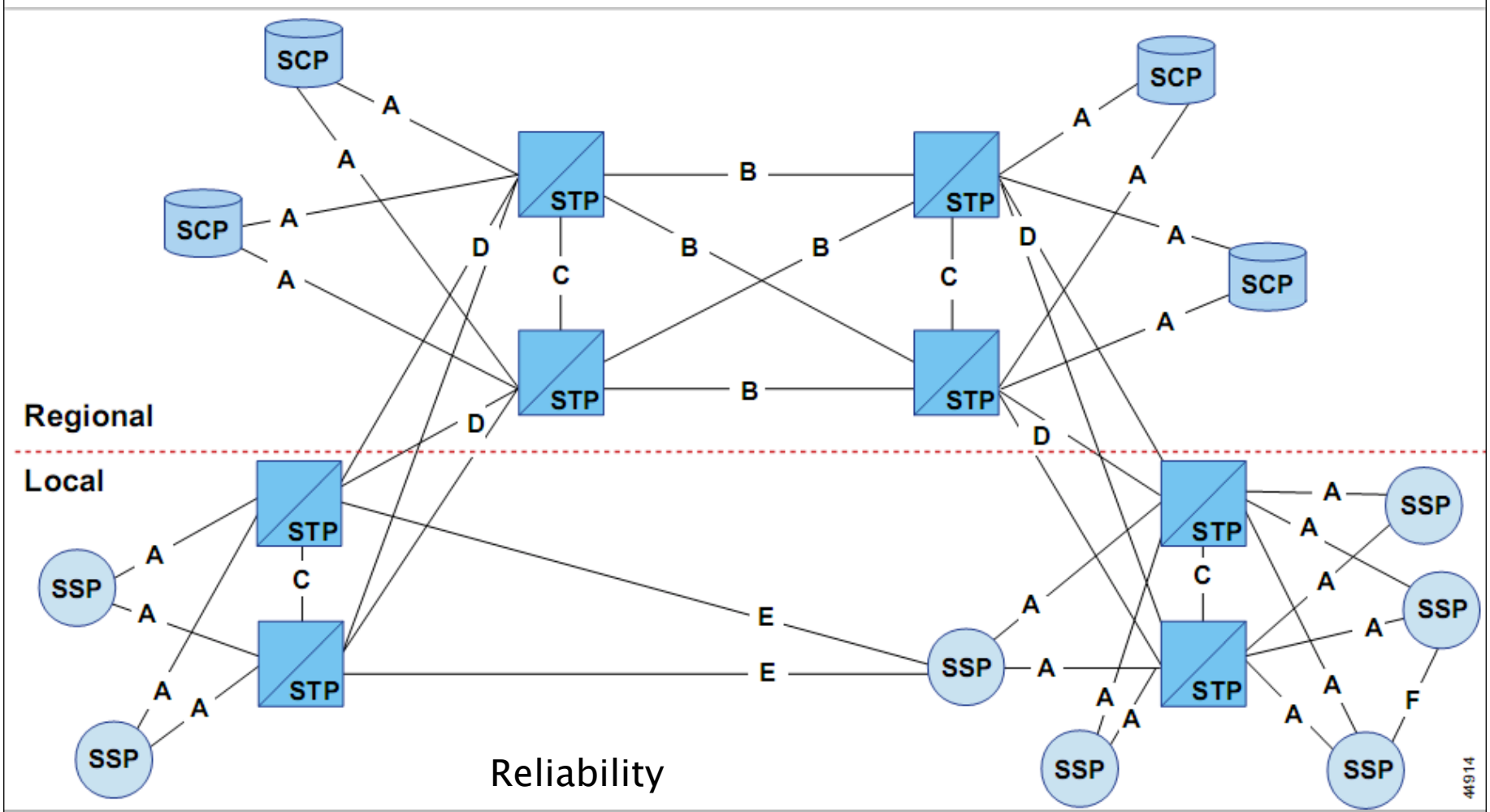
Telecommunications Infrastructure Security

Getting in the SS7 kingdom: hard technology and disturbingly easy hacks to get entry points in the walled garden.

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

SS7 network



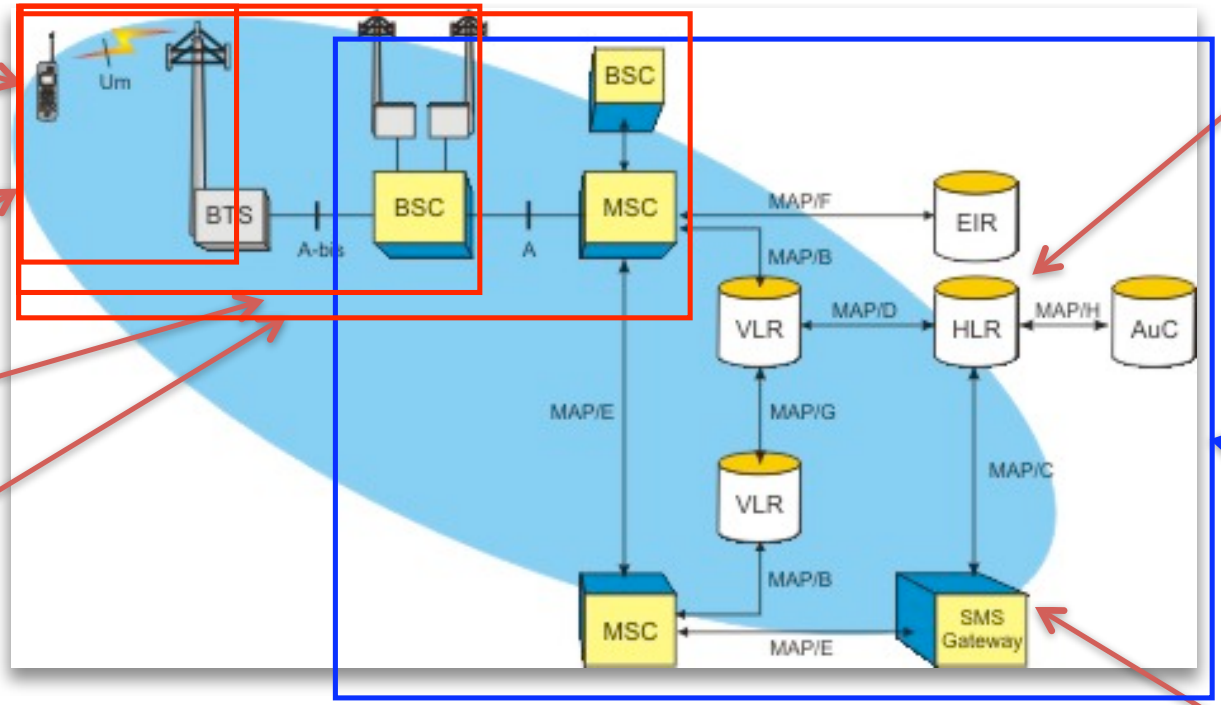
P1 Security Inc, http://www.p1security.com

Why do we have SS7?

Steve Jobs and Steve Wozniak in 1975 with a bluebox

- Thanks to hackers!
- 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

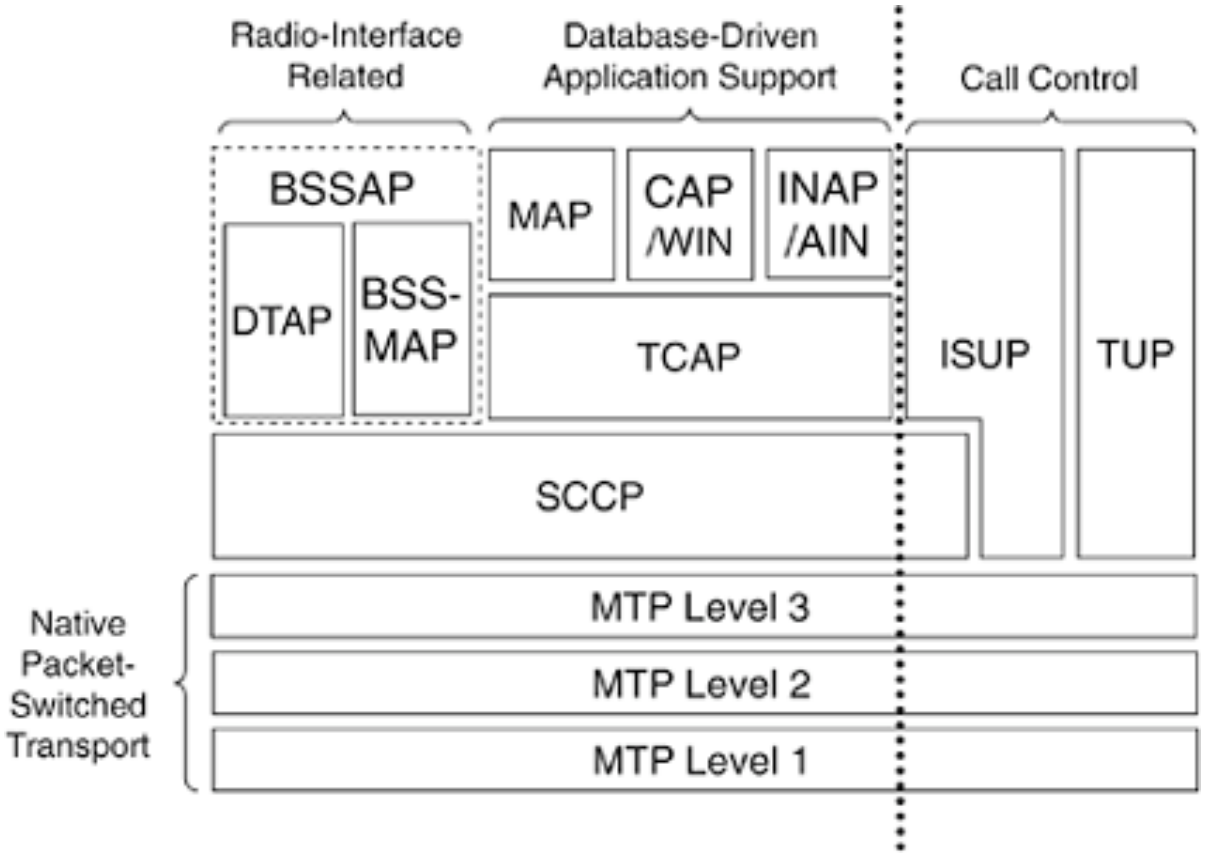
How to get in?



- **HLR/VLR** Home Location Register, Visitor Location Register
- **AuC** : Authentication Center (within HLR)
- **EIR** : Equipment Identity Register
- **MSC** : Mobile Switching Center
- **STP** : Signaling Transfer Point (i.e. Router)
- **LIG** : Legal Interception Gateway?

- **Illegal :** SQL Injection? Uhh?
- **Consulting** : Nahh... not possible! (?)
- **Product** : Yes please!

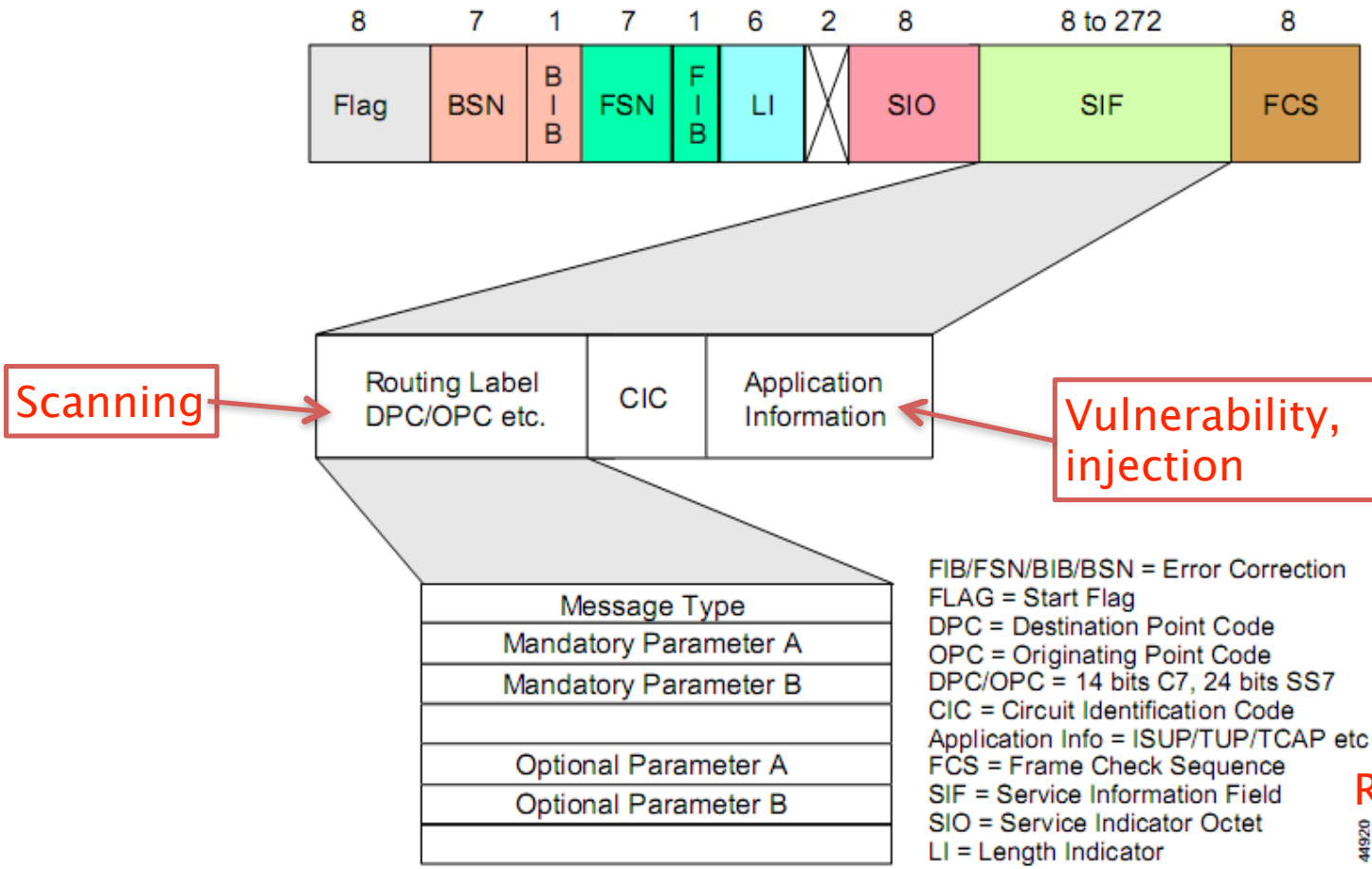
Under the hood: SS7 stack



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.

MSU: Message Signal Unit



Reach of MSUs!

Entry points in an SS7 network

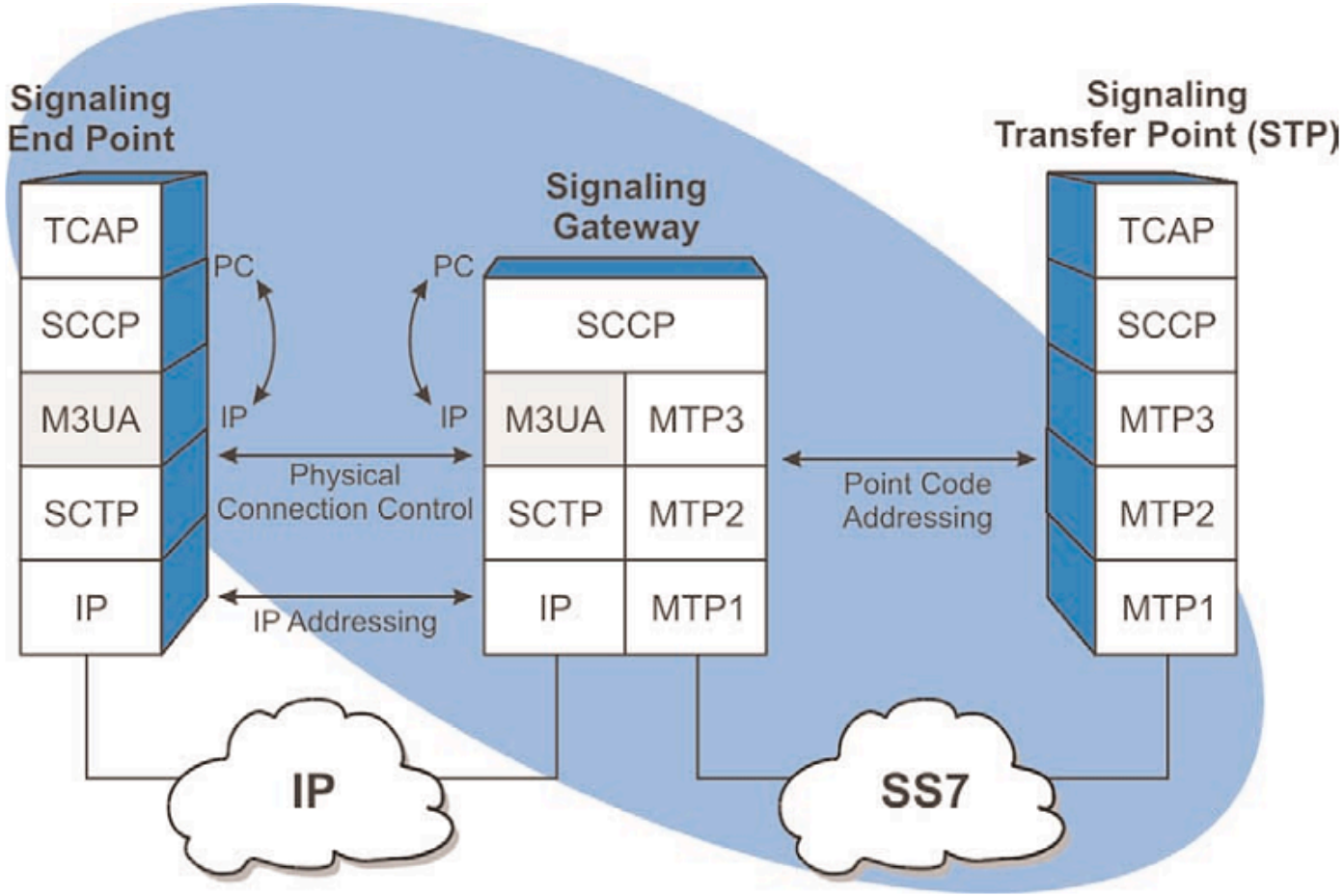
- Peer relationships between operators
- STP connectivity
- SIGTRAN protocols
- VAS systems e.g. SMSC, IN
- Signalling Gateways, MGW
- SS7 Service providers (GRX, IPX)
- GTT translation
- ISDN terminals
- GSM phones
- LIG (pentest & message relaying madness)
- 3G Femtocell
- SIP encapsulation

SS7 and IP: the SIGTRAN evolution and problems

Basics of IP telephony
SIGTRAN protocols & SCTP scanning

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

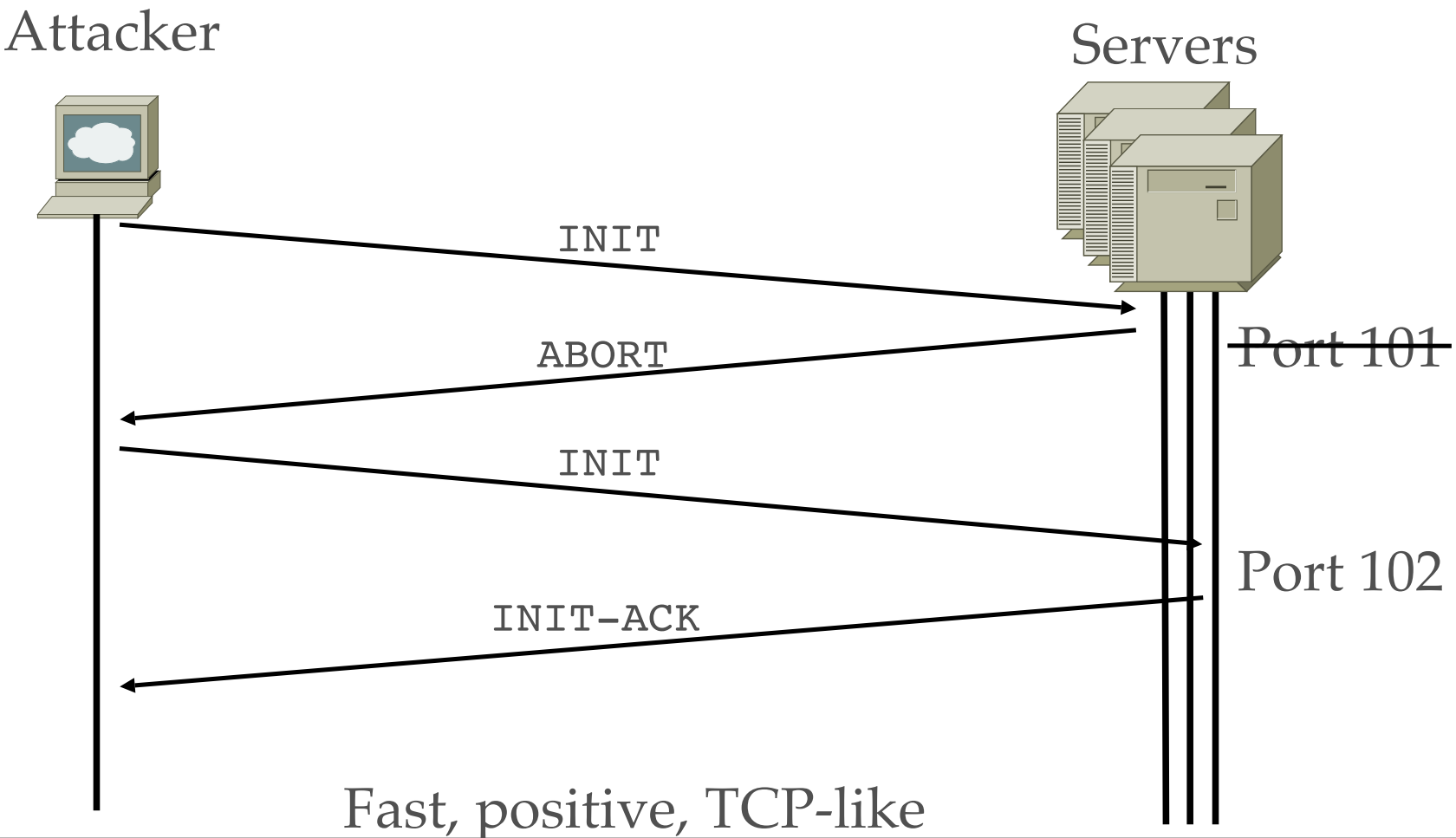
SIGTRAN Protocol: M3UA Protocol Adaptation Layer



SCTP Specs & Advantages

- RFC4960
  - 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 stealth scan



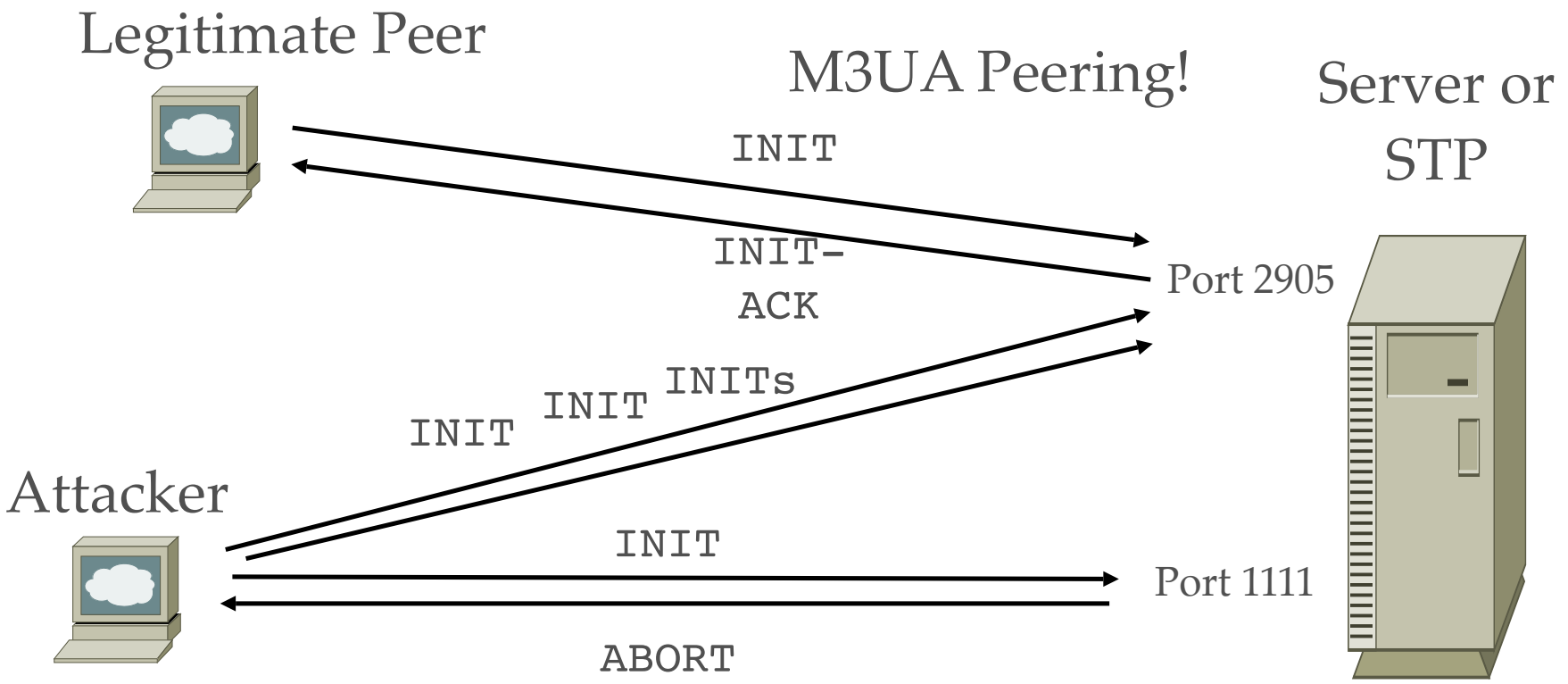
SCTPscan: Mapping SIGTRAN

- SCTPscan
  - Linux, BSD, MacOS X, Solaris, ...
  - IP scan, portscan, fuzzing, dummy server, bridge
  - Included in BackTrack
- 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

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#
```

UA Peering Tricks



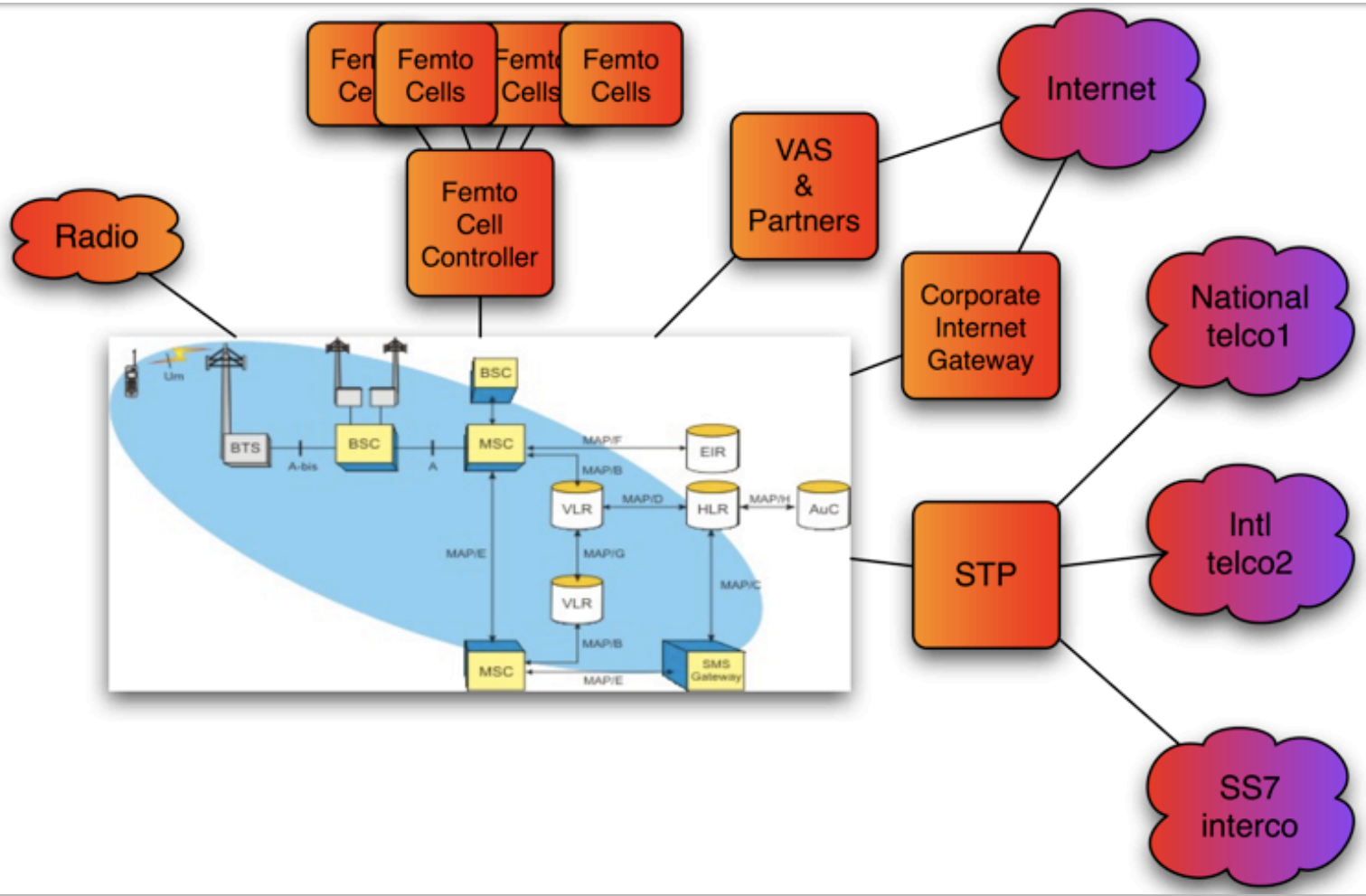
No answer on actual peering port: How rude! but useful

Scanning the SS7 perimeter

SS7 scanning and audit strategies

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

SS7 Perimeter Boundaries



STP as SCCP Firewall

- A “kind of” NAT (GTT and SSN exposure)
  - SubSystems allowed by STP, protection=route
  - SubSystem scanning & Message injection.
- NI (Network Indicator) Isolation
  - NI=0 : International 0, outside world
  - NI=2 : National 0, telco Internal
  - NI=3 : National 1, country-specific
- List of Signaling Point Code for each perimeter, automation needed.

International SPC List

3-246-1	…	GoodWillComm Ltd.
3-246-2	…	Service Ltd.
3-246-3	…	Black Sea Telecom Ltd.
3-246-4	…	Mobitel Ltd
Germany		
2-033-0	Düsseldorf	Viaphone GmbH
2-033-1	Frankfurt	Viaphone GmbH
2-033-2	Frankfurt	Vodafone D2 GmbH
2-033-3	Düsseldorf	Vodafone D2 GmbH
2-033-4	Hamburg	Talkline GmbH
2-033-5	Haar	CompleTel GmbH
2-033-6	Stuttgart	Tesion Communikationsnetze Sudwest GmbH & C KG
2-033-7	Frankfurt	KPN Telecom BV
2-034-0	Stuttgart	Star Telecommunications Deutschland GmbH
2-034-1	Frankfurt am Main	ICS Interactive Communications Services GmbH
2-034-2	Düsseldorf	Storm Telecommunications Ltd.
2-034-3	Düsseldorf	KDD Telecomet Deutschland GmbH
2-034-4	Düsseldorf	Interurbana Net GmbH

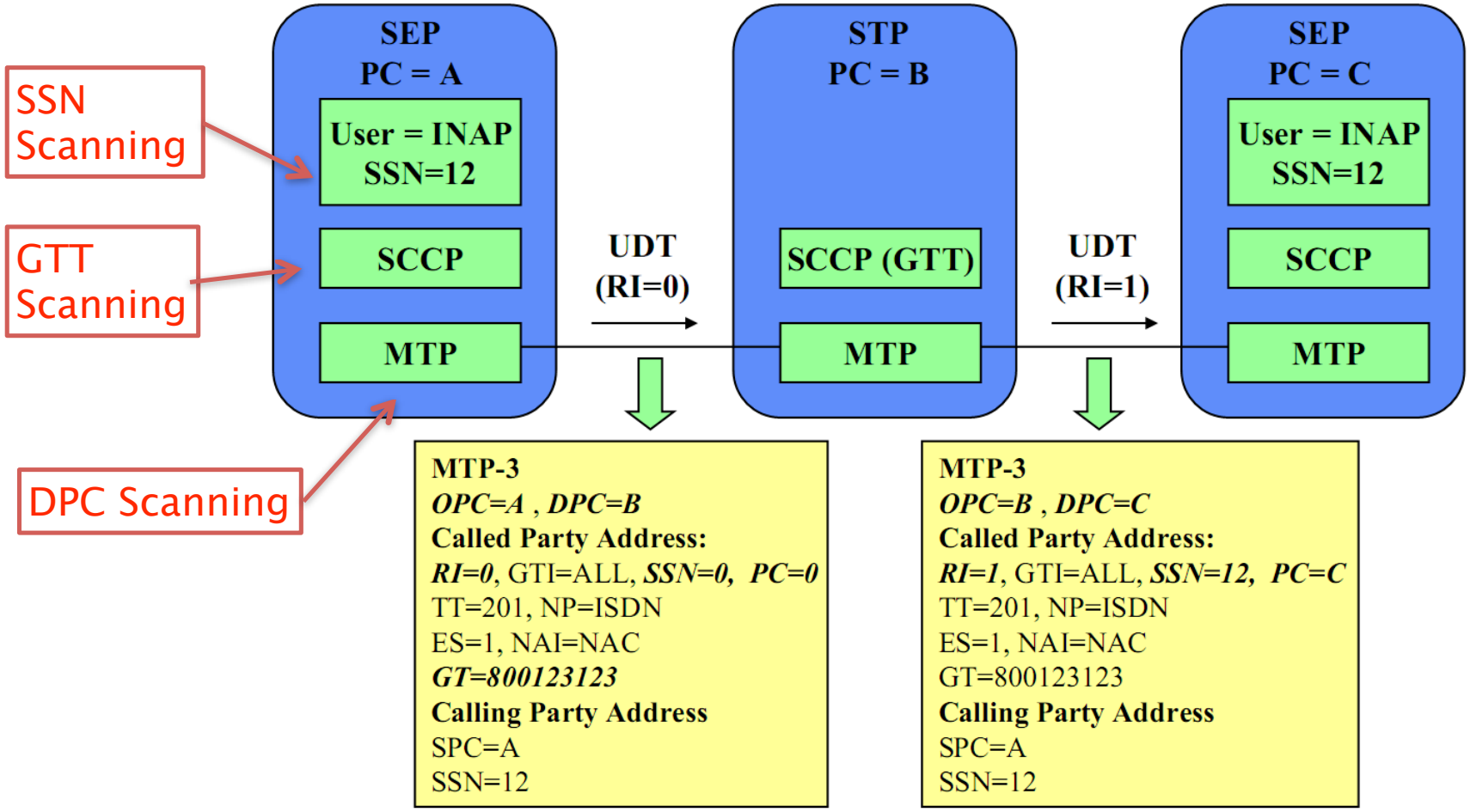
Understanding SPC

- Hints on the address plan and network topology
  - Different SPC lengths
    - ITU : 14 bits
    - ANSI : 24 bits
  - Many different SPC formats
    - Decimal
    - ITU: 3-8-3, 5-4-5,
    - ANSI: 8-8-8
- ss7calc
  - Like ipcalc, Open Source,
  - http://www.p1sec.com/corp/research/tools/ss7calc/

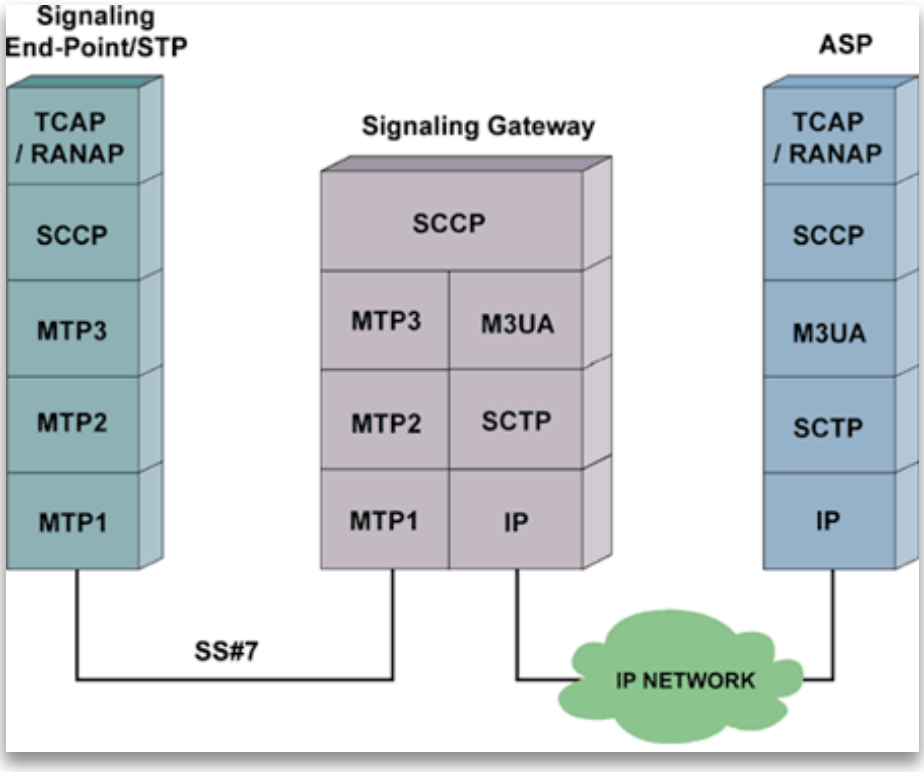
Comparison with TCP/IP

TCP/IP	SS7
IPsec endpoint scan, MPLS label scan, VLAN tag scan	SCTP endpoint scan
Arp or Ping scan	MTP3 or M3UA scanning
Ping scan using TCP SYN	SCCP DPC scanning
TCP SYN or UDP port/service scanning	SCCP SSN (SubSystem Number) scanning
Application (*AP) traffic injection (e.g. MAP, INAP, CAP, OMAP...)	Service-specific attacks and abuses (e.g. attacks over HTTP, SMB, RPC, ...)

STP boundary: attacking SS7



Stack de-synchronization: more exposure & attacks



- Different stacks standardized by different people with different goals

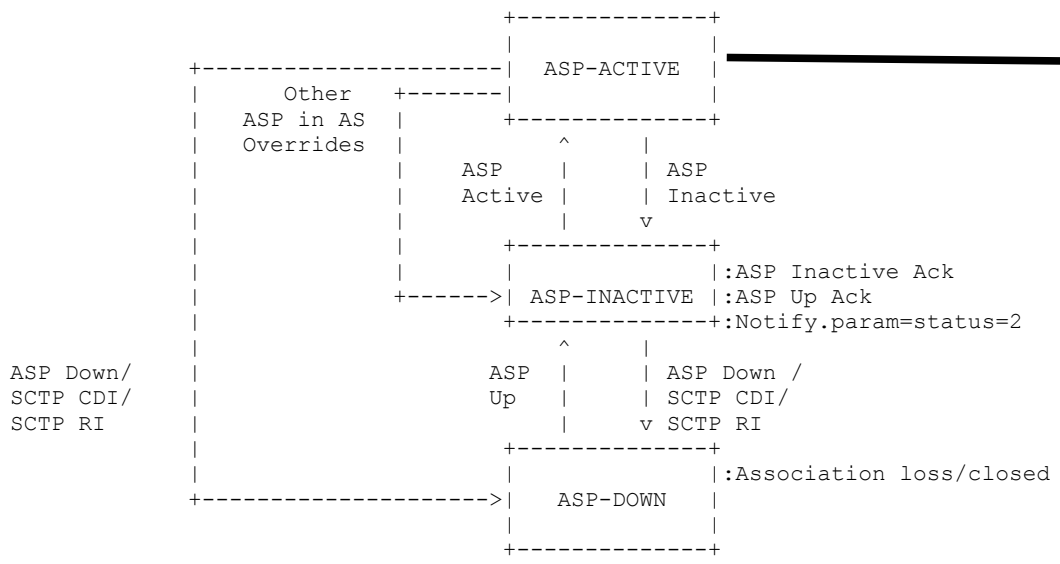
→ SubSystem scanning

→ Topology discovery (needed for IP-based topologies)

- Action available depends on State Machine's state
- Needs a special engine to inject attack at proper time/state

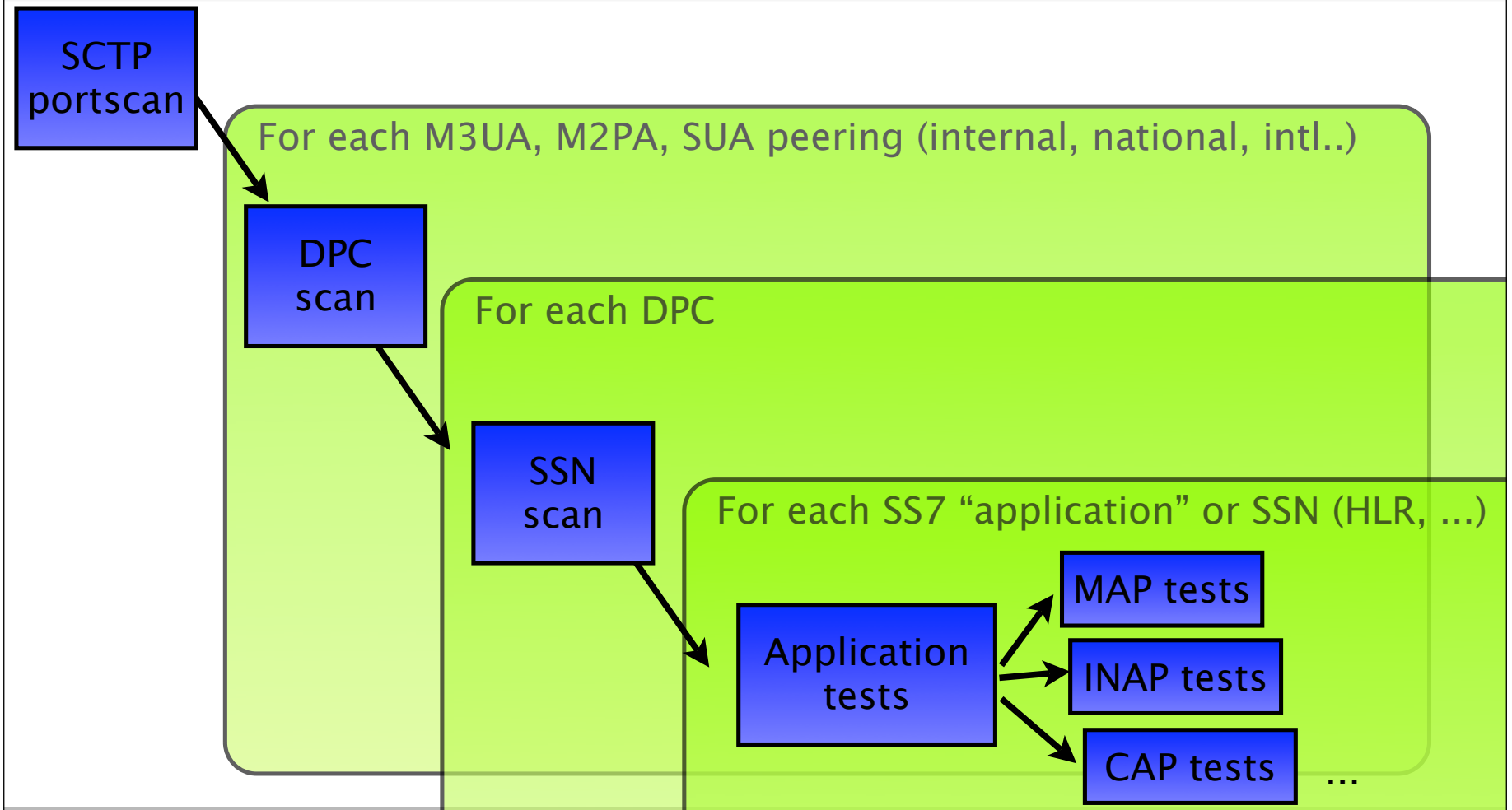
M3UA Finite State Machine

Figure 3: ASP State Transition Diagram, per AS



- M3UA test
- SCCP tests
- MAP tests
- INAP tests
- Each depends on configuration

SS7 Audit Strategies

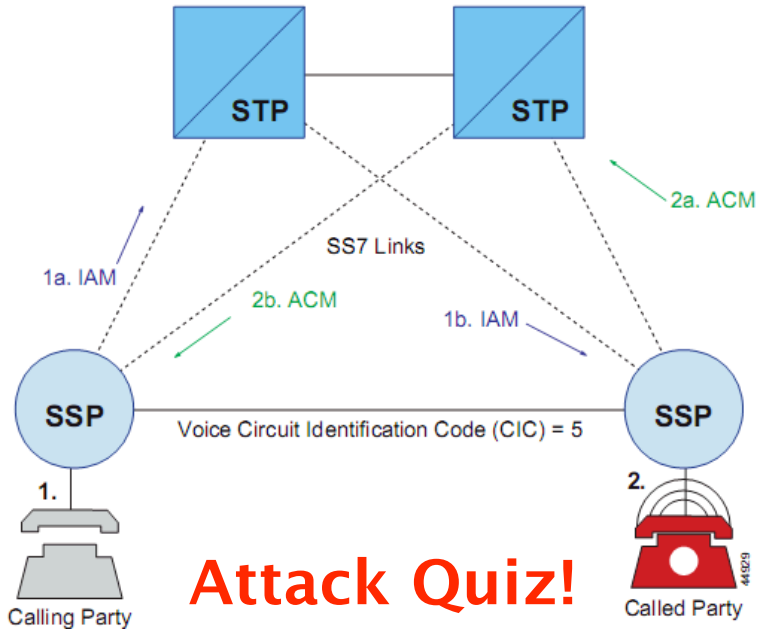


Example of SS7 protocol: ISUP & related attacks

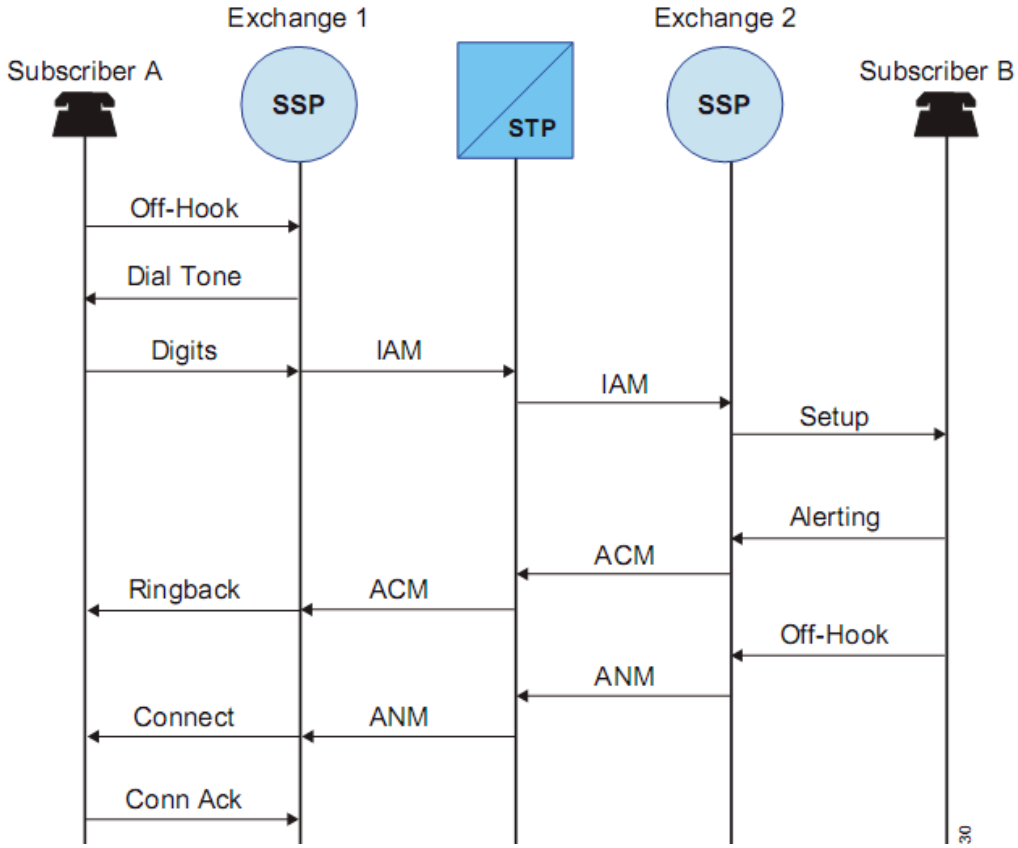
ISUP message types
ISUP call flows

ISUP Call Initiation Flow

IAM attack: Capacity DoS

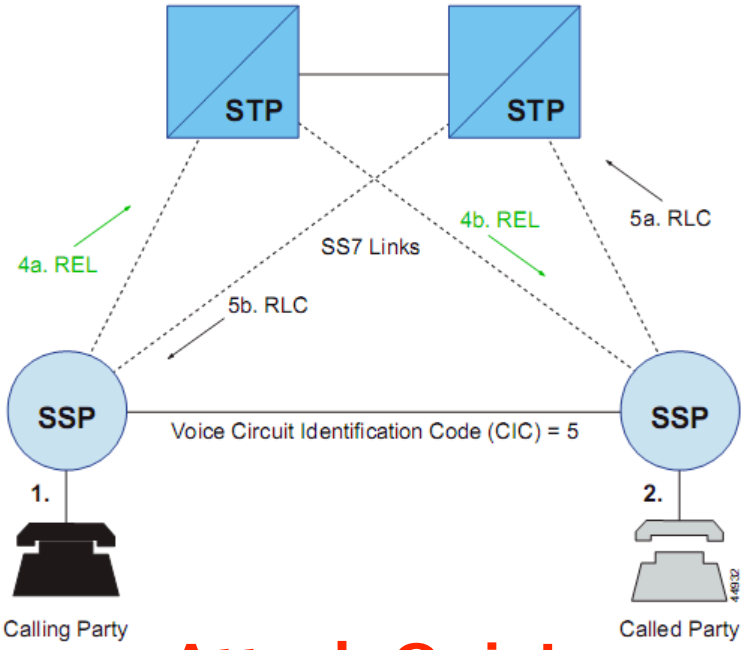


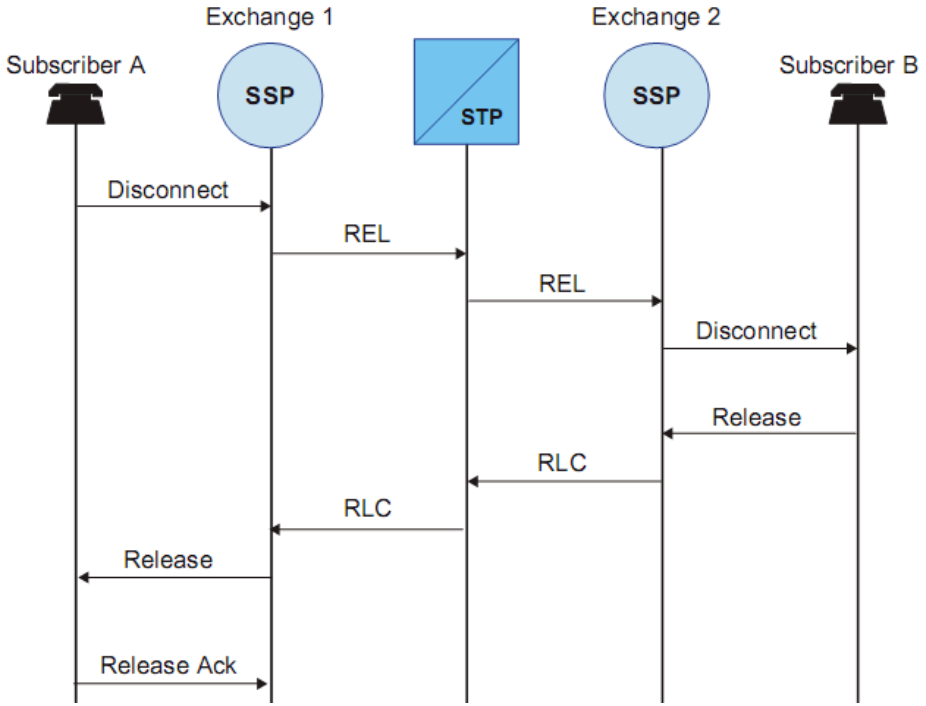
Attack Quiz!



ISUP Call Release Flow

REL attack: Selective DoS





Attack Quiz!

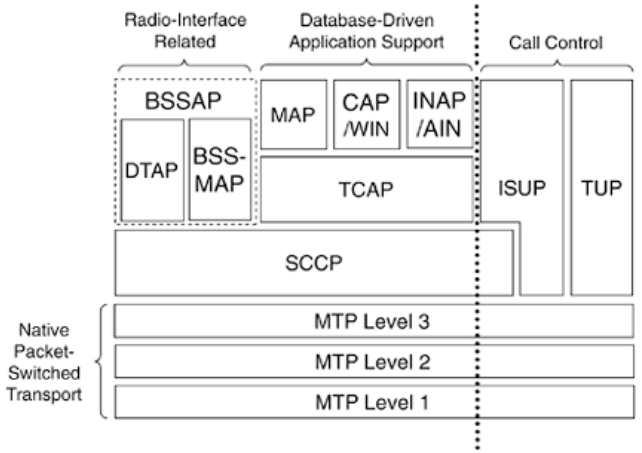
A Practical SS7 Information Gathering

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.



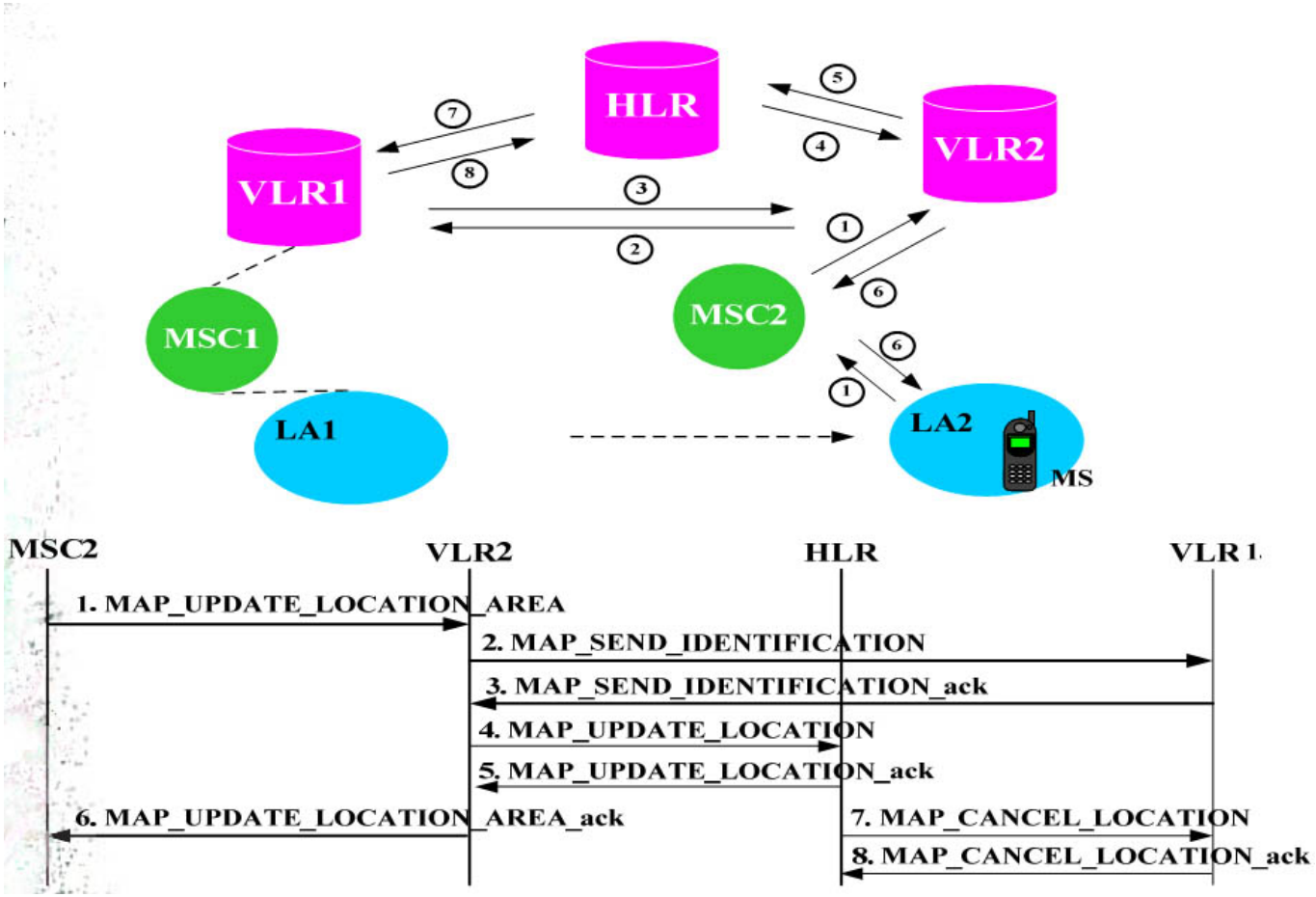
- **Real world usage: Identification for SPAM, 150 EUR for 10k, HTTP APIs & GW**
- **Attack: Global tracking and geolocation of any phone**

A practical, user-targeted SS7 attack

Disabling incoming calls to any subscriber

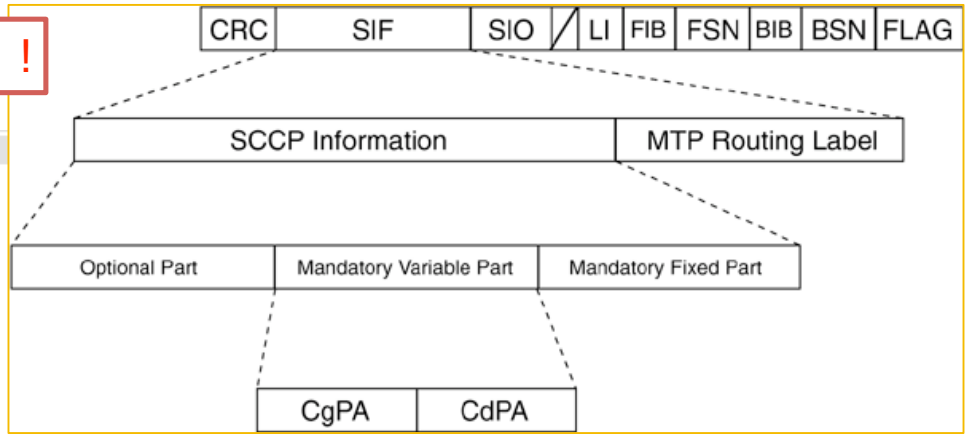
P1 Security Inc, http://www.p1security.com

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)
```

New perimeters, New threats

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

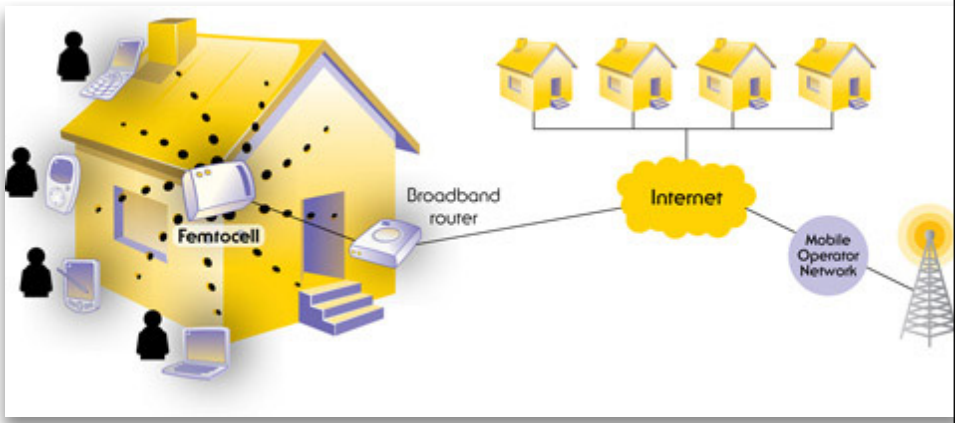


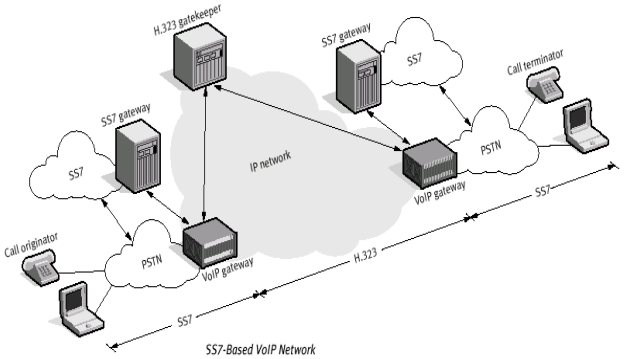
Image Credit: Intomobile

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**

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

Getting secure...

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

Tools and methods

- Manual SS7 audit & pentest (hard!)
- Product Testing (Customer Acceptance)
  - telco equipment reverse engineering and binary auditing
  - Huawei MGW (vxWorks + FPGAs), Femtos, ...
- Automated scan of SS7 perimeters
  - SS7 interconnect (International and National)
  - Core Network
  - Femto Cell access network
  - SIP & Convergent services
  - Hint: P1sec SIGTRANalyzer product ;-)

Current developments

- SCTPscan
  - Bridging support, instream scanning
  - Open source
- ss7calc – SS7 Point Code calculator
- 7Bone – Open Research SS7 backbone
- P1sec SIGTRANalyzer
  - SS7 and SIGTRAN vulnerability scanning
  - Commercial product

Conclusions

- SS7 is not closed anymore
- SS7 security solution are industrializing
  - Pentest to continuous scanning
  - Security services and products
- Mindset are changing: more open to manage the SS7 security problem, education still needed.
- Governments put pressure on telco, National Critical Infrastructure Protection initiatives etc..

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
- Slides and Tools on http://www.p1security.com