



**Computer Networks & Software, Inc.**



**GMPLS Network Security: Gap Analysis**

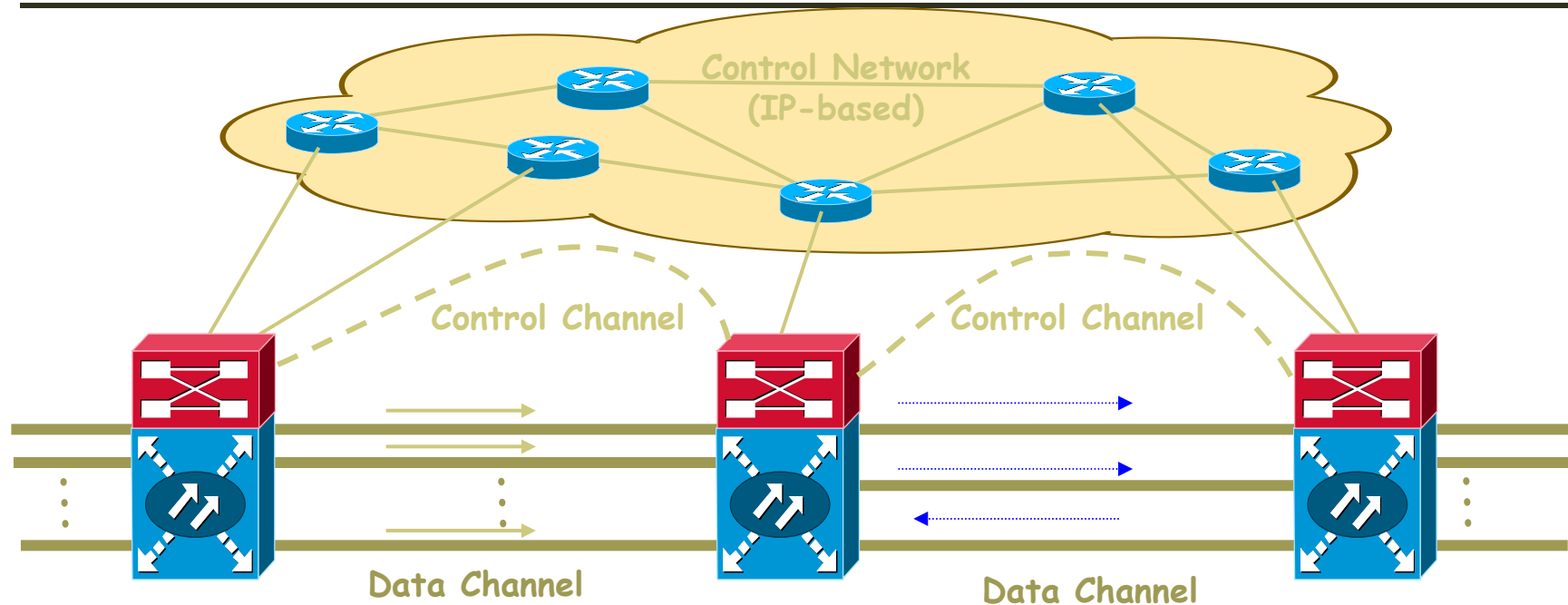
***Vikram Ramakrishnan  
Chris Wargo  
Sherin John***

**Computer Networks & Software, Inc.  
7405 Alban Station Court  
Suite B-215  
Springfield, VA 22150**

**IEEE/ICNS 2008**

- ❖ **New Network Technologies**
- ❖ **Accompanying Security and Concerns**
- ❖ **Vulnerabilities / Security Gaps**
- ❖ **SigSec™ - A defensive tool**

- ❖ Many new network technologies are based on label switching concepts
- ❖ Concepts such as Generalized Multiprotocol Label Switching (GMPLS) and other new network technologies (MPLS-TE, T-MPLS etc) are emerging for use in high-speed data networks.
- ❖ The concept of a control plane is becoming more popular
- ❖ It provides the ability to perform automated and immediate provisioning of network resources as well as recovery from network faults and dynamic reactivity
- ❖ Control plane based architecture allows a single command to provision an end to end connection and provides ability to optimize network usage
- ❖ Control Plane concepts are expected to be part of networks envisioned beyond current research
- ❖ May one day be used to support NextGen service oriented architectures and Net-Centric operations



- ❖ **Generalized Multiple Protocol Label Switching (GMPLS) extends Multi Protocol Label Switching (MPLS) to provide the control plane for devices that can switch packet, time, wavelength, and fiber domains.**
- ❖ **The control plane utilizes a suite of protocols, including LMP, RSVP-TE, OSPF-TE, BGP, CR-LDP, IS-IS.**

- ❖ **NextGen systems propose advanced concepts**
- ❖ **Demand greater dependency on data communications**
- ❖ **Increased reliance on automated procedures for routine operator tasks**
- ❖ **Service disruptions / degradation have increasingly serious impacts**
- ❖ **Increased data traffic by nature opens up a larger target area for individuals / organizations with malicious intent.**
  - **Corollary: Needle in a haystack**



- ❖ MD5, can be cracked.
- ❖ Keys are not always securely, frequently, or dynamically distributed
- ❖ Successful attack on a network or on a Service Provider's infrastructure may cause
  - Observation, modification, or deletion of data.
  - Injection of spurious data into a traffic stream
  - Traffic pattern analysis
  - Disruption of connectivity
  - Degradation of quality of service
  - Denial of Service (DoS)



- ❖ Risk of service disruption increases by not securing the control plane with the right type of security
- ❖ E.g.: Triggering recovery actions under false failure indication can destabilize the core network
- ❖ Security mechanisms typically geared towards providing authentication and confidentiality
- ❖ Still leaves exploitable “gap” in the security framework of GMPLS and related networks



- ❖ IPsec tunnels provide security for the control plane traffic.
  - The reality is many implementations of IPsec let 'unencrypted' packets through to the destination
  - IPsec prevents the contents of the encrypted packet from being viewed
  
- ❖ The chain of trust model is very vulnerable to any illicit access into the network
  - If a rogue control packet can be tunneled into the network, effect will ripple out impacting all nodes.
  - The network is open to insider attacks such as a 'pressured insider' or a 'disgruntled employee/ex-employee'
  - Traditional security cannot protect against such attacks



- ❖ Router or control plane node may be subverted by loading malware software or a virus
  - Remote operator may gain full control of control plane node through a trojan.( virus scanners and firewalls are not fool proof)
  - The chain of trust model provides no defense.
  - Systems that allow firmware upgrades are susceptible to “sleeper” implementation” attacks.
    - Malicious lines of code inserted in firmware waiting for specific time/ input to trigger a standalone / coordinated attack
- ❖ Unauthorized nodes may obtain a routing adjacency where an IGP (Interior Gateway Protocol) has been enabled by mis-configuration, or where authentication is not used
  - May result in attacks like traffic redirection





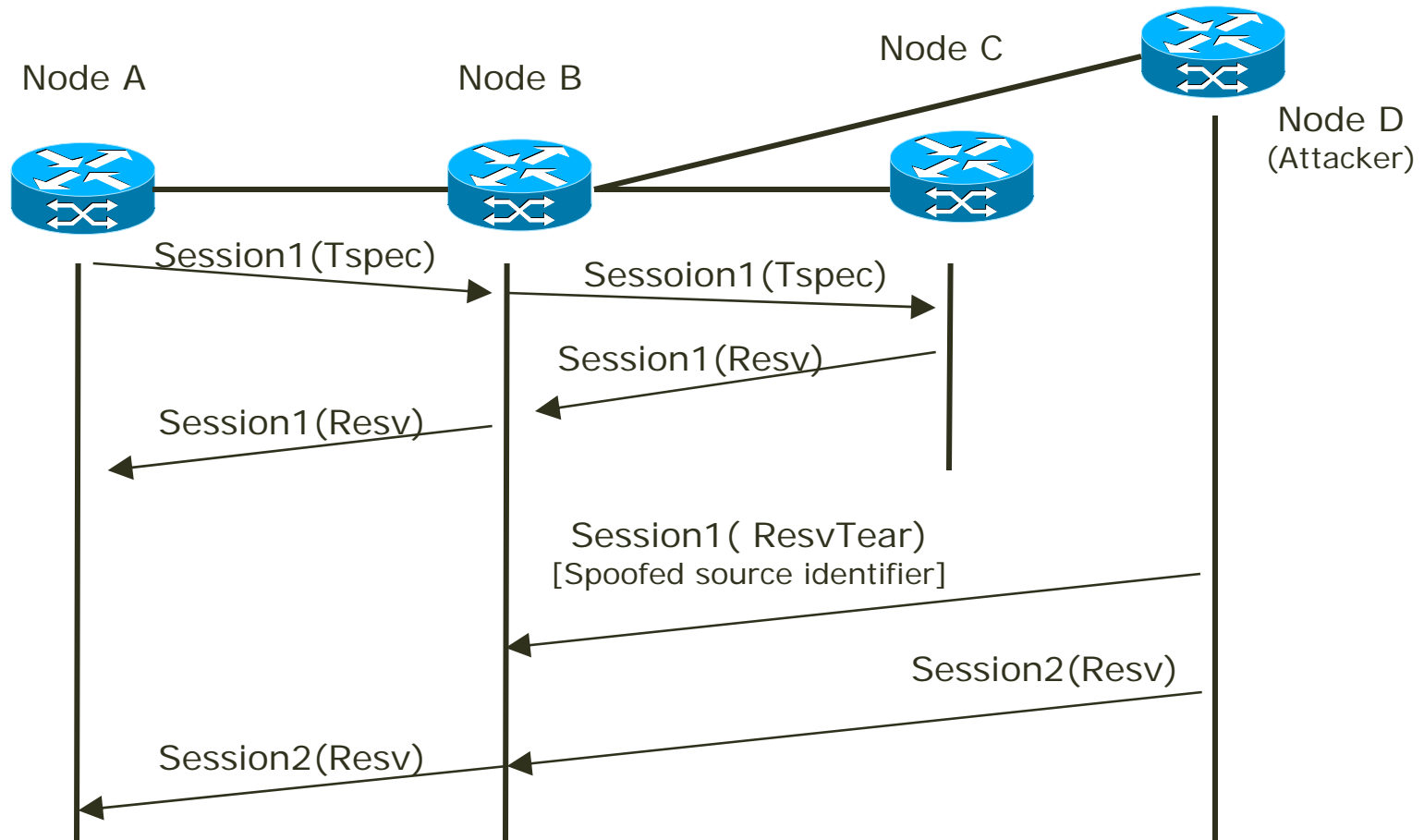
## Gap Analysis - Summary

Type Of Attack	Total Number Detectable* (Numbers may change as study progresses)
Denial Of Service	60
Protocol Exploitation	10
Man In the Middle	6
Impersonation	7

Attack Levels	# detected
Critical	7
High	59
Medium	32
Low	5

Our research has shown that there are a number of possible attacks that will pass through traditional security defense mechanisms.

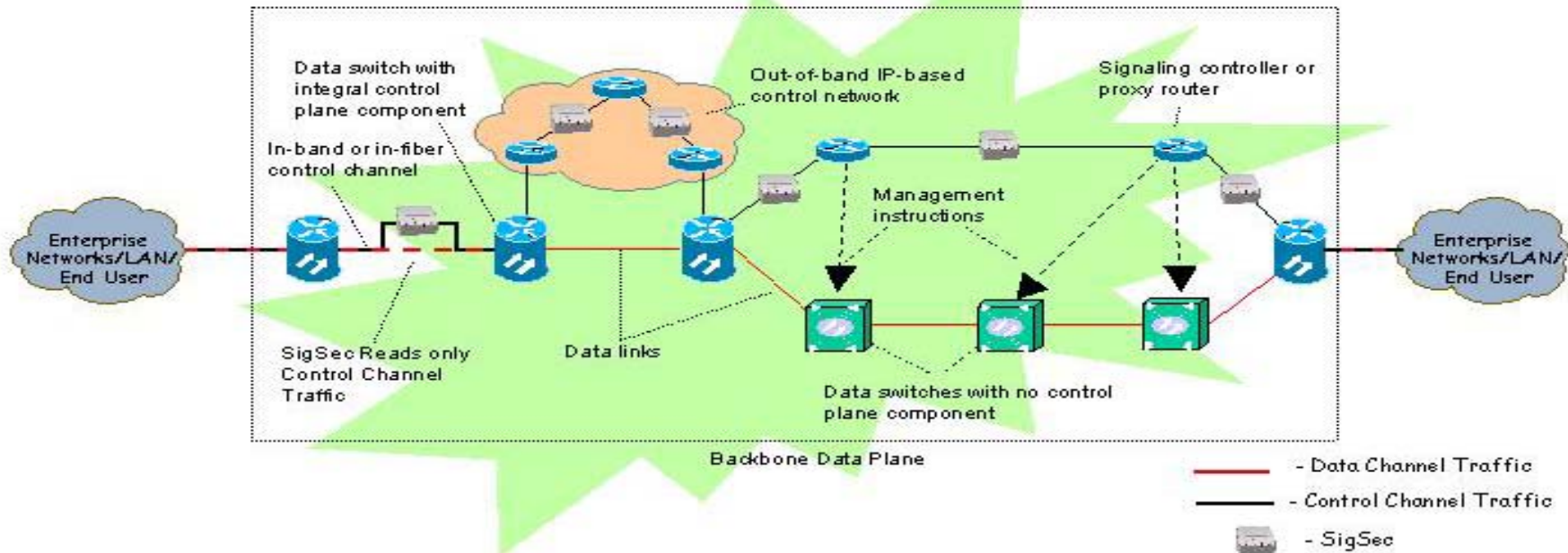
# Attack example - Spoofed Teardown



- ❖ **Based on our analysis of the security gap that exists we at CNS are developing a prototype software based Intrusion Protection System for the GMPLS Control Plane**
- ❖ **‘SigSec™ Core’ detects all known semantics and syntax related inconsistencies of the GMPLS control plane protocols**
- ❖ **‘SigSec™ Core’ detects many attacks that may pass through semantic and syntax analyzers**
  - **Able to detect Unknown attacks through tracking unexpected protocol exchanges/state changes**
  - **SigSec™ can detect many previously known attacks using a FSM analyzer and proprietary attack profiles**



# SigSec™ Deployment and Features



Features	Advantages	Benefits
Data Switch/router or IPS appliance	Flexibility in product line	One-stop shopping for end-users
<i>Bump in the link</i> deployment	Real-time/in-line intrusion detection/ protection	<ul style="list-style-type: none"> <li>• Works with range of switch manufacturers</li> <li>• Prevents network interruption</li> <li>• Allows upgrade of infrastructure</li> </ul>
Security framework definition	Security domain delineation	Differentiators
Detects attacks from network users, managers, or malware	Interrupts attacker in motion	Offer higher degree of network service
Non-signature-based	No constant attack profile updates	Enhances operation continuity
All emerging backbone protocol approaches	Greater market penetration	Increases sales
Linux with off-the-shelf computer/components	Low cost integration approach	Broadens potential customer base



**Computer Networks & Software, Inc.**



# Thank You !

CNS, Inc is currently seeking  
partners for the SigSec™  
Project.

Contact us at

[Chris.wargo@cns.com](mailto:Chris.wargo@cns.com)