telesoft
TECHNOLOGIES

Real Time Intercept from Packet Networks, Challenges and Solutions

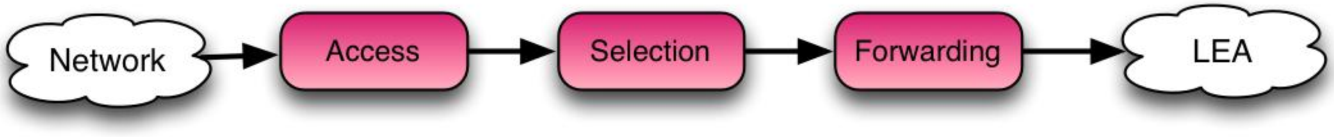
Presented by Keith Driver

Packet Intercept

- Packets are everywhere
  - – LAN networks
  - – WAN networks/ Carrier Ethernet
  - – 3G Telephony networks
  - – CDMA 2000 Networks
  - – ISP Networks
  - – Etc etc etc

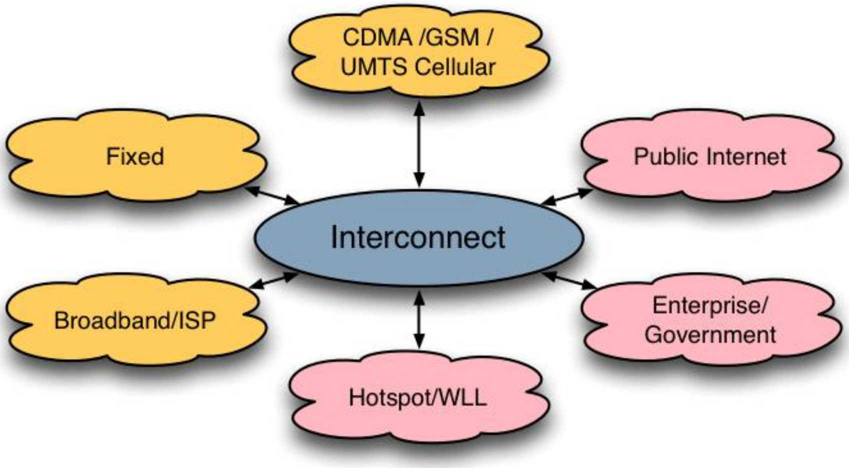
Packet Intercept

- Issues
  - – Access to the packets on the wire
  - – Selection of packets on the wire
  - – Accumulation/ Forwarding of packets



Access to packets

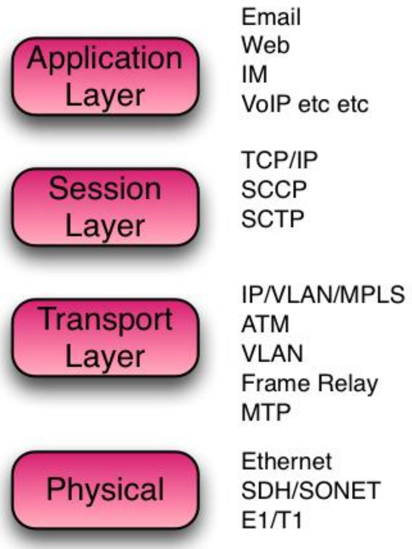
- Range of network types
  - – CDMA/UMTS cellular
  - – GSM cellular
  - – PSTN
  - – WiMax, WiFi
  - – Sattelite
  - – LAN/WAN



- Roughly divisible into Telecom and Data
  - – Also Valid
    - Cellular/ Fixed
    - Enterprise/Operator

Access to packets

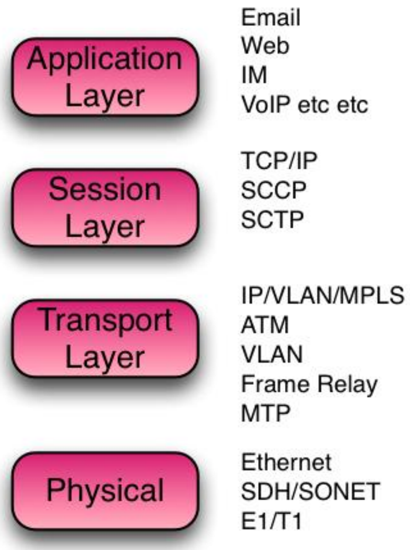
- Physical access to the transport
- Range of Media
  - Ethernet, E1/T1 , SDH/SONET, GE, CarrierEthernet, etc
  - LAN/ISP
    - Span ports
    - Hubs
    - Passive taps
  - WAN/3G/CDMA 2000/etc
    - Passive taps
    - Internal interception functions
    - SPAN ports



- Optical and electrical transports

Access to packets

- Transport protocol handling
  - MPLS
  - VLAN tags
  - ATM (IMA)
  - PPP (ML-PPP)
  - PoS (Packet over Sonet)



Application Layer
Email
Web
IM
VoIP etc etc

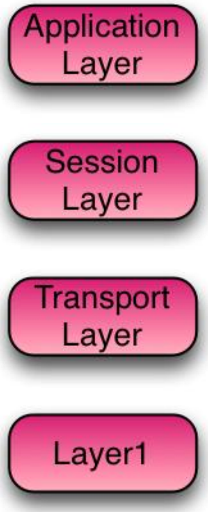
Session Layer
TCP/IP
SCCP
SCTP

Transport Layer
IP/VLAN/MPLS
ATM
VLAN
Frame Relay
MTP

Physical
Ethernet
SDH/SONET
E1/T1

Selection of packets

- A major problem
  - – What are the criteria for selection?
  - – Lower layers
    - Label address (i.e. IP Address, ATM address) ?
    - Protocols used?
  - – Upper Layers
    - Protocol/Service
    - Session Identity
    - User Identity (email address/ IM id etc)
    - Cross packet identities
- And packet selection must be done in real time



Selection of packets

- Generically requires hardware support
  - Line rates are too fast for software
- Selection on labels easier
- Selection on protocol contents much harder
  - Requires Deep packet Inspection
  - Complex matching criteria
  - Cross packet assembly for matching
  - Session buffering to extract the whole session from embedded triggers (e.g. email cc:)

Selection of packets

- Very hard for routing nodes to do this
  - ‘Internal interception’
- Many nodes are L2 switches with little packet inspection
  - Most switches have a stated aim to keep the packet for a minimum time
- Effort required for inspection usually means added hardware to the node
- Limited then by manufacturer capability

Identity

- Subscriber Identities
  - Many, Many identities
  - Each human probably has 50 used often
- Terminal / equipment identities
  - Many terminals used by one target
- Network Assigned identities
  - Networks use these for obfuscation and mobility reasons
- Application/Entity identities
  - Not only humans and equipment have identity

Identity

- Conclusions
  - – Each human can have many identities
  - – Identities can be changed frequently
  - – Identities can be used only once
  - – Identities can be changed by location
  - – Anonymisation services exist on the internet
    - http://www.anonymizer.com
    - http://www.onion-router.net.
  - – Keeping track is VERY difficult when faced with knowledgeable adversaries
- But it can be done with sophisticated software analysis

Cyphering

- Cyphering is a major issue
  - – Network based protection
    - 3G information cyphered to the RNC
    - 2G data cyphered to the SGSN
    - IMS sessions protected end to end from the terminals
  - – Application based cyphering -
    - Skype
    - HTTPS
  - – User based cyphering
    - PGP
    - X.509 SMIME etc

Cyphering

- What can be done?
  - Mobile Network based cyphering
    - Access to CK/Kc for the session from core network
  - IMS - end to end - very difficult
  - Skype - proprietary - very difficult.
  - PGP/SMIME - powerful encryption

- Best hope is to record the cyphered session and apply cryptographic techniques afterwards
- Not Real time though

Cyphering

- A big problem that will get bigger
- As communication networks migrate to offering end to end transparent pipes
  - More user based encryption
  - More encryption algorithms
- But connection records are still available
  - (time / duration etc)
- Patterns of use are still available
- Keys may be available through other means than SIGINT

Accumulation of packets

- Packets rarely travel alone
- Most packets form streams to carry a higher layer service
  - Telephone call
  - Web session
  - Email
  - Etc
- Packets therefore need to be acquired, and presented in sequence
- Buffering is one solution to this

Buffering (or not)

- Buffering can be useful
  - But it is resource expensive (memory)
  - Controversial in evidential environments
- Allows session reassembly
  - Which enables L7 protocol presentation
  - Allows cross packet pattern recognition
- Provides post analysis capability
- Allows session recovery
- But can delay delivery
- Requires very large resource in high bandwidth links (STM-64/10G etc)

Handover of product

- Standardized
  - ES 101 671,
  - ES 102 232.x
  - J-STD-025,
  - PacketCable
  - ATIS
- Often with national/local variants
- Buffering is sometimes allowed
- Session reassembly is sometimes desired
  - I.e. presentation as email / Web page image etc.

Challenges review

- Acquisition
  - – Physical interfaces differ
  - – Internal Interception limited
- Selection
  - – High data rates make this difficult
  - – Cyphering prevents DPI
  - – Identity obfuscates communication
- Accumulation/Forwarding
  - – High data rates
  - – Buffering is expensive

Solutions!

- Problems split into roughly 2 domains
  - LAN/ISP type access with Gb ethernet transports
  - WAN/Core network access where transport is
    - High capacity fibre
    - E1/T1 ATM
    - E1/T1/PoS PPP/HDLC
    - Carrier ethernet.
    - GE/10GE

Solutions!

- In the 1G ethernet domain
  - Many companies have adapted IDS systems (usually from SNORT)
  - Several companies have hardware acceleration to assist with this
- Very useful in enterprise or ISP domain
- Kit is relatively small and powerfull.

- But somrthing bigger is needed in the core

Solutions!

- Ethernet based solutions tend not to work so well in other environments
  - Specialised , distributed equipment is needed
  - Full network coverage
- Probes cope with the complex Layer 1/ and transport stacks
  - Probes cope with the variety of protocols, telephony and data (ATM/ MPLS / Carrier E etc)
  - Probes offer a pre-processing function to DPI

Large scale Solutions!

- Telesoft Technologies specialize in the provision of such probes - HINTON product
  - 3G/CDMA 2000/GSM network access
  - Large , distributed networks
  - Access to telephony and data sessions
  - TDM legacy and Packet intercept
  - Highly distributable and scalable
  - Hardware accelerated
  - Centralised Handover
  - Decyphering available with complete access
  - Location (including Abis/Iub) , Call content, SMS, CDR
- Proven, large and small scale deployments for intercept

Thank you for watching

TECHNOLOGIES

www.telesoft-technologies.com

Telesoft Technologies Ltd
Observatory House
Blandford Dorset
DT11 9LQ UK

T. +44 (0)1258 480 880
F. +44 (0)1258 486 598
E. sales@telesoft-technologies.com

Telesoft Technologies Inc
Suite 601
4340 Georgetown Square
Atlanta GA 30338 USA

T. +1 770 454 6001
F. +1 770 452 0130
E. salesusa@telesoft-technologies.com