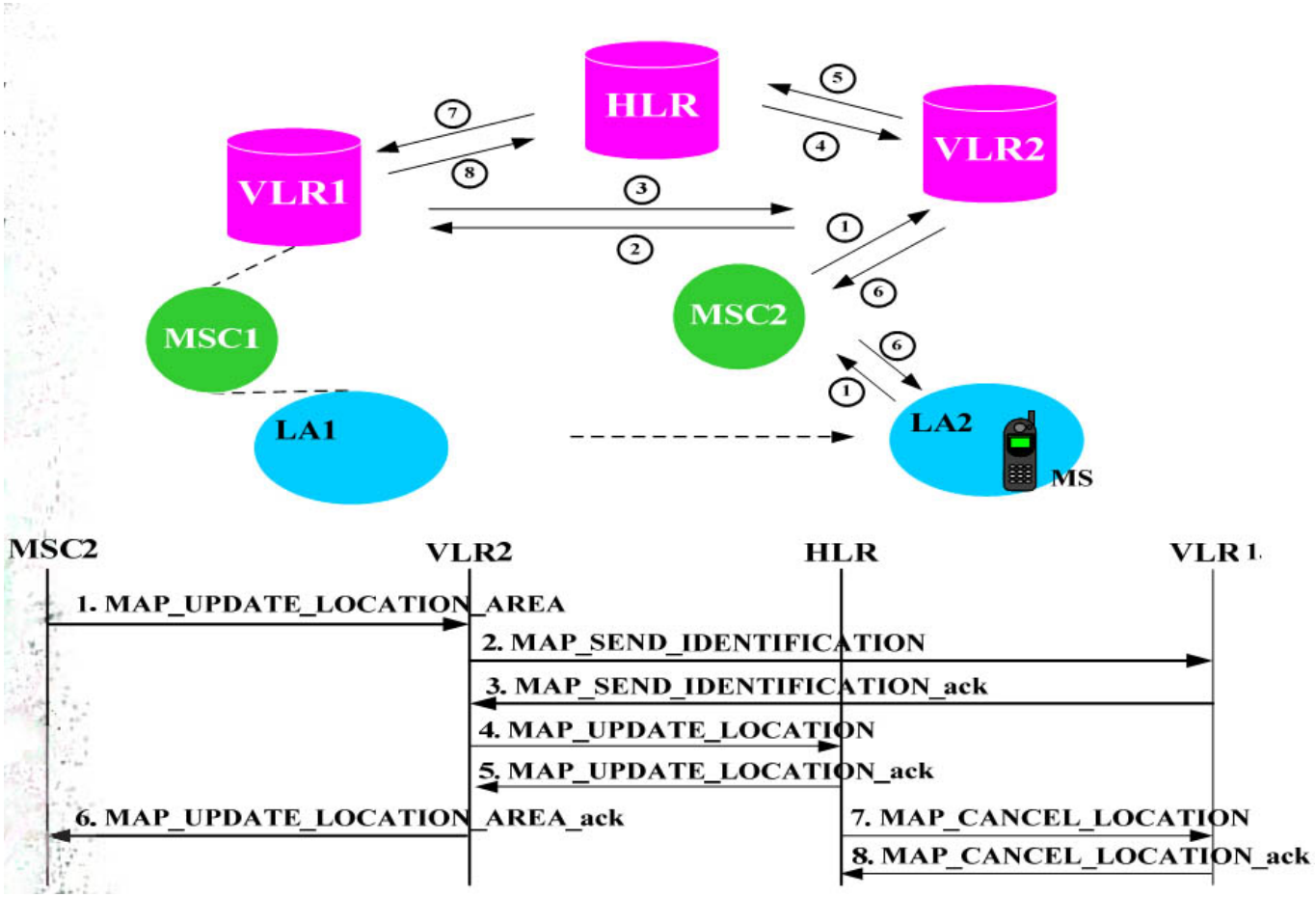
Disabling incoming calls to any subscriber

P1 Security Inc, http://www.p1security.com

Location Update process

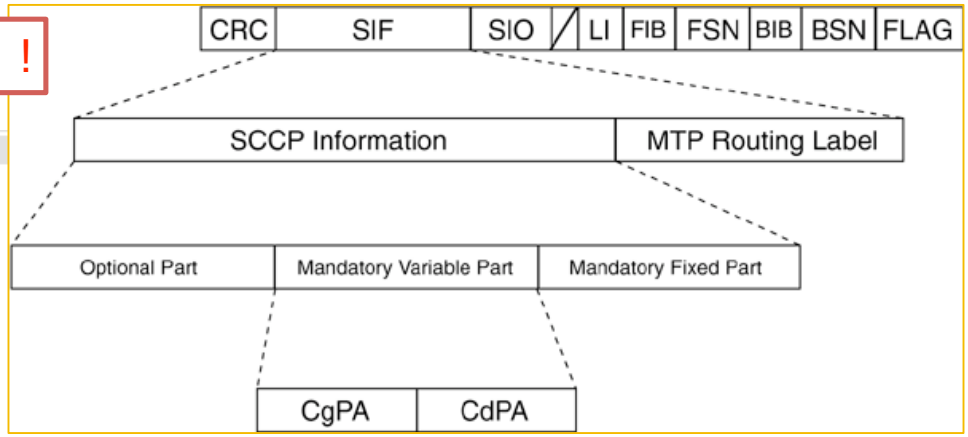
- The MAP **updateLocation (UL)** message contains subscriber's IMSI and MSC/VLR addresses.
- Once UL reaches the HLR, it changes the serving MSC/VLR address in subscriber's profile using MAP **insertSubscriberData** messages.
- From then on the HLR will use MSC/VLR addresses from it as addresses of real MSC/VLR.
- It's not even necessary to complete whole UL-ISD-ISDack-ULack transaction!
- The HLR will complete the operation by sending a MAP **cancelLocation** message to the serving VLR to delete subscriber's information from it.

Location Update Call Flow



Attack implementation

IMSI scanning / querying needed !




```
GSM Mobile Application
  Component: invoke (1)
    invoke
      invokeID: 1
      opCode: localValue (0)
        localValue: updateLocation (2)
      imsi: 520092999999999F9
      TBCD digits: 250029999999999
      msc-Number: 91839099999999
        1... .... = Extension: No Extension
        .001 .... = Nature of number: International Number (0x01)
        .... 0001 = Number plan: ISDN/Telephony Numbering (Rec ITU-T E.164) (0x01)
        Address digits: 380999999999
        Country Code: 380 Ukraine length 3
      vlr-Number: 91839099999999
        1... .... = Extension: No Extension
        .001 .... = Nature of number: International Number (0x01)
        .... 0001 = Number plan: ISDN/Telephony Numbering (Rec ITU-T E.164) (0x01)
        Address digits: 380999999999
        Country Code: 380 Ukraine length 3
      vlr-Capability
        Padding: 4
        supportedCamelPhases: C0 (phase1, phase2)
        Padding: 4
        supportedLCS-CapabilitySets: F0 (lcsCapabilitySet1, lcsCapabilitySet2, lcs(
```

Attack success

```
GSM Mobile Application
  Component: invoke (1)
    invoke
      invokeID: 1
      opCode: localValue (0)
        localValue: insertSubscriberData (7)
      msisdn: 919799999999F9
        1... .... = Extension: No Extension
        .001 .... = Nature of number: International Number (0x01)
        .... 0001 = Number plan: ISDN/Telephony Numbering (Rec ITU-T E.164) (0x01)
        Address digits: 79999999999
        Country Code: 7 Russian Federation,Kazakstan length 1
      category: 0A
      subscriberStatus: serviceGranted (0)
      teleserviceList: 4 items
        TeleserviceList: shortMessageMO-PP (34)
        TeleserviceList: shortMessageMT-PP (33)
        TeleserviceList: emergencyCalls (18)
        TeleserviceList: telephony (17)
      provisionedSS: 3 items
        Ext-SS-InfoList: forwardingInfo (0)
        Ext-SS-InfoList: forwardingInfo (0)
        Ext-SS-InfoList: forwardingInfo (0)
```

3G: New threat perimeters

The walled garden is opening up...

Femto Cell & user control

- Node B in user home, IPsec tunnel, SIGTRAN
- Real world example: ARM hw with RANAP
- Insecure
  - Untested hw
  - Unprotected IPsec
  - No regular pentest
  - No tools! Need for Binary vulnerability audit

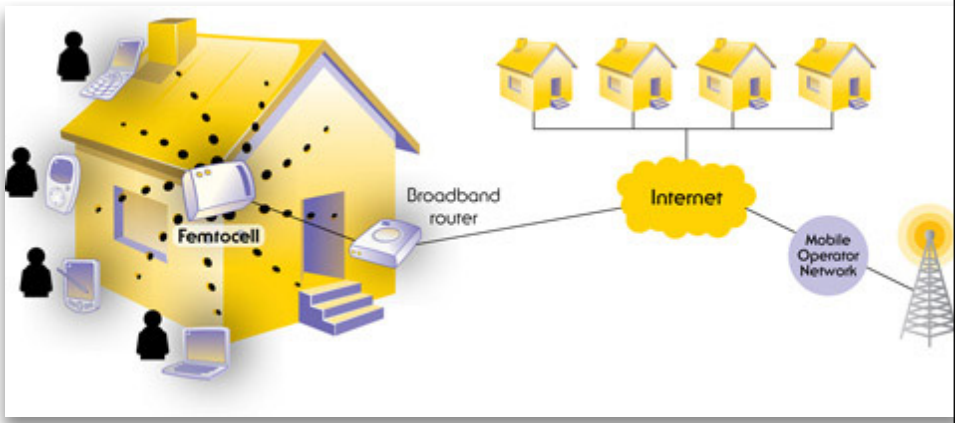


Image Credit: Intomobile

Femto-cell attack vectors

- Unaudited Proprietary software from Alcatel
  - Attack: **Binary vulnerability audit gives 0day**
  - Attack: **Vulnerable Linux 2.6 kernel**
- Global settings for IPsec tunnels
  - Attack: **Border access**
- Lack of SS7 and SIGTRAN filtering
  - Attack: **Injection of RANAP and SS7 in the Core Network**

Injecting SS7 through SIP

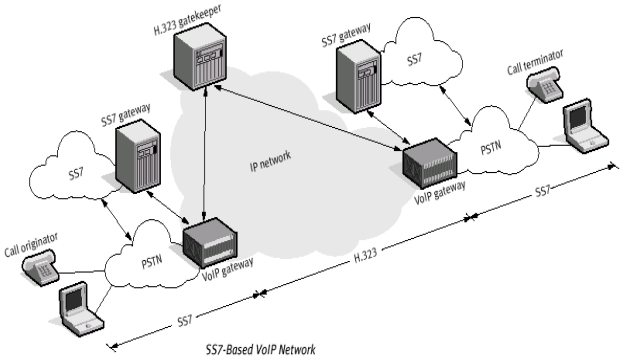
New perimeters, new entry points, new threats

Entry points in an SS7

- Peer relationships between operators
- STP connectivity
- SIGTRAN protocols
- VAS systems e.g. SMSC, IN
- Signalling Gateways, MGW
- SS7 Service providers
- GTT translation
- ISDN terminals
- GSM phones
- LIG (pentest & message relaying madness)
- 3G Femtocell
- And... SIP encapsulation

SIP to SS7 ?

- SIP is used to connect two SS7 cloud
- Support to bridge SS7 context through SIP



- SIP injection of SS7 adds a header to standard SIP headers
  - New SS7 perimeter, even for non-telco

Other ways into the phone system

- XOT – X25 over TCP
  - Legacy Systems
  - “No, we don’t have any x25 in our network anymore”
- Databases (Oracle, DAP, ...)
- Two standards...
  - Default Passwords, lame security level, large insecure binaries (made us create cxBin)
  - Ultra-segmented networks

Getting secure... again

How to secure an insecure network being more and more exposed?

P1 Security Inc, http://www.p1security.com

Tools and methods

- Pentest on all known perimeters
  - SS7 interconnect, Value Added Services
  - Core Network vs. Intranet
  - Femto Cell access network
  - SIP, Convergent services
- Reverse engineering, binary auditing, equipment, Consumer Acceptance Testing
- P1security SIGTRANalyzer, no other known.
  - Open Source and commercial developments

Current developments

- SCTPscan
  - Bridging support, instream scanning
  - Open source,
- SIGTRANalyzer
  - SS7 and message injection audit, information gathering, leak analysis,
  - Commercial product
- CXbin
  - Automated binary vulnerability auditor
  - Not only for telco now, general usage security tool

Conclusions

- SS7 is not closed anymore
- Industrializing the solution
  - From pentest to continuous testing (hardware and operations)
  - Security services and products
- Mindset are changing: more open to manage the SS7 security problem.

Credits

- Key2, Emmanuel Gadaix, Telecom Security Task Force, Fyodor Yarochkin
- Bogdan Iusukhno
- Skyper and the THC SS7 project
- All the 7bone security researchers

- CISCO SS7 fundamentals, CISCO press
- Introduction to SS7 and IP, by Lawrence Harte & David Bowler
- Signaling System No. 7 (SS7/C7) – Protocol, Architecture and Services, by Lee Dryburgh, Jeff Hewett

THANKS!

- Questions welcome
- Philippe Langlois, phil@p1sec.com
- More slides on http://www.p1security.com