CQR

IEEE COMMUNICATIONS SOCIETY

IEEE

Reef Point SYSTEMS

EXTREME SECURITY FOR A CONVERGED WORLD

IEEE CQR 2006, London

Validating Deployment Readiness for Fixed Mobile Convergence (FMC)

Scott Poretsky

Reef Point Systems

sporetsky@reefpoint.com

Quality FMC Networks

- **Service Providers now planning Fixed-Mobile Convergence (FMC) deployments**
  - **Unlicensed Mobile Access (UMA)**
  - **IP Multimedia Subsystem (IMS)**

Quality Network

- **Secure**
- **Available**
- **Deterministic**
- **Scales/Performs**

Network Users Observe “Quality”

Eliminate Security/Performance Tradeoff

Does TSA run your network?

“The first line of protection starts by deploying a high-performance infrastructure…These [Security] mechanisms consume server resources so need to rely on solid performance.” [1]

FMC Test and Deployment Challenges

- **Capacity Challenges**
  - Handset sales projected to exceed 100 million by 2009
  - Millions of subscriber endpoints requiring simultaneous authentication and access to the network
- **Control Plane Performance Challenges**
  - 100s of 1000s of roaming users cause frequent setups and tear downs
- **Security Challenges**
  - Heightened security risks for networks and handsets
  - Off-net mobile users introduce vulnerable “Phantom Last Mile”
  - Need to eliminate trade-off of security and performance

Unprecedented Network Demands Require Thorough Device Testing

Test Innovations for FMC Deployments

- **Test tools do not exist to validate deployment readiness**
  - **Need to:**
    - **benchmark control plane capacity and performance**
    - **benchmark data plane forwarding performance**
    - **evaluate IP, SIP, and IKE DoS protection**
    - **benchmark performance during DoS attacks**

- **Necessary to develop FMC test topologies combining**
  - **Freeware test tools**
  - **Internally-developed test tools**
  - **Commercial test tools**

Test Innovations are Required to Validate Deployment Readiness

UMA Performance Benchmarks

- **Authorization**
  - AAA/RADIUS lookup rate
- **Tunnel Establishment**
  - IPsec tunnel establishment rate (TPS)
  - IPsec tunnel setup delay
  - IPsec tunnel capacity
- **Media Flow Performance**
  - IPsec forwarding performance
    - Throughput, delay, jitter, MOS
  - Voice microflow rate-limiting
- **DoS Protection**
  - IKE DoS attacks
  - IP DoS attacks
  - IP Malformed packets

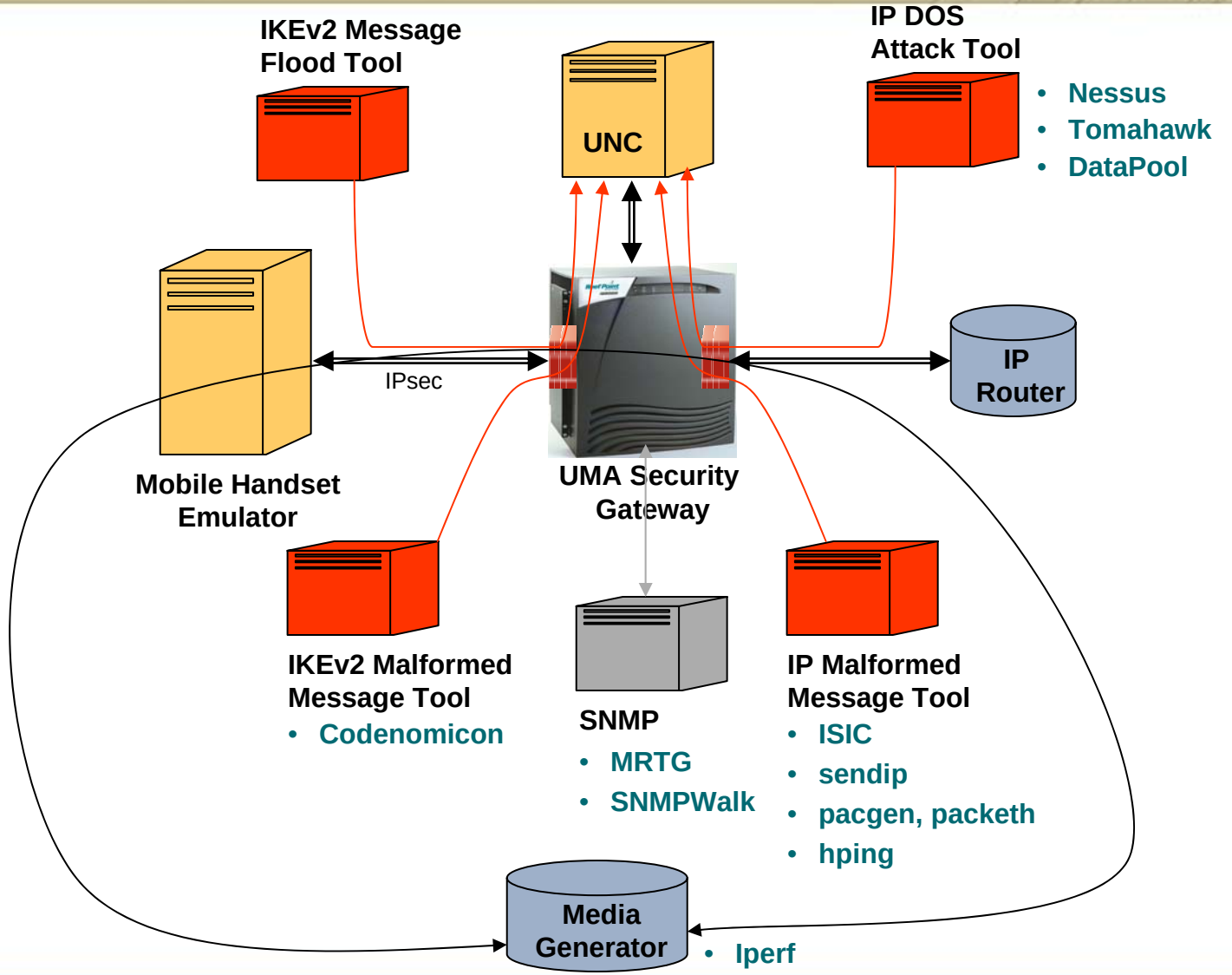
REPEAT BENCHMARK TESTS with:
- **All Supported Crypto Suites**
- **Under DoS Attacks**

UMA Security Risks:

ID Spoofing
IP Malformed Packets
IP DoS Attacks
IKE Malformed Packets
IKE DoS Attacks

UMA Introduces Unprecedented Testing Requirements

UMA Benchmark Topology



IMS Performance Benchmarks

- **Authorization**
  - AAA/DIAMETER lookup rate
- **Call Establishment**
  - Encrypted signaling
    - IPsec tunnel capacity
  - SIP call control
    - CAPS, CPS
    - SIP call pinhole capacity
- **Media Flow Performance**
  - SIP media pinhole capacity
  - SIP media forwarding performance
    - Throughput, delay, jitter, MOS
  - SIP media microflow rate-limiting
- **DoS Protection**
  - SIP DoS attacks
  - IP DoS attacks
  - IP malformed packets

REPEAT BENCHMARK TESTS with:

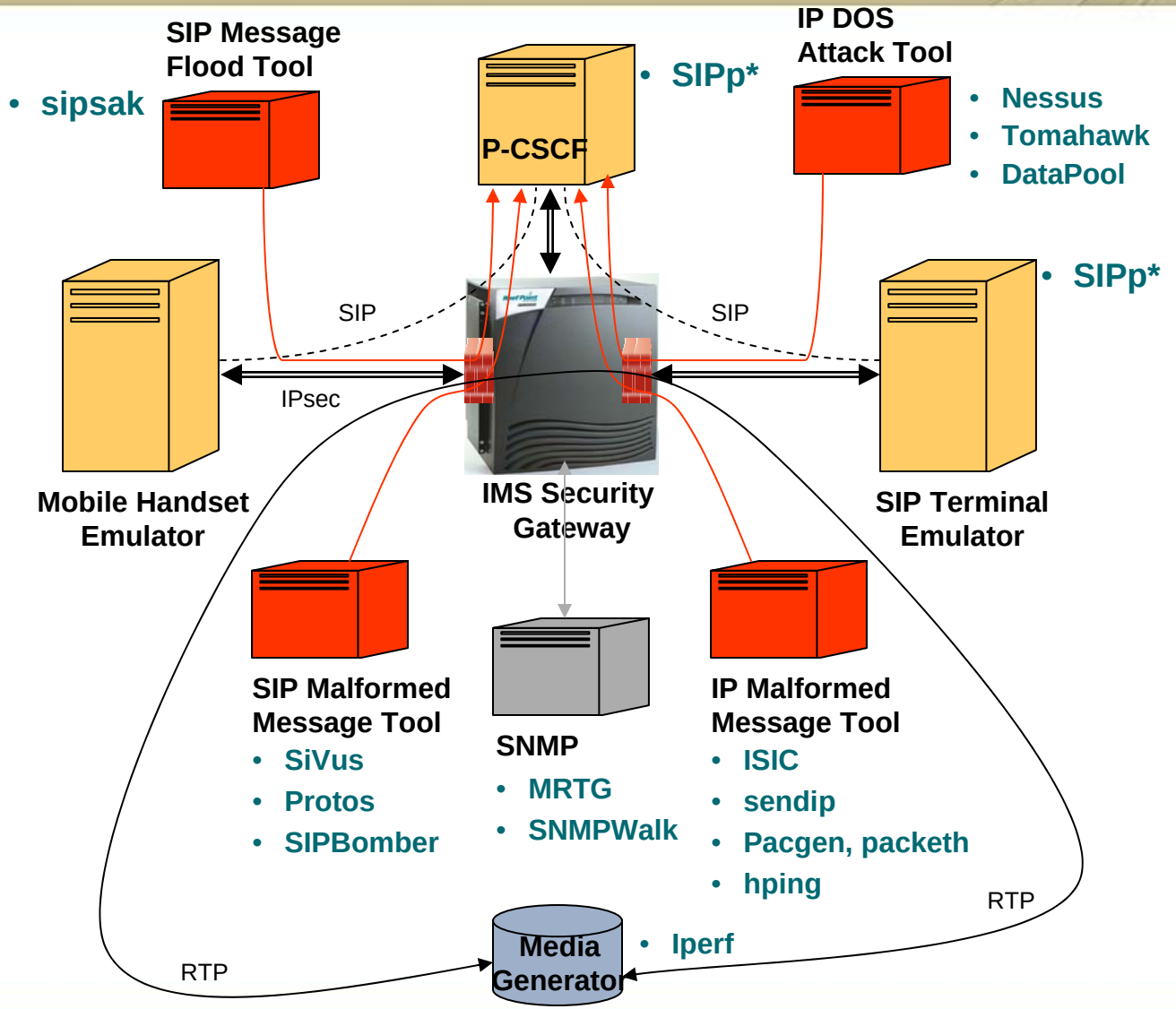
- All Supported Crypto Suites
- Under DoS Attacks
- With and Without Security Gateway

Security Risks:

ID Spoofing
IP Malformed Packets
IP DoS Attacks
SIP Malformed Packets
SIP DoS Attacks
RTP Media Flooding

IMS Introduces Unprecedented Testing Requirements

IMS Benchmark Topology



*SIPp REQUIRES MODIFICATIONS:

- Support for 3GPP SIP headers
- Extensions for signaling media characteristics

Conclusions

- **Network Users demand quality FMC networks for voice and multimedia communication**
- **FMC networks introduce unprecedented scaling, performance and security test and deployment requirements**
- **Test innovations are required to validate FMC deployment readiness**
  - **Smart application of freeware test tools**
  - **Internally-developed test tools**
  - **Build test topologies combining all tools**

References

[1] Schäfer**,** Günter, Sisalem Dorgham, and Kuthan, Jiri,

"DENIAL OF SERVICE ATTACKS AND SIP INFRASTRUCTURE: Attack Scenarios and Prevention Mechanisms",
www.snocer.org/Paper/sisalem_dos.pdf, 2005.

Reef Point SYSTEMS

EXTREME SECURITY FOR A CONVERGED WORLD

Scott Poretsky
Reef Point Systems
8 New England Executive Park
Burlington, MA 01803 USA
main +1 781 505 8300 / fax +1 781 505 8316
sporetsky@reefpoint.com
www.reefpoint.com