High-Speed Traffic Analysis for Security: Challenges & Approaches

C-DAC

Asia-Pacific Advanced Network 32nd Meeting,

India Habitat Centre, New Delhi

Presentation Outline

- Introduction
- Observations & Findings
- Active and Passive Measurements
- Challenges and approaches
- Interesting Works

Introduction

- Evolution
  - Copper to Fibre
  - Merging of LAN & WAN Technologies
  - Gigabits at LAN and Multi-Gigabits at Backbone
  - IPv4 to IPv6
  - High-speed TCP
  - e-Governance, e-Science Application and Social computing

Vulnerabilities

- Backbone
  - Security concerns with respect to routing (BGP)
  - Concerns with respect to Infrastructure
    - DoS, DDoS, DNS, botnets
- User End
  - Malware, Reconnaissance, Data-Exfiltration, Buffer overflows, DDoS etc.,

Interesting findings

- DDoS Attacks breaks the 100 Gbps barrier (2010)
- Application-Layer DDoS increasing in sophistication
- DNS has emerged as key attack target
- IPv4-IPv6 security concerns
- Mostly attack targets are targeted over specific customer service and aimed at network services (DNS)

Threats observed

- DDoS towards User End
- Misconfigurations and failure of devices
- Botnets / Compromised hosts
- HTTP, SMTP and DNS most targeted (DDos)
- Average time to mitigate DDoS is 20 minutes
- Zombie Computers (Botnet)

Infrastructure Protection

- Backbone
  - ACLs
    - RFC 1918, 3330, 3704
  - Blackholing
  - DNS Sinkhole, Scrubbing
  - Committed access rate (rate limiting)
  - Stateful Firewall, IPS
    - *Most of them fail to handle DDoS*
- Customer End
  - ACL, Stateful Firewall, IDS/IPS, UTM, Malware prevention

Traffic Analysis: Objective

- Trend analysis
- Prevention of intrusions and attacks
- Anomaly detection
- QoS/SLA Validation
- Network Provisioning & Design

Obtain Statistics

- Host/Interface based (IP address)
- Application based (Port based)
- Application classification (Application header analysis)
- Temporal (time based)
- Protocol based (TCP, UDP, ICMP..)

Aspects examined

- Packet Level
  - Bits per second (rate)
  - Size of packets
  - Latencies, RTT
  - Throughput
  - Availability
  - Packet drops & errors
  - Deep packet inspection
  - Header analysis
- Connection Level
  - Connection rate
  - Direction of traffic (incoming/outgoing)
  - Stateful inspection
  - Flow analysis
- Application profiling
- Vulnerability assessment
- Compliance with standards (RFCs)

Traffic Analysis

- Active Measurement
- Passive Measurement
- Header based Analysis
- Deep Packet Inspection
- Handling encrypted packets
- Signature based detection
- Detecting Anomalies

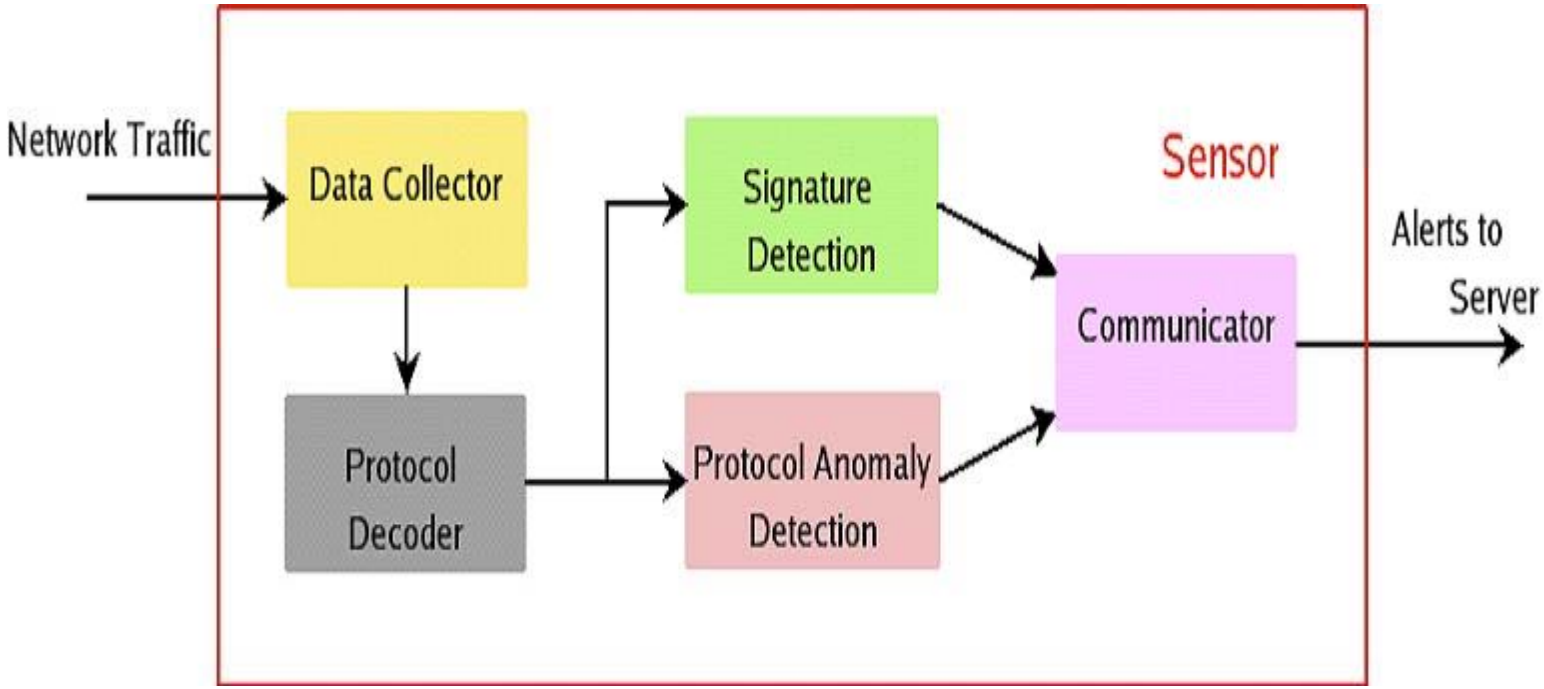
Active Measurement

- Interferes the network and carries out measurement by injecting specifically crafted probe packets
  - *Ping, traceroute (network tomography)*
  - *Capprobe, pathchar (delay, capacity estimation)*
- Vulnerability measurement
  - *Nessus, nmap*
- Network Interface statistics
  - *SNMP (polling)*

Passive Measurement

- Pure observations and analysis of traffic
- Packet Analysis
  - *Sniffers, tcpdump, Wireshark*
- Flow level monitoring
  - Netflow, IDS (like Snort/Bro)
- Traffic Classification
  - *CoralReef*
- TCP
  - Tstat (TCPtrace) – multigigabit-per-second traffic analysis tool

Passive Capture and Analysis



Packet Capture

- Standard Ethernet linecards
  - *libpcap*
  - *libnetfilter_queue (libipq)*
  - *libnids*
- Dedicated Hardware
  - Like Endace DAG
- Formats
  - *Pcap, erf, etherpeek, snoop, flow records*
  - *RRD*
- Challenges
  - *Scalability, efficient memory management*

High-Speed Packet Capture

- Network support in OS is generic and hence time taken for packet to move from network adapter to user space is high
  - Latency and per-packet processing load
- Performance
  - System costs to bring packets from network to user space/application
  - Application processing cost (classification, checksum etc..)
- Solutions
  - Memory mapped packet buffers (PF_RING) and DNA
  - NetFPGA

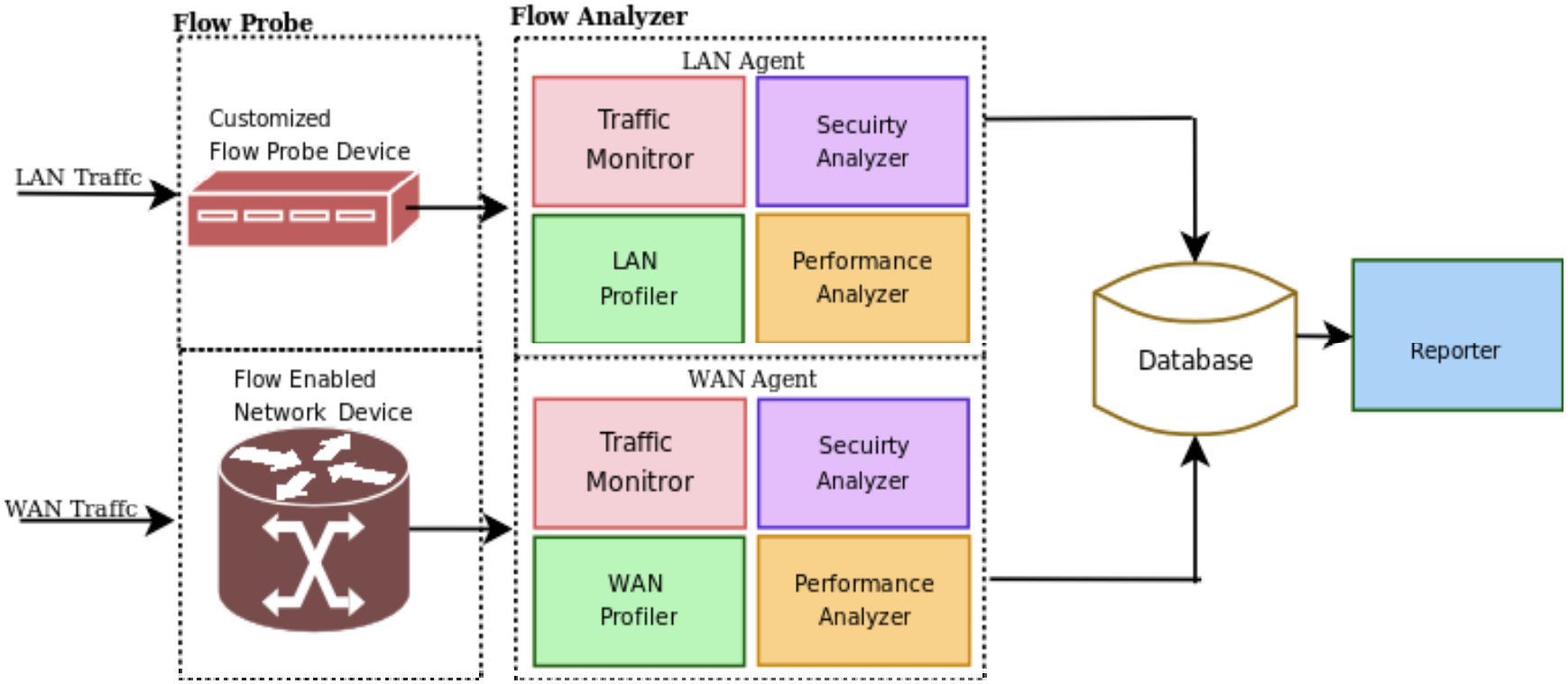
Header Analysis

- Threshold based:
  - Find no. of packets generated by internal hosts to a destination port in a time interval
  - TCP SYN, UDP Packets based analysis
  - Scanning of Sequential destination addresses (after randomn IP address generation)
  - Traffic towards unallocated IP addresses (IANA/bogon lists)
  - Number of distinct destination IP
- Application header analysis

Deep Packet Inspection Challenges

- Content Matching Complexities
  - Control Vs Data Packets (more content oriented packets)
  - Large % HTTP Traffic with large packet sizes
  - Number of signatures to be analyzed (> 10,000)
  - Variable size of signatures, regular expression match and stateful understanding
  - Packet fragments and Stream reassembly
- Compressed & Encrypted traffic

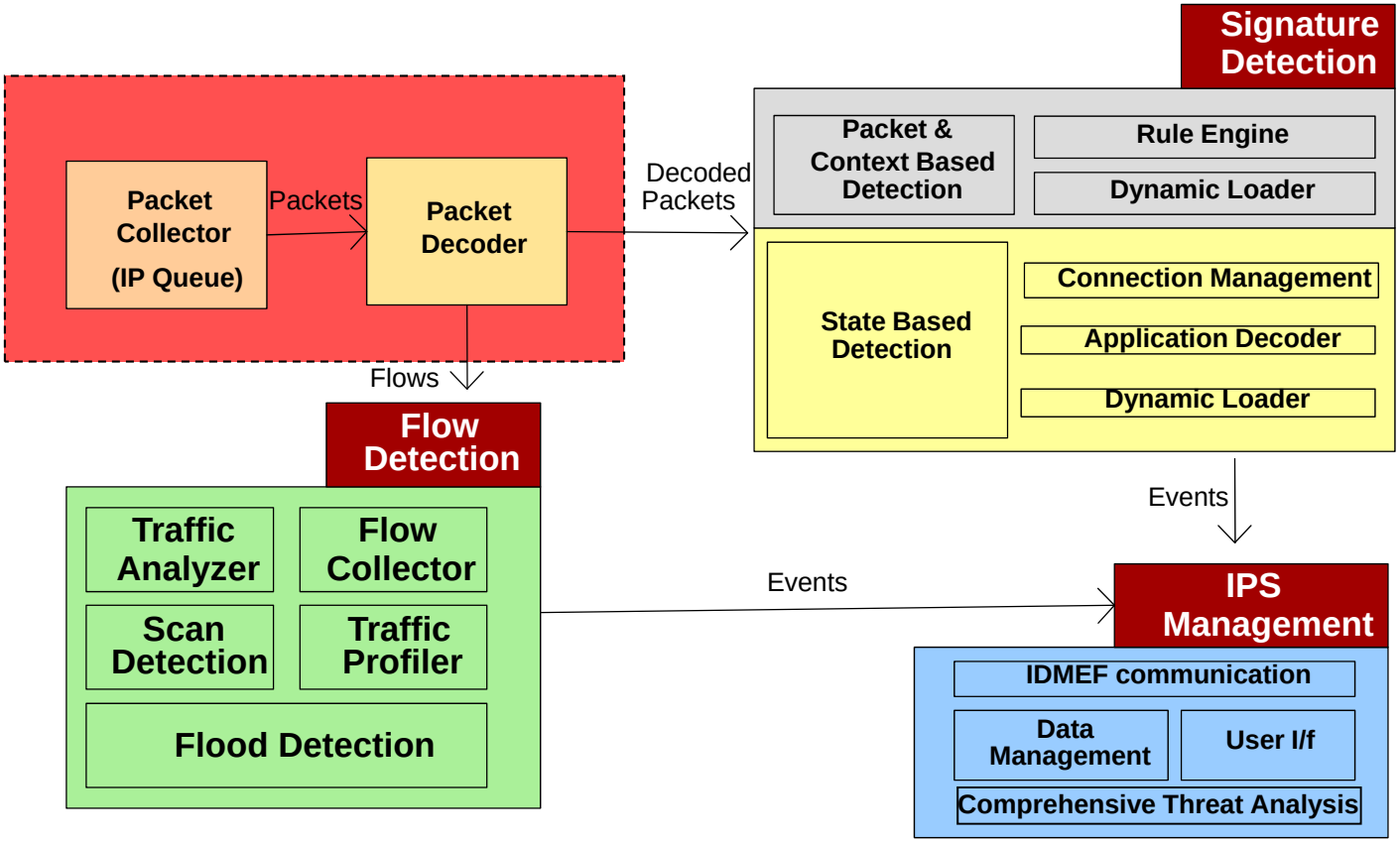
Flow Analyzer



Our Approach

- Use both active and passive measurement to devise effective network management system
  - **Adrisya** a Flow based passive measurement analyzer and anomaly detection solution
  - **EDGE** system was developed and deployed for monitoring Backbone routers and LAN resources
  - **GYN** (Guard Your Network) Intrusion Prevention Appliance (Multi-core based packet splitting)
  - **NetFPGA based Content Matching**
  - **Security Assessment System** (SAS) on top of Globus for grid environment
- Devised **Threat-Aware IDS Model** using active and passive techniques to profile traffic and changing vulnerabilities (host level) in a network and utilize the same for detecting relevant intrusions

Analyzers


Signature Detection
Packet & Context Based Detection
Rule Engine
Dynamic Loader
Packet Collector
(IP Queue)
Packets
Packet Decoder
Decoded Packets
State Based Detection
Connection Management
Application Decoder
Dynamic Loader
Flows
Flow Detection
Traffic Analyzer
Flow Collector
Scan Detection
Traffic Profiler
Flood Detection
Events
Events
IPS Management
IDMEF communication
Data Management
User I/f
Comprehensive Threat Analysis

Interesting Works

Worms: Issues and Approaches

- Target Scanning
  - Random, hit-list, permutation, passive scanning, etc (Staniford et. al)
  - Anomalies (Connections to many unique IPs, receiving too many RST packets..)
- Worm distribution
  - Self-carried, embedded/secondary channel
  - Anomalies (Single-packet UDP, similar and identical content sent in network, secondary channel can be detected easily/prevented by firewall)
- *Detecting Worm activation*
  - *More of host analysis issue*

Data Exfiltration: Issues & Approaches

- Covert channels
  - Cabuk et. al and El-Atawy and Al-Shaer (2009) show that DNS and HTTP can be used as covert channels
  - SIDD framework: High speed transparent network bridge to detect data exfiltration over network (Yali Liu et. al)

Packet Sampling

- Braun et. al, “Packet Sampling for Worm and Botnet detection in TCP Connections”
- Small number of packets from beginning of every TCP connections considered

Key References

- World Wide Infrastructure Security Report, 2010, Arbor Networks
- Experiences of Internet Traffic Monitoring with Tstat, Alessandro Finamore, Marco Mellia, Michela Meo, and Maurizio M. Munafo`, Politecnico di Torino, Dario Rossi, TELECOM ParisTech, IEEE Network, May/June 2011
- 10 Gbit/s Line Rate Packet Processing Using Commodity Hardware: Survey and new Proposals, Luigi Rizzo, Luca Deri, Alfredo Cardigliano
- Locating Network Domain Entry and Exit point/path for DDoS Attack Traffic,, IEEE TRANSACTIONS ON NETWORK AND SERVICE MANAGEMENT, VOL. 6, NO. 3, SEPTEMBER 2009
- Covert Channels (data exfiltration)
  - Cabuk, S., Brodley, C. E., and Shields, C. (2009), “IP covert channel detection,” ACM Trans. Inf. Syst. Secur., 12 (4): 1–29
  - El-Atawy, A. And Al-Shaer, E. (2009), "Building Covert Channels over the Packet Reordering Phenomenon," The 28th Conference on Computer Communications, IEEE (INFOCOM' 2009), Apr 19-25, 2009, 2186-2194
  - SIDD: A Framework for Detecting Sensitive Data Exfiltration by an Insider Attack, Proceedings of the 42nd Hawaii International Conference on System Sciences – 2009

Acknowledgements

All these works are based on the support from Department of Information Technology (DIT), Ministry of Communication and Information Technology (MCIT), Govt. of India

Thank you

subbu@cdac.in