Security & Vulnerability Analysis of Wireless Messaging Protocols & Applications

Atique Ahmed Khan

Pak Con 2004, Karachi

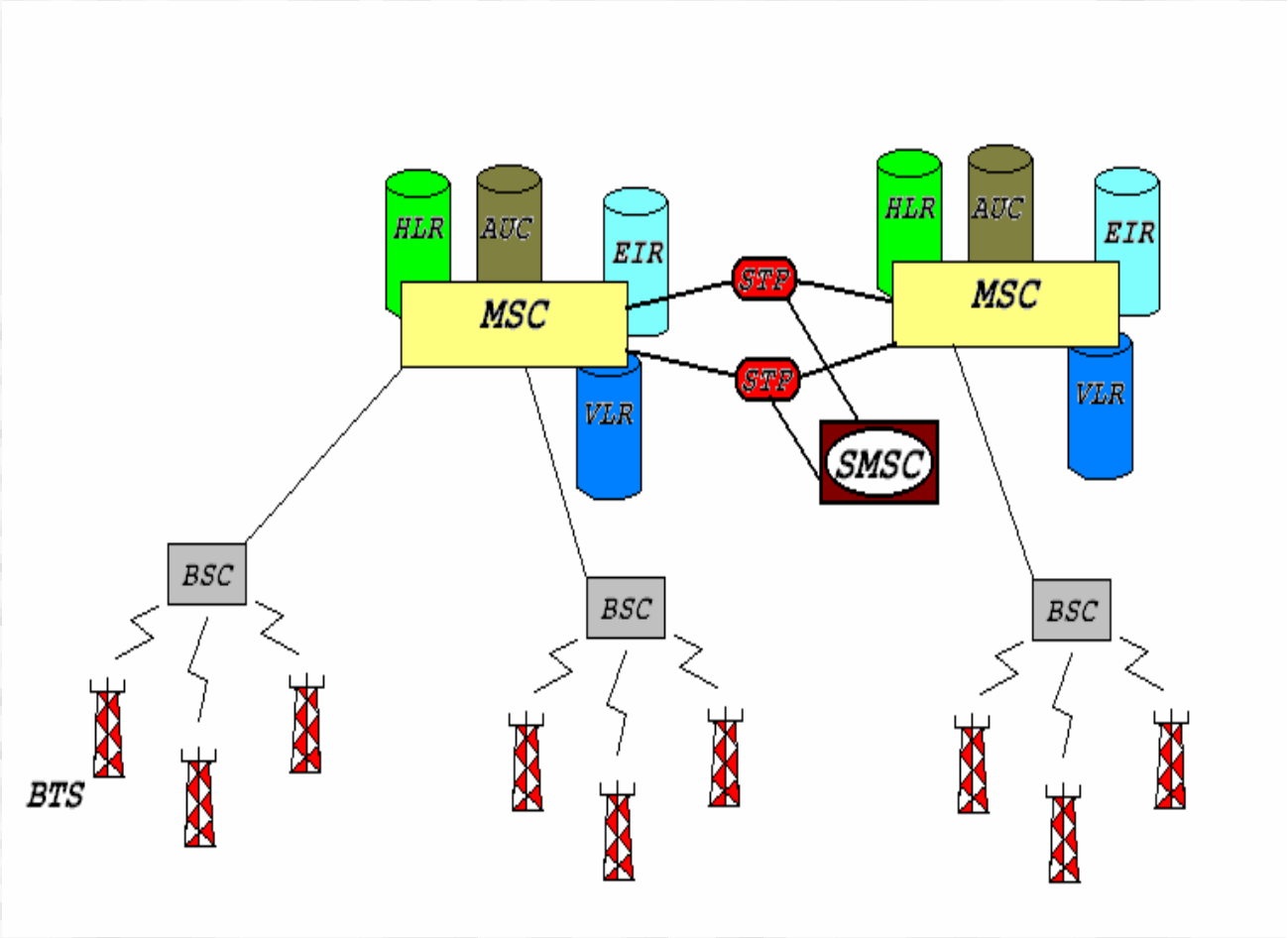
Agenda

- Cellular Communication Networks
- Wireless Messaging Protocols
- SMPP Over TCP/IP
- Wireless Messaging Applications
- SMS Vulnerability Analysis
- Improving the Security
- Conclusion

Cellular Communication Networks

Pak Con 2004

BTS
BSC
MSC
Registers
STP
SMSC



Base Transceiver Station (BTS)

- Air interface to the mobile
- Wireless link from mobile phones
- Covers one cellular area

Base Station Controller (BSC)

- Governs multiple BTS
- Controls handovers, transmission power
- Divides frequency slots among BTS

Mobile Service Switching Center (MSC)

- Heart of communication network
- Performs call controlling
- Monitors registration, authentication, location updating, roaming
- Uses many registers

The Registers

- **Home Location Register (HLR)**
- **Visitor Location Register (VLR)**
- **Authentication Center (AUC)**
- **Equipment Identity Register (EIR)**

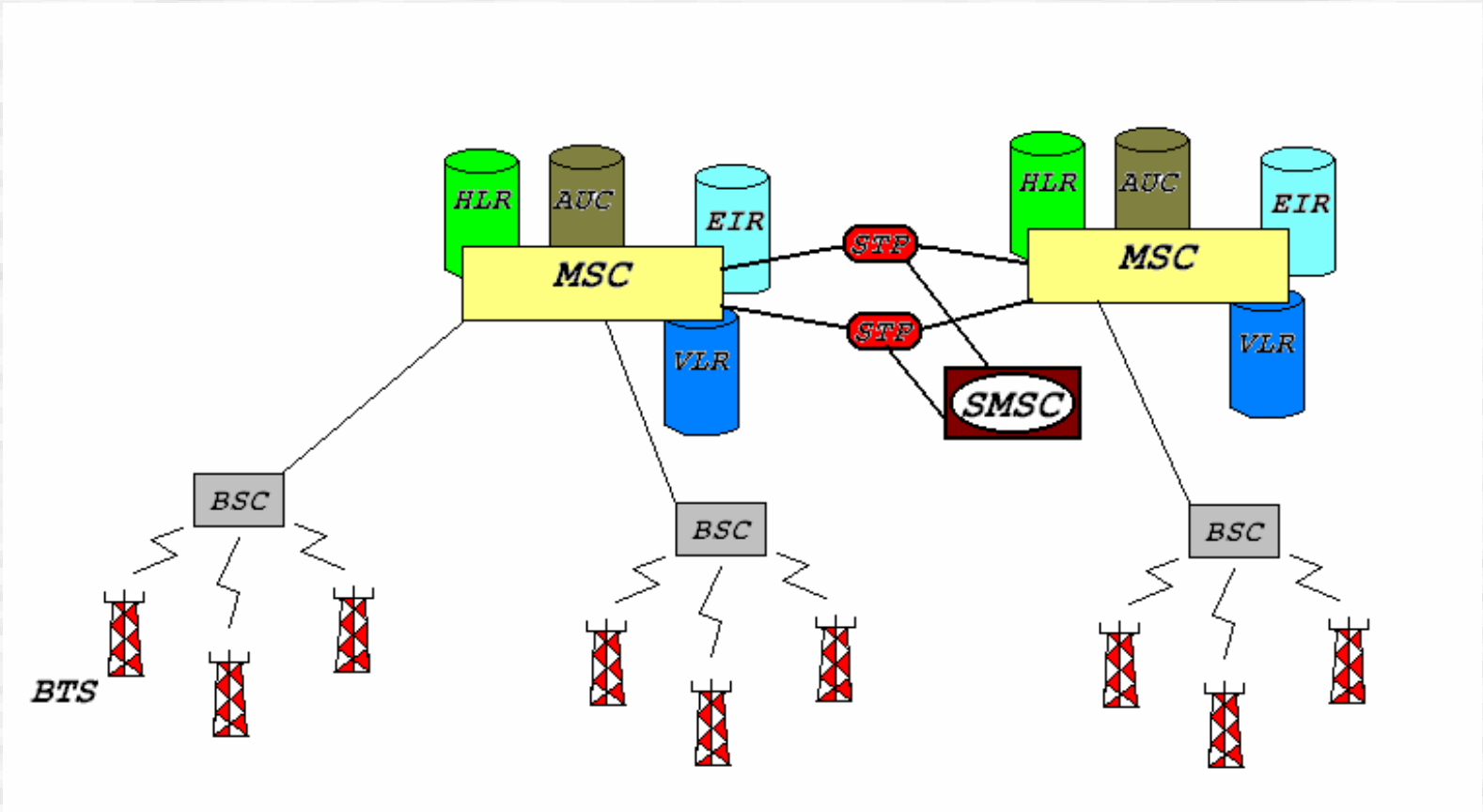
Signaling Transfer Point (STP)

- Acts as a router
- Responsible for all kinds of data transportation
- Many carriers use IP Network as inter-STP connections
- Uses SS7

Short Message Service Center (SMSC)

- The place where all SMS are stored
- Uses store-&-forward technique
- Open to IP network
- Uses specific protocols over TCP/IP like SMPP, UCP and CIMD2

Putting It All Together



Wireless Messaging Protocols

Short Message Peer to Peer (SMPP)

- Most popular SMS protocol
- Developed by SMS Forum
- ESME can bind/unbind to SMSC using SMPP
- ESME can submit or query SMS over SMPP
- Can have SS7 or TCP/IP as underlying protocols

Universal Control Protocol (UCP)

- Formed by ETSI for paging networks
- Strong competitor to UCP
- Content-based reverse charging
- Popular in Western Europe
- Supported by many SMSC vendors

Open Interface Specifications (OIS)

- Originated by Sema Group, now Schlumberger
- Not so popular
- Makes Vodafone network accessible by ESME

Computer Interface to Message Distribution (CIMD)

- Formed by Nokia for their proprietary SMSC
- CIMD2 is used nowadays
- Supports sockets and serial ports
- Only Nokia and CMG are its users

Telocator Alphanumeric Protocol (TAP)

- American originated protocol for 2-way paging networks
- Supposed to be a legacy protocol
- Used as interface to paging and SMS systems
- Does not support ring tone and multi media message transfer

Simple Mail Transfer Protocol (SMTP)

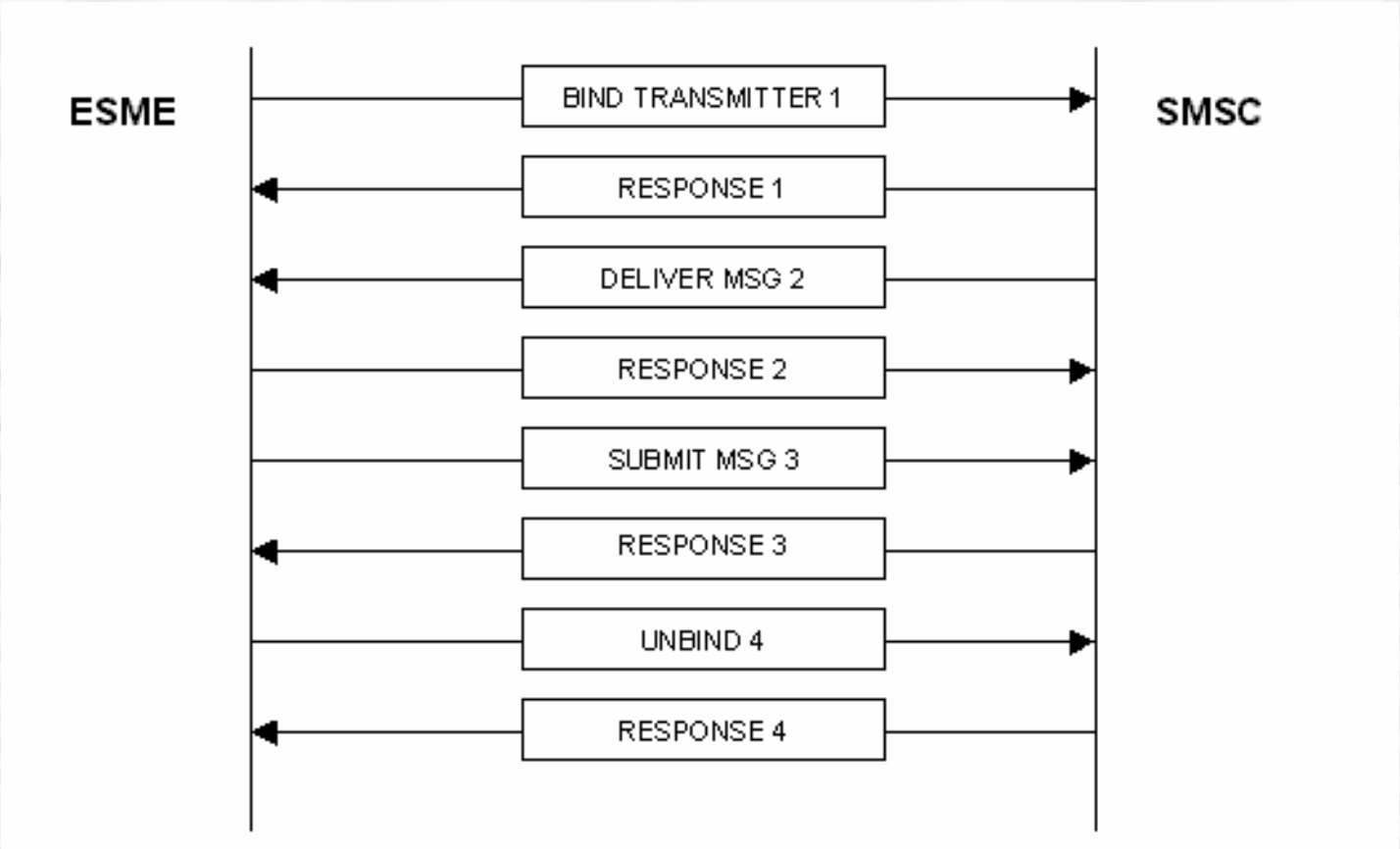
- Formed by IETF for Email transfer
- Used by mobile phones for Web2SMS, MMS transmission and mail2mobile services
- Also used for facsimile services

SMPP over TCP/IP

SMPP PDU				
PDU HEADER (MANDATORY)			PDU BODY (OPTIONAL)	
COMMAND LENGTH	COMMAND ID	COMMAND STATUS	SEQUENCE NUMBER	PDU BODY
4 OCTETS	LENGTH = (COMMAND LENGTH VALUE - 4) OCTETS			

- SMPP packet can travel over SS7 and TCP/IP networks
- APIs are used to make ESME SMS-powered
- Same packet for command and data transfer between ESME and SMSC

A Message Transfer to SMSC



Current Wireless Messaging Applications

Types of Applications

- Information Services
- Location-Based Services (LBS)
- Communication & Entertainment Services

- Citibank's Citialerts
- Shazam Entertainment
- Jurong Point Shopping Center
- KDDI
- BattleMail KungFu
- SMS2Email
- Instant Messaging

SMS Vulnerability Analysis

- Attacks can cause serious blow to Quality of Service (QoS), Security, Privacy and normal routine of life
- Inherited Network flaws also make this system more vulnerable

Categories of Vulnerable Areas

- SMSC-Kernel
- Connection between ESME and SMSC
- Air Interface of GSM
- Network Equipments of GSM
- Operating system of mobile phone

Denial of Service (DOS)

- SMSC has a public IP address
- Firewalls increase the latency in message transmission
- DOS attack waste the bandwidth, if not compromising the system
- What about DDOS?

Service Interruption

- Similar to DOS
- Poorly tested platform, containing several holes and 0-day exploits
- Like 'WinNuke' vulnerability
- Launched by deliberately crafted SMPP packets

Service Hijacking

- Control over compromised target
- Unauthorized access can damage the network
- Message capturing, alteration and blocking of data transmission

Buffer Overflow

- Part of Service Hijacking
- Occurs due to uncheck bounds of allocated memory
- Can cause arbitrary command execution
- Buffer overflow can occur in OS underlying SMSC, database or server

Password Compromise

- Accomplished by Social Engineering and Brute force technique
- Password for SMSC can be detected using trial & error
- Piggybacking

Packet Sniffing

- Capturing of packet from network
- Captured packets can give valuable information

Spoofing

- False packets from some other source
- Packets can be created by any packet creation utility
- Obfuscates the identity of sender
- Malicious control message under the disguise of trusted user

Radio Frequency Jamming

- Purely over Air Interface
- Disrupts SMS as well as voice calls
- Jamming equipment generates noise in GSM signal spectrum

Operation Support System Penetration

- More important than Network Equipment is OSS
- Holds crucial information like billing and GSM network structure
- OSS is accessible via IP Network

Mobile Code

- SMS Spam
- Mobile Virus
- SMS Crash

Improving the Security

Air Interface Algorithm

- Radio communication encryption must be enhanced
- Currently used algorithm is A5 and has four levels of encryption
- A5/3 is recommended
- A5/3 has been broken in 1999

Proprietary Encryption

- For intra-network communication
- Must use state of the art cryptographic technique
- White list of devices connected to IP Network must be maintained

Firewalls

- SMSC as well as OSS must be behind firewall
- Firewall must be properly configured
- IDS must be installed
- SSL, VPN or other secure connection must be used

Mobile Security

- Proper Virus Scanners installation with mobile phone operating system
- Unsigned code must be disabled
- Beware from Malware and suspicious Emails

Conclusion

- Wireless Messaging is a very effective medium
- EMS, MMS, LBS, VR technologies can increase its importance manifolds
- Migration of Communication Equipments over IP networks may increase security threats
- Precautions and effective measures must be taken to secure sensitive applications
- If you think it is secure…think again!

Thank You!