

Telecom Security for Olympic Events

Prepared for:

2006 CQR Conference

Contact:

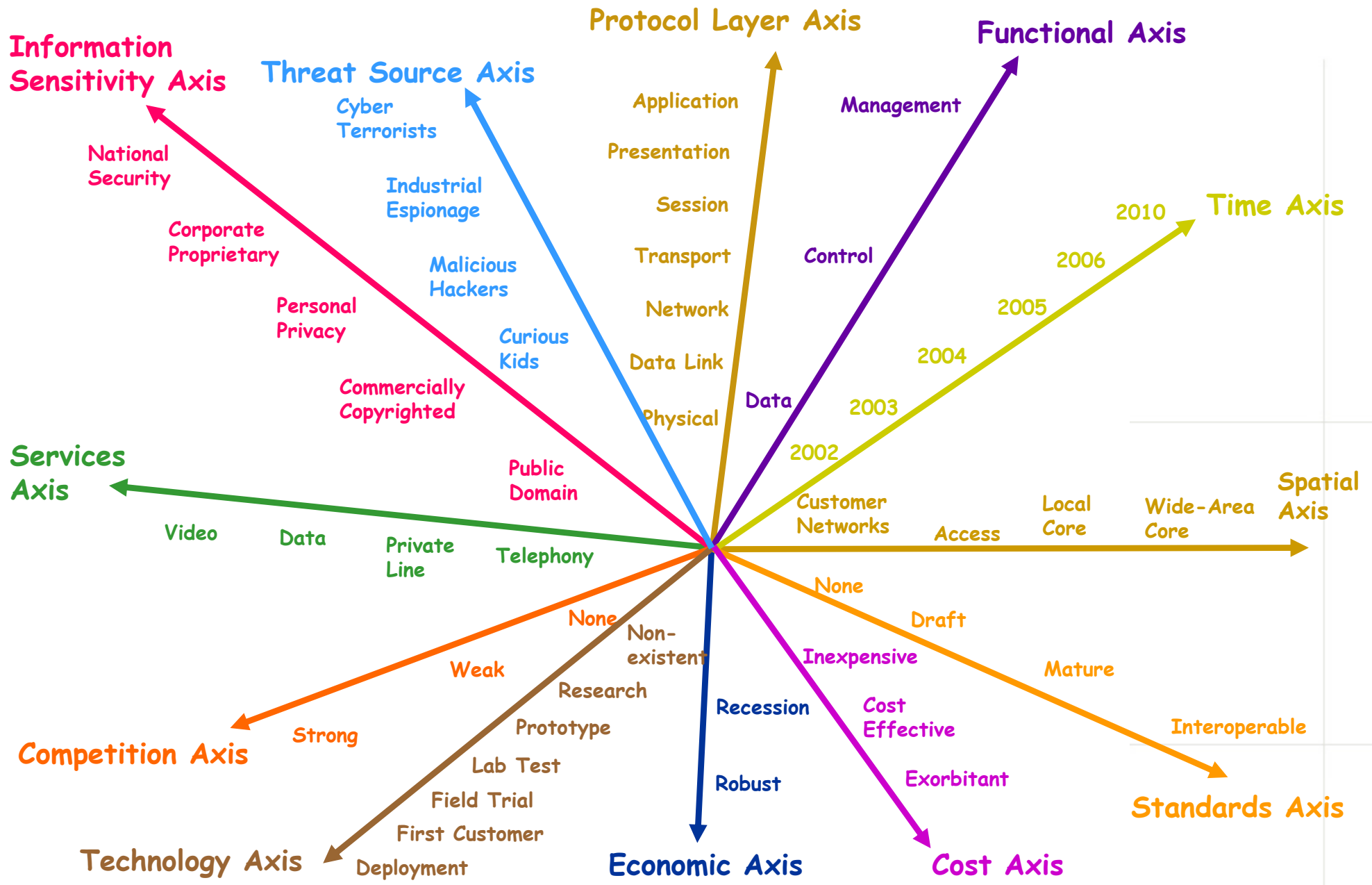
John Kimmins

jkimmins@telcordia.com

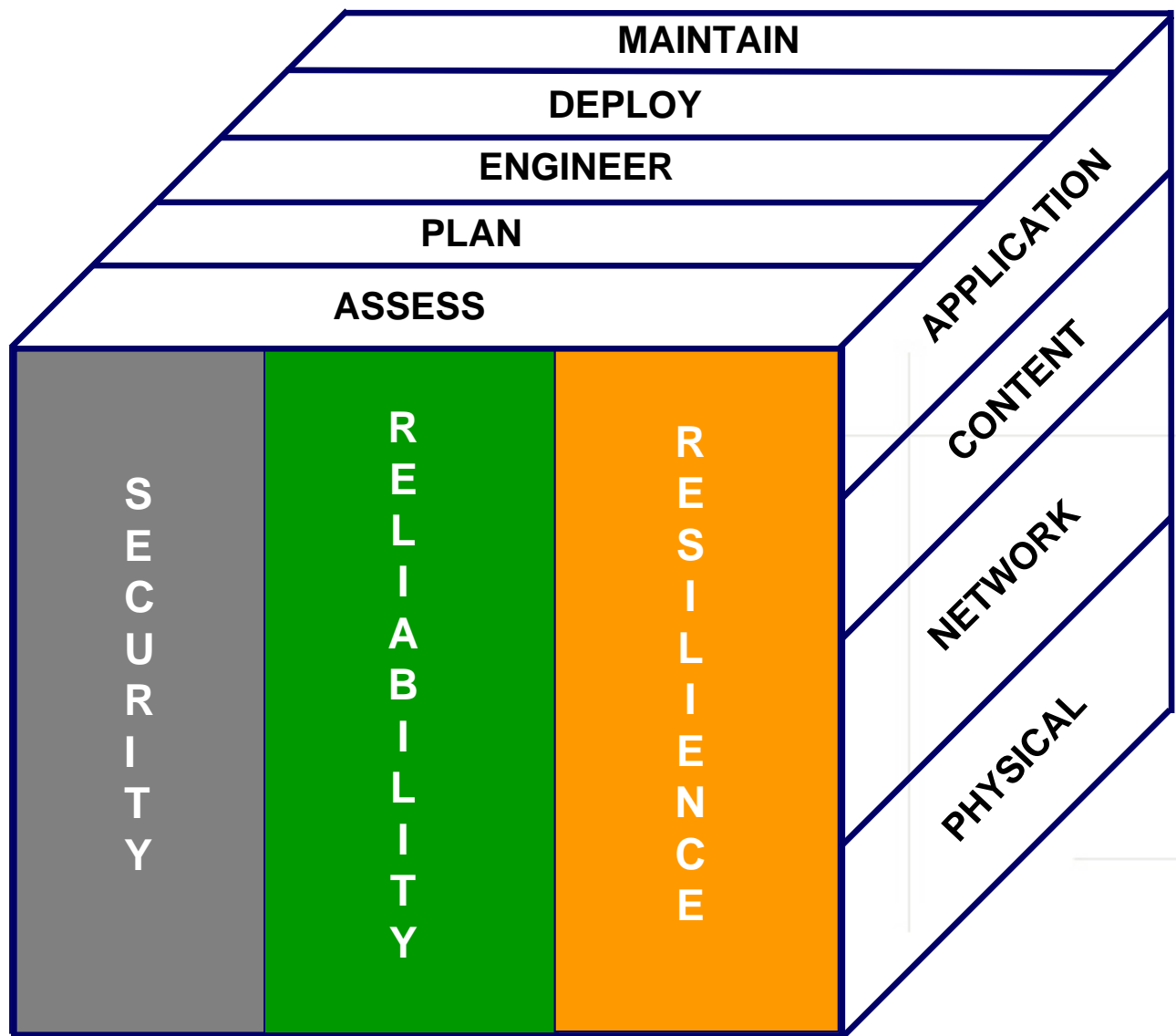
June 7, 2006



Multi-Dimensional Challenge



Another Look at Dimensions



Major Technical Security Challenges



- Circuit
- Packet

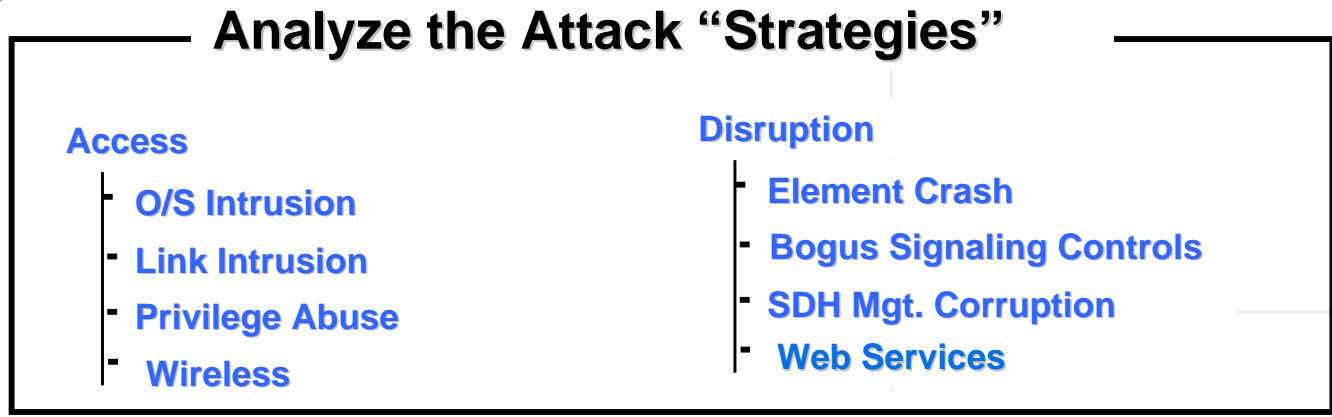
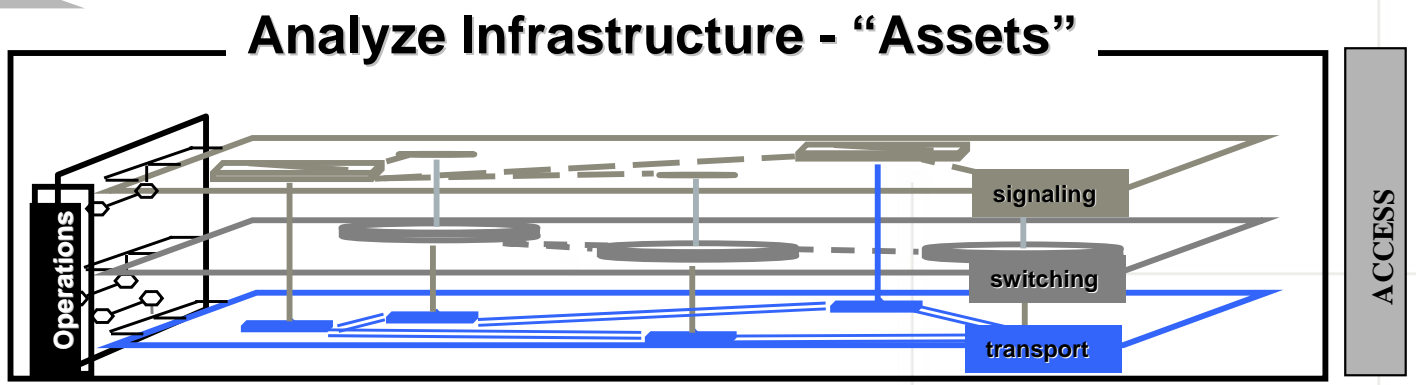
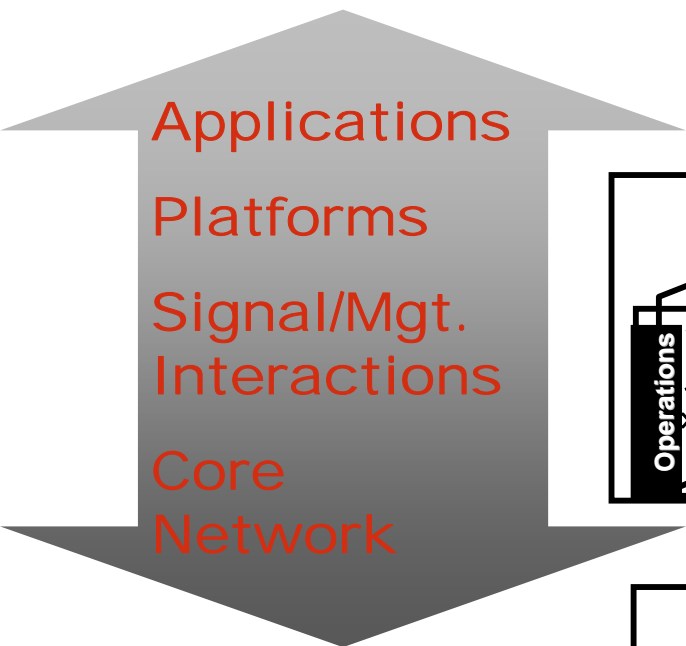
- Backbone
- Operations

- Internet
- Wireless

- Web Applications
- Node Security
- Operations Flow-thru
- New Services
- Software Integrity
- Routing & Addressing
- Legacy Systems
- Denial of Service
- Security Management
- Mobile Devices

End-to-end approach to security

Applications




Athens Olympic – Lessons Learned

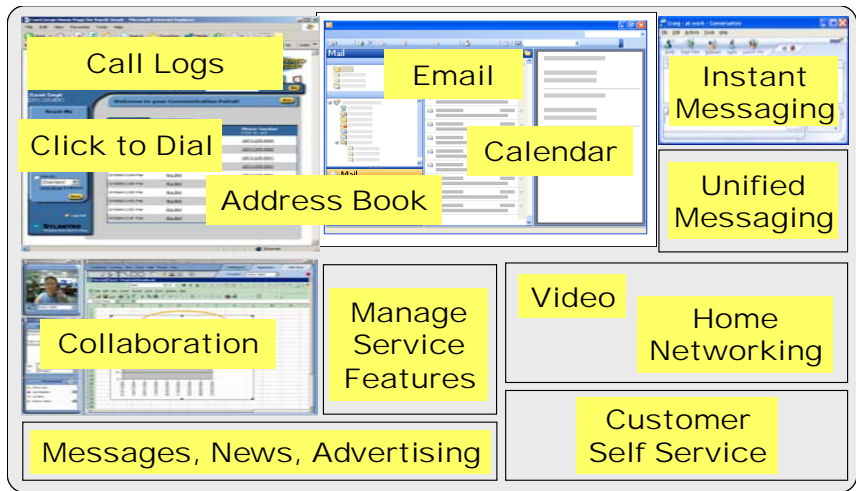
Telecom Perspective

- Perform baseline security assessment to identify/address gaps before events
- Manage vulnerability remediation
- Integrate Network & IT network security functions
- Establish new management interfaces to support information sharing and enhance incident detection/response
- Create security awareness program across a broad range of users
- Increase and train security staff to handle 7x24 support
- Address interconnection with legacy and new networks
- Manage vendor support throughout period
- Address security for Major Web Portals
- Implement strict configuration management for security elements and telecom/IT infrastructure


Converged Communications....

Multiple Applications Accessed over Multiple Devices via Communications Portal

- 
- call notification
 - click to dial



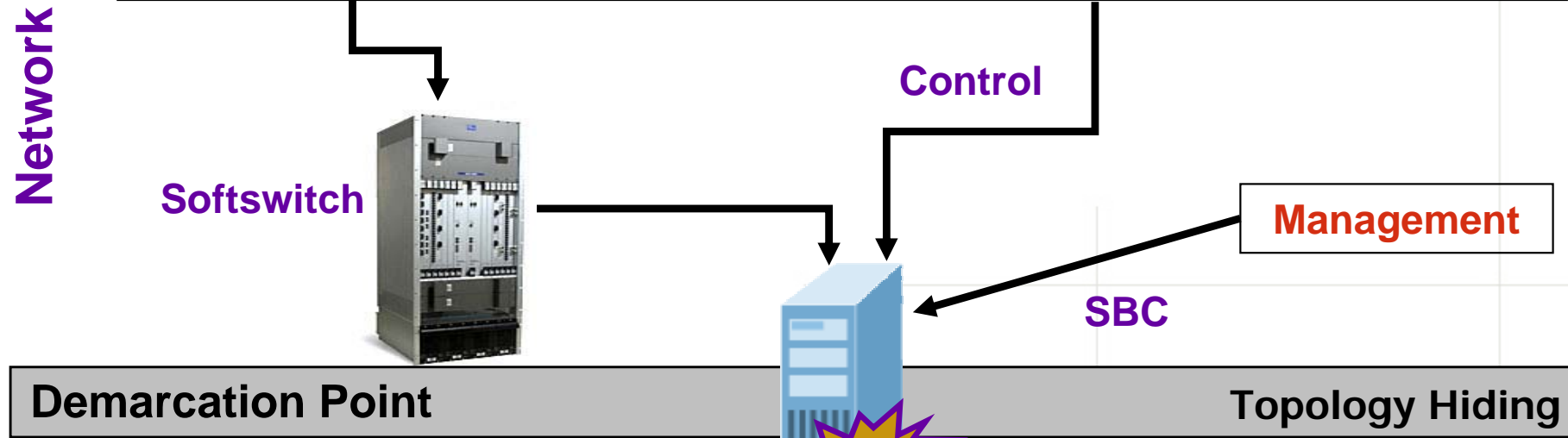
- 
- audio exchange
 - call management

- 
- call notification
 - call disposition
 - call logs with click to dial

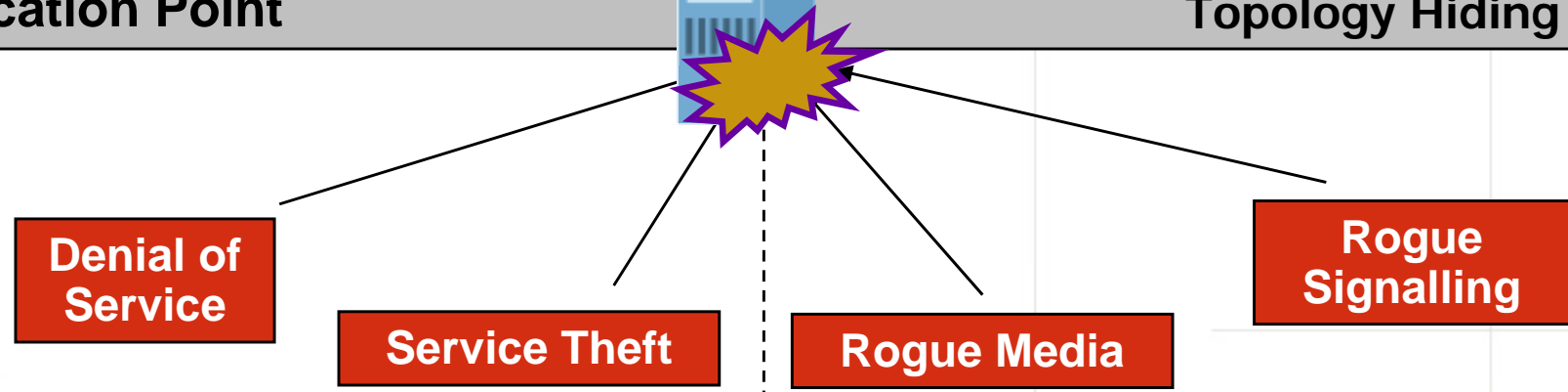
- 
- directories with click to dial
 - call notification
 - call disposition
 - call logs with click to dial
 - service management

Evolving Security Boundaries

Trusted VoIP Network



Threats

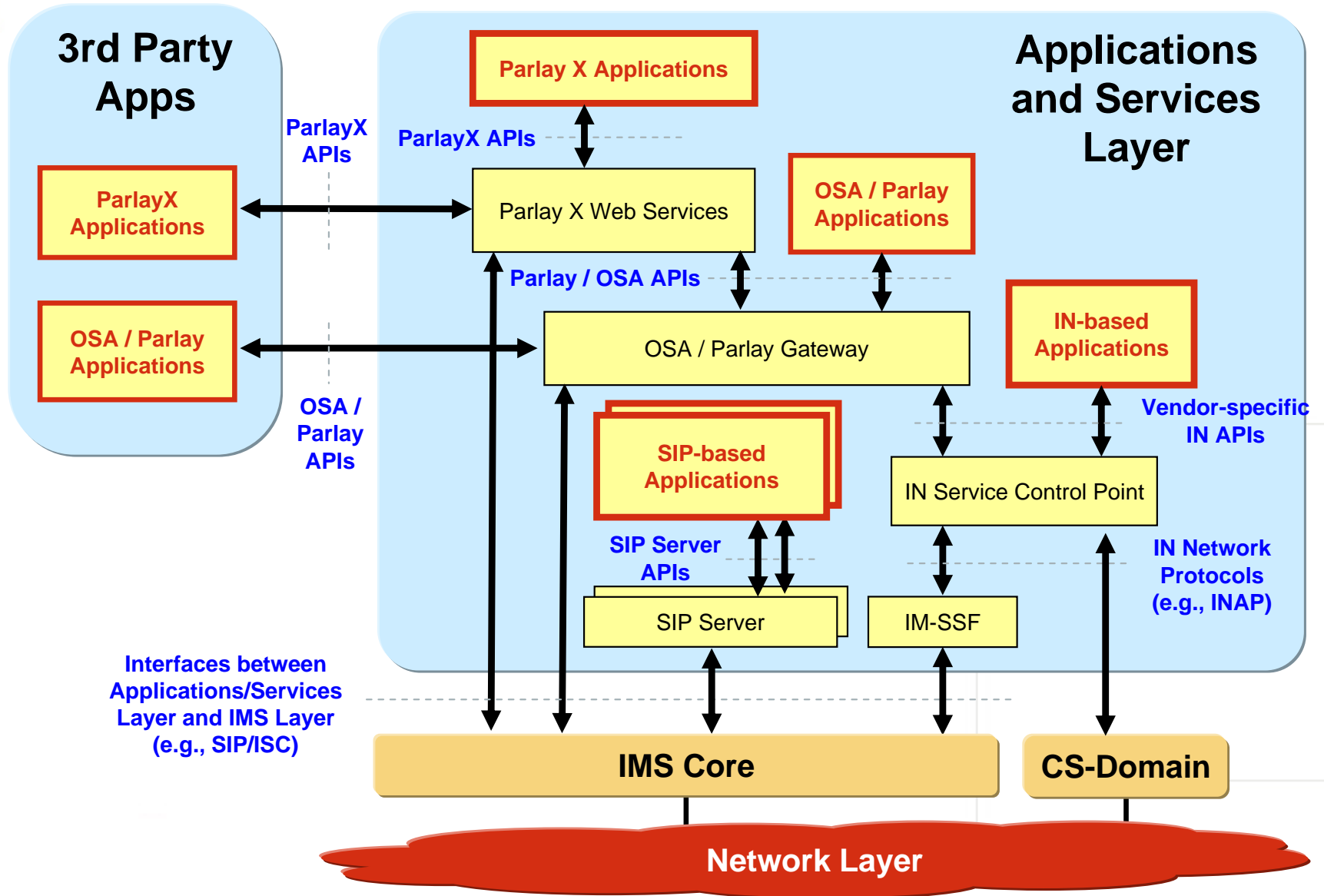


Malicious

Malfunction

IMS: A Security Perspective

Third Party Application Providers

Security Roadmap for Network/Service Infrastructures

Benchmark Security

- Address risk
- Platforms, applications & protocols
- Process flows
- Security architecture
- Security management

Procurement Process Controls

- Vulnerability Assessment
- Processes
- Security design
- Operations testing & turn-up

New Services Rollout

- Controls process
- Vulnerability assessment
- Procedures
- Training
- Service testing & turn-up

Threat & Vulnerability

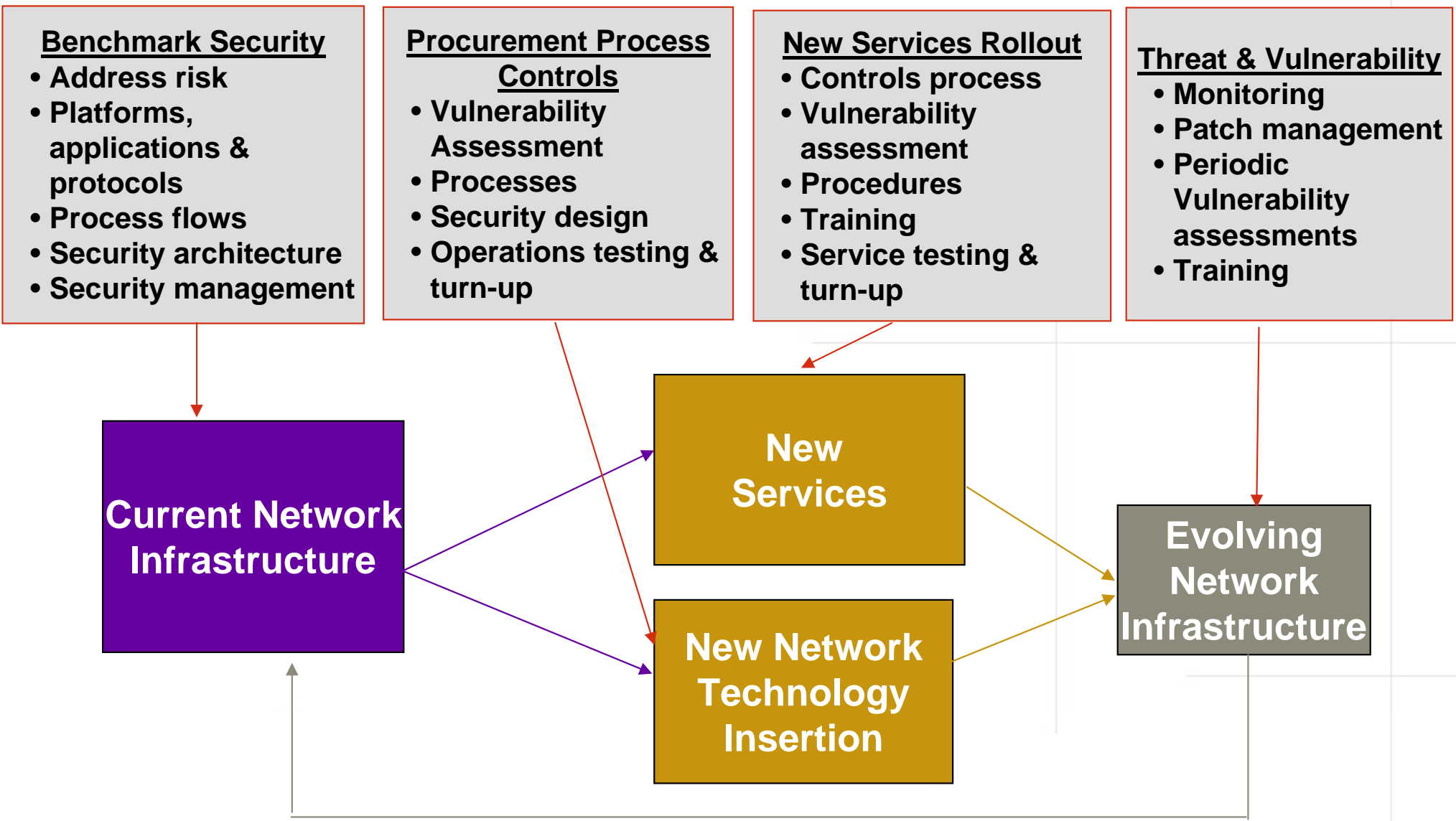
- Monitoring
- Patch management
- Periodic Vulnerability assessments
- Training

Current Network Infrastructure

New Services

New Network Technology Insertion

Evolving Network Infrastructure



New Security Directions

- Balancing Defense-in-Depth across networks, platforms, interfaces and applications
- Recognizing security as part of QoS policy management
- Integrating security operations capabilities
 - Technical and organizational aspects
- Utilizing identity management
- Providing end-to-end Information Security
- Developing common “look & feel” interfaces