IP and The Internet

The Good, Bad and Ugly

Regarding

Lawful Interception, Criminal Investigation and Intelligence Gathering

Presented By:

Dr. Jerry Lucas
President
TeleStrategies

ISS World Europe
1 October 2008
Prague, CZ

TeleStrategies®

My Perspective

The Ugly Are IP and internet developments that have no meaningful LI solutions today no matter how much money you have to spend. Only Legislative actions can have immediate impact

The Bad Are IP and Internet Developments that can be addressed regarding LI and Intelligence Gathering but the solutions are expensive

The Good Are Lawful Intercept, Criminal Investigation and Intelligence Gathering Developments that are made possible because of IP and the Internet

Agenda

First The Ugly

Then The Bad

And Yes The Good

Plus

Overview of Conference Agenda

First The Ugly

1. IP Identity Management
2. Encryption
3. File Exchange Networks
4. Synthetic Worlds
5. IP TraceBack

1. Lack of IP Identity Management

- Scenario: Correlating Criminal Identification with network and service usage.
- Issues: Application services and increasingly decoupled from network services.
  - Cross-domain IDM neither exists or is mandated.
  - Users carry 100's of application-layer identities – one for each service they use; e.g., voice, IM, email, bank, gaming, information sites, etc.
  - Increasingly difficult to correlate subjects with network identifiers.
    - Dynamically assigned
    - Pre-paid accounts
    - Public networks
    - NAT
    - Open mobile networks
  - IP anonymizers (relays) can further decouple/fragment communications

2. Encryption

- Encrypted SMS
- Anonymous Email Service
- Secure Instant Messaging
- Encrypted Email
- Encrypted Webmail
- Encrypted VoIP
- Encrypted GSM Voice Calls
- And More!

Source: KOMMLABS

3. File Exchange Networking

What's File Exchange Networking?

- User uploads file to a web site (RAPIDSHARE for example)
  - File can contain criminal content
  - File can be edited/modified online
- Same user ID and password distributed to other users (e.g. criminals)
- User ID/password can be distributed off network

Why This is More Problematic than P2P?

- File can be quickly uploaded/removed – not so with P2P networks where files are propagated throughout P2P network
- P2P is slow to distribute file if only a few users have interest
- Content on P2P networks do not require authentication, so it is available for intercept if you know what file to ask for
- File exchange network hosts may be out of reach of warrant
- Public wifi/access provides anonymous file distribution
- User IDs can be setup dynamically

4. Synthetic Worlds

1. What A Synthetic World: It's a computer-based simulated environment intended for it's users to inhabit and interact via avatars

2. Example: Second Life
    * 15M Total Residents
    * Used for education, religion embassies and more
    * Also used by criminals (money laundering) and terrorist groups

3. What's The Ugly Problem?
    * Activities take place within a computer complex!
    * Can't Tap It!

5. IP Traceback

Problem Of Finding The Source Of An IP Packet

The Difficulty:

A. IP network is basically stateless
B. Source IP spoofing is rather easy
C. Multi Management Domains

Additional IP Traceback Problems

1. Current IP Traceback R&D focused on DDoS attacks not criminal investigations

2. Must build into NGN standards

3. Modifying existing IP infrastructure not practical

Now The Bad

6. Increasing access speeds and data clutter
7. Exploding IP application growth
8. CDR availability
9. P2P communications
10. Open wireless systems

6. Increasing Access Speeds and Data Clutter

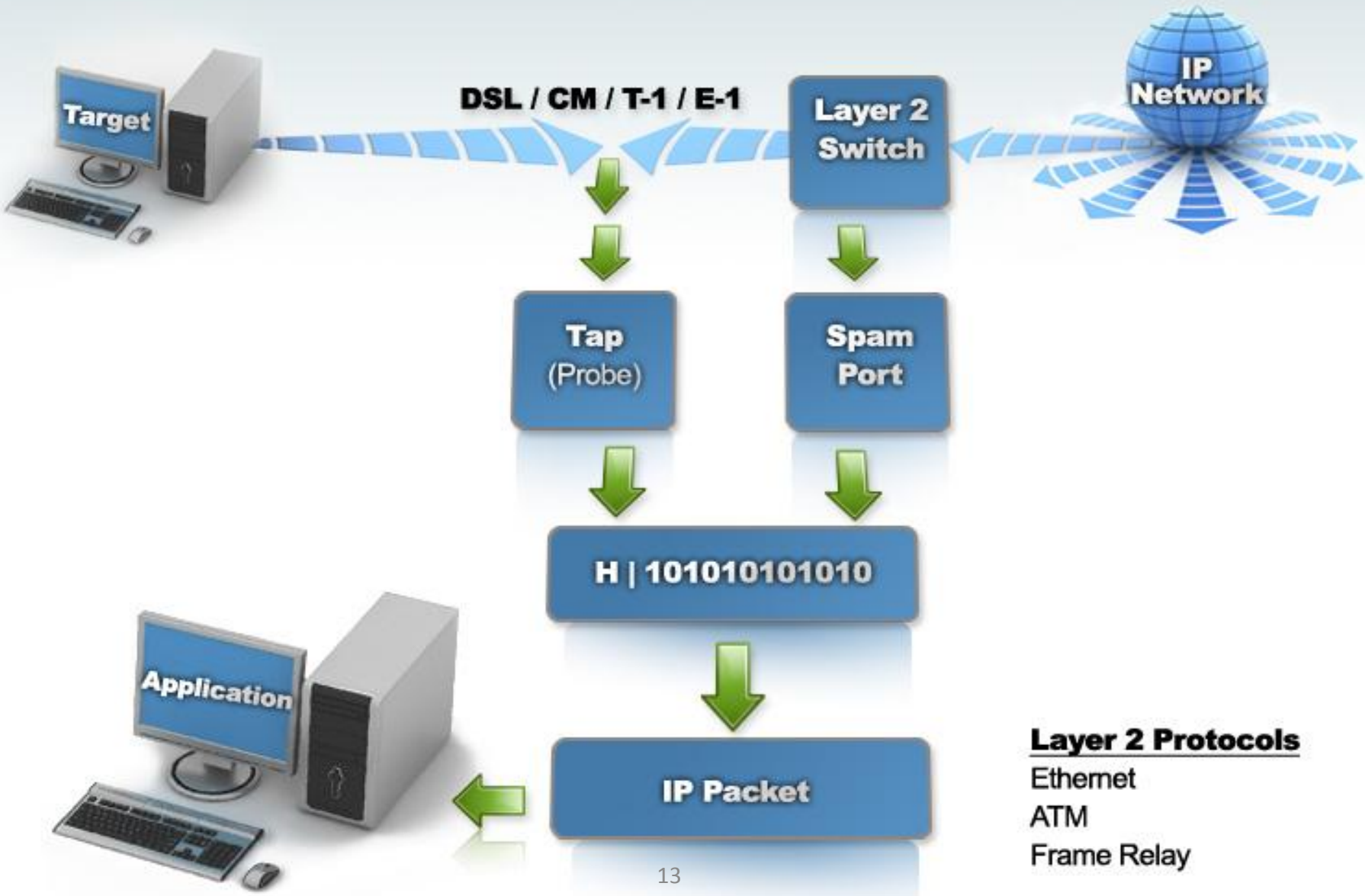
The Problem Driver

(A) Increasing DSL/Cable Modem
Access speeds, e.g. to 100 Mbps today
Multiplexed to 40 Gbps

(B) Multi-Service Usage
* VoIP
* Email
* P2P
* Cable TV
* IPTV and more

IP Challenge #1

IP Link Layer 2 Intercept



Layer 2 Protocols

Ethernet

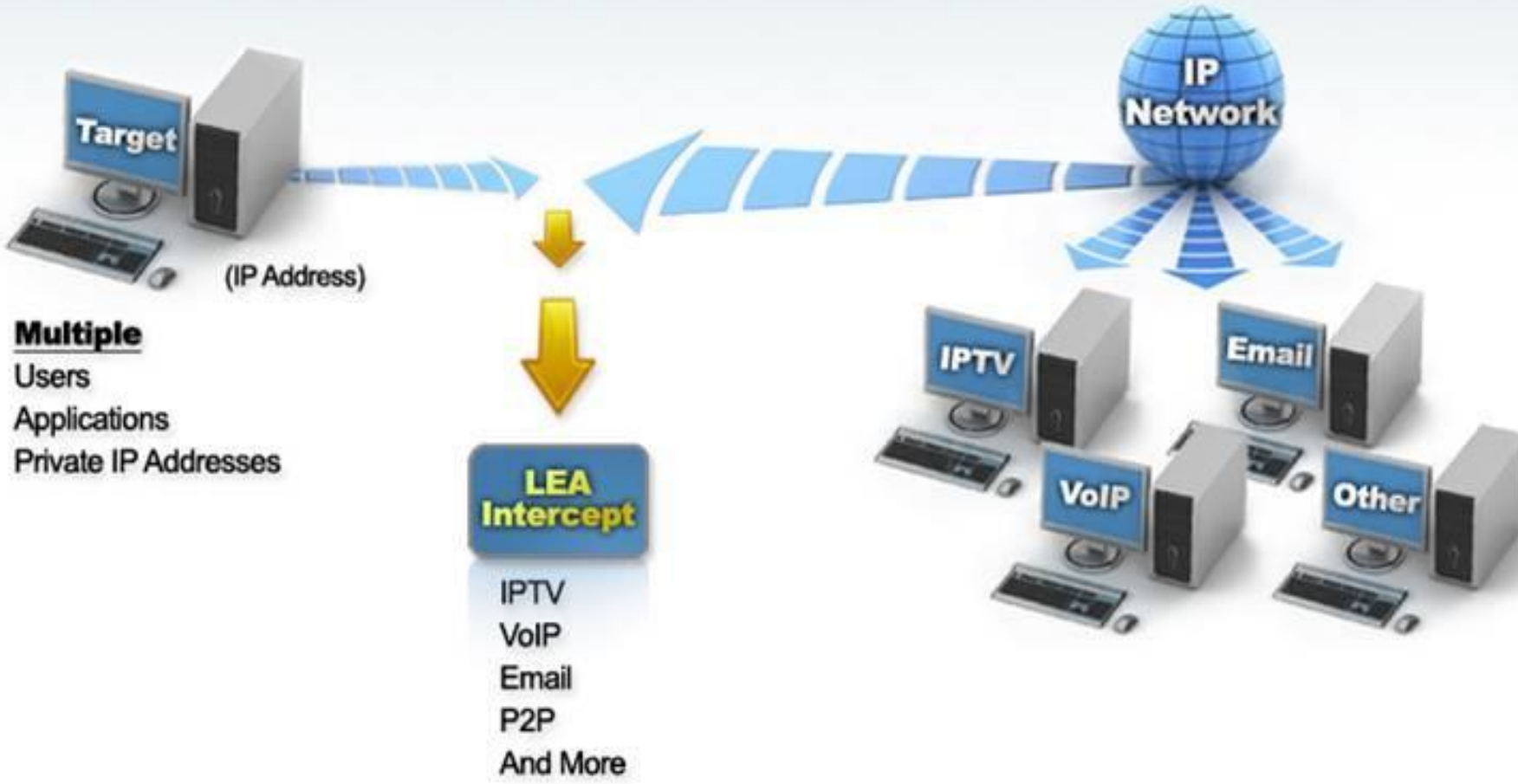
ATM

Frame Relay

IP Intercept at Layer 2 (link layer)

- Advantage: non-disruptive IP data intercept, complete packet trail, transparent
- Issues:
  - Reconstructing/rebuilding application data
  - Keeping up with new application protocols
  - Encryption
  - Location of intercept points (completeness)
  - Quality of source – “Purpose built” intercept equipment versus add-ons to network routers and/or application servers.

DSL / Cable Modem Clutter



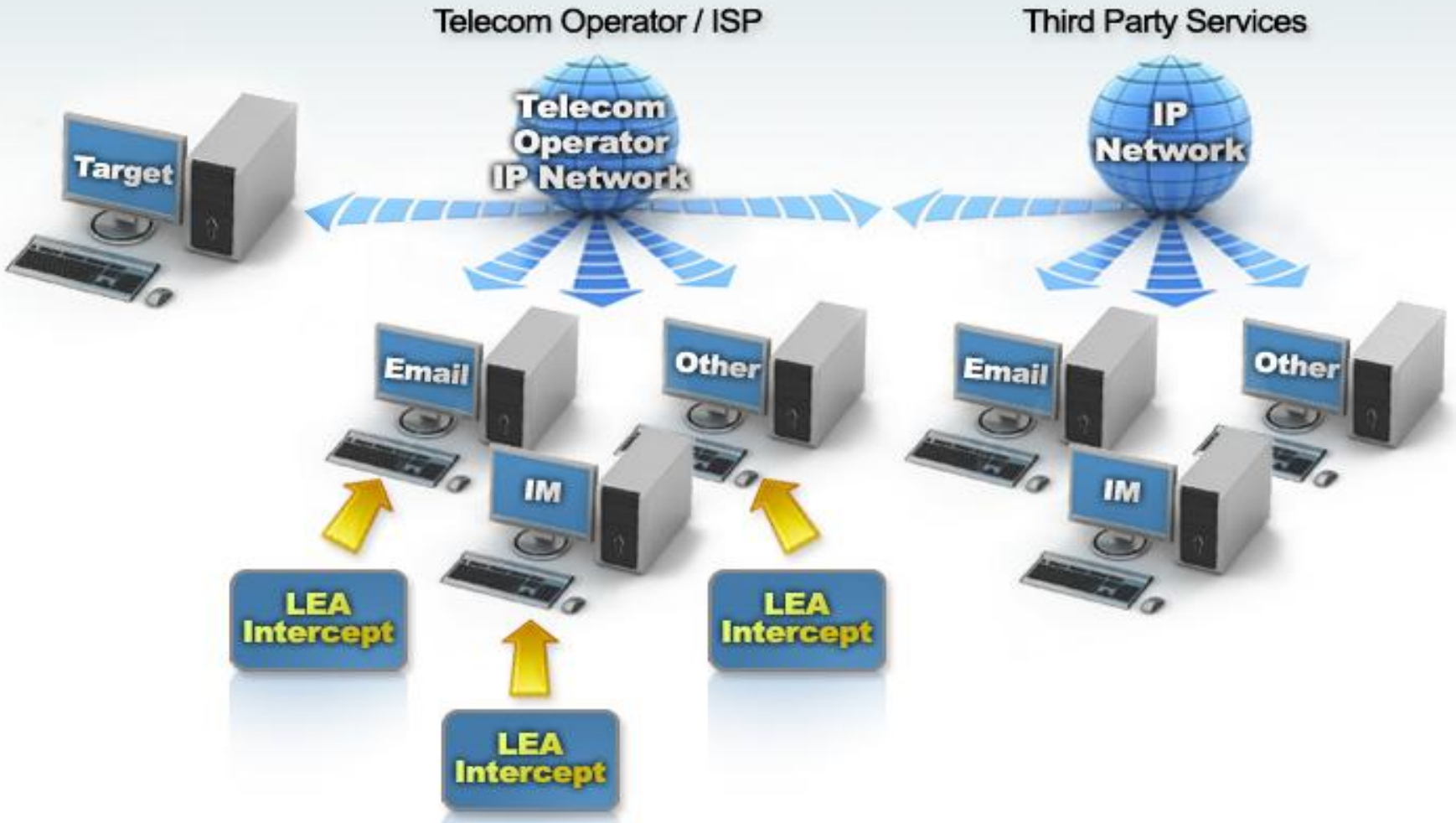
Increasing DSL/Cable modem clutter

- Scenario – layer 2 packet intercept on high-speed access port (10mbps+).
- Issues: non-relevant data/noise hides real content.
  - Users – Network interface address shared by multiple users hidden by NAT
  - Heavy media apps – IPTV, VoD, etc.
  - Viruses/destructive traffic
  - Disguised content – Content sent via over-the-top services (e.g., chat on Xbox, webinars, etc).

7. Exploding IP Application Growth

IP Challenge #2

IP Application Layer 7 Intercept



7. IP application layer (7) Intercept

- Advantages: No application decoding, know exactly how service was used.
- Issues:
  - Invasive – OAM overhead for service provider
  - Access – Nonstandard, non-existent or incomplete
  - Coverage – third-party service
  - Completeness – real time access vs. event logging
  - Distributed service architects – IMS and SDPs
  - Identity – AAA can be local to AS

8. CDR Availability

A. Not collected by telecom operator

B. Nomadic targets

C. Non-Completed call

And More!

Challenge #7: Vanishing CDR Production

- Scenario – LE relies on billing system, CRM and usage-processing systems for pen register and historical usage.
- Issues: CDRs are going away.
  - Flat/bundled rate is prevailing billing model -> no CDR, no record for pen register, no billing archive to search on, etc.
  - Over the top services supported by advertising – again, no CDRs.
  - CDR collection infrastructure is very expensive, not an ad-hoc solution.
  - CDRs, to the extent they may/may not exist going forward, may not be complete enough anyway for LE

8. Collecting and Correlating CDR's on Nomadic Targets

Why is this a Challenge?

- Target at fixed location using different terminals/networks
- Target using same terminal at different locations
- Mix of networks data in different formats and mix of target identities

Impact on Lawful Interception?

- Can't assume 100% CDR capture
- Correlating complex data in different formats, different target CDR's and more
- Need to rely on target profiling techniques and tools

9. Peer-To-Peer Communications

IP Challenge #5
Peer-to-Peer Applications

The Old Way

Telecom Servers

P2P Skype

Cloud of Skype Users

P2P BitTorrent

Cloud of Users with Content

9. Peer-to-Peer Applications

- Scenario – Content distribution over P2P file and voice networks.
- Issue: P2P protocols don't have a server or centralized control architecture to monitor
  - Peers at local hotspot
  - Anonymous – no authentication
  - Needle in haystack – 10M+ clients, billions of flies
  - Relay Files – store data that doesn't belong to you, or is used by the target
  - Localized transmission/distribution – bypass aggregate taps
  - Encryption
  - Fragmented data – by design
  - Massive data flows 50 – 80% of internet traffic

10. Open Wireless Systems

- Scenario – Misuse of powerful, open wireless networks and platforms that anybody can develop an application for.
  - Handset as powerful as a PC with all kinds of media possibilities.
  - Wide range of network service primitives; e.g., location, presence, messaging, etc.
  - Multi-megabit connectivity
- Issues: Phone is wide open for third party applications.
  - Not closed system like today
  - Plethora of applications and web-based services (long-tail)
    - Infinite possibilities for consumer, and criminals.
    - Peer to peer, application VoIP, bi-directional video streaming, etc.
  - Many delivered over the top by third parties, everything will need to be decoded.
  - Operators may charge on service primitives – transport, location, charging, presence, QoS, etc. – fragmented service records, no application service usage.

Top Ten IP and Internet Challenges

The Ugly

1. IP Identity Management
2. Encryption
3. File Exchange Networks
4. Synthetic Worlds
5. IP Traceback

The Bad

6. Increasing Access Speeds and Data Clutter
7. Exploding IP Applications
8. CDR Availability
9. P2P Communications
10. Open Wireless Systems

The Good News

1. ISS For Telecom ROI
2. CDR Mining
3. Social Networks
4. Data Fusion Centers
5. Web 2.0 Mashups
6. Web 3.0
7. Regulatory/Legislative Developments
6. Standards (e.g. ETSI/TC LI)
7. ISS Vendor Commitment
8. LEA/DHS/DoD Awareness

1. ISS For Telecom ROI

A. The Good: An ISS Platform for lawful interception compliance can be used for increasing telecom operator revenues, ARPU and customer experience

B. Why Telecoms Are Interested? Today's broadband access business model not working, e.g.

- Flat Rate Pricing
- Fixed Network Capacity
- Unlimited Usage

C. One Solution Deploy A DPI Platform

Deep Packet Inspection (DPI) For:

- Lawful Intercept
- Traffic Management (or Throttling)
- Network Security
- Content Screening (or Censorship)
- Legal Compliance (or Data Leaking Protection)
- And More

2. CDR Mining

- Detect targets using unanswered calls as a mode of communications
- Human habits and identity
- Identify groups
- Access raw data a big plus
  (e.g. CDR's have more information than billing statements)
- Skype users create patterns
- And More

3. Social Networking

From Wikipedia:

A Social Network is a social structure made up of nodes (individual or organizations) that are tied by one or more specific types of interdependency, such as

- Values
- Visions
- Ideas
- Financial
- Friendships
- Dislikes
- Conflict
- Trade

4. Data Fusion Centers

Deployed Primarily in the U.S.

What are they?

- Data hubs for gathering and sharing information between local, state and federal law enforcement
- Goal: All levels of government share the same information
- Staffed by intelligence analysts

Fusion Challenges

1. Policy Fusion
2. Personal Relationship Fusion
3. Hardware Fusion
4. Data Fusion

And

International Fusion Center Interconnection

Web 1.0, 2.0 And 3.0

Web	Capabilities	Intelligence Implications
Web 1.0	WWW as a collection of web sites	Allows search across massive data stores
Web 2.0	Transition to network composing platform and a network of interacting services	Creates meta data, information tagging (e.g. Google et al) and integration with open source information
Web 3.0	Semantic web, collaboration in 3D shared space (e.g. Second Life)	Allows intelligence agents to reason using knowledge on the web

Top Ten IP and Internet Challenges

The Ugly

1. IP Identity Management
2. Encryption
3. File Exchange Networks
4. Synthetic Worlds
5. IP Traceback

The Bad

6. Increasing Access Speeds and Data Clutter
7. Exploding IP Applications
8. CDR Availability
9. P2P Communications
10. Open Wireless Systems

The Good News

1. ISS For Telecom ROI
2. CDR Mining
3. Social Networks
4. Data Fusion Centers
5. Web 2.0 Mashups
6. Web 3.0
7. Regulatory/Legislative Developments
6. Standards (e.g. ETSI/TC LI)
7. ISS Vendor Commitment
8. LEA/DHS/DoD Awareness

Conference Agenda Overview

Track 1: ISS for Lawful Interception

Track 2: ISS for Criminal Investigation and Intelligence Gathering

Track 3: ISS for Data Retention and Regulatory Compliance

Track 4: ISS for Audio/Video Forensics and Biometric Speaker Identification*

Track 5: ISS Product Demonstrations and Training*

*** Tracks 4 and 5 for LEA, Internal Security and Intelligence Analysts Only**

Thank You for Joining Us at ISS World Europe and Have a Great Conference