Columbia - Verizon Research
Securing SIP: Scalable Mechanisms
For Protecting SIP-Based Systems

Henning Schulzrinne
Eilon Yardeni
Somdutt Patnaik
Columbia University
CS Department

Gaston Ormazabal
Verizon Labs

David Helms
CloudShield

Agenda

- Denial of service threats: RTP & SIP
  - Pinhole filtering
  - SIP DOS detection and mitigation strategy
- Implementation: CloudShield
- Testing methodology and results

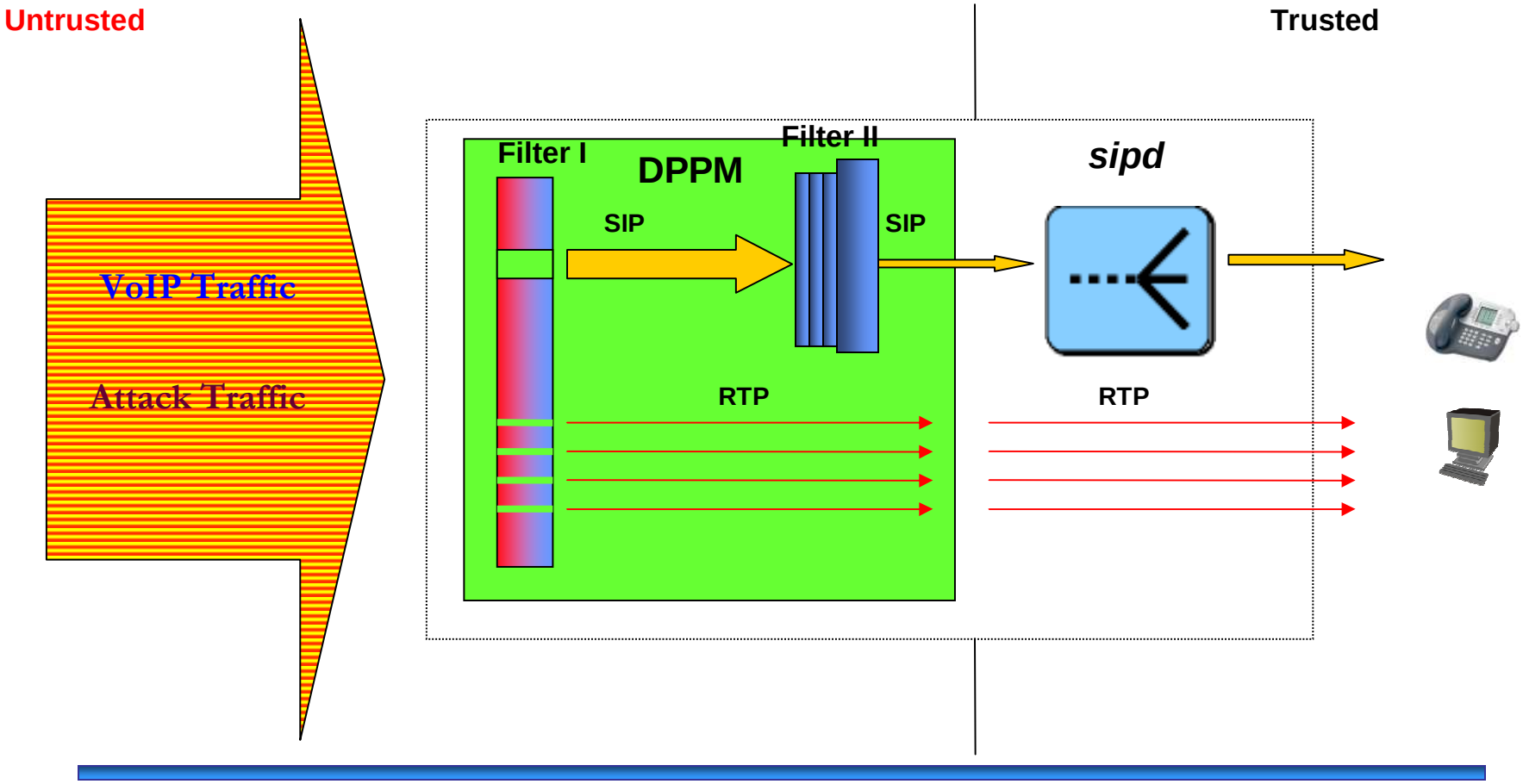
Background

- Telephony services migrating to IP becoming attractive DoS targets
- Attack traffic traversing the perimeter reduces availability of signaling and media for VoIP service
- Attack targets:
  - SIP infrastructure elements (proxy, softswitch, SBC)
  - End-points (SIP phones)
  - Supporting services (e.g., DNS)
- Carriers need to solve perimeter protection problem for security of VoIP services
  - Protocol-aware application layer gateway
  - SIP DoS/DDoS attack detection and prevention
- Test tools verify performance & scalability

Goals

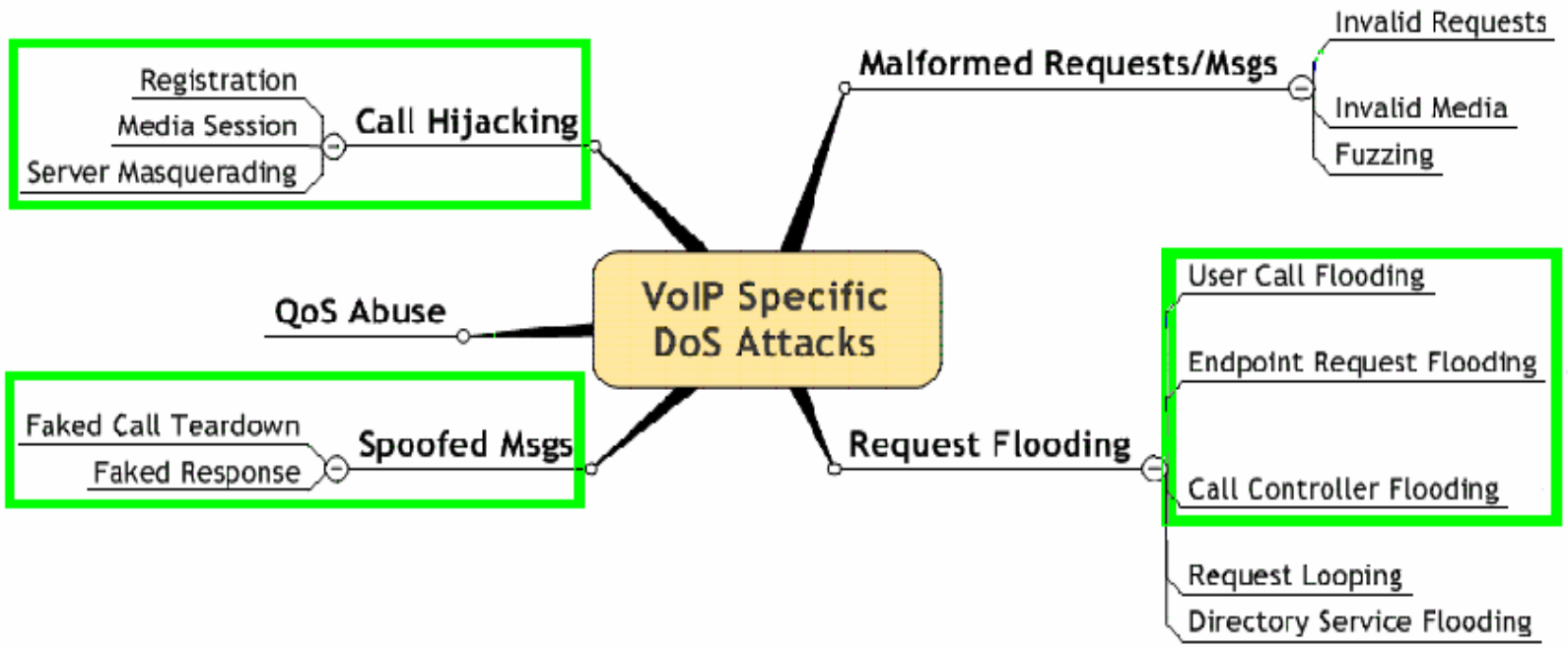
- Build a prototype of the fastest dynamic pinhole filter firewall for RTP media
- Study VoIP DoS for SIP signalling
  - Definition – define SIP specific threats
  - Detection – how do we detect an attack?
  - Mitigation – defense strategy and implementation
  - Validation – validate our defense strategy
- Generate requirements for future security network elements
- Generate the test tools and methodology strategies for their validation

Problem Overview



Scope of Our Research

Scope of current work



Basic Strategy and Motivation

- Implementation flaws are easier to deal with:
  - Systems can be tested before used in production
  - Systems can be patched when a new flaw is discovered
  - Attack signatures could be integrated with a firewall
- Protocol & flooding attacks are harder to defend against
- Commercially available solutions for general UDP/SYN flooding, but none for SIP
- → address protocol and flooding attacks *specifically* for SIP

Main Focus of our Strategy

- **VULNERABILITY: SIP over UDP → spoofing SIP requests**
  - **Registration/call hijacking**
  - **Modification of media sessions**
  - **Session teardown**
  - **Request flooding**
  - **Error message flooding**
  - **SIP 'Method' vulnerabilities**
- **STRATEGY: Two detection and mitigation filters**
  - **Media: SIP-aware dynamic pinhole filtering**
  - **SIP: Rule-based detection and mitigation filters**

Media Filters

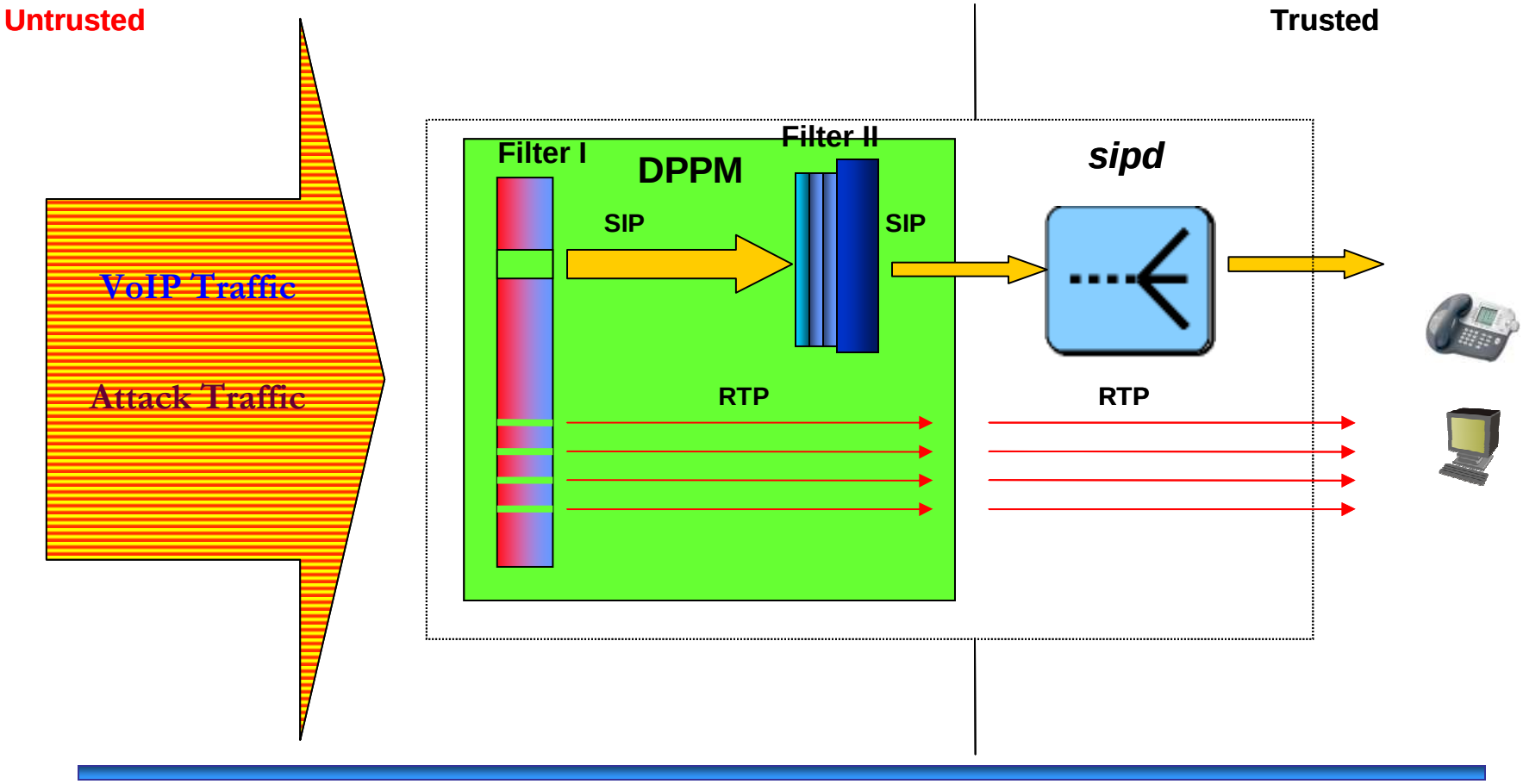
Implemented large scale SIP-aware firewall using dynamic pinhole filtering

- **Media filter as first-line of defense against DoS attacks:**
  - **Only signaled media channels can traverse the perimeter**
  - **End systems are protected against flooding by random RTP**
- **The RTP pinhole filtering approach is a good first-line of defense, but…**
  - **Signaling port is subject to attack**

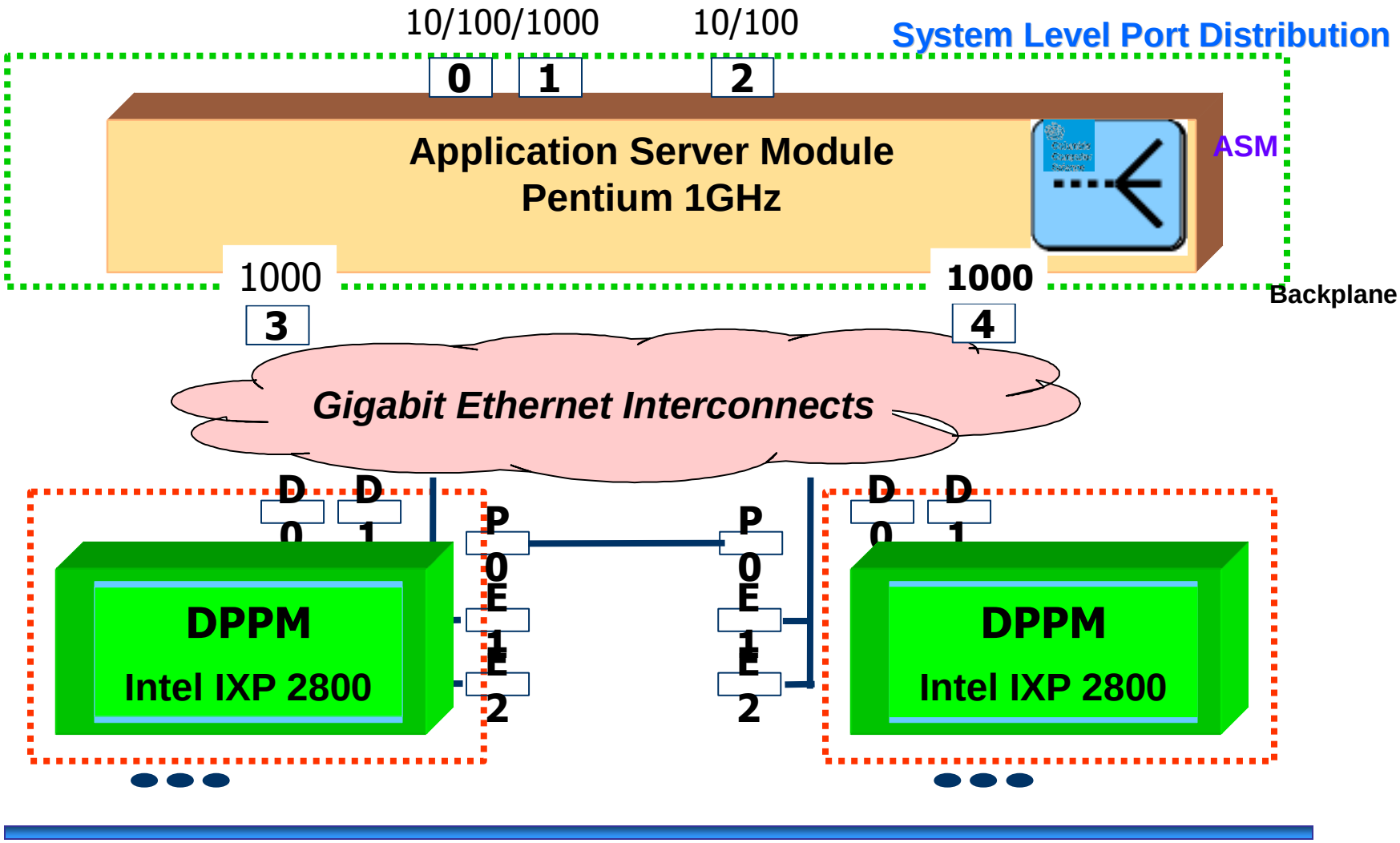
Ongoing - SIP DoS Detection and Mitigation Filters

- Authentication based - Return Routability Check
  - For UDP use SIP's built-in digest authentication mechanism
    - Use null-authentication when no shared secret is established
    - Filter out spoofed sources
- Rate limiting
  - Transaction based
    - Thresholding of message rates
      - ✓ INVITE
      - ✓ Errors
    - State Machine sequencing
      - ✓ Filter "out-of-state" messages
      - ✓ Allow "in-state" messages
  - Dialog based
    - Maintain a database of INVITE sources (Contacts) to verify and accept a BYE message only from legitimate source addresses
- Method vulnerability based

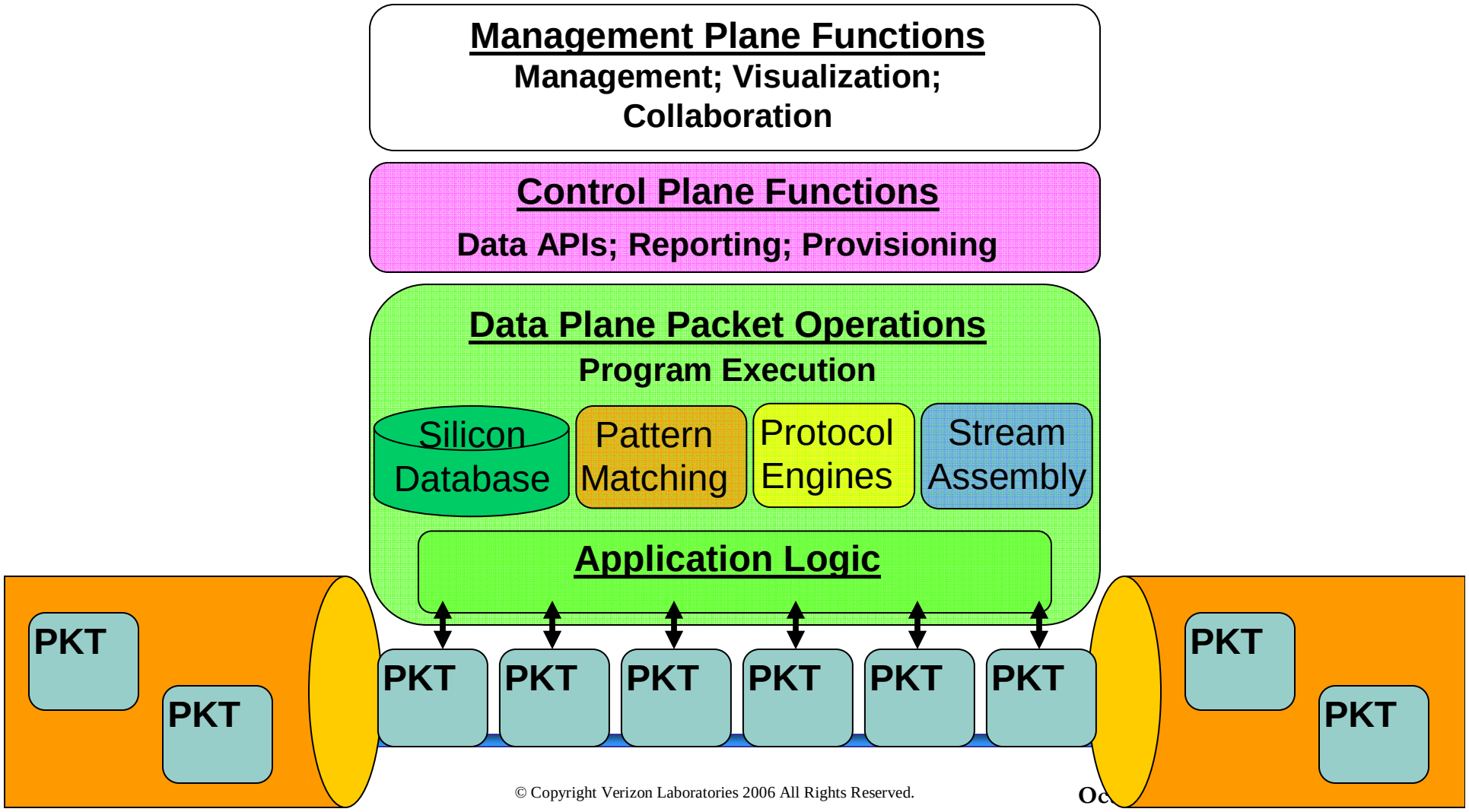
Mitigation Solution Overview



CloudShield CS-2000



CS-2000 Processing Pipeline



Prototype Implementation

- Use network processor to filter RTP media and SIP authentication attempts to the proxy and rate-limit messages based on particular heuristics:
  - Utilize wire-speed deep packet inspection
  - Thresholds are kept internal in the DPPM
  - State is only kept at CloudShield in CAM tables
- Use the firewall controlling proxy model for media filtering and the authentication filter
  - Columbia's SIP Proxy *sipd* controls the CloudShield Deep Packet Inspection Server
  - Utilize the *Firewall Control Protocol* to establish filters in real time
  - Insert filters for Media Ports and SIP UAs that are being challenged

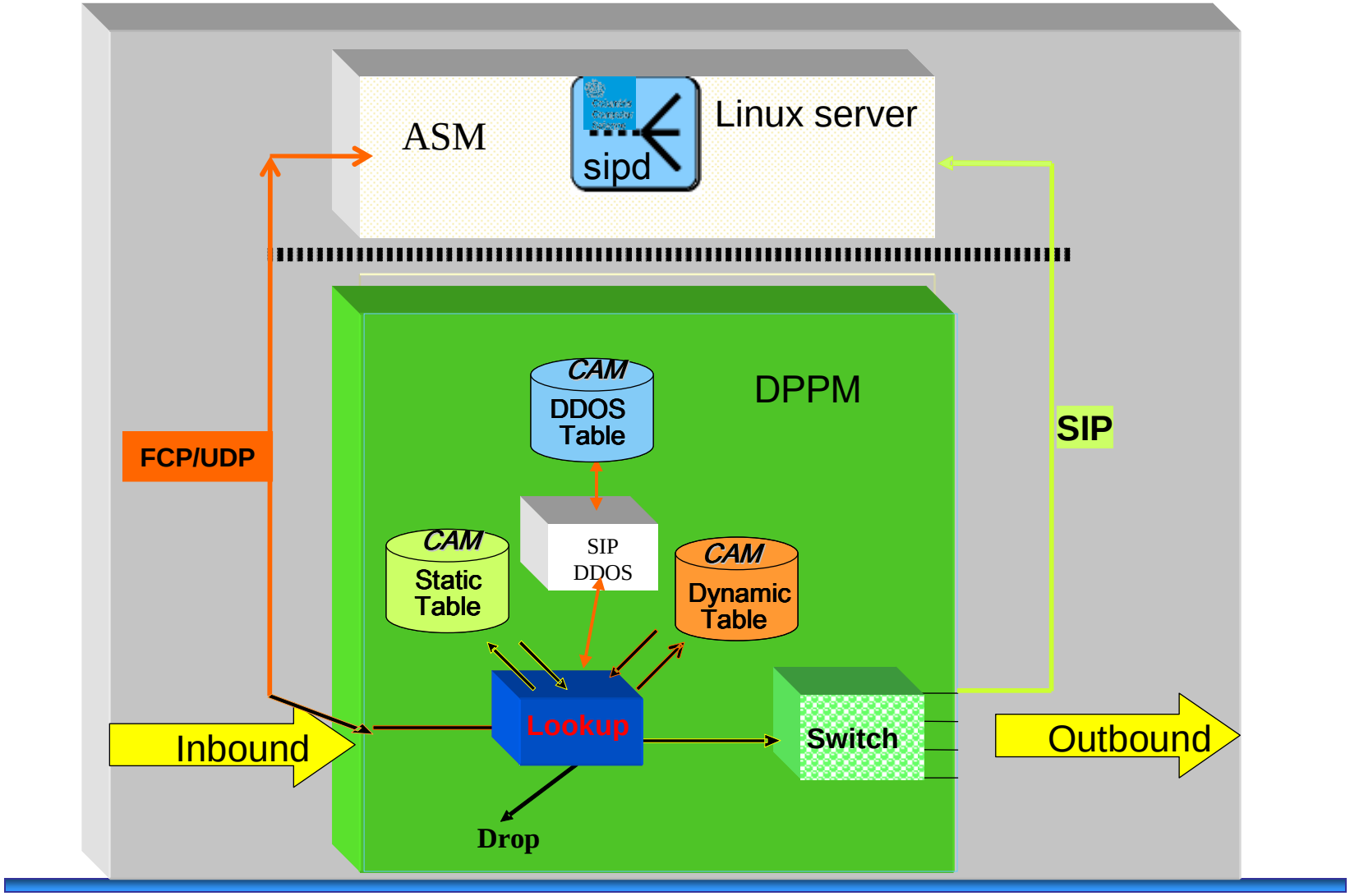
Pinhole Firewall Components

- Static Filtering
  - Filtering of pre-defined ports (e.g., SIP, ssh)
- Dynamic Filtering
  - Filtering of dynamically opened ports (e.g., RTP)
- Switching Layer
  - Perform switching between the input ports
- Firewall Control Module
  - Intercept SIP call setup messages
  - Get RTP ports from the SDP
  - Maintain call state
- Firewall Control Protocol
  - The way the Firewall Control Module talks with the CloudShield
  - Push dynamic table updates to the data plane
  - Could be used by multiple SIP Proxies that control one or more CloudShield firewalls

CS-2000 Data Plane Execution

Part of SIP-proxy Executed in the Linux Control Plane

Integrated DDOS and Dynamic Pinhole Filter

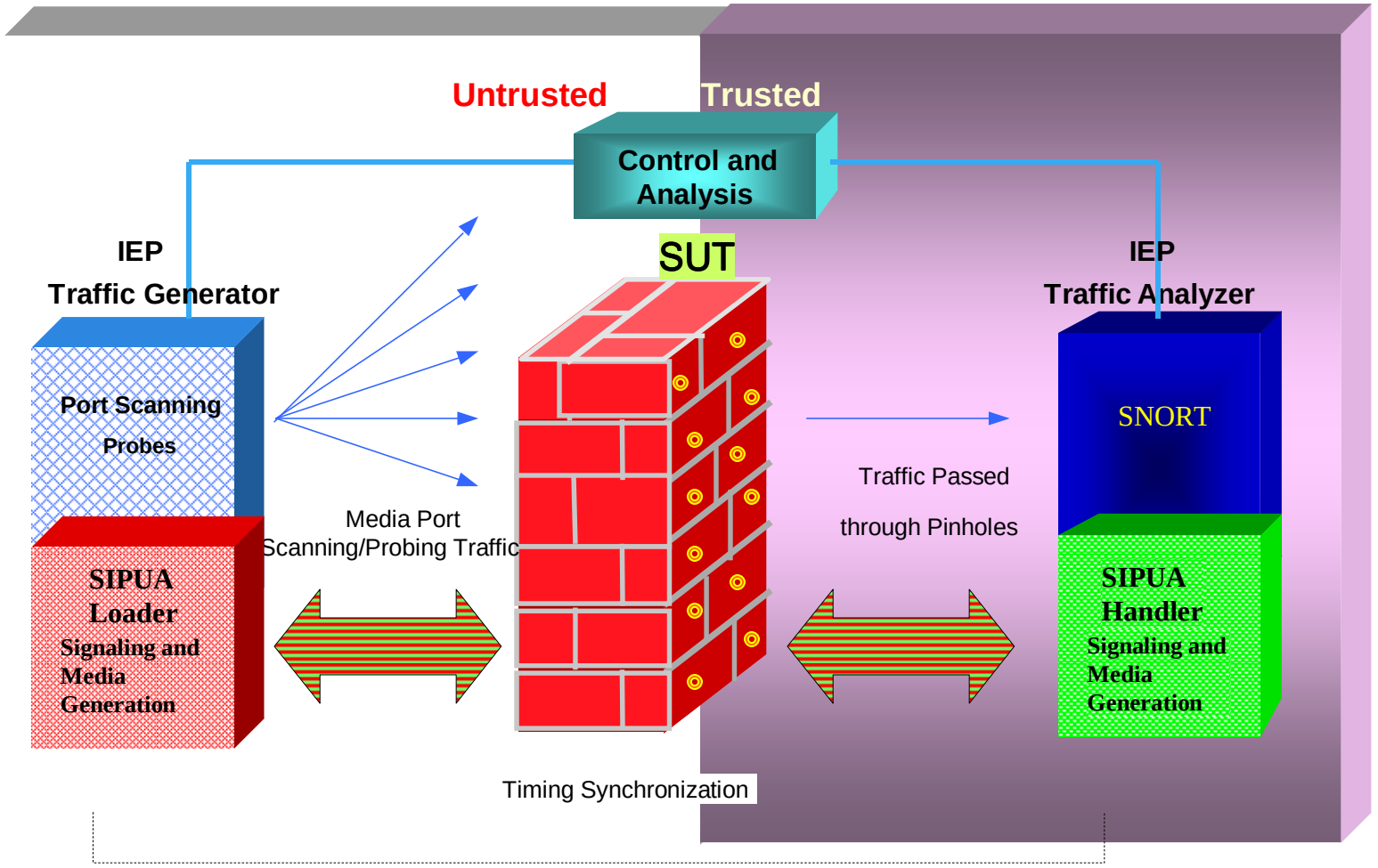


Integrated Testing and Analysis Tool

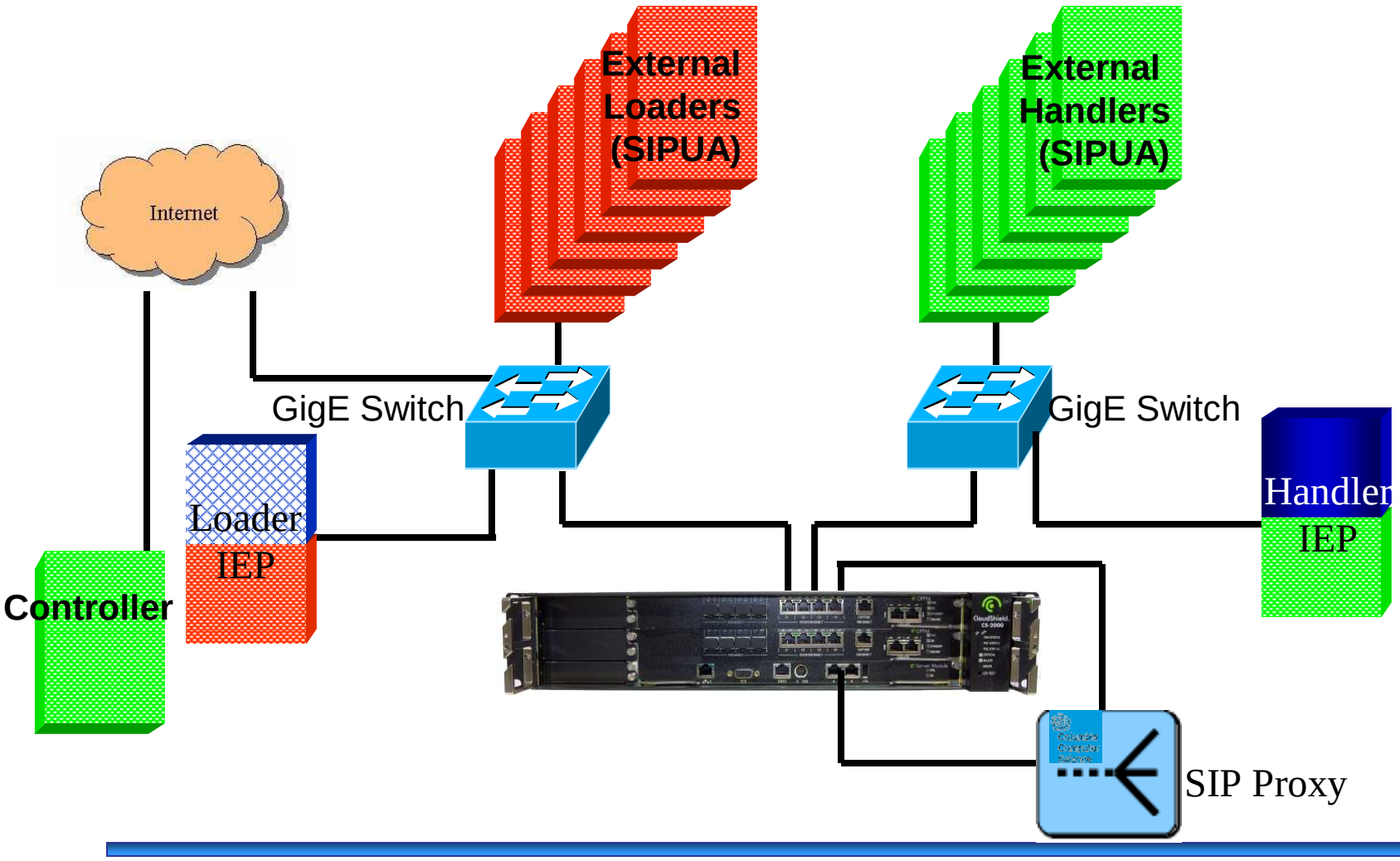
Pinhole Filter Integrated End Point Tool Components

- SIPUA Test Suite
  - Loader/Handler
  - Establishes calls using SIP
  - Sends 160 byte RTP packets every 20ms
    - Settable to shorter interval if needed for granularity
  - Starts RTP sequence numbers from zero
  - Dumps call number, sequence number, current timestamp and port numbers to a file
- Scanning Probes
  - nmap
- Automated Script based Control Software
- Timing Devices
- Data Analysis Module
  - Analyze handler's file for initial and teardown call delays,
    - Number of packets dropped before pinhole opening
    - Number of packets crossing after pinhole closing
  - Scan results for pinhole coverage
- Protocol Analyzer
  - SNORT
- Graphical Displays

Integrated End Point



Testbed Architecture



Testing And Analysis Methodology

- Problem parameterized along two independent vectors
  - Call Rate (calls/sec)
    - Related to performance of SIP Proxy in Pentium
  - Concurrent Calls
    - Related to performance of table lookup in IXP 2800
- Generate external load on the firewall
  - SIPUA Loader/Handler in *external* load mode
  - Generates thousands of concurrent RTP sessions
  - For 30K concurrent calls have 120K open pinholes
  - CAM table length is 120K entries
    - Search algorithm finds match in one cycle
- When external load is established, run the IEP analysis
  - SIPUA Loader/Handler in *internal* load mode
  - Port scanning and Protocol analyzer
  - Increment calls/sec rate
- Measure pinhole opening and closing delays
  - Opening delay data provided in units of 20 ms packets
  - Closing delay data provided in units of 10 ms packets
- Detect pinholes extraneously open

Pinhole Filter Data Results

Concurrent calls	Calls/Sec	SIP Proxy		SIP RAVE	
		Open delay	Close delay	Open delay	Close delay
10K	300	0.75	0	0.25	0
15K	300	0.74	0	0.33	0
20K	300	0.73	0	0.34	0
25K	300	0.75	0	0.26	0
30K	300	0.8	15.51	0.26	0
30K	200	0.83	0.02		

Conclusions

- Demonstrated SIP vulnerabilities in media and signaling
- Implemented some "carrier-class" mitigation strategies
- Built a validation testbed to measure performance
- Need to generalize methodology to cover a broader range of cases and apply anomaly detection, pattern recognition and learning systems

Thank You!

Henning Schulzrinne
Eilon Yardeni
Somdutt Patnaik
Columbia University
CS Department

Gaston Ormazabal
Verizon Labs

David Helms
CloudShield