

Analysis of Network Packets

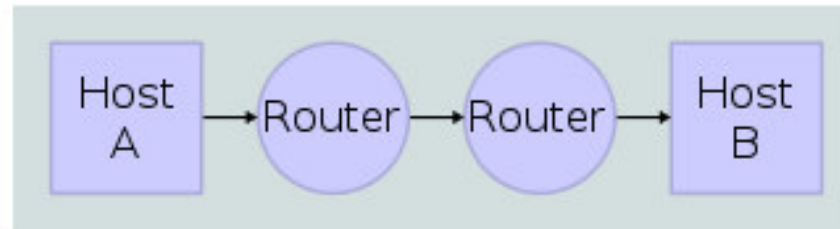
*C – DAC Bangalore
Electronics City*

Agenda

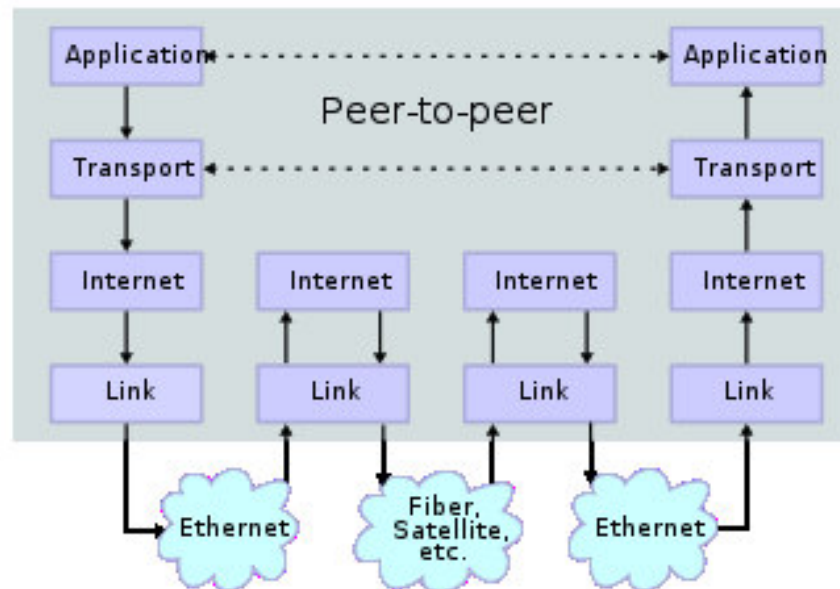
- TCP/IP Protocol
- Security concerns related to Protocols
- Packet Analysis
 - Signature based Analysis
 - Anomaly based Analysis
- Traffic Analysis
 - Analysis in security perspective
 - Analysis in QoS/Performance perspective
- Research Challenges

Encapsulation of headers

Network Connections

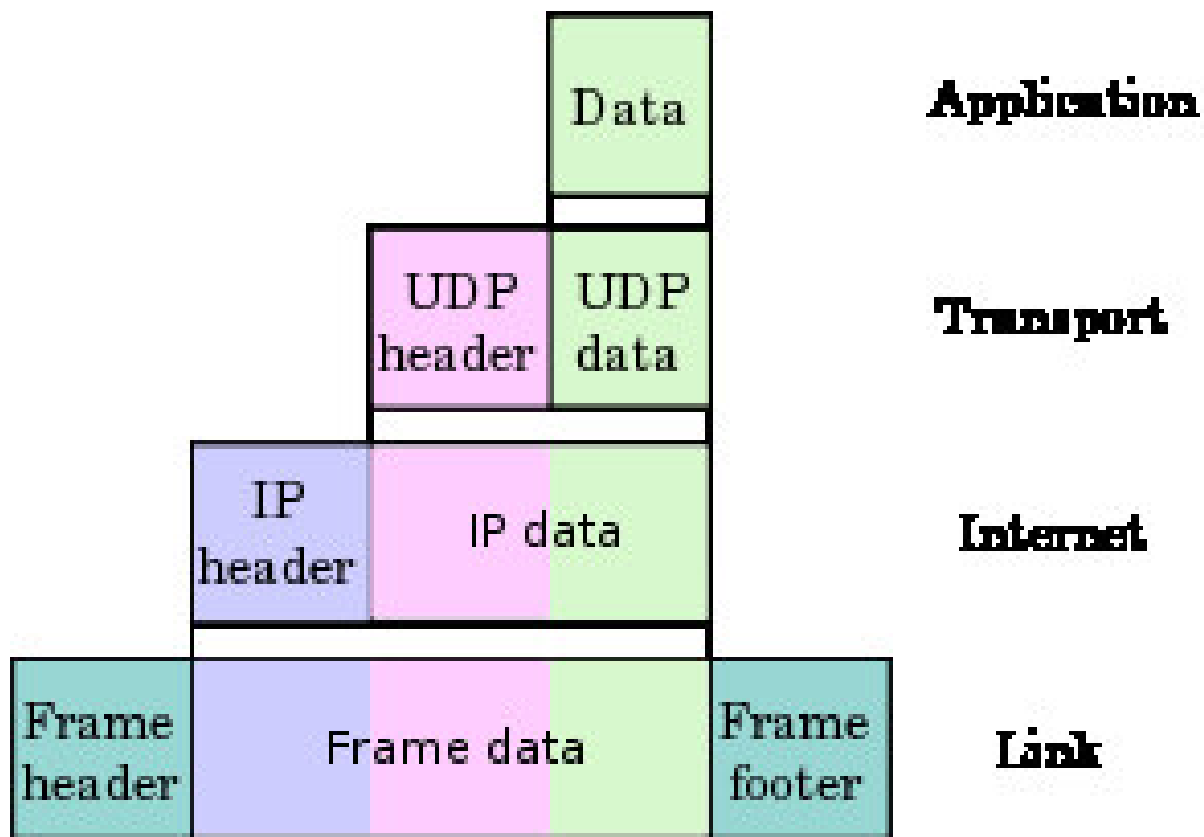


Stack Connections



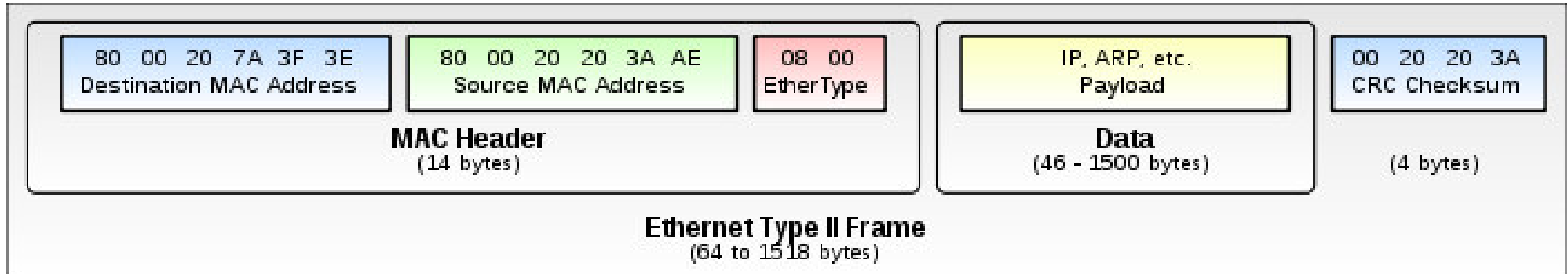
Source: wiki

Encapsulation of headers



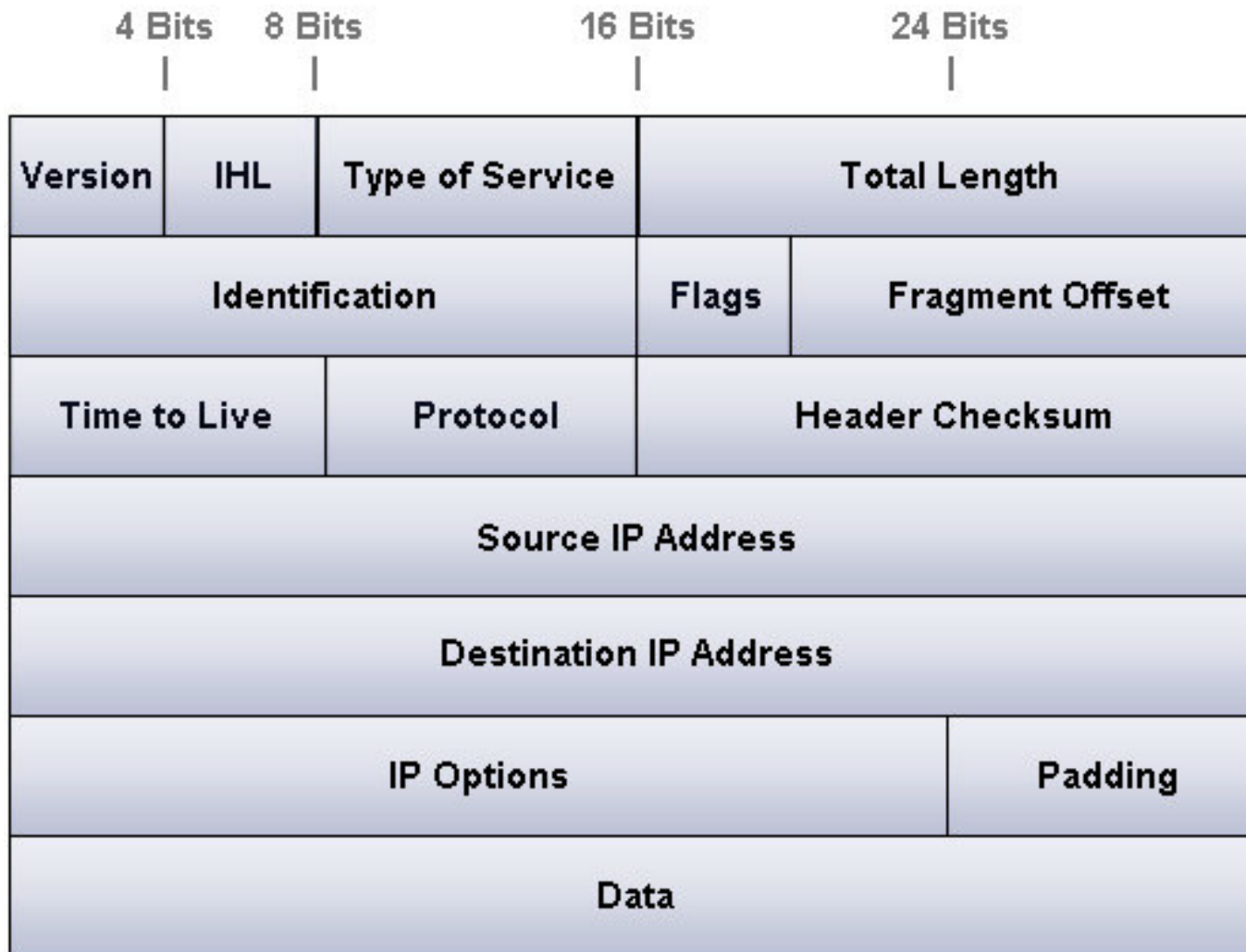
Source: wiki

Encapsulation of headers



Source: wiki

Encapsulation of headers



Source: learn-networking.com

No. ->	Time	Source	Destination	Protocol	Info
1	0.000000	172.16.16.35	172.16.16.3	TCP	51906 > http-alt [SYN] Seq=2797507738 Win=5840 Len=0 MSS=1460 TSV=619
2	0.000107	172.16.16.3	172.16.16.35	TCP	http-alt > 51906 [SYN, ACK] Seq=3702197649 Ack=2797507739 Win=65535 L
3	0.000144	172.16.16.35	172.16.16.3	TCP	51906 > http-alt [ACK] Seq=2797507739 Ack=3702197650 Win=183 Len=0 TS
4	0.000236	172.16.16.35	172.16.16.3	HTTP	GET http://iacas.adbureau.net/jserver/site=dictionary.com/area=search
5	0.000688	172.16.16.3	172.16.16.35	HTTP	HTTP/1.1 407 Proxy Authentication Required (Access is denied.) , M
6	0.000736	172.16.16.35	172.16.16.3	TCP	51906 > http-alt [ACK] Seq=2797508574 Ack=3702198166 Win=216 Len=0 TS
7	0.002998	172.16.16.35	172.16.16.3	HTTP	GET http://iacas.adbureau.net/jserver/site=dictionary.com/area=search
8	0.128926	172.16.16.3	172.16.16.35	TCP	http-alt > 51906 [ACK] Seq=3702198166 Ack=2797509549 Win=65535 Len=0
9	0.911932	172.16.16.3	172.16.16.35	HTTP	HTTP/1.1 200 OK (application/x-javascript)
10	0.951460	172.16.16.35	172.16.16.3	TCP	51906 > http-alt [ACK] Seq=2797509549 Ack=3702199012 Win=269 Len=0 TS

```

0080 3d 73 65 61 72 63 68 2f 61 61 6d 73 7a 3d 37 32      =search/ aamsz=72
0090 30 78 33 30 30 2f 6b 65 79 77 6f 72 64 3d 78 33  0x300/ke yword=X3
00a0 43 53 41 4d 49 78 33 45 68 73 67 48 45 41 44 2f  CSAMIX3E hsgHEAD/
00b0 70 61 67 65 69 64 3d 39 33 39 36 31 30 30 30 2f  pageid=9 3961000/
00c0 72 61 6e 64 6f 6d 3d 34 37 31 30 32 32 33 31 35  random=4 71022315
00d0 36 20 48 54 54 50 2f 31 2e 31 0d 0a 48 6f 73 74  6 HTTP/1 .1..Host
00e0 3a 20 69 61 63 61 73 2e 61 64 62 75 72 65 61 75  : iacas. adbureau
00f0 2e 6e 65 74 0d 0a 55 73 65 72 2d 41 67 65 6e 74  .net..Us er-Agent
    
```

Frame (901 bytes) NTLMSSP / GSSAPI Data (32 bytes)

Security Concerns

- Wired Vs Wireless scenarios
- Point to Point Vs Broadcast
- Connection oriented Vs Connectionless
- State based and stateless
- Headers and packet payloads

Packet Inspection

- Signature Based
 - Header based
 - Deep Packet Inspection
- Behavior based
 - Statistical analysis
 - Datamining
 - Protocol Analysis (....)

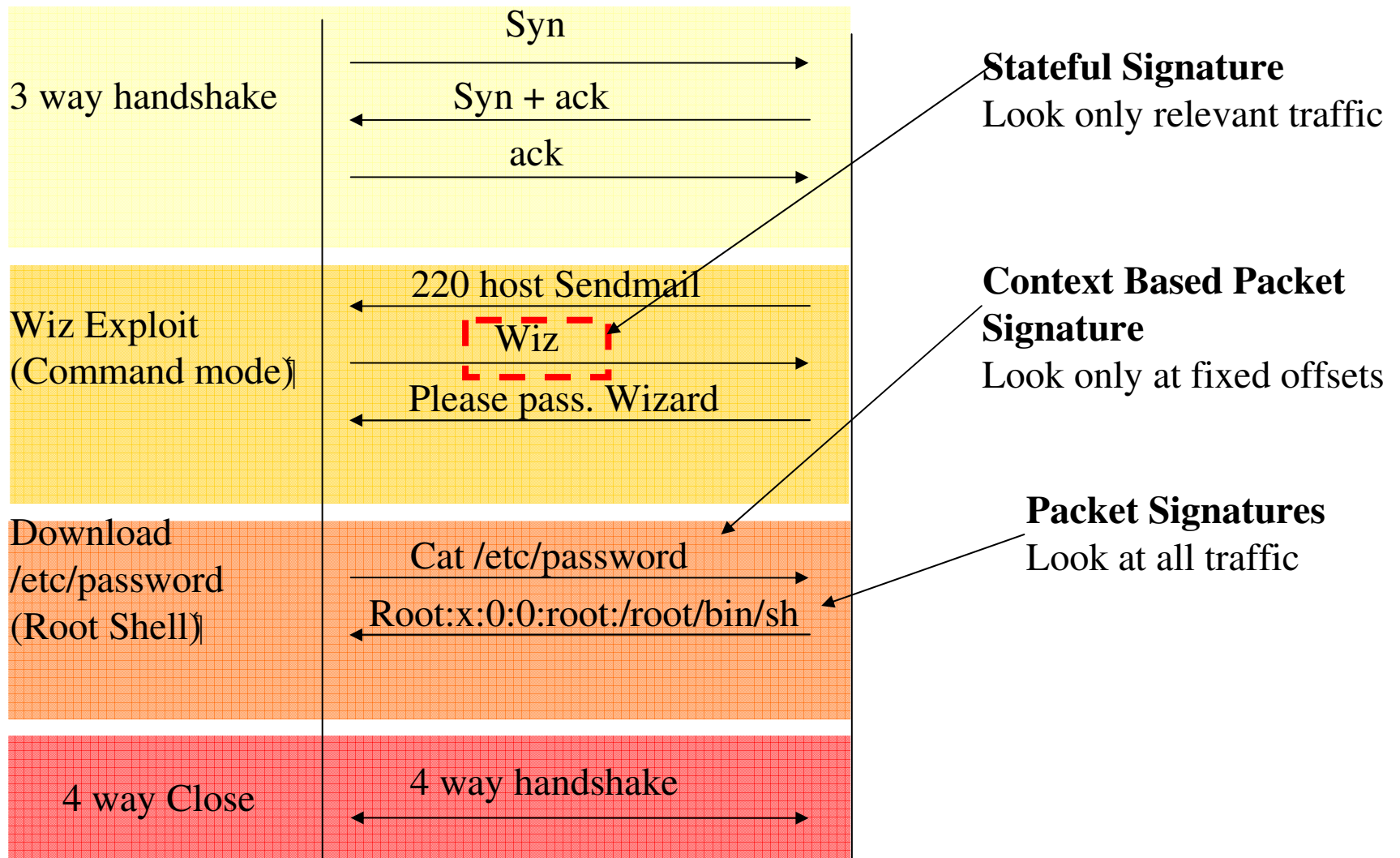
Snort Signature

- alert tcp \$EXTERNAL_NET any -> \$HTTP_SERVERS \$HTTP_PORTS
(msg:"EXPLOIT HP OpenView CGI parameter buffer overflow attempt";
flow:established,to_server; uricontent:"/OvCgi/"; isdataat:2100;
pcre:"^/OvCgiV[^\.]*\.exe[^\x20]{2000,}/*");

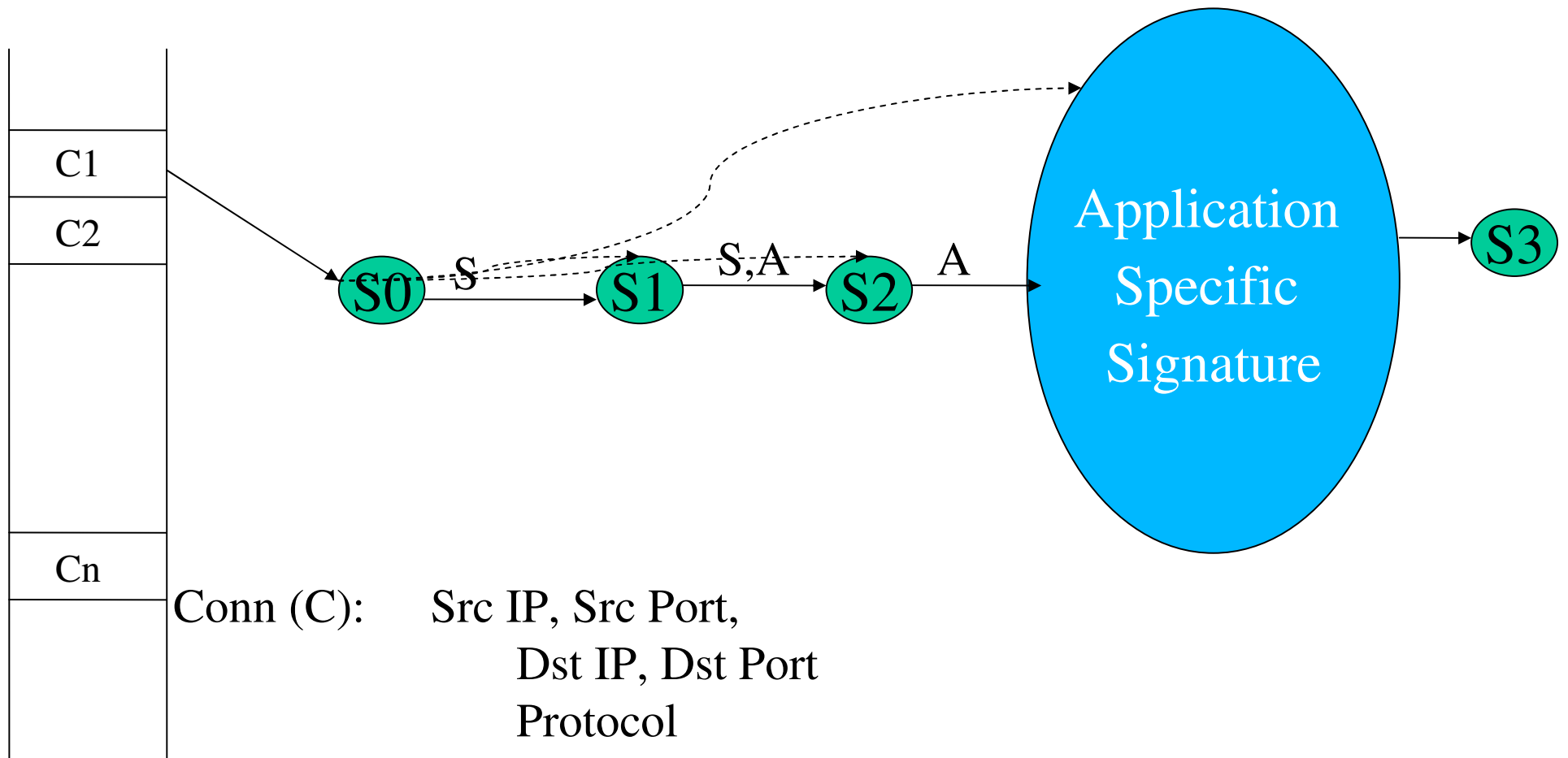
Snort Signature

- alert tcp \$EXTERNAL_NET \$HTTP_PORTS -> \$HOME_NET any (msg:"EXPLOIT DirectX SAMI file CRawParser attempted buffer overflow attempt"; flow:to_client,established; content:"x3CSAMIx3E"; nocase; content:"HEAD"; distance:0; nocase; pcre:"^\x3C[^\x3E\x0a]{500}/Ri");
- metadata:policy balanced-ips drop, service http; reference:cve,2007-3901;
- reference:url,www.microsoft.com/technet/security/Bulletin/MS07-064.msp;

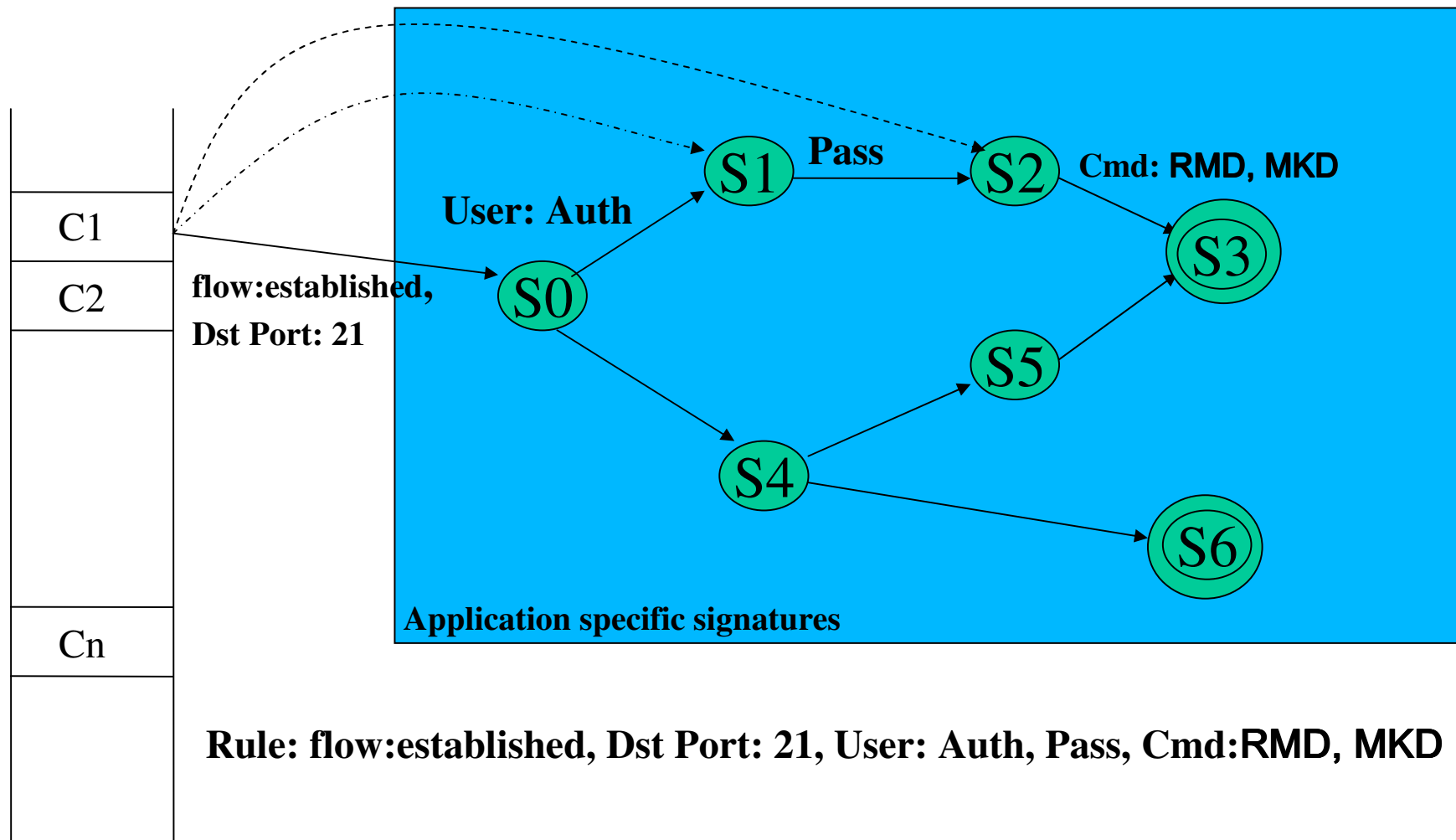
Types of Signature Detection



Example State based Evaluation



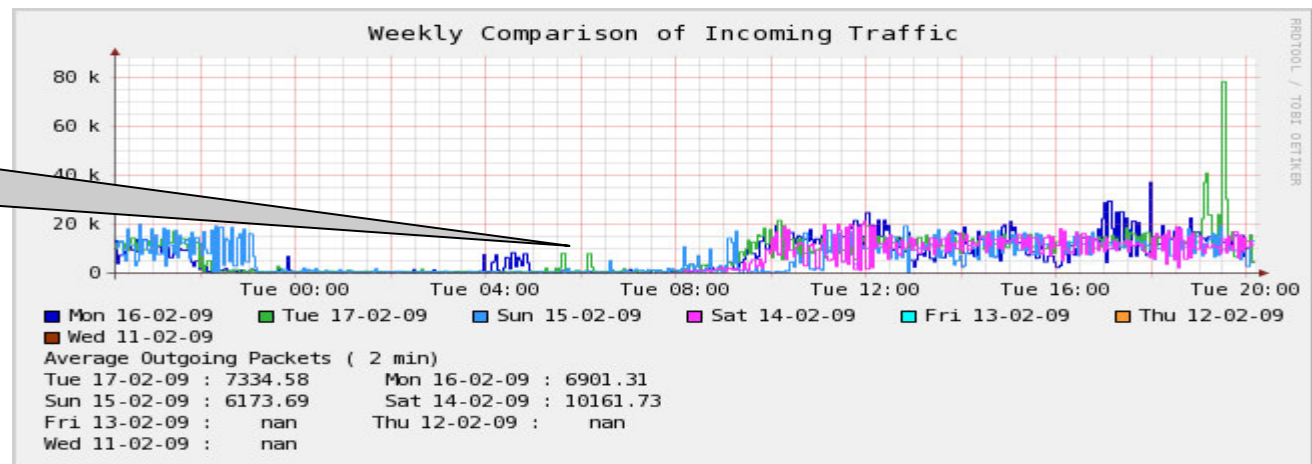
Example State based Evaluation



Traffic Analysis

- Network Traffic analysis is the process of capturing network traffic and inspecting it closely to determine what is happening on the network
- Provides the details of network activities and their communication pattern in a network

Non working time Traffic is Very less



Traffic Analysis in Security Perspective

- Anomaly Detection

- Traffic Analysis can be done to detect traffic anomalies.
- By means of proper profiling, traffic deviation can be detected in network, host and application level.
- Time based profiling has to be done and threshold values can be set for normalcy.
- Suitable for detecting attacks like flooding, DoS and DdoS, Probing etc , which will create changes in normal traffic pattern.

Goal of Traffic Analysis

- Network traffic analysis helps to
 - Network monitoring
 - Network planning
 - Performance analysis and improvement
 - prioritize important traffic with guaranteed bandwidth
 - Security analysis
 - Detect and deny anomalous traffic to make our network safer

Network Traffic Analysis

- Traffic analysis making use of traffic data of a communication to identify
 - Who communicate with whom and When
 - What types of messages
 - How long are the messages
 - Duration of communication

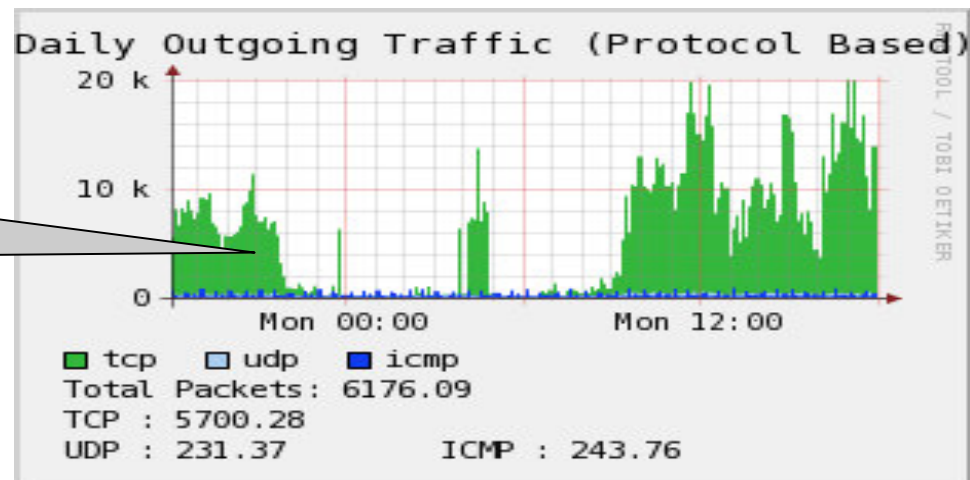
Traffic Analysis - Steps

- Identify the goals of analysis
 - Performance
 - security
 - planning
- Have access to packets
 - Passive
 - Active
- Figure out ways to extract useful information from the packets
 - Packet decoding , aggregation etc ..

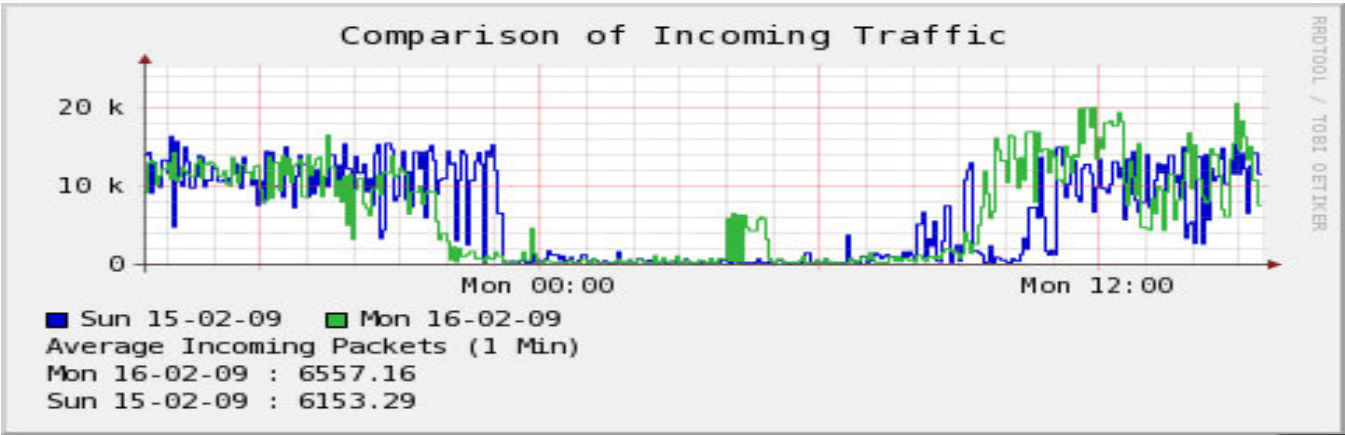
Protocol Based Traffic Analysis

- Identify the traffic distribution based on different protocols
- Can be useful for providing priority to commonly used protocols
- Traffic uses protocol like ICMP can be used for network diagnosis

92 % of total traffic is
TCP

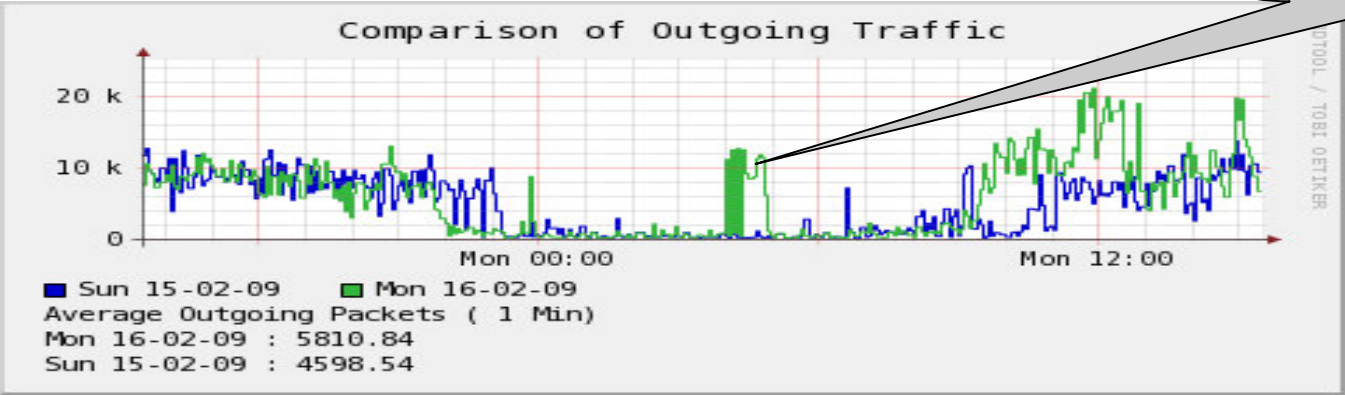


Traffic Analysis in Security Perspective



Day wise Comparison of Incoming traffic

Change in traffic Pattern



Day wise Comparison of Outgoing traffic

Parameters for Traffic Analysis

- In Traffic analysis, the pattern of communication is more important than the content.
 - Analysis is mainly based on packet header
 - Traffic analysis can be done even in encrypted traffic
- Most of the traffic analysis requires minimum information like
 - Time and duration of a communication
 - Details of the communication stream
 - Identities of the communicating parties
 - volume of data

Protocol Distributions

- Traffic analysis data has to be provide traffic details in different granularity
 - Application based
 - HTTP
 - SMTP
 - DNS
 - Transport Protocol based
 - TCP
 - UDP
 - SCTP
- Host (IP) Based

Application Based Traffic Analysis

- Different application traffic have different pattern
 - Web , DNS, FTP , P2P
- Identify these patterns are the basic aim of application based traffic analysis
- Application behaviours are different in even request and response (control and data) traffic of same application
 - Eg : FTP

Application Based Traffic Analysis

- Conventional methods uses port numbers in packet header to identify the application
 - Eg : port 80 for HTTP, 25 for SMTP etc
- Most of the emerging application selects the port numbers by dynamic negotiation based on resource availability
 - Eg: H.323 class of protocols
 - P2P application

Application Based Traffic Analysis

- Application classification based on the port numbers are inaccurate in current context.
- Protocol based decoding is required to identify application which uses dynamically assigned port numbers
- Stateful Traffic analysis is using for identify these types of application

Application Based Traffic Analysis

State less Analysis

- Based on individual packet inspection
- not considering any related stream of packets, sessions , protocols or application for analysis
- It is not a 'true' application aware classification
- only can relate to protocols spawned on standard port

Application Based Traffic Analysis

State full Analysis

- Based on detailed analysis of complete data streams (related packets).
- Identify and preserve the context of packets.
- Through the protocol based decoding, it can be identify the application which is using dynamic port numbers

Host Based Traffic Analysis

- Identify the distribution traffic based on IP address
- More useful for detailed understanding of the Host behaviour.
- Traffic pattern of critical hosts like web server, mail server and DNS server are important

Host Based Traffic Analysis

- Identify the top 'n' hosts which is sending and receiving more traffic in the network
- Useful for detecting abnormal behaviour of a worm, botnet , malware affected host

Traffic Analysis in Security Perspective

- Generally an intrusion detection system fall in to two categories
 - Signature Based
 - Basically relay on the signature(Pattern) of known attacks
 - Anomaly Based
 - Based on the unusual behaviour on a network , host , application etc.
 - Attacks are assumed to be those that are out of normal activities
 - Capable to detect new attacks as well as known attacks

Traffic Analysis – Anomaly Detection

- Flood Detection
- Attack that attempts to cause a failure in a network entity by providing more input than the entity can process.
 - Can be detected using number of connection requests, arrival rate of packets, number of packets etc..

Traffic Analysis – Anomaly Detection

- Denial of Service Attacks (DoS)
- Prevention of authorized access to a system resource or the delaying of system operations and functions.
- Specifically targeted for a particular system or application.
- Can be detected through host, service based profiling

Traffic Analysis – Anomaly Detection

- Port Scan Detection
- Attack that sends client requests to a range of server port addresses on a host/ network, with the goal of finding an active port and exploiting a known vulnerability of that service.
- Number of connection request can be useful for detecting some types of scanning
- Can be detected using host / service based profiling.

Re constructive Traffic Analysis – Network forensics

- It is an off-line traffic analysis techniques
- Archive all traffic and analyze subsets as necessary according to the requirements.
- In-dept analysis is possible

Traffic Analysis in Monitoring perspective

- The purpose of network monitoring is to collect useful information from various parts of the network so that the network can be managed and controlled using the collected information
- To identify the activities in the network, participating hosts, using application, communication time is also part of monitoring.

Traffic Analysis in Performance Perspective

- Through active traffic analysis we can calculate performance related parameters like packet drop, throughput, delay etc .
- Traffic analysis will helps to improve the performance of network, by identifying the bottleneck, under / over utilized links and other performance related issues.
- helps to provides priority to critical application

Research Challenges

- Encrypted traffic
- Compressed traffic
- Identifying contexts
- Accurate Continuous learning
- Performance and latencies

References

- Introducing Traffic Analysis - George Danezis and Richard Clayton
- Survey and Taxonomy of Packet Classification Techniques DAVID E. TAYLOR
- Active Traffic Analysis Attacks and Countermeasures - Xinwen Fu, Bryan Graham, Riccardo Bettati and Wei Zhao
- Focusing on context in network traffic Analysis - John R. Goodall, Wayne G. Lutters, Penny Rheingans, and Anita Komlodi