Mobile Telecommunications

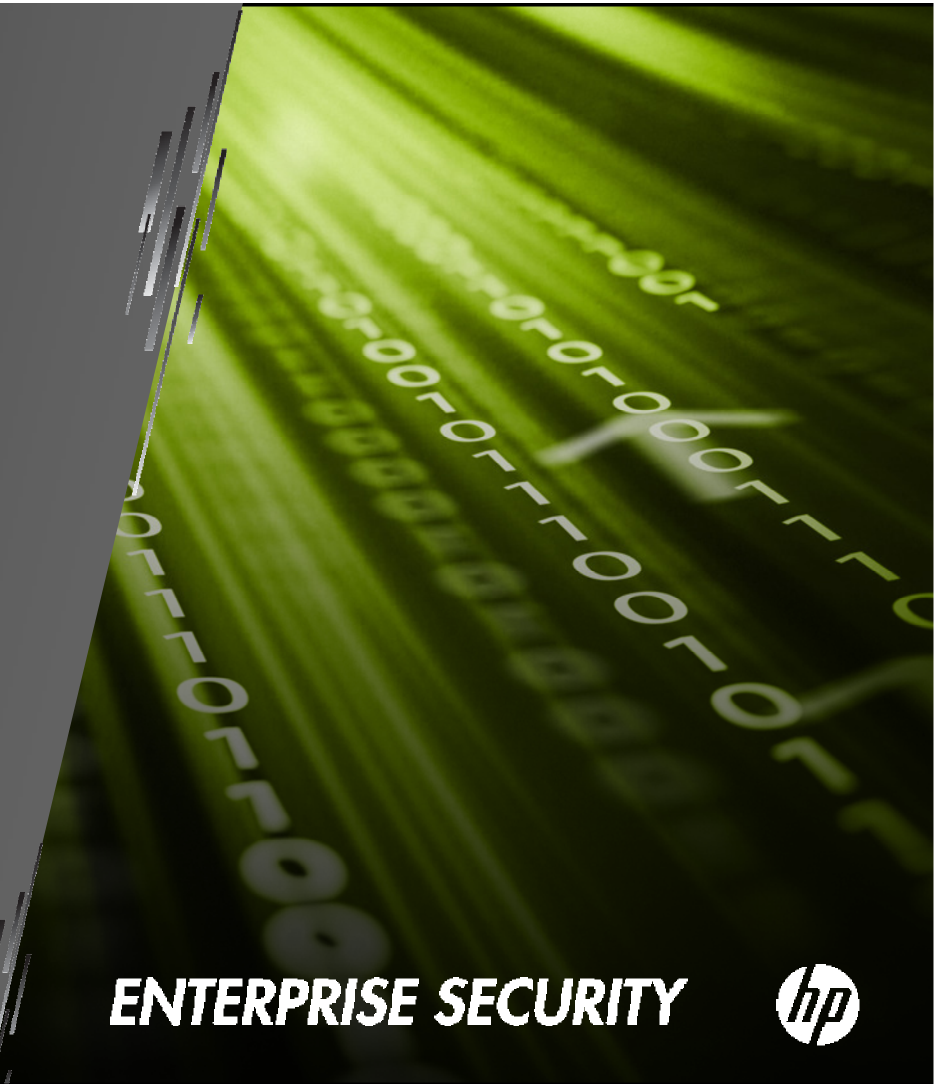
An Overview of Vulnerabilities

Damanjit S. Uberoi
Chief Solutions Architect
& Evangelist, South Asia

Agenda

- Threat landscape
- Common Exploits
- Technology Requirements
- Response Posture

Threat Landscape



The Threat Landscape

Internal Threats

Configuration tampering - for financial gain

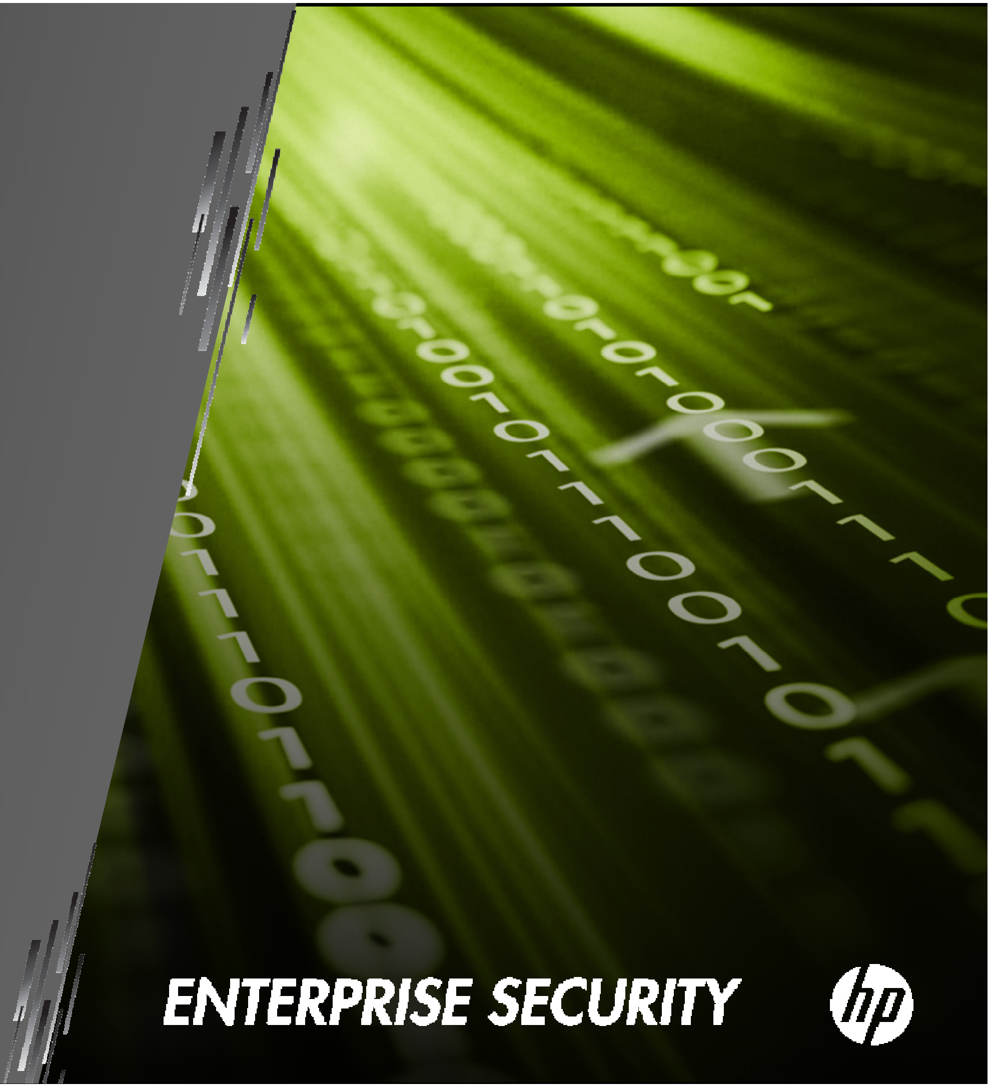
Insider collaborator

External Threats

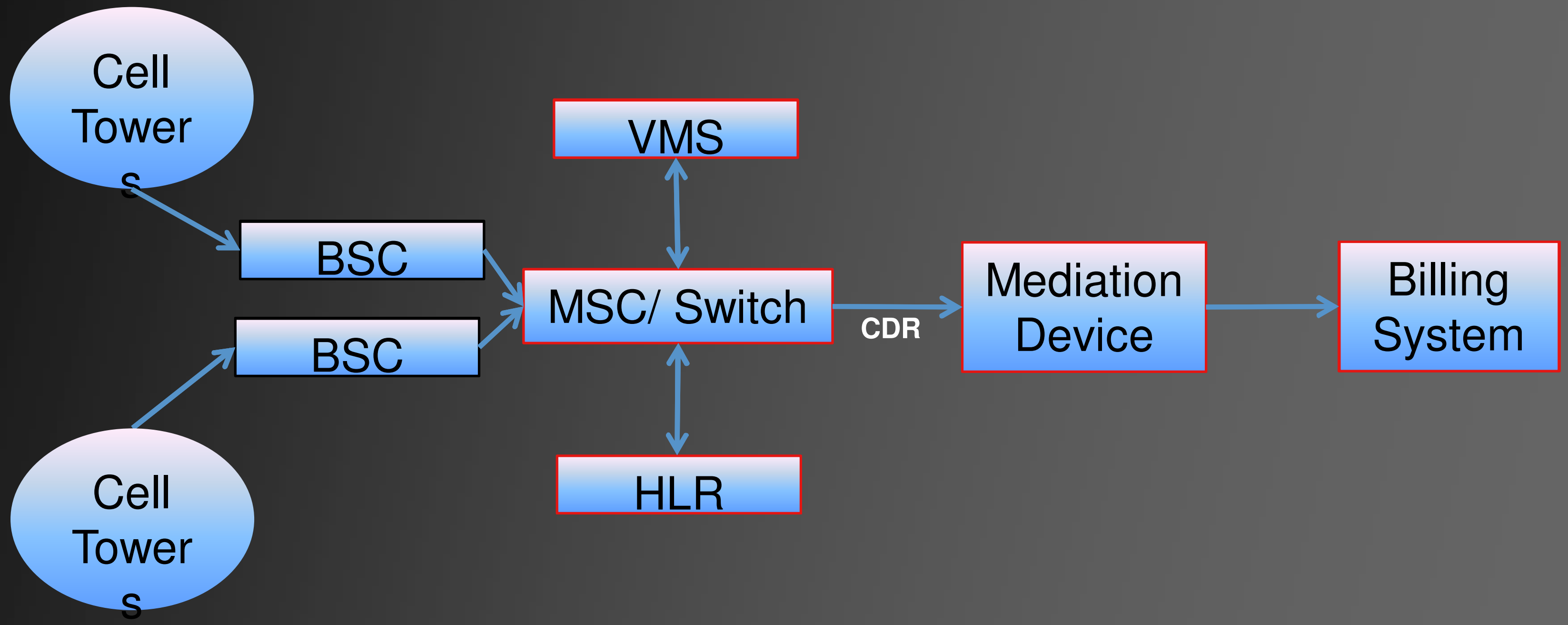
Undetected / unauthorized use

National security concerns

Common Exploits



Typical Mobile Communications Architecture



Account Number: [illegible] Airtel Number: [illegible]

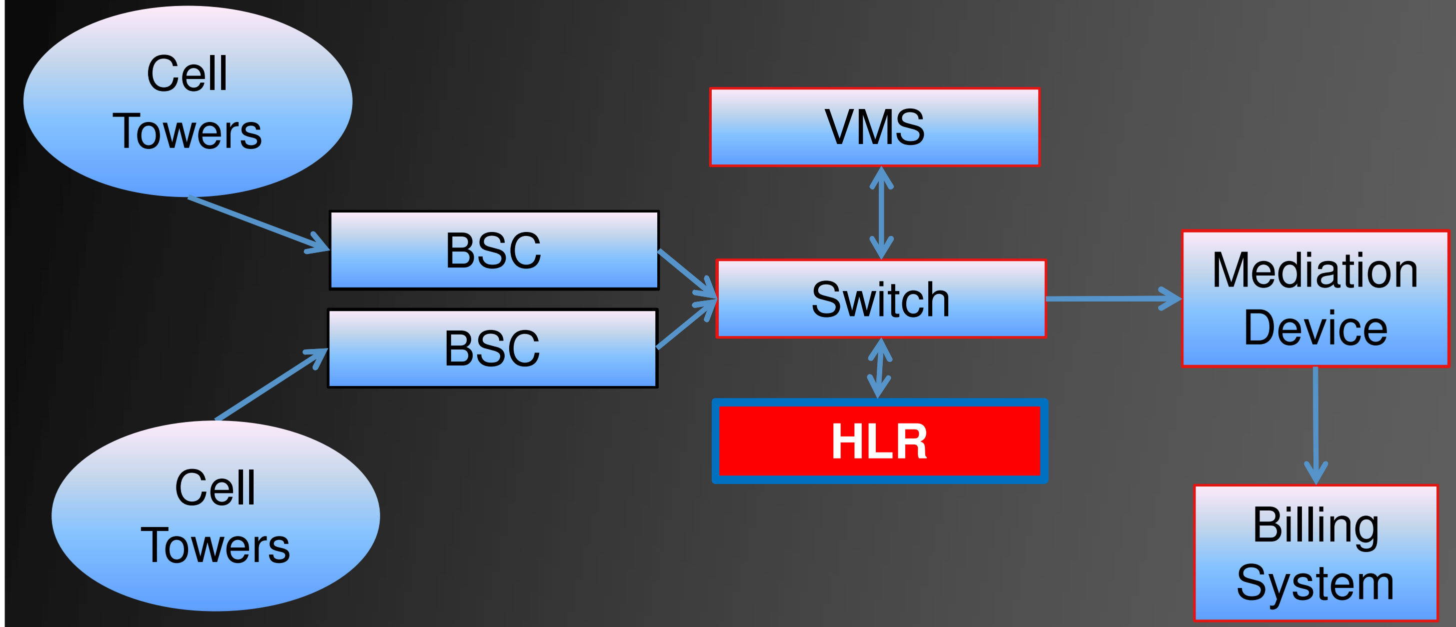
Make New Payment

Invoice Number	[illegible]
Bill Period	[illegible]
Invoice Date	[illegible]
Amount Due	[illegible]
Email ID	[illegible]
Pay Amount	[illegible]
Select Your Card Type	○ Net Banking ● Credit Card ○ Debit Card
Choose Your Card Type/Net Banking Account	Visa/Master Credit Card

Submit

*International Cards are not accepted

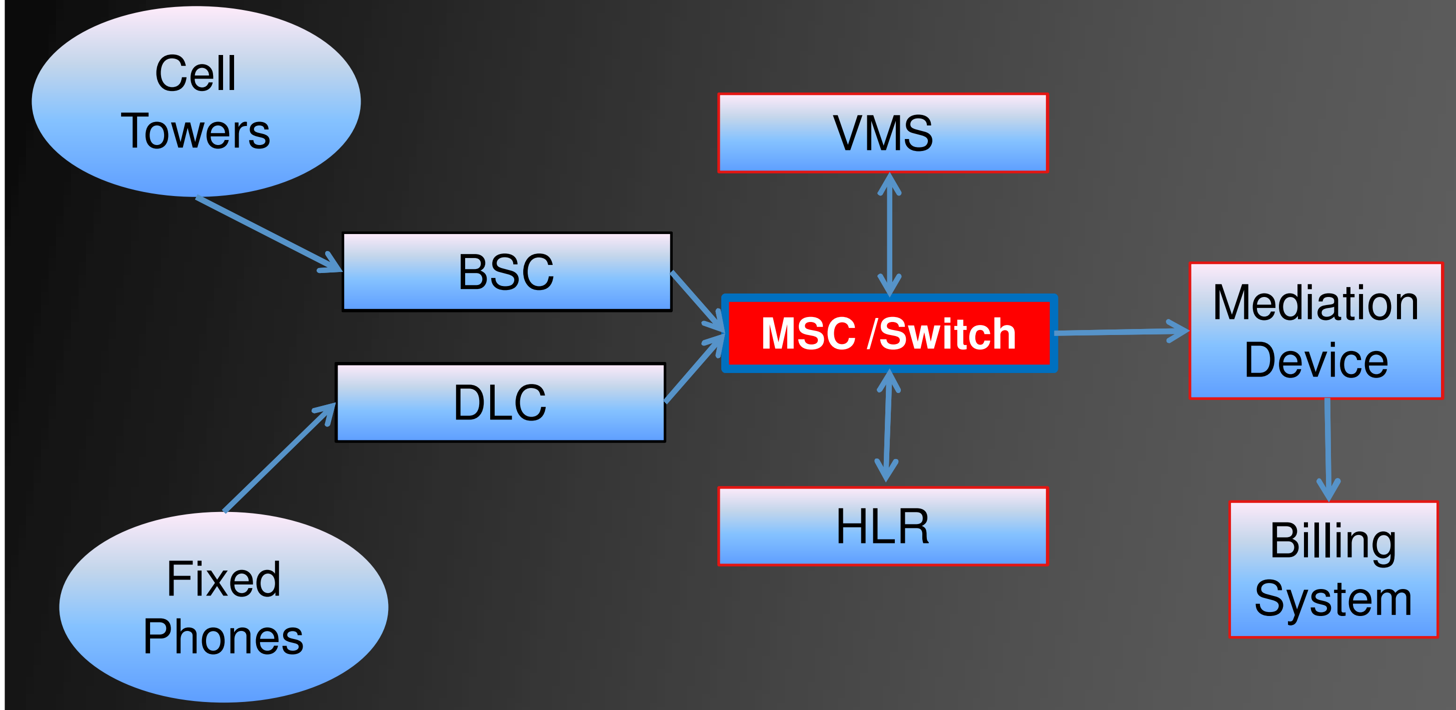
Scenario 1 - HLR Configuration Changes



Solution
Correlation of configuration change Logs in HLR can provide real time alerts on such threats ; users other than OSS should not be making changes

Unauthorized user can exploit this resource by ***adding VAS and other fixed billing elements*** in the HLR without the same being available in the BSS. The VAS can then be used unrestrictedly without being charged

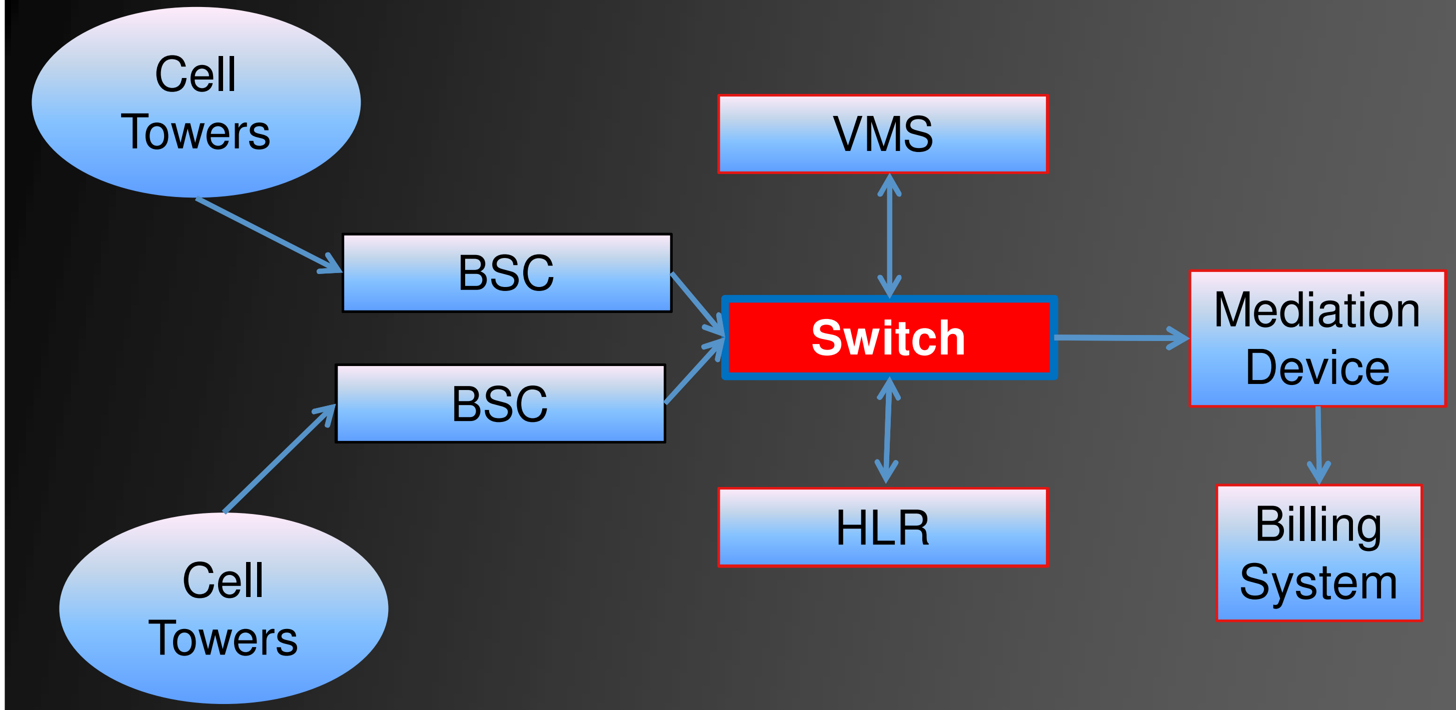
Scenario 2 – MSC Configuration Change



Solution
Correlation of configuration change Logs in MSC can provide real time alerts on such threats.

By **modifying the CDR creation mechanism of a MSC** an unauthorized user can disable the CDR generated by some user accounts resulting in utilization of the network without a record of the usage ever being sent to the billing system and subsequently in huge loss of revenues to the organization

Scenario 3 – MSC CDR Level Changes



Cell Towers

BSC

BSC

Cell Towers

VMS

Switch

HLR

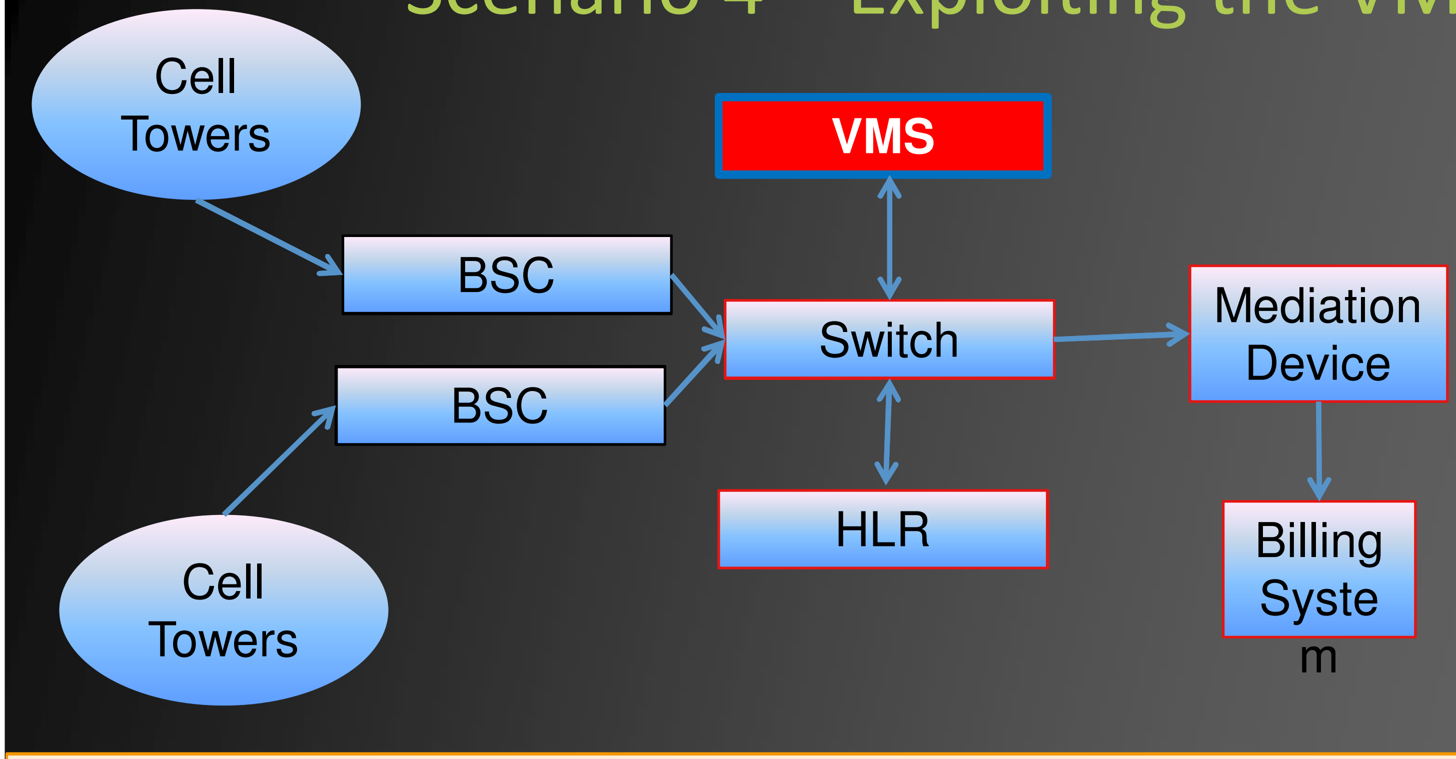
Mediation Device

Billing System

Solution
Correlation of configuration change Logs in MSC can provide real time alerts on such threats along with alerts on CDR modifications.

A switch can also be exploited by **switching off CDR for a particular number for particular duration.** The fraudulent user can utilize the network without a record of the usage ever being sent to the billing system for that particular duration…

Scenario 4 – Exploiting the VMS

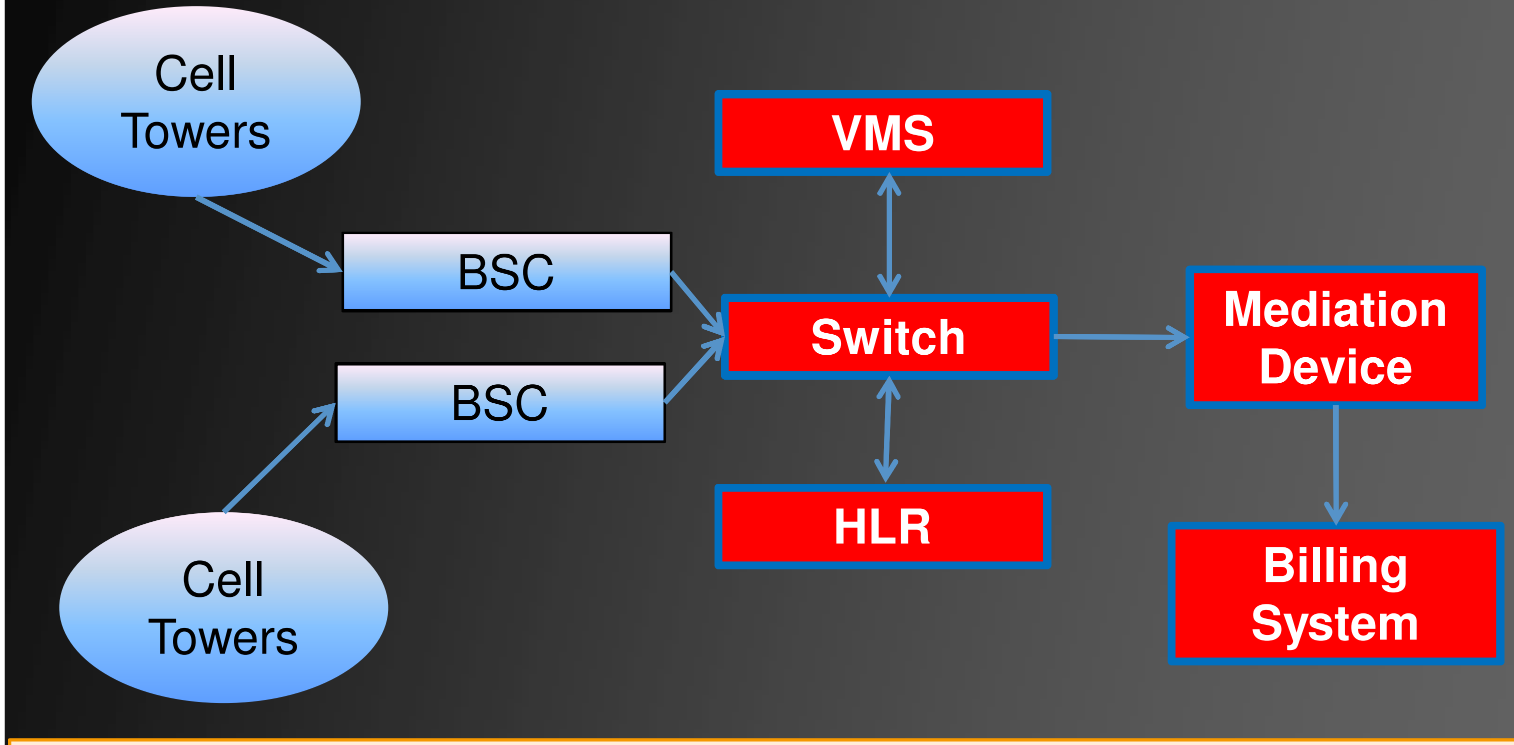


Solution
Correlation of threshold violation in DID/DOD Logs in VMS can provide real time alerts on such threats along with alerts on CDR modifications.

Pattern Discovering & logging high threshold cases

This system can be exploited by ***adding an invalid mailbox number*** (i.e. mobile telephone number) to a VMS registry. When the fraudster dials into the VMS and is asked for their mobile identification number, they simply enter in the false mailbox number. Once authenticated, the caller is able to make outbound calls using the added functions and call back features of the VMS. The CDR from this usage cannot be billed because the switch records the invalid mailbox number as the calling number

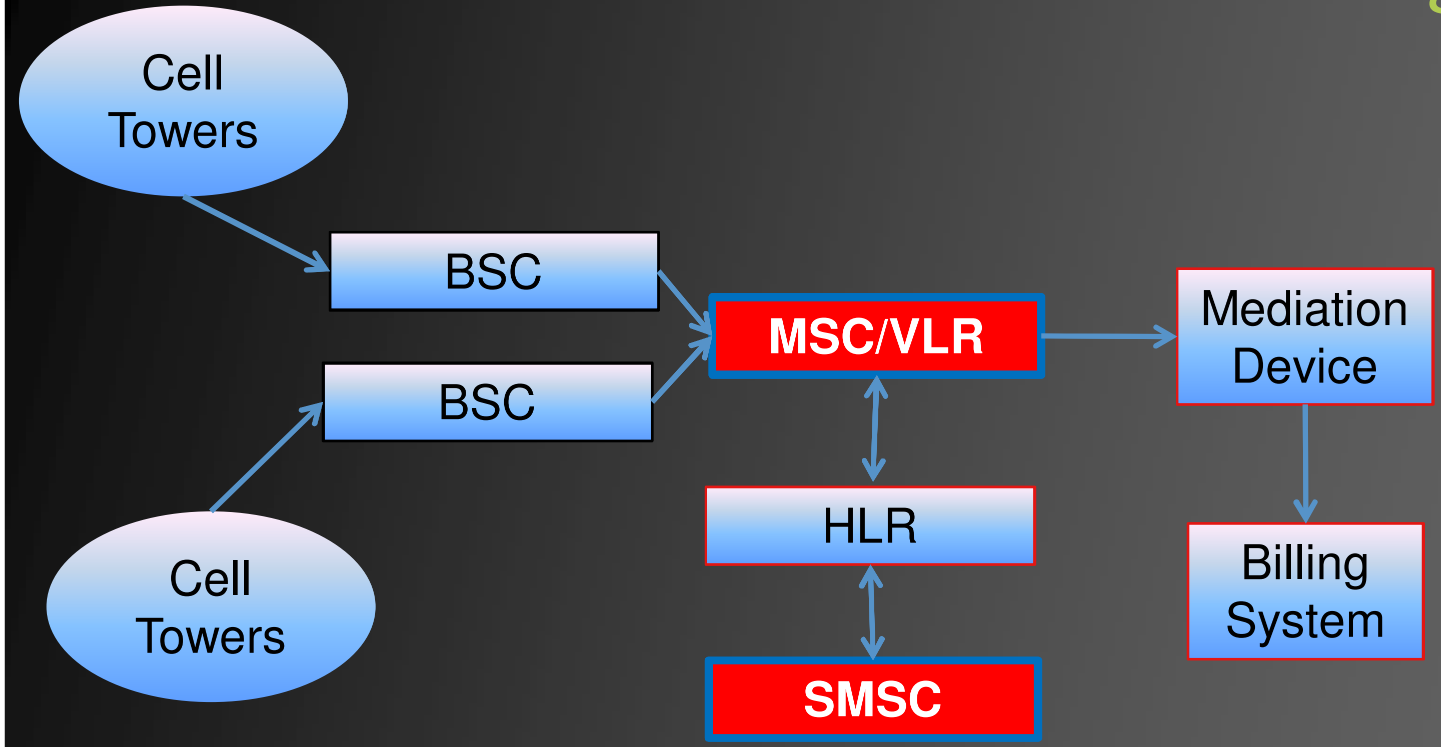
Scenario 5 - Device Level Logs Modification



Solution
Log once collected can not be modified (WORM) thus all the evidence and logs would be centrally stored.

System administrators of all the critical devices can ***completely delete the logs*** from the respective devices after making all fraudulent changes within device, thus deleting all the records and evidences of fraud

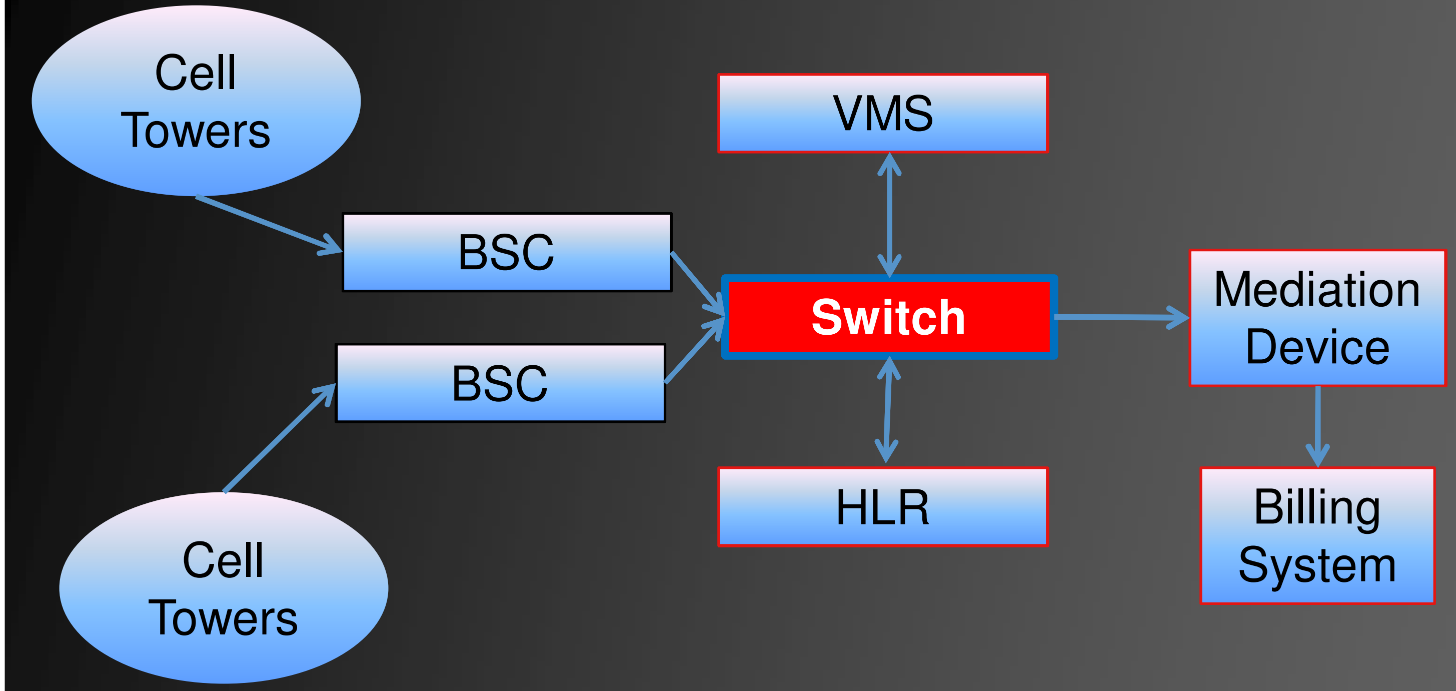
Scenario 6 – SMSC & VLR Changes



Solution
Real time correlation alerts by comparing the logs of VLR and MSME and alerts on configuration level changes of VLR.
Dynamic Log polling is required here

A fraudster can simulate non PLMN numbers and trick the SMSC into believing that a legitimate roaming users in sending SMSs. This can go unnoticed till such time the interconnect settlement is disputed by the roaming partner carrier.

Scenario 7 – External Fraud at STP & MSC



Solution
Using pattern discovery of call release code only from premium number and setting up threshold for such incidents we can report and provide real time alert.

External threats around missed calls from an international & premium numbers have increased in which while calling back to that particular number; users are charged sudden high amount by third-party international operators which leads to customer dissatisfaction and harms the base operator's brand reputation.

Technology Requirements

ENTERPRISE SECURITY

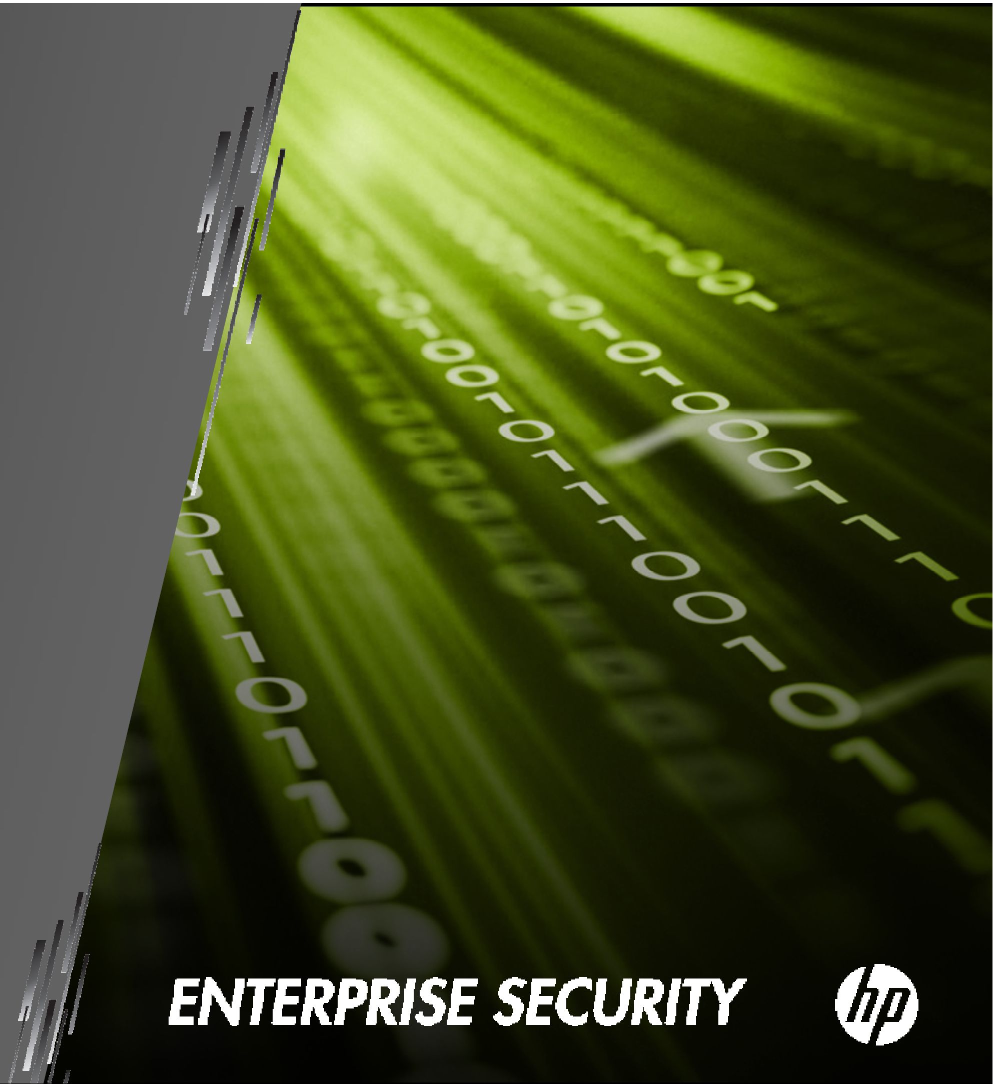
Multidimensional Comparison

Compare arbitrary fields on per-case basis

- Flexibility in terms of log collection
  - Parsing
  - Classification of various occurrences

- Forensic Capabilities
  - Efficient storage and query mechanisms
  - Better suited for deep pattern analysis
  - Adaptability to evolving scenarios

Response Posture



When Should You Process

Real time?

- Feasibility in terms of log volumes
  - Massive overheads at collection layer
  - Capacity limitations of event processing
- Benefits
  - Weigh timeliness vs. ROI…

When Should You Process… (*contd.*)

Offline - Batch Mode

- Feasibility in terms of log volumes
  - Eases pressure on collection layer
  - Eases pressure on capacity of event processing
- Benefits
  - Lower cost = Stronger Justification for ROI
  - Better suited for deep pattern analysis

THANK YOU

DAMANJIT.UBEROI@HP.COM

+91 965.097.2015