# CQR

# Proceedings of Experts Workshop on Network & Payload

*Hosted by:*

BT

IEEE COMMUNICATIONS SOCIETY

BT

Lucent Technologies
Bell Labs Innovations

*Technical Sponsorship by :*

Bell Labs, Lucent Technologies
IEEE COMSOC CQR

6 October 2006

London, U.K.

# Welcome

## Jim Runyon

## Chair, Network & Payload Experts Workshop

Technical Manager, Bell Labs NRSO
Co-Leader, NRSC Special Study on DCS Outages
Leader, NRSC Special Study on Network Synchronization
Leader, NRSC Special Study on Northeast Power Outage
Leader, NRSC Special Study on DS3 Simplex Conditions
Leader, NRIC Wireless and Internet Network Reliability Sub-Team
Leader, Homeland Security – Physical Security Sub-Team
Project Manager, NRIC Industry Best Practices Web Site

# Welcome

## Stuart Goldman

**Co-Chair, Network & Payload Experts Workshop**

Consulting Member of Technical Staff, Bell Labs NRSO
Contributor, IETF IEPREP, ECRIT, GEOPRIV
Member, NSTAC NGNTF VTMWG
Contributor, ITU-T SG-11, SG-2
Vice-Chair, ATIS PTSC-SAC
Chair, ATIS PTSC-IOP
Past-Chair, ATIS NIIF
Inventor, 14 U.S. Patents

# Agenda

| | |
|---|---|
| 9:00 | Welcome, *Rick Krock & Peter Hoath, IEEE CQR 2007 Workshop Co-Chairs* |
| 9:05 | EC ARECI Study, 8 Ingredient Framework, *Karl Rauscher, Bell Labs* |
| 9:35 | Message from Host, *David Donegan, BT* |
| 9:50 | Introductions, *All* |
| 10:00 | Overview of 2 Ingredients, *Jim Runyon, Network & Payload Workshop Chair* |
| 10:15 | Electronic Voting, *All* |
| 10:30 | Identification of Top Concerns, *All* |
| *12:30* | *Lunch* |
| 13:30 | Guidance for Addressing Top Concerns, *All* |
| 15:00 | Electronic Voting and Feedback, *All* |
| 15:15 | Next Steps and Closing Remarks, *Karl Rauscher* |

# ARECI Study

*The aim of this study is to develop a forward-looking analysis of the factors influencing the* ***availability*** *of electronic communication networks and of the adverse factors acting as potential barriers to the development of global networked economies by lowering their dependability.*

Information Society and Media
Directorate-General

# 8 Ingredient Framework

## COMMUNICATIONS INFRASTRUCTURE

| | | | |
|---|---|---|---|
| Power | Software | Payload | Human |
| Environment | Hardware | Networks | Policy |

NRIC

WIRELESS EMERGENCY RESPONSE TEAM

NATIONAL SECURITY TELECOMMUNICATIONS ADVISORY COMMITTEE NSTAC

NRSC

CQR

IEEE

IEEE COMMUNICATIONS SOCIETY

| Workshop | Ingredients | Date | Location | Hosting Stakeholders |
|---|---|---|---|---|
| 1 | Power<br>Environment | Tuesday<br>October 3 | Rome, Italy | Ministry of Communications, Italy |
| 2 | Network<br>Payload | Friday<br>October 6 | London, U.K. | BT |
| 3 | Hardware<br>Software | Wednesday<br>October 11 | Berlin, Germany | Rohde and Schwarz |
| 4 | Policy<br>Human | Wednesday<br>November 15 | Brussels | t.b.d. |

*"These ground breaking workshops are bringing together experts for rigorous discussions on Europe's future communications networks. The systematic coverage of all eight of the fundamental ingredients of communications infrastructure will lead to improving the availability and robustness of our networks. These workshops are a* ***necessary role model*** *for achieving consensus for Europe's ICT community. I am certain that the output of these workshops will provide bold, actionable and much needed guidance to the communications industry, member state governments and European Commission. I strongly urge the* ***continuation of this process****."*

- Dr. Luisa Franchino, Director General, Italian Ministry of Communications

5 October 2006

REPVBBLICA ITALIANA

*Ministero delle Comunicazioni*

**Experts Workshop**
**on Power & Environment**
3 October 2006 - Rome, Italy

# Message from the Host

## David Donegan

Head of Business Continuity, BT Group

# Overview of 2 Ingredients

**Networks**

**Payload**

The various topological
- configurations of nodes
- synchronization
- redundancy
- physical and logical diversity
- network interconnections
- availability
- operations

Transported Content on network
- Signaling
- Voice
- Data
- Multimedia

Payload Security
- Information interception
- Information corruption

Traffic patterns and statistics

# Intrinsic Vulnerabilities

## Networks

## Payload

| VULNERABILITY |
|---|
| capacity limits |
| points or modes of failure |
| points of concentration (congestion) |
| complexity |
| dependence on synchronization |
| interconnection (interoperability, interdependence, conflict) |
| uniqueness of mated pairs |
| need for upgrades and new technology |
| automated control (*via software) |
| accessibility (air, space or metallic or fiber) |
| border crossing exposures |

| VULNERABILITY |
|---|
| unpredictable variation |
| extremes in load |
| corruption |
| interception |
| emulation |
| encapsulation of malicious content |
| authentication (mis-authenticaton) |
| insufficient inventory of critical components |
| encryption (prevents observablity) |

# Workshop Notes

## Identification of Top Concerns (page 1 of 7)

1 End-to-end security between content providers' equipment to information provider is needed

2 The integrity of global supply chain, especially with new and unknown suppliers, needs to be linked to network equipment vendors (i.e. unknown vulnerabilities can be introduced)

3 Identification and authentication information should be maintained through the various networks and network types (e.g., across different networks)

4 End-user identification and authentication from physical access to application layer should be maintained

5 Payload overload capabilities are needed for both wanted and unwanted offered traffic (e.g., peer to peer traffic)

6 Dynamic network control are needed since users can create virtual networks with no fixed boundaries.

7 There is a need for security awareness within the network. Security status and awareness monitoring implies that security metrics are needed

8 New applications and services need to tested for correctness and good behavior

9 The impact of video traffic on bandwidth causes major network management problems (e.g., facilities, management)

# Workshop Notes

## Identification of Top Concerns (2 of 7)

10 SPIT (SPAM over IP Telephony) will negatively impact network capacity

11 Network protection is needed against viruses or SPAM that is encapsulated (or encrypted) and traveling across the network

12 There are no standards for 100 GB Ethernet

13 Anticipating customer bandwidth demand is a concern because of emerging applications (e.g., self built applications by the customer). Bandwidth is dictated by the end customer

14 The various degrees of resilience in convergence between voice and data network (e.g., WIFI, GSM, UMTS, ADSL) is a concern.

15 The network should be able to determine the user's access methods and allocate appropriate resources, and limit the allocated resources to only what the user can obtain from the access method.

16 End-user traceability through the network in the context of multiple technologies and networks is needed

17 The security of infrastructure that provides services (routers, switches) should be both logically (cyber) and physically secure for the control, user, and management planes

# Workshop Notes

## Identification of Top Concerns (3 of 7)

18 The future network has the appearance of a highly resilient mesh network, but it may be compromised by the lack of physical diversity brought about by old infrastructure limitations (i.e. it doesn't have the perceived diversity).

19 Protecting the legacy network against attack is important since there are insufficient SS7 firewalls

20 For core IP networks, traffic engineering (vs. over-engineering) is needed to efficiency handle multi-cast traffic.

21 Off-shore (i.e. outside the area of legislation) maintenance of the network (including contact centers, support centers, and development networks) requires traceability and trustworthiness of maintenance actions

22 Physical security concerns for co-location common areas, common facilities (e.g., ducts) is a continuing problem (e.g., calling before you dig).

# Workshop Notes

## Identification of Top Concerns (4 of 7)

23 Remote access control by third party suppliers to networks, including uncontrolled physical access at common sites (plugging directly into equipment) is a serious vulnerability

24 Frame (cabinet) level alarming is being used to manage physical security access to equipment

25 Sensitive user-plane data and control data protection is needed

26 Mechanisms are needed for tracing user activities (i.e. from the user) and traceability (i.e. back towards the user).

27 There are commercial implications of network management mandates by the government

# Workshop Notes

## Identification of Top Concerns (5 of 7)

28 Market demand (i.e. offered traffic) can exceed network capacity (e.g., local hot spots such as sports stadiums). Providers must plan for these cases.

29 The robustness of network equipment to electronic attack or the effects of misconfiguration is a concern.

30 Environment (e.g., temperature) conditions affects network performance and are not modeled in network performance metrics.

31 Virtual users (e.g., home appliances with IP addresses) cause different traffic profiles than humans. Modeling traffic patterns far enough into the future is needed.

32 New applications typically have no security and will compromise the networks' resiliency and robustness. No one wants to pay for added security.

33 With the increased number of common components in many platforms, there is a increase in 'common mode failures.' Strategies are needed to mitigate against cascade failures and prevent amplification effects.

34 Vendor diversity may not give the resilience expected (e.g., use of common components, Operating Systems and platforms).

# Workshop Notes

## Identification of Top Concerns (6 of 7)

35 End-to-end traceability issues need to be addressed (e.g., who, what, when. Step-by step-traceability, how long to store the information, NAT issues, different forms of identity of the end user (i.e. E164 address, IP address, etc))

36 End user devices are becoming part of the network (e.g., user have access to signaling SIP).

37 Hijacking of control protocols is a concern (i.e. standards are freely available in public domain resulting in movement from a closed to an open network)

38 Content: how to verify that it conforms to the relevant standard (e.g., MPEG misreporting file size through open parameters). Options should be closed off. Who is responsible?

39 Where should standards conformance be confirmed (e.g., at the gateway)?

40 Content launched onto the network must conform to standards? Whose responsibility should that be? How does net neutrality play into this?

41 Standards divergence: do we need consolidation and who should lead?

42 Many versions of the same standard co-exist on a network. Options cause headaches. Even change requests become options and create more holes.

43 Different interpretations of standards by different people occur even at the option level.

# Workshop Notes

## Identification of Top Concerns (7 of 7)

44 Backward compatibility with TDM causes problems. Is there a way to reduce the backward dependency which adds complexity and creates vulnerabilities?

45 Per hop and per network behaviour is understood but end-to-end conformative service delivery (i.e. feature transparency) has not been addressed.

46 End point authentication and authorisation with respect to user mobility is needed (i.e. authenticate the terminal, person, service set, etc.). Verifying the compatibility of end point terminal with the network is needed.

47 Priority at the packet level is needed. Protocols are crude for providing priority services. Priority is needed both for signaling and payload. Misuse of priority could lead to DoS.

# TOP VOTED CONCERNS

# Workshop Notes

## Summary: Top Voted Concerns

7 **There is a need for security awareness within the network.  Security status and awareness monitoring implies that security metrics are needed**

- 3 Identification and authentication information should be maintained through the various networks and network types (e.g., across different networks)
- 4 End-user identification and authentication from physical access to application layer should be maintained
- 5 Payload overload capabilities are needed for both wanted and unwanted offered traffic (e.g., peer to peer traffic)
- 16 End-User traceability through the network in the context of multiple technologies and networks is needed

9 **The impact of video traffic on bandwidth causes major network management problems (e.g., facilities, management)**

- 12 There are no standards for 100 GB Ethernet
- 13 Anticipating customer bandwidth demand is a concern because of emerging applications (e.g., self built applications by the customer).  Bandwidth is dictated by the end customer
- 15 The network should be able to determine the user's access methods and allocate appropriate resources, and limit the allocated resources to only what the user can obtain from the access method.
- 20 For core IP networks, traffic engineering (vs. over-engineering) is needed to efficiency handle multi-cast traffic.

IEEE COMMUNICATIONS SOCIETY

# Workshop Notes

## Summary: Top Voted Concerns

**36 End user devices are becoming part of the network (e.g., user have access to signaling SIP)**

- **Non standard standards.**
  - 38 Content: how to verify that it conforms to the relevant standard (e.g., MPEG misreporting file size through open parameters). Options should be closed off. Who is responsible?
  - 39 Where should standards conformance be confirmed (e.g., at the gateway)?
  - 40 Content launched onto the network must conform to standards? Whose responsibility should that be? How does net neutrality play into this?
  - 41 Standards divergence: do we need consolidation and who should lead?
  - 42 Many versions of the same standard co-exist on a network. Options cause headaches. Even change requests become options and create more holes.
  - 43 Different interpretations of standards by different people occur even at the option level.

**46 End point authentication and authorisation with respect to user mobility is needed (i.e. authenticate the terminal, person, service set, etc.). Verifying the compatibility of end point terminal with the network is needed.**

# Guidance for
# TOP VOTED CONCERNS

# Workshop Notes

## Guidance for Addressing Top Concerns (page 1 of 5)

**7 There is a need for security awareness within the network. Security status and awareness monitoring implies that security metrics are needed**

3 Identification and authentication information should be maintained through the various networks and network types (e.g., across different networks)

4 End-user identification and authentication from physical access to application layer should be maintained

5 Payload overload capabilities are needed for both wanted and unwanted offered traffic (e.g., peer to peer traffic)

16 End-User traceability through the network in the context of multiple technologies and networks is needed

**Countermeasures:**

- Using a rules-based analysis that correlates multiple sources of information (e.g., expert system) addresses this problem
- Businesses should have a homogeneous security policy
  - Providers will have to identify what needs to be protected
- There are two potentially conflicting concerns: 1) monitoring the security of the network, and 2) monitoring the activity of the users (privacy issues)
- A standardized definition of metrics needs to be created at a business or service level (note: There is an ISO group addressing this item)
  - Auditing against SOX also addresses this issue
- Recommendations are needed on deployment of geo-probes (i.e. network monitors) for protocol anomaly detection
  - IDS/IPS intrusions detection mechanisms can be used at the edges of the network. Deep packet inspection capability in the core network probably cannot be done.
- End user equipment security will be required to address malware.

# Workshop Notes

## Guidance for Addressing Top Concerns (page 2 of 5)

**9 The impact of video traffic on bandwidth causes major network management problems (e.g., facilities, management)**

12 There are no standards for 100 GB Ethernet

13 Anticipating customer bandwidth demand is a concern because of emerging applications (e.g., self built applications by the customer). Bandwidth is dictated by the end customer

15 The network should be able to determine the user's access methods and allocate appropriate resources, and limit the allocated resources to only what the user can obtain from the access method.

20 For core IP networks, traffic engineering (vs. over-engineering) is needed to efficiency handle multi-cast traffic.

**Countermeasures:**

- Standards are needed
  - For higher bandwidth (e.g., 100 GB Ethernet)
  - For Bandwidth optimization in multi-cast networks
  - For signaling (e.g., video on demand, enhanced video)
  - For CAC (note: CAC is needed but does not solve the problem of exponential bandwidth growth)
  - For standardized compression schemes beyond MPEG4 for HDTV
- Uni-cast may require localized (i.e. close to the customer) video servers and intelligent packet filters
  - Uni-cast video requires detailed planning and engineering, using memory in place of bandwidth
- Tools for lawful intercept of video are needed

## Guidance for Addressing Top Concerns (page 3 of 5)

**36 End user devices are becoming part of the network (e.g., user have access to signaling SIP)**

Issues include:

- Is SIP traffic “genuine”?
- Is the sender allowed to send it?
- Hijacked end user device can be used as DoS agent

**Countermeasures:**

Force encryption of network control messages

Authentication and authorisation of network control messages is needed but will come at a cost.

Firmware protocols are OK for blocking less sophisticated attackers only

Physical network connections are the definitive identity points. Forcing the correlation of the physical layer access with higher protocol layers will identify the packet sender (i.e. the application is tagged with the location)

Force the use of two factor authentication. However, this creates usability/mobility issues across different devices and locations. This could require multiple tokens.

Limit the rates on signalling or sessions to prevent DoS

Detect anomalous traffic patterns.

Incorporate a Trusted Computing Model to shut down devises with unauthorized software modifications, or have some form of security method running on the end user device.

# Workshop Notes

## Guidance for Addressing Top Concerns (page 4 of 5)

**Non standard standards.**

**38 Content: how to verify that it conforms to the relevant standard (e.g., MPEG misreporting file size through open parameters). Options should be closed off. Who is responsible?**

**39 Where should standards conformance be confirmed (e.g., at the gateway)?**

**40 Content launched onto the network must conform to standards? Whose responsibility should that be? How does net neutrality play into this?**

**41 Standards divergence: do we need consolidation and who should lead?**

**42 Many versions of the same standard co-exist on a network. Options cause headaches. Even change requests become options and create more holes.**

**43 Different interpretations of standards by different people occur even at the option level.**

**Countermeasures:**

Standards certification needs to be created and required.

Standards should drive technology rather than the other way around. Skype bucks the trend.

Interconnect tests can be very costly, are time intensive, and can only perform a reduced set of tests in practice.

Formal application testing would help solve problem.

Protocol enforcement should be carried out by appropriate authorities (i.e. Protocol Police).

Standards bodies should be lobbied to reduce or eliminate the number of options at the inception of a standard.

Standards bodies are voluntary so a higher authority should limit options

Agreements between autonomous systems for QoS need to be established. Carriers cannot be forced to go to the latest vendor software release. Vendors cannot be forced to go to the latest release of the standards.

Inter-network communications need to be standardised.

# Workshop Notes

## Guidance for Addressing Top Concerns (page 5 of 5)

**46 End point authentication and authorisation with respect to user mobility is needed (i.e. authenticate the terminal, person, service set, etc.). Verifying the compatibility of end point terminal with the network is needed.**

No unification of authentication/authorisation across networks and terminals (e.g., secure token, iris scan, fingerprint, SIM card).

**Countermeasures:**

Careful trade-off between authentication choices and privacy must be considered.

Careful trade-off between security and resource are needed to accomplish this item (e.g., airport security lines).

Authentication should be considered at the network operator boundary and not at the device.

Technology that can reduce the overhead of providing authentication and authorisation services for every transaction should be examined .

Federated identity techniques should be integrated (i.e. one password to your table of passwords) with multi-factor authentication to increase security.

# Next Steps

IEEE CQR to Publish Proceedings on Web (October 2006)

Workshops 3 & 4 (October-November 2006)

Public Workshop (January 2007, Brussels)

ARECI Study Final Report to European Commission (February 2007)

IEEE CQR International Workshop (May 2007, Florida)

# Participants

Jim Runyon, Bell Labs

Stuart Goldman, ATIS, IETF, ITU-T & Bell Labs

Peter Hoath, IEEE CQR, BT

Robert Margrie, NISCC / CESG

Romeo Zwart, AMS-IX

Alistair Munro, University of Bristol

Fernando Sanchez, Lucent Technologies

Jorge Rabadan, Lucent Technologies

Kourosh Teimoorzadeh, SFR

Fabrice Bulian, SFR

Karl Rauscher, Bell Labs & IEEE CQR

David Donegan, BT

Alan Dye, Lucent Technologies

Ingolf Karls, Infineon Technologies

Emma Griffiths, Lucent Technologies

Aleksei Resetko, Lucent Technologies

Stuart Wyatt, McAfee

Stuart Bargman, Juniper Networks

Ray McKeown, BT

Bertrand Marquet, Alcatel

David Shaw, Lucent Technologies

Rick Krock, IEEE CQR & Bell Labs