Metanoia, Inc.

Critical Systems Thinking™

Network Infrastructure Security in Cellular Data Networks: An Initial Investigation

Kavita Barapatre, Nirlesh Koshta, IIT Bombay, Mumbai, India
Vishal Sharma, Metanoia, Inc. and IIT Bombay
Fabio Ricciato, Forschungszentrum Telekommunikation Wien (FTW), Vienna, Austria

Outline of the Talk

- **Motivation – why worry about *infrastructure security*?**
- **GSM /GPRS network architecture & critical interfaces**
- **Attacks exploiting security loopholes in GSM/GPRS**
- **Impact of unwanted traffic: viruses, worms, trojans, …**
- **Testbed setup and testing scenarios**
- **Methodology: nature of tests possible, what else is needed**
- **Tools for investigating network security**

Outline of the Talk

- **Motivation – why worry about *infrastructure security*?**
- GSM /GPRS network architecture & critical interfaces
- Attacks exploiting security loopholes in GSM/GPRS
- Impact of unwanted traffic: viruses, worms, trojans, …
- Testbed setup and testing scenarios
- Methodology: nature of tests possible, what else is needed
- Tools for investigating network security

Why *Infrastructure Security* ?

Network Security

Information Security

- Keeping user’s info. protected

- Subject of cryptography

- Not subject of this talk

Infrastructure Security

- Sustaining ability of network elements to provide connectivity between communicating entities

- Subject of this talk

Cellular GSM/CDMA networks moving to an IP core …

- Network increasingly open
- Control/data segregation inherently less stringent
- Increased threats! … Exposure to wireline-like security risks

Motivation (contd)

- Interplay of IP and complex structure of cellular networks
  - ⇒ Gives rise to subtle phenomena …

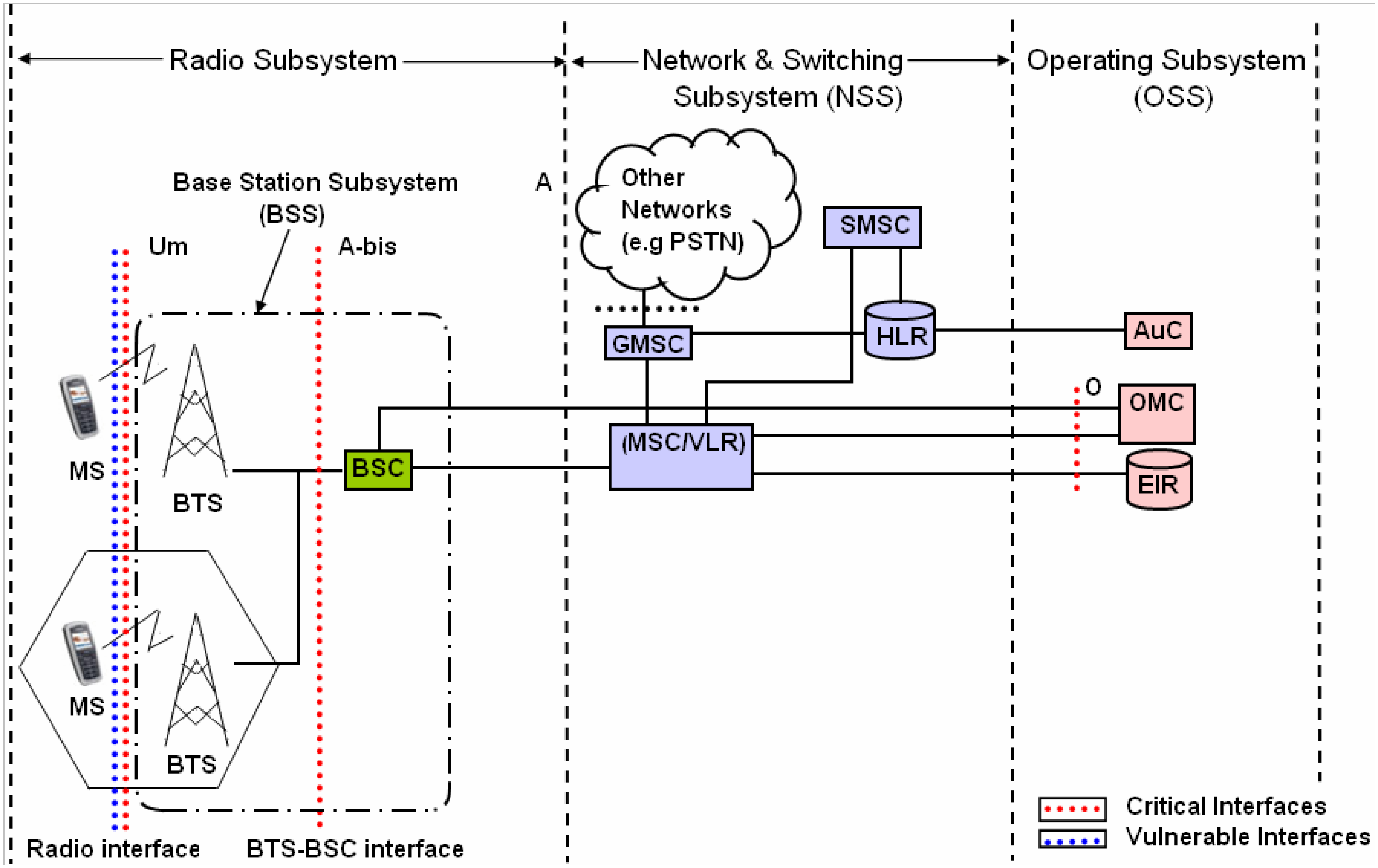
    … that may not be easily conceived
  - ⇒ Need to be found empirically via intelligent experimentation

- Provider *infrastructure* security becomes *key,* imperative to …
  - Investigate susceptibilities and risks
  - Evaluate options, fixes, and solutions
  - Propose techniques and tools for proactive/reactive action

Outline of the Talk

- Motivation – why worry about *infrastructure security*?
- **GSM /GPRS network architecture & critical interfaces**
- **Attacks exploiting security loopholes in GSM/GPRS**
- **Impact of unwanted traffic: viruses, worms, trojans, …**
- Testbed setup and testing scenarios
- Methodology: nature of tests possible, what else is needed
- Tools for investigating network security

GSM Network Architecture

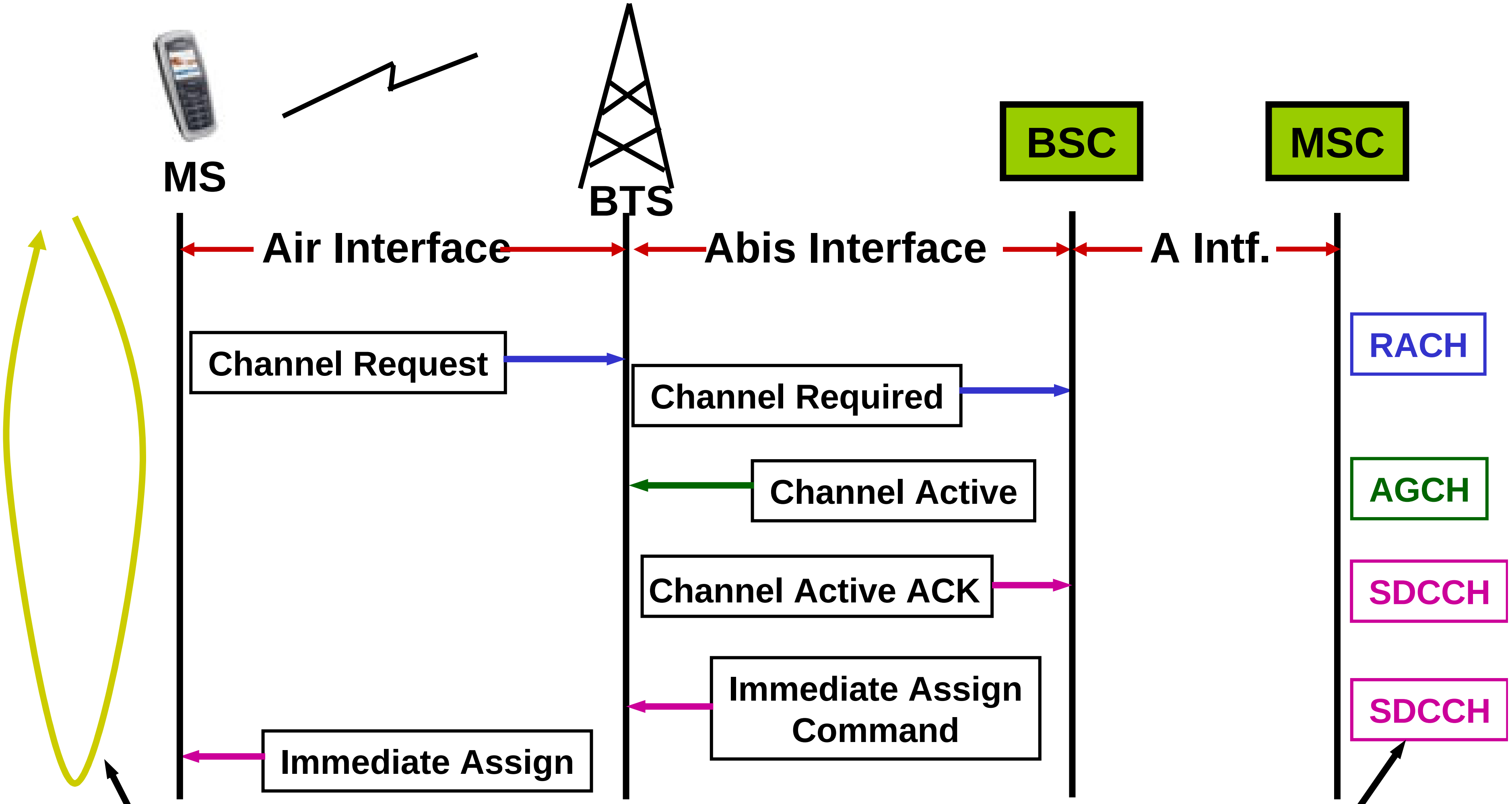


Vulnerabilities in GSM

Flaws in authentication and encryption

- No subscriber auth. in initial part of mobile originated call
- Radio interface well protected, fixed infrastructure vulnerable
- Access to AuC allows attacker to obtain auth. key
  - Encrypted MS ↔ BS traffic can be captured & deciphered
- GSM encryption has been broken!
  - Large scale attacks can be launched with relatively small traffic vols.

A Signaling Channel DoS Attack in GSM



MS

BTS

BSC

MSC

Air Interface

Abis Interface

A Intf.

Channel Request

Channel Required

Channel Active

Channel Active ACK

Immediate Assign Command

Immediate Assign

RACH

AGCH

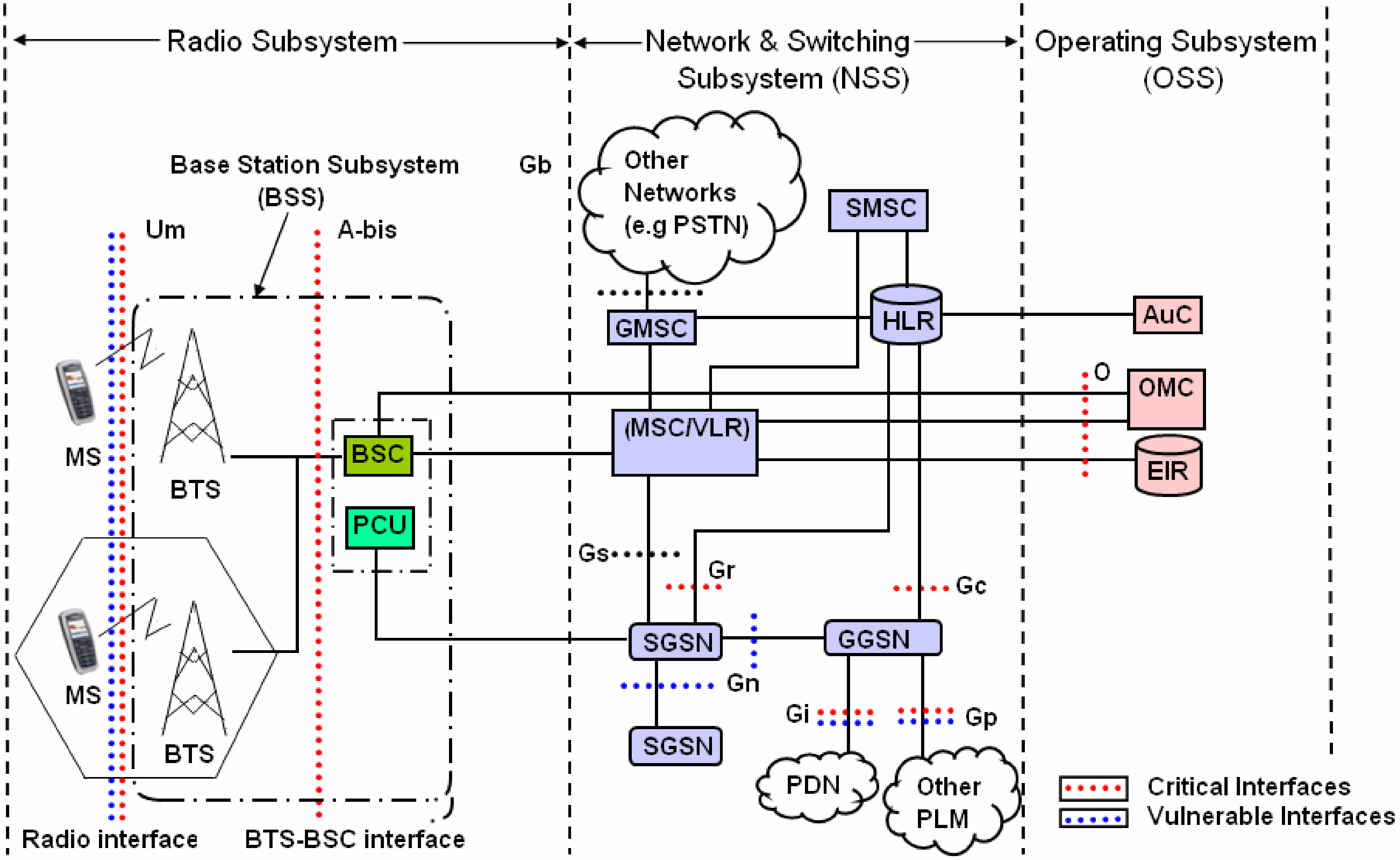
SDCCH

SDCCH

Malicious MS now repeats exercise

Signaling channels end up assigned & “lockout” genuine MSs

GPRS Network Architecture



Vulnerabilities and Criticalities in GPRS

Critical Interfaces

Gi: Exposed to Internet and corporate networks

Gp: Primary interconnection pt. between operator's n/w and untrusted external n/ws

Gc: Allows access (via HLR) to key user info. from remote network during roaming

Vulnerable Interfaces

Gi: Exposed to all threats from Internet: viruses, DoS, and malicious network traffic

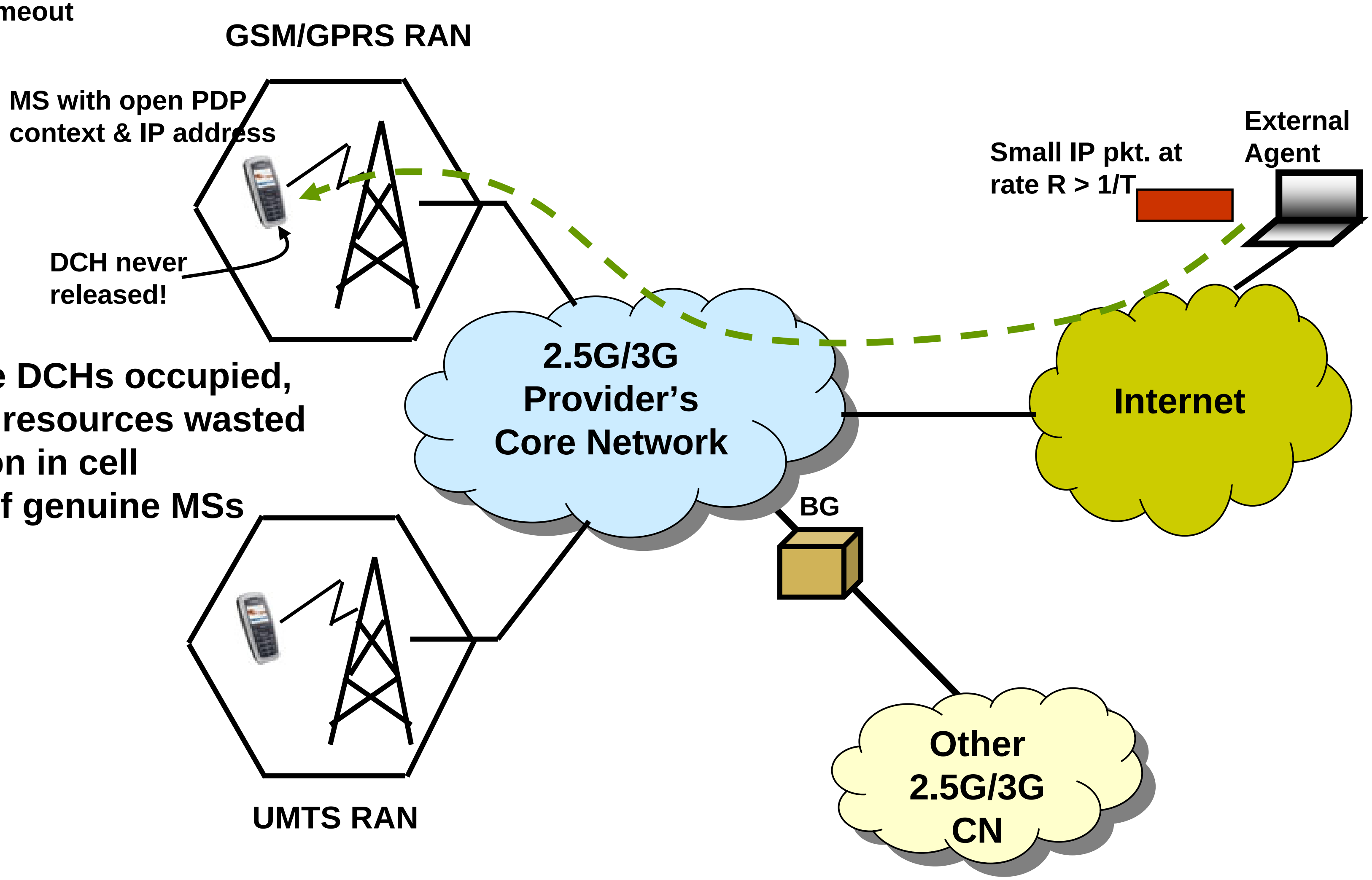
Gp: Connection hijacking, over-billing from a roaming network during handover

Gn: Not encrypted by default

A DCH “Lockout” Attack in GPRS

T = DCH release/dynamic reassignment timeout

With multiple DCHs occupied, logical radio resources wasted
- ➔ **Congestion in cell**
- ➔ **Lockout of genuine MSs**



GSM/GPRS RAN

MS with open PDP context & IP address

DCH never released!

Small IP pkt. at rate R > 1/T

External Agent

2.5G/3G Provider’s Core Network

Internet

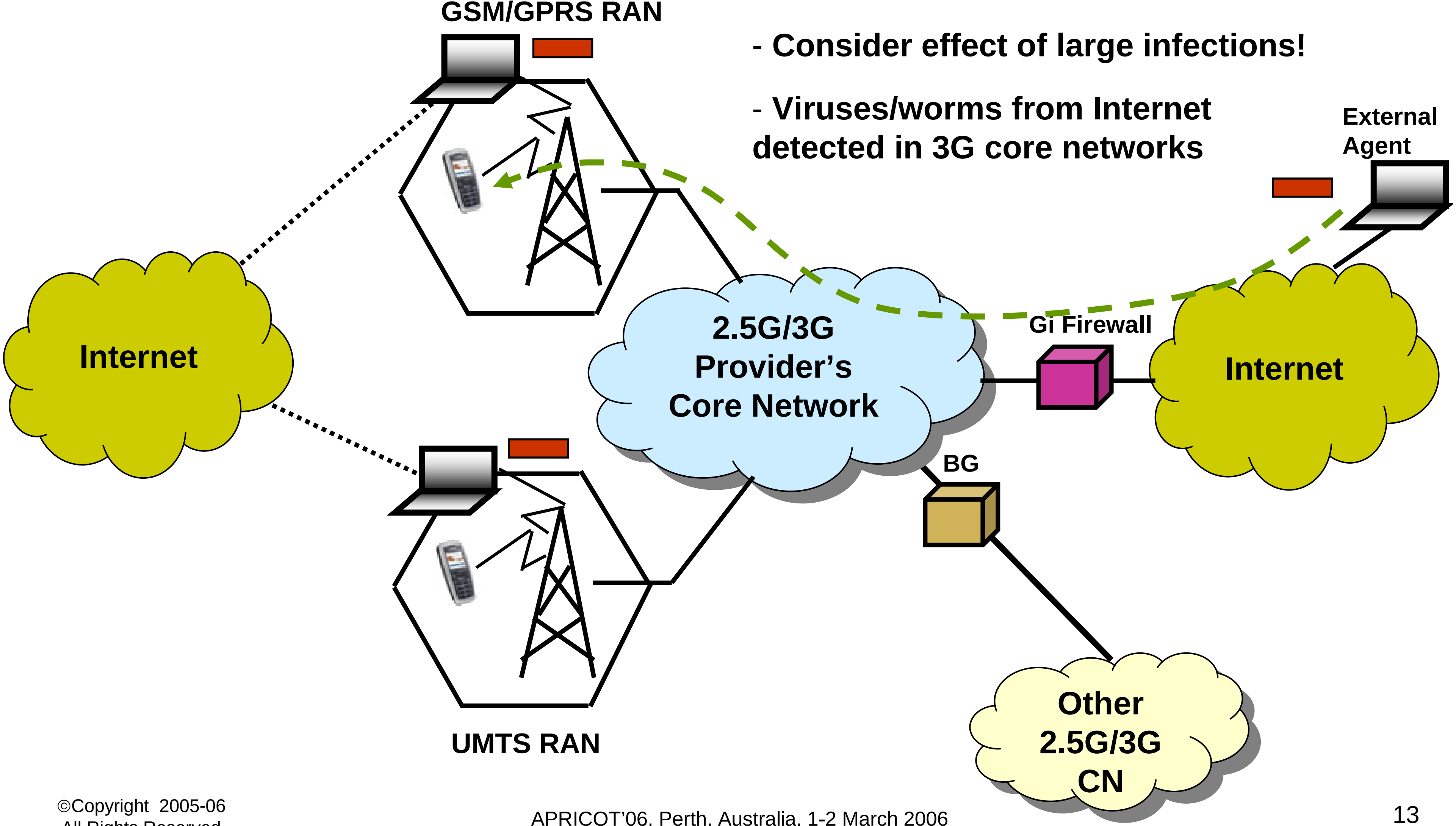
BG

Other 2.5G/3G CN

UMTS RAN

Impact of Unwanted Traffic: Viruses, worms, trojans, …

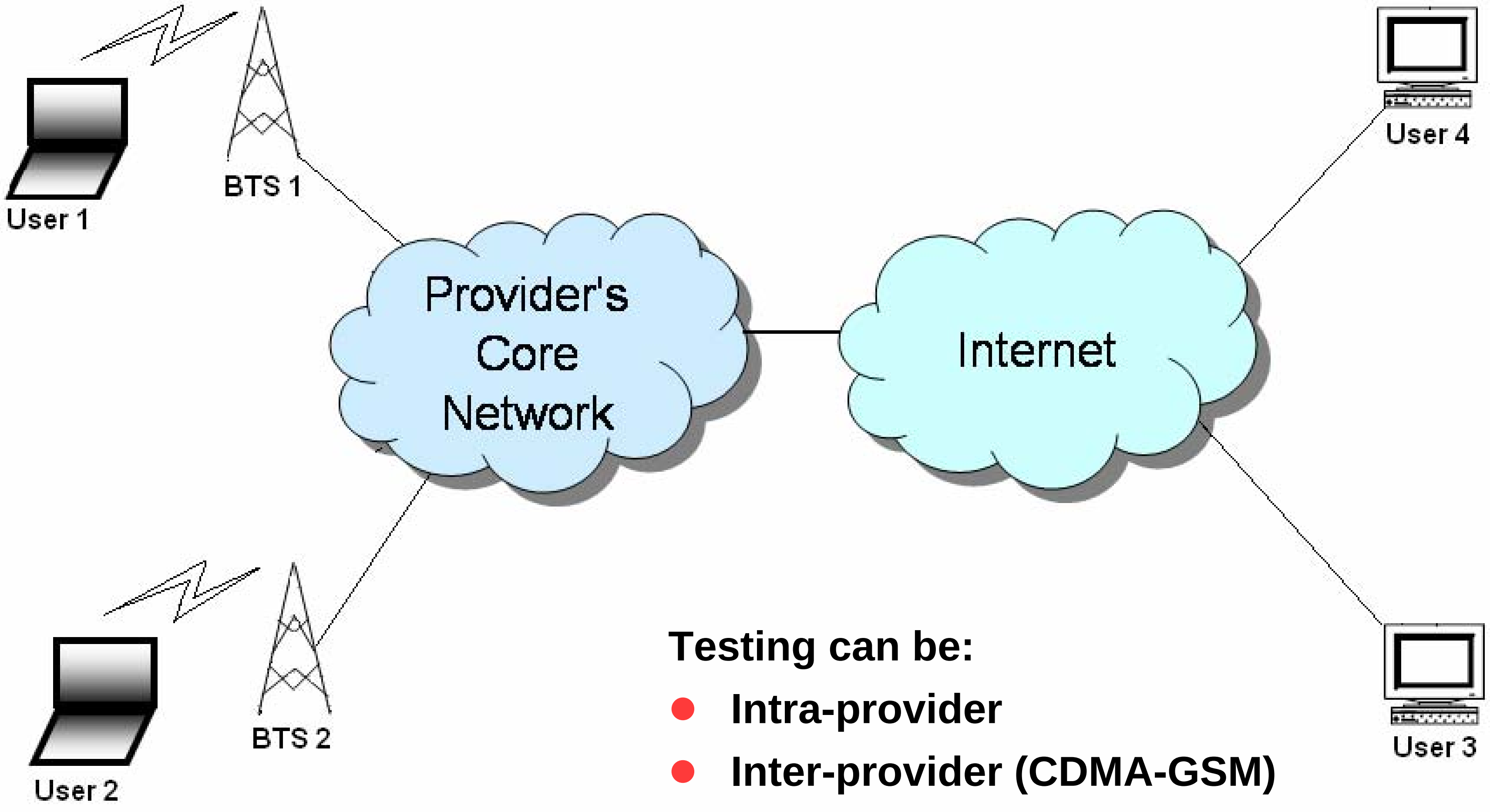
- **Attacker can be inside your n/w!**
- **Consider effect of large infections!**
- **Viruses/worms from Internet detected in 3G core networks**



Outline of the Talk

- Motivation – why worry about *infrastructure security*?
- GSM /GPRS network architecture & critical interfaces
- Attacks exploiting security loopholes in GSM/GPRS
- Impact of unwanted traffic: viruses, worms, trojans, …
- **Testbed setup and testing scenarios**
- Methodology: nature of tests possible, what else is needed
- Tools for investigating network security

Experimental Test-bed Setup & Testing Scenarios



Testing can be:

- **Intra-provider**
- **Inter-provider (CDMA-GSM)**
- **Wireless-wireline**

Outline of the Talk

- Motivation – why worry about *infrastructure security*?
- GSM /GPRS network architecture & critical interfaces
- Attacks exploiting security loopholes in GSM/GPRS
- Impact of unwanted traffic: viruses, worms, trojans, …
- Testbed setup and testing scenarios
- **Methodology: nature of tests possible, what else is needed**
- Tools for investigating network security

Testing Methodology

Taxonomy of Tests

Active Probing

Direct malicious generated traffic to SP's network or to a remote m/c on network. E.g.

- **SYN attack**
- **Tear-drop attack**
- **Smurf attack**

Exploit various types of commun.

- **Port-to-port**
- **IP address spoofing**

Infer network parameters: RTT, buffers

Passive Listening

Provoke remote attacker(s) to attack m/c under observation

- **Invoke attacks, HoneyD as "bait"**
- **Run intrusion detection systems on attacked m/c**
- **Apply intelligent algorithms for proactive threat inference**

Outline of the Talk

- Motivation – why worry about *infrastructure security*?
- GSM /GPRS network architecture & critical interfaces
- Attacks exploiting security loopholes in GSM/GPRS
- Impact of unwanted traffic: viruses, worms, trojans, …
- Testbed setup and testing scenarios
- Methodology: nature of tests possible, what else is needed
- **Tools for investigating network security**

Network Security Investigation

Investigative Tools

Detect

- NMAP
- Netcat

Exploit

- Honeyd
- PackEth

Analyze

- Snort
- NTOP

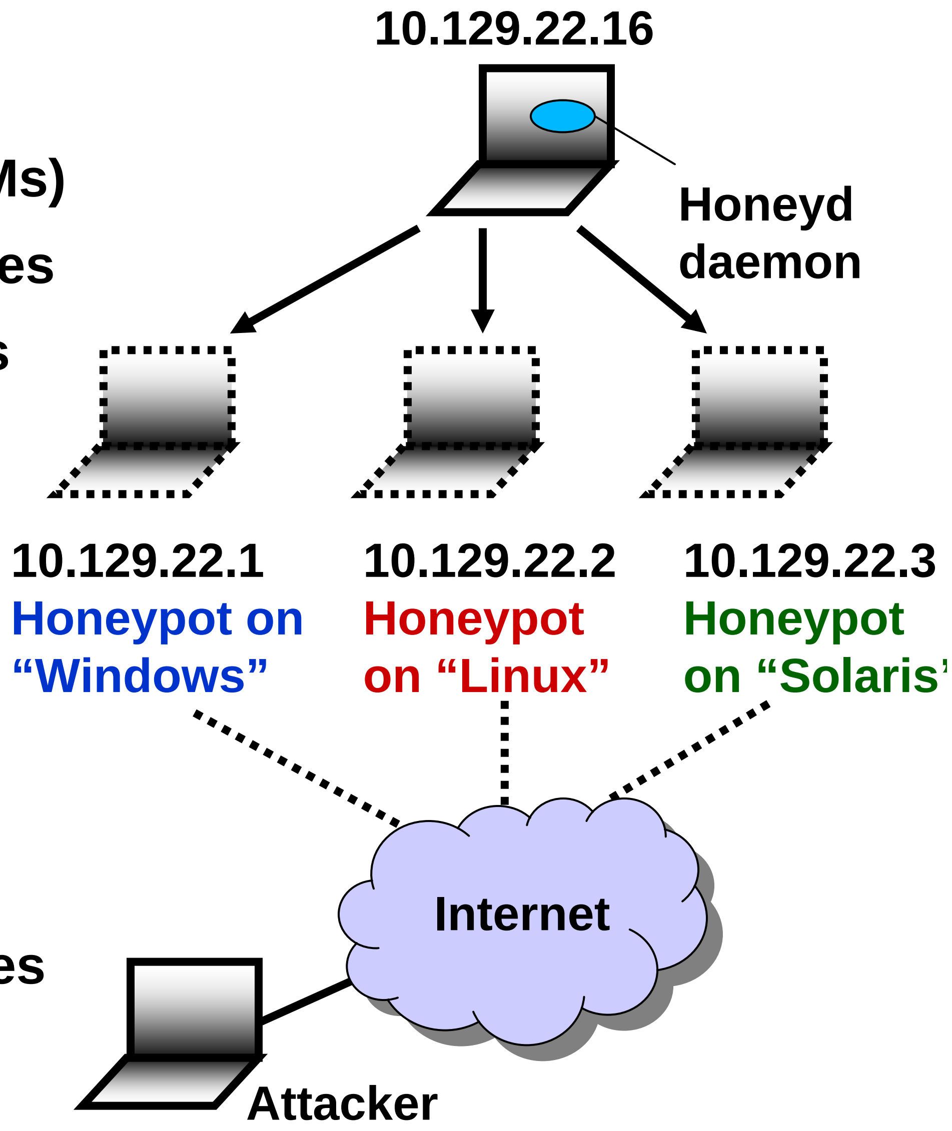
Tools for Detecting Vulnerabilities

- **Network MAPper (NMAP)**
  - **Determines running apps. on target m/c**
  - **Identifies open ports, OS, firewalls used by remote host(s)**

- **Netcat**
  - **Utility used to read/write across network connections using TCP/UDP protocol(s)**
  - **Feature-rich, network debugging and exploration tool**

Tools for Exploiting Vulnerabilities

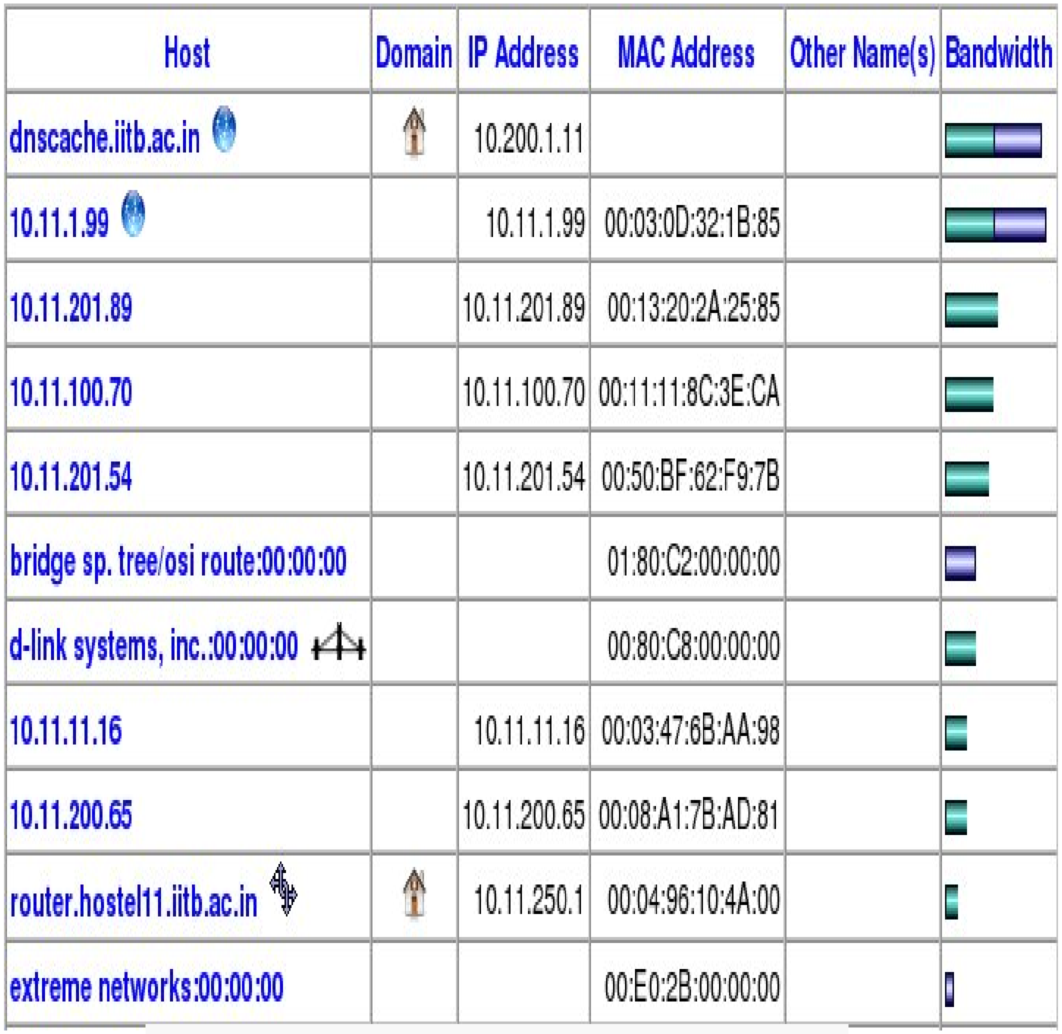
- **HoneyD:**
  - Creates virtual machines (VMs)
  - VMs have unique IP addresses
  - Lure attackers to themselves
  - Can be Windows or Linux
- **PackETH**
  - Packet generator
  - Generates packets of any protocol - ARP, TCP, UDP, ...
  - User configurable pkt. profiles



Tools for Analyzing Vulnerabilities

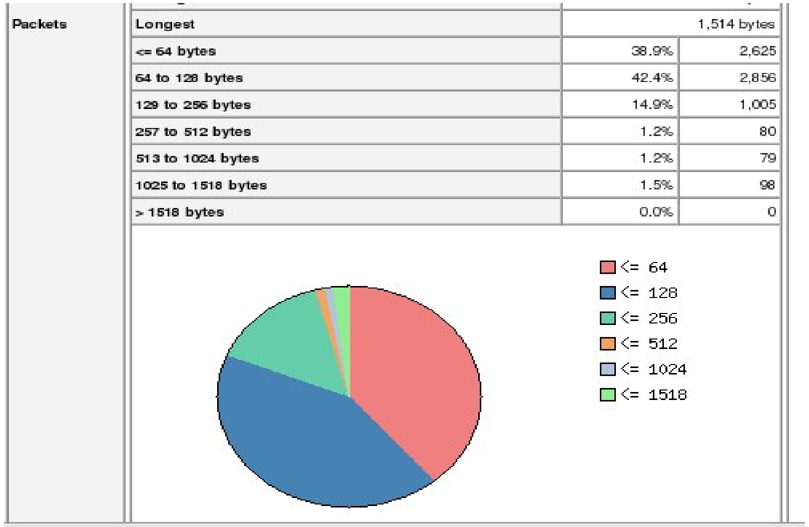
- Snort
    - Real-time traffic analysis & packet logging
    - Usable in multiple modes:
        - Packet sniffer
        - Data logger
        - Intrusion detection
    - Generates variety of alerts – usable for proactive detection
- NTOP
    - Traffic usage monitor & packet analyzer
    - Supports mgt. activities: planning, opt., detection
    - Tracks ongoing attacks, generates alarms

NTOP at Work



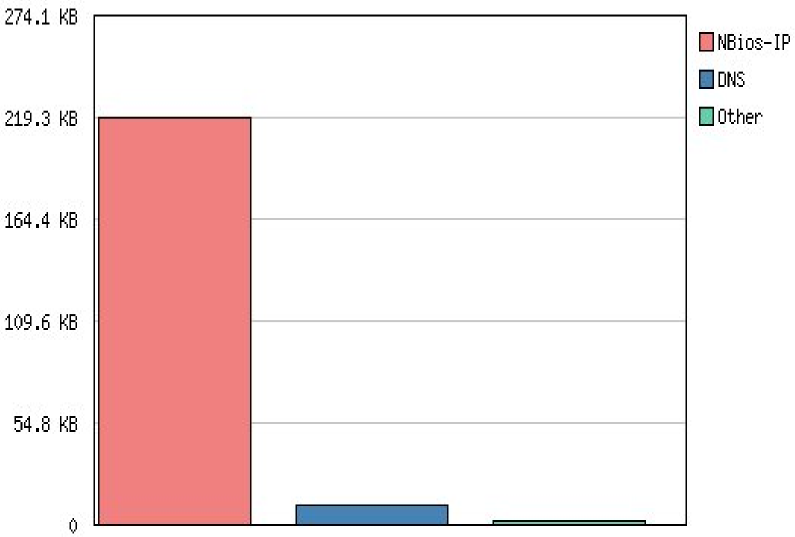
Host	Domain	IP Address	MAC Address	Other Name(s)	Bandwidth
dnscache.iitb.ac.in		10.200.1.11			
10.11.1.99		10.11.1.99	00:03:0D:32:1B:85		
10.11.201.89		10.11.201.89	00:13:20:2A:25:85		
10.11.100.70		10.11.100.70	00:11:11:8C:3E:CA		
10.11.201.54		10.11.201.54	00:50:BF:62:F9:7B		
bridge sp. tree/osi route:00:00:00			01:80:C2:00:00:00		
d-link systems, inc.:00:00:00			00:80:C8:00:00:00		
10.11.11.16		10.11.11.16	00:03:47:6B:AA:98		
10.11.200.65		10.11.200.65	00:08:A1:7B:AD:81		
router.hostel11.iitb.ac.in		10.11.250.1	00:04:96:10:4A:00		
extreme networks:00:00:00			00:E0:2B:00:00:00		

Traffic breakdown by hosts seen



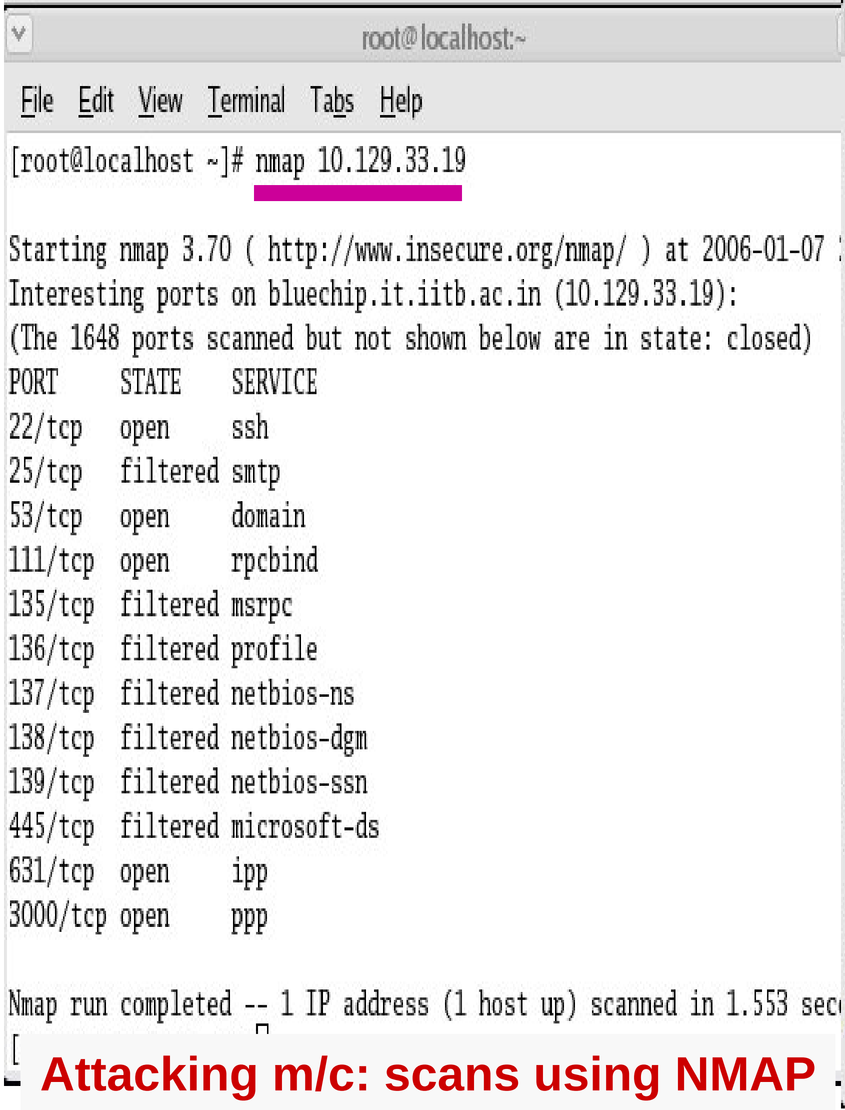
Packets	Longest	1,514 bytes	
	<= 64 bytes	38.9%	2,625
	64 to 128 bytes	42.4%	2,856
	129 to 256 bytes	14.9%	1,005
	257 to 512 bytes	1.2%	80
	513 to 1024 bytes	1.2%	79
	1025 to 1518 bytes	1.5%	98
	> 1518 bytes	0.0%	0

Packet size distribution

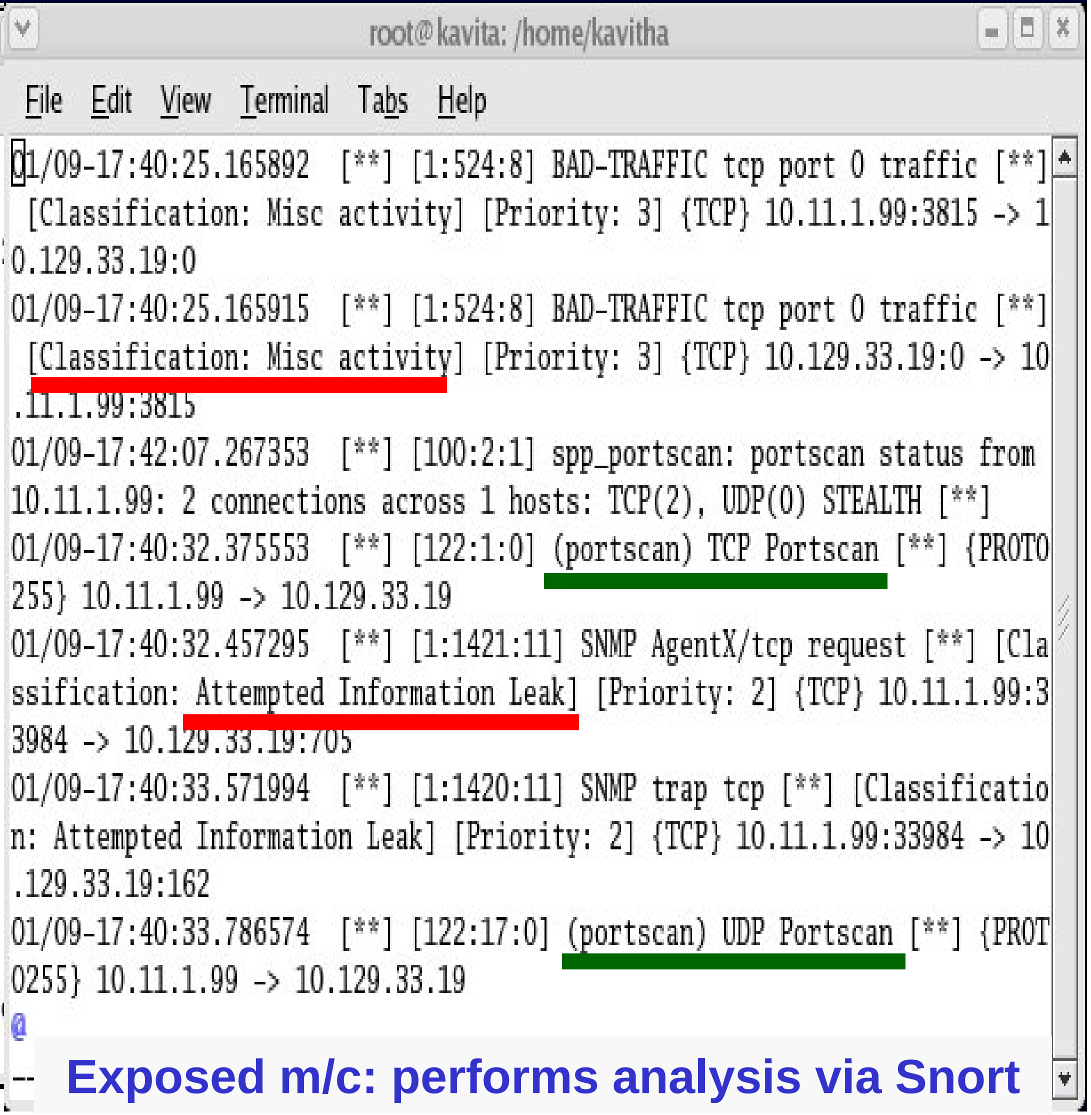


TCP/UDP distribution by major protocols

NMAP and Snort Working in Conjunction



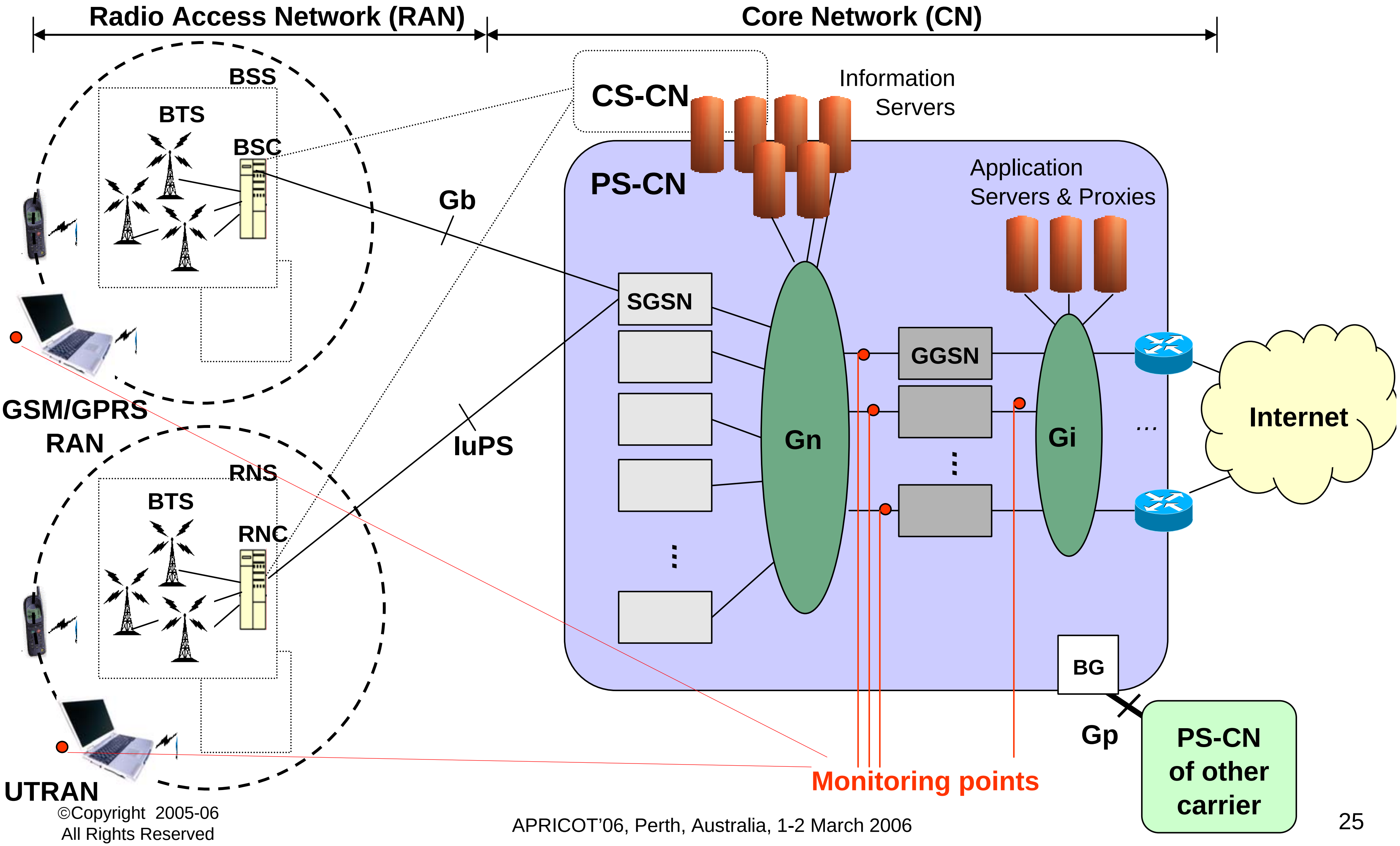
```
[root@localhost ~]# nmap 10.129.33.19

Starting nmap 3.70 ( http://www.insecure.org/nmap/ ) at 2006-01-07 
Interesting ports on bluechip.it.iitb.ac.in (10.129.33.19):
(The 1648 ports scanned but not shown below are in state: closed)
PORT     STATE    SERVICE
22/tcp   open     ssh
25/tcp   filtered smtp
53/tcp   open     domain
111/tcp  open     rpcbind
135/tcp  filtered msrpc
136/tcp  filtered profile
137/tcp  filtered netbios-ns
138/tcp  filtered netbios-dgm
139/tcp  filtered netbios-ssn
445/tcp  filtered microsoft-ds
631/tcp  open     ipp
3000/tcp open     ppp

Nmap run completed -- 1 IP address (1 host up) scanned in 1.553 sec
[
```



```
01/09-17:40:25.165892  [**] [1:524:8] BAD-TRAFFIC tcp port 0 traffic [**]
 [Classification: Misc activity] [Priority: 3] {TCP} 10.11.1.99:3815 -> 1
0.129.33.19:0
01/09-17:40:25.165915  [**] [1:524:8] BAD-TRAFFIC tcp port 0 traffic [**]
 [Classification: Misc activity] [Priority: 3] {TCP} 10.129.33.19:0 -> 10
.11.1.99:3815
01/09-17:42:07.267353  [**] [100:2:1] spp_portscan: portscan status from
10.11.1.99: 2 connections across 1 hosts: TCP(2), UDP(0) STEALTH [**]
01/09-17:40:32.375553  [**] [122:1:0] (portscan) TCP Portscan [**] {PROTO
255} 10.11.1.99 -> 10.129.33.19
01/09-17:40:32.457295  [**] [1:1421:11] SNMP AgentX/tcp request [**] [Cla
ssification: Attempted Information Leak] [Priority: 2] {TCP} 10.11.1.99:3
3984 -> 10.129.33.19:705
01/09-17:40:33.571994  [**] [1:1420:11] SNMP trap tcp [**] [Classificatio
n: Attempted Information Leak] [Priority: 2] {TCP} 10.11.1.99:33984 -> 10
.129.33.19:162
01/09-17:40:33.786574  [**] [122:17:0] (portscan) UDP Portscan [**] {PROT
0255} 10.11.1.99 -> 10.129.33.19
@
```

Attacking m/c: scans using NMAP -- **Exposed m/c: performs analysis via Snort**

What More is Needed



Summary

- Cellular infrastructure security … critically important in future
- Analyzed GSM /GPRS from a vulnerability standpoint
- Highlighted key aspects, such as
  - Critical interfaces
  - Sample attacks
  - Effects of unwanted traffic!
- Presented our testbed setup and testing scenarios
- Focused on nature and types of test portfolio
- Reviewed tools and techniques to assess security

Glossary and Suggested Reading

AuC	Authentication Center
AGCH	Access Grant Channel
BG	Border Gateway
BS	Base Sation
BTS	Base Transiver Station
CDMA	Code Division Multiple Access
CN	Core Network
EIR	Equipment Identity Register
GGSN	Gateway GPRS Support Node
GMSC	Gateway Mobile Switching Center
GPRS	General Packet Radio Service
GSM	Global System for Mobile Communication
HLR	Home Location Register
IP	Internet Protocol
MS	Mobile Station
MSC	Mobile Switching Center
OMC	Operations Management Center

Glossary (contd.)

PCU	**Packet Control Unit**
PDN	**Packet Data Network**
PSTN	**Public Switched Telephone Network**
RACH	**Random Access Channel**
RAN	**Radio Access Network**
RTT	**Round Trip Time**
SDCCH	**Slow Dedicated Control Channel**
SGSN	**Serving GPRS Support Node**
SMSC	**Short Messaging Service Center**
UMTS	**Universal Mobile Telecommunication System**
UTRAN	**UMTS Terrestial Radio Access Network**

Suggested Readings

- **H. Yang, F. Ricciato, S. Lu, L. Zhang, "Securing a Wireless World", *Proceedings of the IEEE.* Volume: 94, Issue: 2, pp. 442-454, Feb 2006.**

  Available: http://ieeexplore.ieee.org/xpls/abs_all.jsp?arnumber=1580512
- **F. Vacirca, F. Ricciato, R. Pliz, "Large-Scale RTT Measurements from an Operational UMTS/GPRS Network."**

  Available: http://userver.ftw.at/~ricciato/darwin/wicon05-ricciato-metawin.pdf
- **Netscreen Technologies Inc,."GPRS Security Threats and Solutions", *Whitepaper,* March 2002.**

  Available: www.juniper.net/solutions/literature/white-papers/200074.pdf
- **W. Enck, P. Traynor, P. McDaniel, T. Porta, "Exploiting Open Functionality in SMS-Capable Cellular Networks", 12th ACM Conference on Computer and Communications Security, Nov 2005.**

  Available: www.smsanalysis.org/smsanalysis.pdf

Suggested Readings (Contd.)

- **E. Barken, E. Biham, N. Keller, "Instant Ciphertext-Only Cryptanalysis of GSM Encrypted Communication", Technion, Computer Science Department, Technical Report CS-2003-05.**

  Available: http://citeseer.ist.psu.edu/663139.html
- **V. Bocan, V. Cretu, "Security and Denial of Service Threats in GSM Networks", *Periodica Politechnica, Transactions on Automatic Control and Computer Science,* Vol 49 (63), 2004.**

  Available: www.dataman.ro/phd/conti2004-2.pdf
- **P. Stuckman, *"The GSM Evolution",* John Wiley and Sons, 2003, ISBN 0-470-84855.**