KNOW THE UNKNOWN®

Next Generation Monitoring of Mobile Networks : A Compulsion !!

Krishna Sirohi
Sr. Advisor, Niksun

The Important Questions

- How Much Is Your Data Worth?
- How Much Is Your Intellectual Property Worth?
- How Much Is Your Reputation Worth?
- Same 3 Questions About Your Customers?

Technology Landscape Is Evolving

NIKSUN

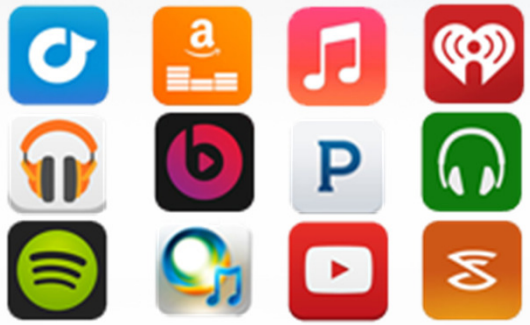
Convergent & Rich

Games and Apps

Virtual & SAS

Portable & Capable

Rich Multimedia



Chats

DYNAMIC INTERACTIVE

ANYTIME | **ANYWHERE** | **REAL-TIME**

Cost of Cyber Attacks and Downtime

- Annual Losses:
  - $400 Billion
  - 508,000 jobs in the U.S & up to $1 trillion globally

    – CSIS: The Economic Impact Of Cybercrime And Cyber Espionage Report
- Recovery:
  - Average $1,035,769
  - 32 days to resolve a cyber attack

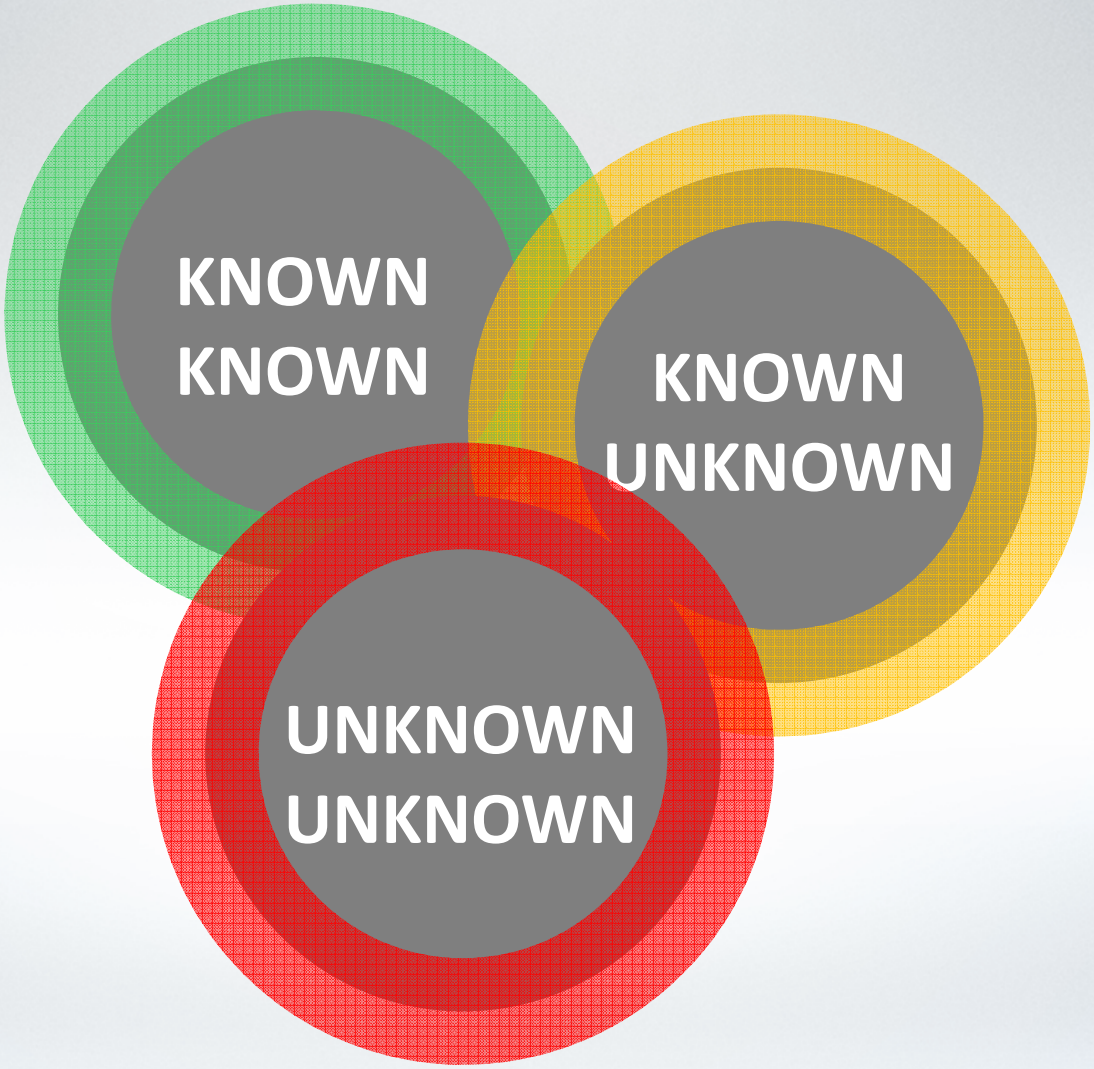
    –Ponemon Institute Cost Of Cyber Crime Study 2013
- Downtime:
  - Average $5,600 per minute
  - $300K+ per hour

    –Gartner: The Cost of Downtime (July 2014)

Challenges


What information was taken?
Why is my application slow?
How did it happen?
Who is responsible?
How to prevent it from happening again?

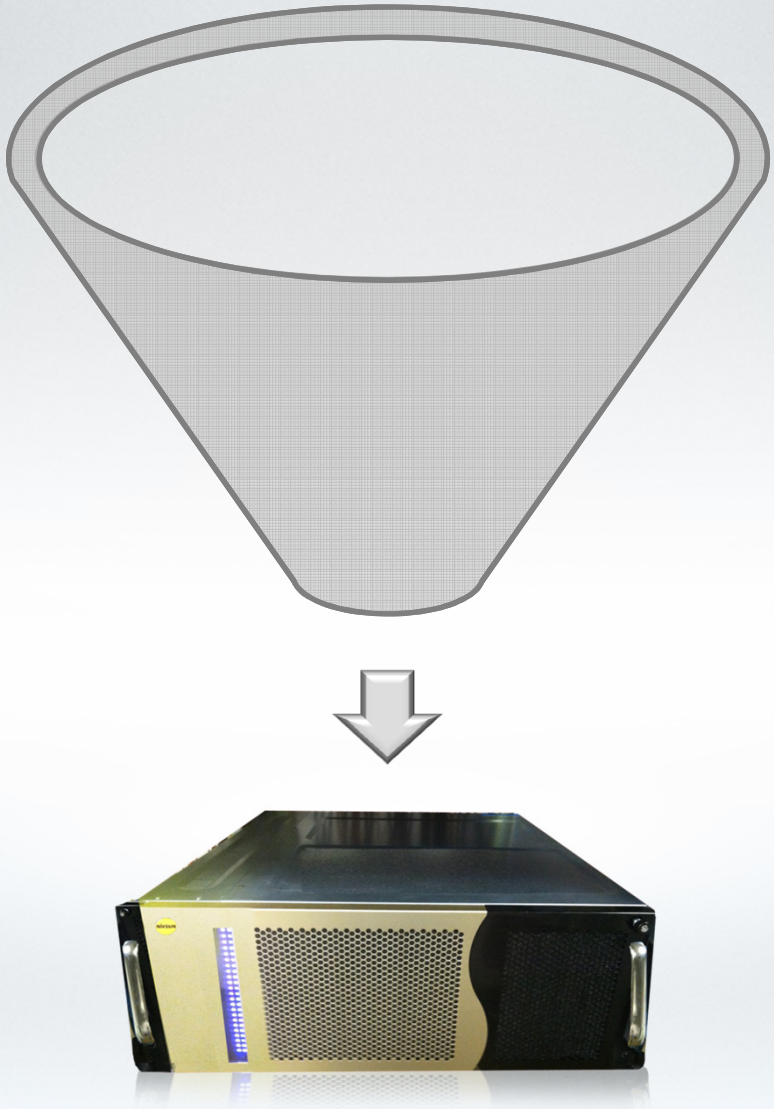
Modes of Intelligence



The Problem

How to Make the Unknown Known

Build Platform Something like …..



Leverage the Platform Capability for ..

Makes The Unknown Known

Continuously Captures All Necessary Data (Within Policy), At Line Speeds, Indexes Everything For Wire Speed Analytics.

Enables Proactive & Historical Analysis Of Knowns & Unknowns

Extremely Incident Resolution

Sophisticated, Real-time Data Mining

Powerful, Intuitive, Easy-to-use Web-based UI & Comprehensive API

Integrated with State of art Tools/Techniques

Modular Solution Can Grow Over Time; Completely Integrated

Out-of-the-box Analytics, Alerting, Reporting, Trending, Intelligence

The Integrated Powerful Security And Performance, All-in-one Common Data Warehouse

Network to Application Performance & Security

Specialize the Solution for ….

Cyber Security

Surveillance, Detection and Forensics

Network Performance

Proactive Network, Service and Application Monitoring

Mobility

Performance and Security Monitoring for Cellular Networks

Complete Suits of solution needed …

NetDetector® NetDetectorLive™	Security Monitoring Detection & Alerting Forensics
NetMobility® NetVoice®	3G & 4G Analysis VoIP Performance
NetVCR® FlowAggregator™ NetBlackBox Pro®	Performance Monitoring Flow Monitoring Troubleshooting
NetRTX™ NetSLM™ NetMulticast™ NetPoller™	SLA/QoS Alerting Advanced Analysis
NetOmni™ NetX™ Central Manager™ NetTrident™	Scalable Monitoring Reports Alerts Forensics
NetReporter™ NetXperts™	Reporting Expert Analysis

Specifics of Securing the EPC

Types of Generic Security Issues in Telecom Operations

- National /Regional Threat
  - The New weapon of warfare – neutralize the target before the first armed maneuvers.
- Competitive Weapon
  - Tarnish the brand – outage or performance ‘Headliners’
- Theft
  - Corporate IP or user data
  - Bandwidth, application or service theft
- Mischief or Errors
  - Network Mis-configuration,
  - Traffic Re-route or user data theft

Advance Persistent Threat (APT) :
Valid for Telecom Operation as well

- A National and Corporate 'time-bomb' controlled by an external entity
  - Spear-fishing and patience – objectives driven stealth take-over of facility controls
  - Multiple back-door access and control mechanisms established
    - It's not about quick returns –
- Establishing a long-term annuity with black-mail or destructive controls

Advanced (A): Advanced operators & techniques

Persistent (P): Persistent and stealthy over long time:"low and slow"

Threat (T): Intention to inflict damage and create loss

Sophisticated, well-founded and focused cyber operation targeting sensitive data, a specific entity or seeking to disrupt service.

Some Examples: Operation Aurora, Stuxnet, RSA incident, Lockheed Martin, etc.

LTE/EPC Security Issues…

4G/LTE is vulnerable to regular IP-based attacks.

- Broadly,
  - Attacks on infrastructure components:
    - DoS by Flooding, Crashes by protocol Fuzzing and Buffer Overflows
  - Theft of services:
    - Avoidance of billing, unauthorized services, impersonation
  - Attacks on other subscribers:
    - Masquerading, Spoofing, Spamming, Privacy Intrusions, Stalking, Over Billing, Fraud, Distributing Malware/Viruses, …
  - Analysis of EPC carrier configuration for competitive use
- EPC-specific threats due to EPC architecture, trust model, characteristics of radio interface

Security requirement in LTE/EPC Networks

- General Security Requirements
  - User Identity Authentication, Authorization and Protection
    - Identification of trusted entities: UEs and core network elements
    - Key management – Key derivation and propagation
    - Mitigation when trusted entities are compromised
  - User data protection
    - Encryption and Integrity protection
    - Bundled key derivation
    - User credential migration - Handover
  - Access Control
    - MME and HSS as security context anchor

Threats against LTE/EPC

- Threats against user identity
- Threats of UE tracking
  - Tracking a user based on IP address that could be linked to an IMSI
  - Tracking based on handover signaling message
- Threats related to handovers
  - Forcing a handover to compromise a eNodeB by strong signal
- Threats related to eNodeBs and last-mile transport links
  - Physical compromise of eNodeB
  - Packet injection at compromised eNodeB

Threats against LTE/EPC (contd.)

- DoS (denial of service) Threats
  - Radio Jamming
  - Distributed attacks from many UEs towards certain parts of the network
  - DoS attacks against the UE itself
- Misuse of network services
  - Flooding from compromised elements
- Threats against the radio protocol
  - Faking or modifying the first radio connection establishment message from the UE
  - Strong signal to attract target UEs to compromised eNodeB

Threats against EPC (contd.)

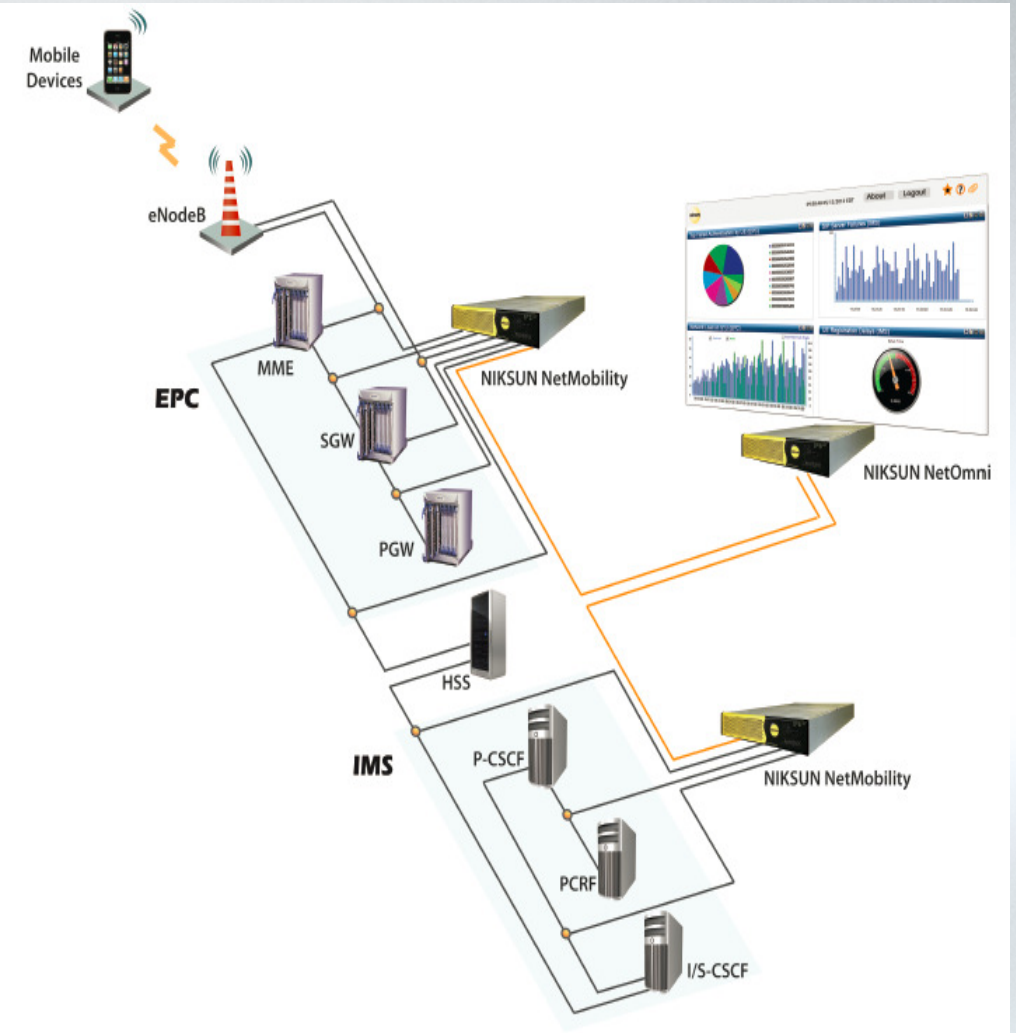
- Threats related to mobility management
  - Disclosure of sensitive data about users location
- Threats from inside the network
  - Malicious employees
  - Poor security policies and non-compliant deployments
  - Both could lead to:
    - Un-authorized access to core network infrastructures
      - Example: Manipulation of control plane data
    - Un-noticed breaches in user and network information
- Manipulation of control plane data
- Unauthorized access to the network

EPC Attack Scenarios

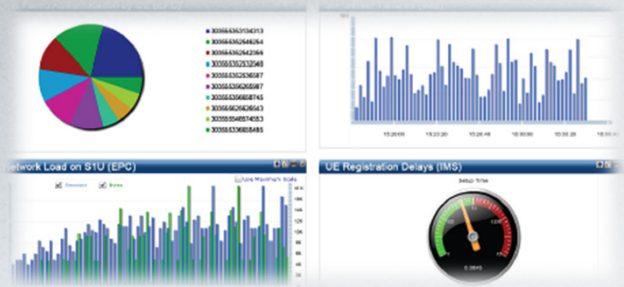
- Repeated Authentication Failures by a UE
  - Typically a mis-configuration or damaged UE
  - Causes a mini storm that loads the MME & HSS
  - Need to be able to trace/locate misbehaving UE
- Authentication storms
  - A deliberate DoS attack from multiple UEs
  - Severely loads MME & HSS
  - Need to enumerate IMSI, IMEI, NAI, IP address for blacklist
- Insider (employee) attacks
  - Login to EPC components and change LTE configurations
  - Location Privacy: tracking IMSIs & NAIs

Monitoring of Mobility – Network Visibility

- In depth analysis of EPC and IMS
- Real-Time Session Correlation
- Proactive Notification of Alarms
- Out of the box dash boards, analysis, alarms and reports

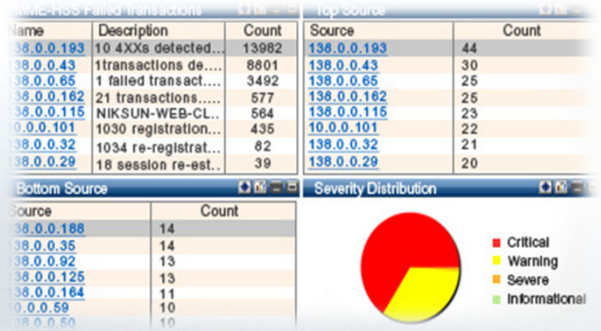


Real-time Mobile Network Analysis



- In-depth analysis as well as system load and performance metrics
- Applications and devices profiling

- Real-time correlation of events between EPC, IMS, and other layers
- Root Cause Analysis



- Real-time alarming on performance issues
- Out-of-the-box Expert Tools to assist with business needs

REPORTS: Real time or scheduled….. Conduct business based on facts

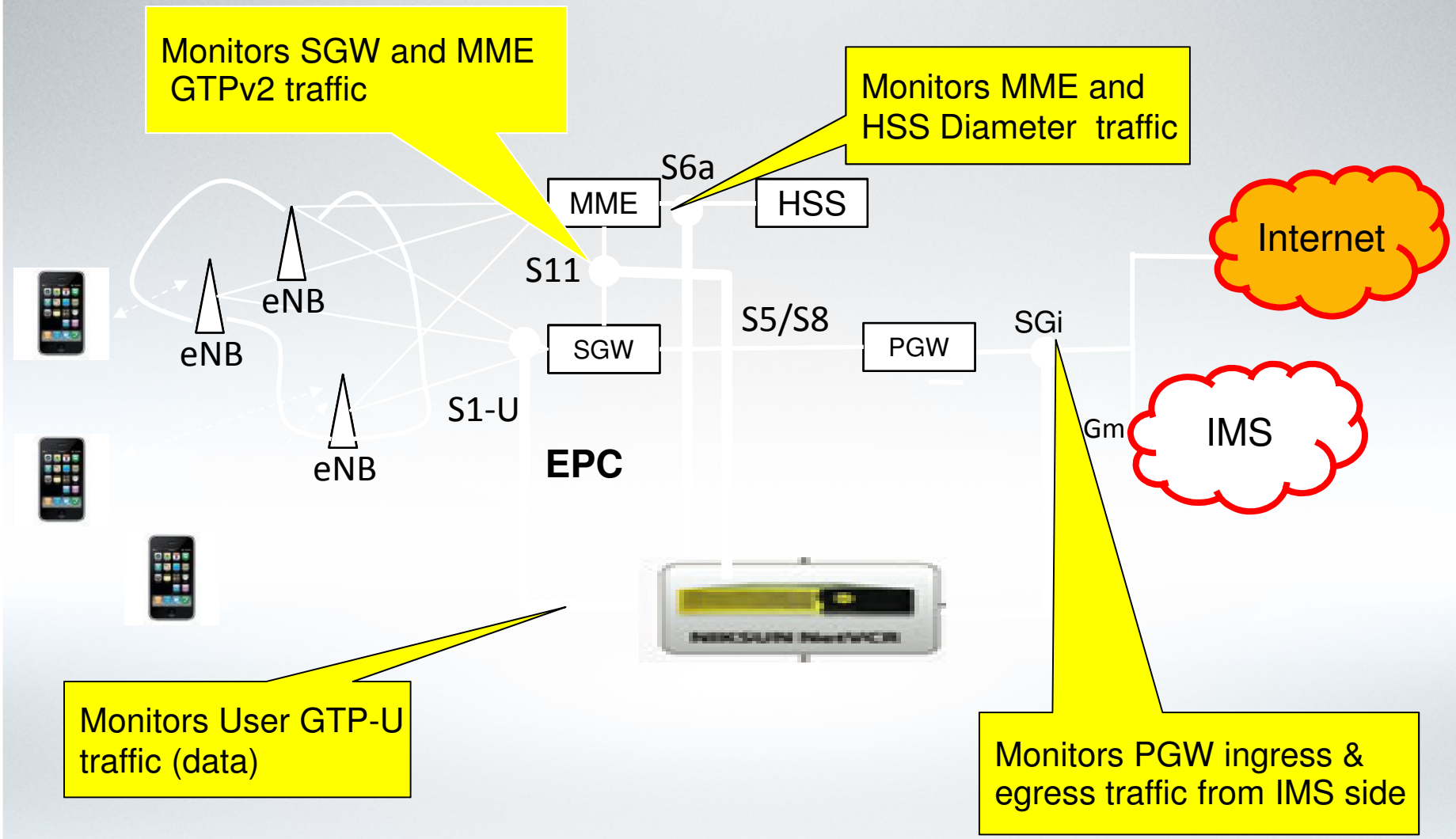
Performance & Security

When traffic behavior deteriorates…. (symptom)

- Authentication
- Unauthorized Traffic
- Restricted Apps
- Excessive traffic
- Denial of Service
- Tracking
- Indentify misbehaving mobile devices
- Spam Bots
- Malware
- Hosts Scans, Port Scans
- Host floods
- Host Pair Utilization
- Trojan (Pink Pony) type apps
- Infected devices, botnets, DoS attacks

…Is it **Performance** or is it a **Security** event??

Important Monitoring Points in 4G Network



Necessary features to ease Network Operations

- Monitoring Support for LTE/EPC and IMS Interfaces
- Monitor load and performance of core network entities and servers
- Network layer KPIs: e.g., *handoff latency, call set up delay, bearer set up latency*
- Service layer KPIs*: e.g., top talkers, registration rates, failed sessions, handoff rates*
- Subscriber application and device profiling to study user behavior and traffic patterns
- Predefined and user configurable displays, alarms and reports for EPC
- Drill down from EPC sessions to packet level details to troubleshoot performance and security problems
- Deep Packet Inspection (DPI) for mobile applications
- Network forensics for application reconstruction
- Possibly - A single device does all these and more

Necessary Security Tool at 4G Operation

- Identify misbehaving mobile devices
  - Infected devices, botnets, DoS attacks
  - Provide data for blocking botnets and propagation
- Trace security issues back to mobile device
- Create profile of traffic during malware propagation to help contain issue real-time
- Generate LTE long term trend reports to visualize anomalies.
- Generate Alarms and Events Reporting
- Track Key Security Performance Indicators (KSI) over time

Telecom Operations – Management Need

- KPI Reports
  - Data volumes by distribution location
    - Application and session details
  - Top locations for session failures
  - Overall Network Health
    - Aggregated reports from all locations
  - Capacity management
    - Connection and data volumes
    - Application information to drive intelligent caching
  - Track performance KPIs over time

Performance Metrics in LTE and IMS

- For operators, the focus is
  - The EPC core
    - Signaling or Control Plane – performance counters
    - User Plane – Traffic and Component KPIs
  - Network and Service Layers KPIs
    - User Devices and usage
    - Applications, Usage bandwidth
- Performance doesn't only means throughput, it also means:
  - Stability and reliability of the network,
  - Security and availability,
  - Scalability … etc

Performance Metrics in LTE and IMS

- Control Plane Performance Counters
  - Network Accessibility
    - “Call” or Bearer setup failures
  - Network Sustainability
    - Call Drops
  - Mobility (Handover)
    - Overall delay from handover preparation, execution and bearer traffic transfer
- User Plane KPI’s measures
  - Network throughput (eNodeB to SGW to PGW)
  - IMS user plane traffic
    - Bearer KPI’s in LTE applies
    - IMS control plane KPI are end-to-end measure (e.g., session setup delay)

Sample Monitoring Methods: EPC/IMS

- Anomaly alerts for unusual levels of various KPI
  - Thresholds for rates of REGISTER, MESSAGE, errors, failures, …
- Scan de-tunneled LTE user data
  - Set thresholds for AUP violations
  - IDS signatures for attacks involving UEs
- Correlate traffic between S11, S5/S8, SGi, Gm, Mw and Cx/Dx interfaces
  - A mismatch implies dropped packets
  - UE tracking and application profiling by correlation NAI and IMSI
- Correlate traffic between LTE & IMS interfaces
  - Get a view of delays and overall “customer experience”.
  - Investigate transactions that have unusual delays

Tracking Mobile Devices

Problem: How to determine device behavior such as device spoofing, most talkative devices and applications per device

- Identify device types with specific application
- Track MEID to detect spoofed devices
- Identify Non-conformant devices

Capacity planning, popular application and user behavior

Application Profiling Per User

Problem: Killer application consumes radio resources and network bandwidth resulting in poor QoS and QoE.

- Identify top applications and associated network traffic distribution
- Identify top clients for a specific application
- Identify top applications for a specific client

Capacity planning, popular application and user behavior

LTE KPIs (Performance)

Metrics	Use	Response
Aggregate rates of LTE traffic rates per device (MME, SGW, PGW, …)	Measure of system load and congestion.	Configure alarms if target thresholds are crossed.
Top Traffic and Request rates per UE	Identify excessive usage by a subscriber	Isolate UE if this is an attack.
Transaction mean response times	Measure of system load and congestion.	Re-balance load if thresholds are crossed.
Handover rates, overall and per UE	Identify cells or UEs with excessive hand offs.	Investigate and re-configure network
Session setup times, session counts & mean durations	Measure of system load and congestion for capacity planning.	Increase capacity

LTE KPIs (Security)

Metrics	Use	Response
Authentication failures, overall and per UE	Identify source of excessive attempts	Isolate UEs if necessary
Overall S6a failures	Identify source of attacks or misconfiguration.	Remediate
Excessive IPsec SA setup failures	Recognize hacking attempt	Block source
Access to LTE servers from new IP addresses	Possible attacks from insiders	Review audit logs, Trace source IP address
IDS Signatures	Identify attempts to attack LTE servers	Trace source IP address

NIKSUN:

Helping You *Know the Unknown*®

For additional information:

Visit us at niksun.com or

email to info@niksun.com