SAND2000-1570C

Intrusion detection considerations for switched networks

Thomas D. Tarman and Edward L. Witzke
Advanced Networking Integration Department

Sandia National Laboratories
Albuquerque, NM 87185

ABSTRACT

Many private and public networks are based on network switching technologies. However, switched networks present a number of challenges to intrusion detection equipment. These challenges include limited visibility of network flows at the edges of the network, high-speed packet processing, and highly-aggregated flows in the core. In addition, switched networks typically implement protocols specific for Layer 2 functions, such as connection establishment and connection routing, which can be attacked to deny service to higher layer protocols and applications. Since these attacks cannot be detected by Internet Protocol (IP) intrusion detection equipment, Layer 2 intrusion detection is required. This paper describes an approach for performing intrusion monitoring in switched, Layer 2 networks, specifically, Asynchronous Transfer Mode (ATM)networks.

Intrusion detection sensors for high-speed, Layer 2 networks face many of the same issues associated with high-speed IP packet filtering for law enforcement purposes. These issues include high-speed context lookup, reassembly of ATM Adaptation Layer (AAL) segments or IP fragments, pattern matching, filter specification, scalability to large networks, and preservation of captured data. These technical issues are discussed in this paper, along with policy issues associated with the requisite supporting infrastructure (e.g., key management, filter configuration policies, and preservation of evidence).

Keywords: Asynchronous transfer mode, ATM intrusion detection, packet filtering, assessment

1. INTRODUCTION

Switched networks form the basis for a variety of public and enterprise networks, including the telephone network, the Internet, and intranets. As voice and data networks continue to converge, the impact of disruption in a single network will become more severe. Disruptions, whether due to a malicious network attacks or component failures, can occur in the switched network services below the Internet Protocol (IP), where most intrusion detection and monitoring functions occur today. These disruptions can cause complete loss of service, and cannot be detected by current intrusion detection devices.

As network infrastructure becomes more critical, monitoring of the public network for malicious attacks and abuse will need to increase. Network security often follows the traditional paradigm in physical security of Detect-Delay-Respond, or DDR. First one must detect that an attack or intrusion is occurring, then the intruder must be delayed while the nature of the attack is assessed. Finally a response should be generated. The delay not only needs to be long enough to conduct an assessment of the attack, but also be sufficient for the response to be generated and take effect, or possibly even complete. Obviously, in this paradigm, attacks cannot be mitigated if they are not detected.

How one performs detect, delay, and response in a network depends on the layer of operation. The Reference Model of Open Systems Interconnection (OSI) developed by the International Standards Organization contains seven layers (Figure 1). One of the key principles applied in constructing this model is that each layer should perform a well-defined function[1]. This model is extensively documented in standards, books, and papers[1,2,3]. Because this paper concerns switched networks, a little background will be given regarding the lower layers of the OSI Reference Model. For information on the upper layers of the model, one is referred to the previously listed references.

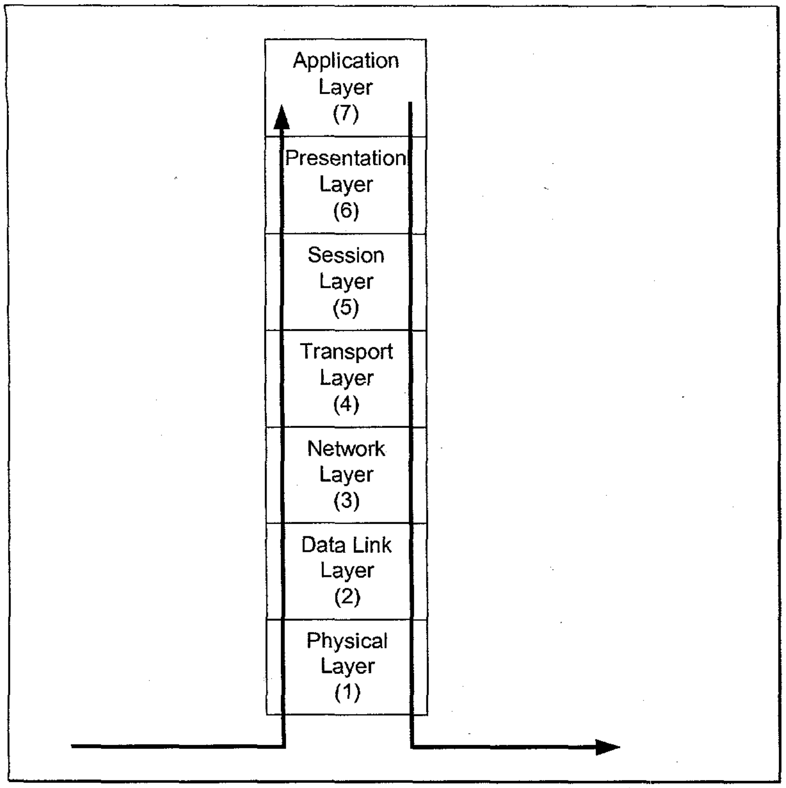

Figure 1: The seven layer OSI reference model

The lowest layer of the OSI model, layer 1, is the physical layer. The purpose of this layer is to move bits over a communication channel. Typical concerns at this layer are network interface cards (size, shape, and transmission rate of the bits) and transmission media (wires, fiber optics, and radio waves).

Layer 2, the data link layer, is responsible for transferring information units, such as characters, from one node to another. Converting information units to bit streams and back, error detection and correction, and buffering, are issues addressed by this layer.

The network layer, layer 3, controls the routing of information within the network. This layer also typically deals with congestion and deadlock prevention[3]. IP routing and assembly of IP datagrams occurs at this layer.

Because IP intrusion detection implementations function at layer 3, IP is dependent on the correct functioning of Layer 2 and below. In addition, native Layer 2 applications such as telephone and video services over Asynchronous Transfer Mode (ATM) use a different Adaptation Layer (AAL) to interface into the ATM network than data transfer services, bypassing IP and hence, layer 3. Therefore, intrusion detection in switched networks (like ATM) must be performed below layer 3.

Switched "Layer 2" networks use a number of protocols to perform functions such as call setup, route determination, and tracking of network state. Denial of service and other attacks on these protocols are possible, and have been described elsewhere[4]. Therefore, the need exists to monitor layer 2 protocol flows to determine whether such attacks are occurring in the network. Because IP intrusion detection products operate at layer 3 (or higher), the attacks to switched network protocols are invisible to them.

However, switched networks pose challenges to network intrusion detection. First, point-to-point data flows over switched networks can only be viewed by intermediate switches. Other nodes in the network (including network intrusion detection equipment) cannot view these flows without requiring a network configuration change. Second, switched networks scale very well, and can therefore grow quite large. To examine protocol flows in large networks, a large number of sensors must be deployed. Since these sensors typically report to a central intrusion assessment entity, it is possible that the assessment entity will become overwhelmed with sensor data. To scale the intrusion assessment function, assessment entities must be deployed

DISCLAIMER

This report was prepared as an account of work sponsored by an agency of the United States Government. Neither the United States Government nor any agency thereof, nor any of their employees, make any warranty, express or implied, or assumes any legal liability or responsibility for the accuracy, completeness, or usefulness of any information, apparatus, product, or process disclosed, or represents that its use would not infringe privately owned rights. Reference herein to any specific commercial product, process, or service by trade name, trademark, manufacturer, or otherwise does not necessarily constitute or imply its endorsement, recommendation, or favoring by the United States Government or any agency thereof. The views and opinions of authors expressed herein do not necessarily state or reflect those of the United States Government or any agency thereof.

DISCLAIMER

in a hierarchical fashion. Finally, with switched networks there is a wide range of individual link rates. For ATM, link specifications range from T1 (1.5 Mbit/s) to OC-192 (10 Gbit/s). Therefore, the intrusion detection system must support a variety of sensor types, from sensors implemented in software that examine network events at the edges, to hardware-based sensors that examine network events in the core.

Implementing intrusion detection and high-speed packet filters on public switched networks requires cooperation from the network providers. Intrusion sensors and filters placed at the public-private network boundary can protect an enterprise network from externally-generated attacks. However, to ascertain the source of the attack with certainty requires sensors that are located in the provider's network. Assessment of attacks originating from the provider's network can be performed by the provider, thereby protecting the provider's interest in hiding the details of the public network's design. Yet, agreements must be in place with the provider to allow law enforcement personnel to access the provider's assessment data when investigating a public network attack. To preserve public trust, these agreements must specify clear conditions under which law enforcement can access this data (e.g., court-issued warrant), and the data must be non-forgeable in order to be admissible in court.

This paper describes a technical approach for implementing intrusion detection functions in public and private switched networks. This approach allows a variety of network sensors to report to a hierarchy of assessment entities that are configured to determine whether a sequence of sensor events indicates an attack, or preparations for an attack. Operational issues are also discussed, including the use of intrusion sensors in public networks for law enforcement purposes, and the issues associated with high-speed filtering, filter configuration, and data protection.

2. SWITCHED NETWORK INTRUSION DETECTION ARCHITECTURE

Switched networks present unique problems for intrusion detection because they use point-to-point physical connections between switches and end systems to deliver information packets directly to the destination, as shown in Figure 2. This is in contrast to networks using broadcast media, where the information packets are broadcast to everyone on that portion of the network, and only the intended recipient copies them off the network and responds (Figure 3). Broadcast media are more conducive to network intrusion detection because the intrusion detection device can be located on a segment and passively "sniff" traffic involving all hosts on the subnet to look for attack signatures. In Figure 3, sensor S1 operates on the uplink to the remainder of the network. Sensors S2 and S3 monitor all traffic broadcast on their respective legs of the network.

However, with switched networks (such as ATM), link sensors have fewer logical connections per physical circuit from which to gather data. This requires distributing sensors throughout the network (i.e., links, switches, and end systems), rather than only on links carrying traffic broadcast to many end systems. In Figure 2, sensor S1 operates on the link from this subnet to the remainder of the network. Sensors S2, S3, S4, and S7 monitor links between switches. Sensors S5, S6, and S8 monitor links between switches and particular end systems, that for one reason or another (location/accessibility, information type, user, etc.) require monitoring. As shown by these figures, sensor placement is more complex in switched networks.

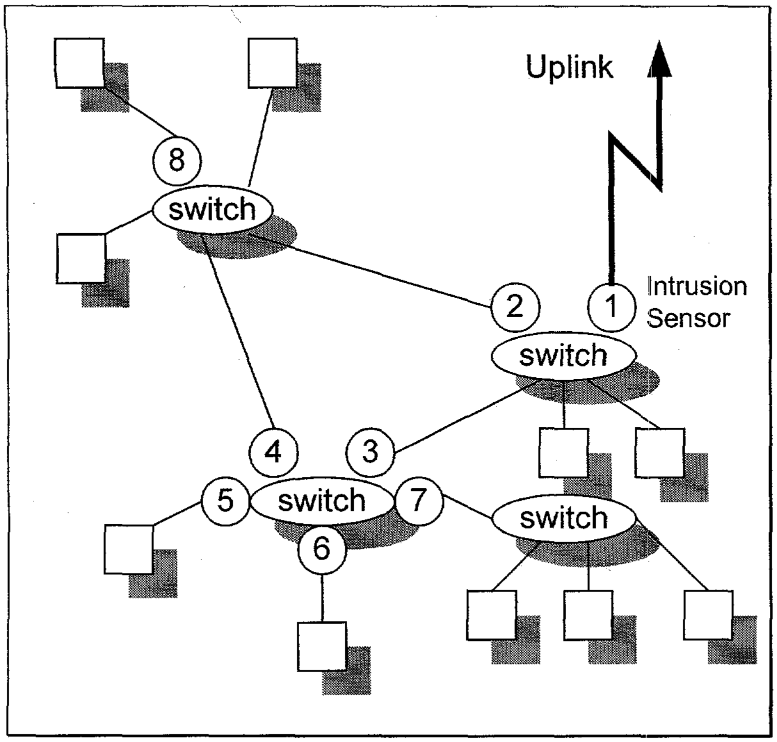

Figure 2: Switched network, with intrusion detection

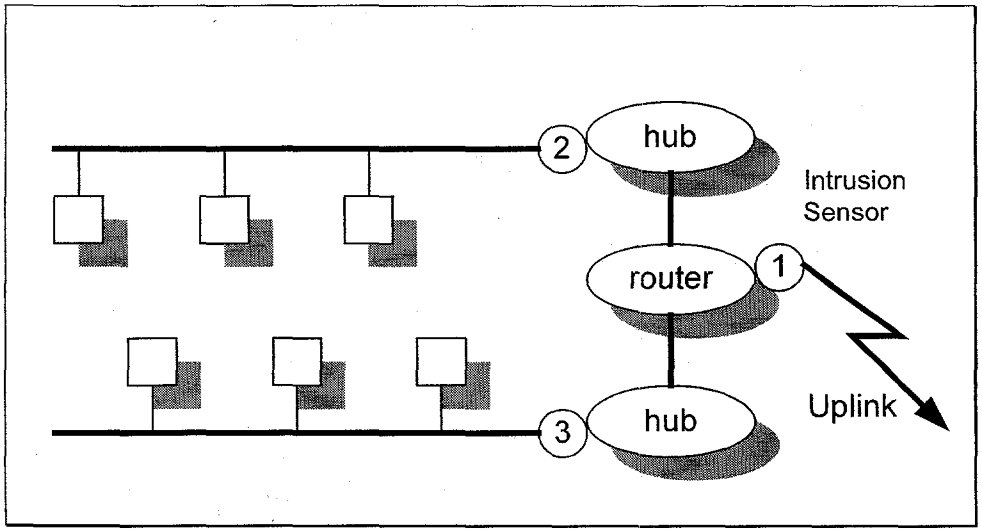

Figure 3: Broadcast network, with intrusion sensors

An architecture for performing intrusion detection in Asynchronous Transfer Mode (ATM) switched networks is shown in Figure 4. There are three main types of components in this network intrusion detection system – sensors, intrusion assessment, and intrusion response. The sensors detect network events such as new connections and new nodes. These events are sent to one or more assessment units, which correlate and evaluate the findings of the sensors, log various items, and initiate responses. Finally, there are response agents to carry out some action based on the evaluation of what was detected. There may also be a user interface component for monitoring and maintenance of the network intrusion detection system. The way these components are arranged is the architecture of the network intrusion detection system. In the remainder of this paper, the authors will describe an intrusion detection system for Asynchronous Transfer Mode networks. Although designed for ATM networks, the information and design considerations also apply to other switched networking technologies.

In the prototype ATM Network Intrusion Detection System developed at Sandia National Laboratories, the components are generally arranged as shown by the solid lines in Figure 4.

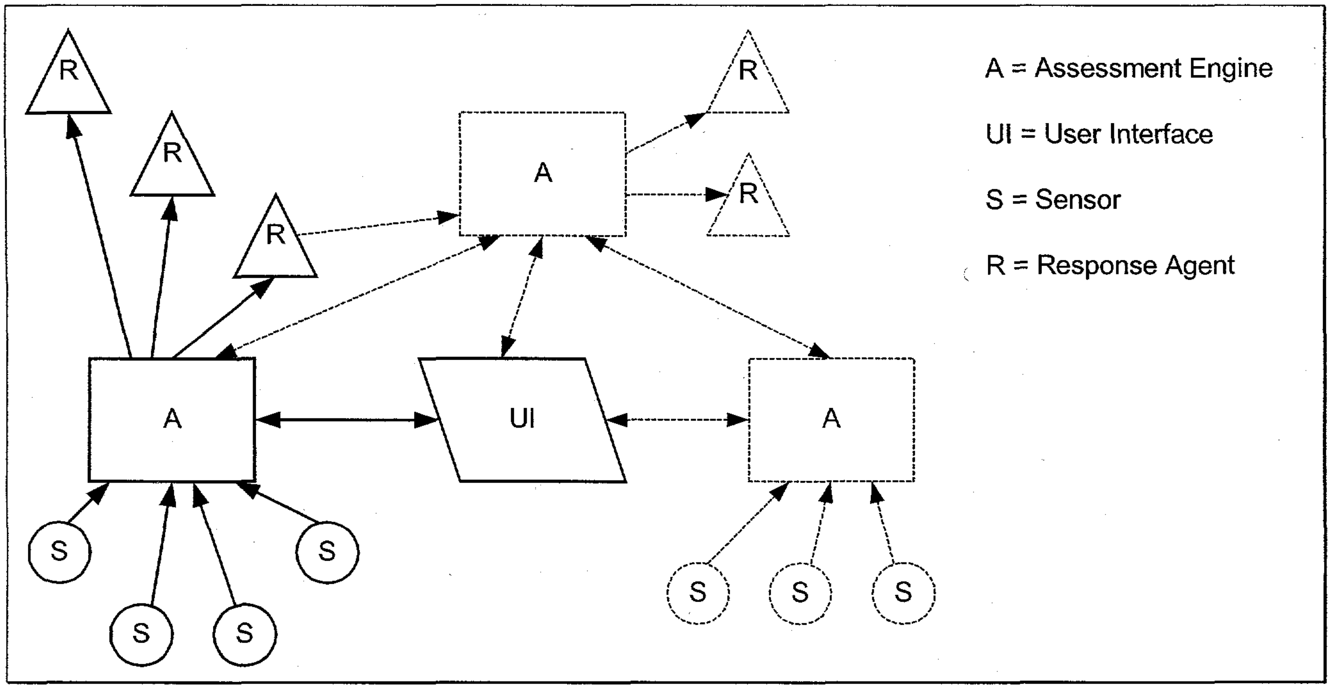

Figure 4: ATM network intrusion detection system architecture

The sensors within the network (similar to those shown in Figure 2) report to an assessment engine. The dotted lines and boxes in Figure 4 represent future scalability, including a hierarchy of assessment engines. The assessment engines initiate responses after evaluation of events from one or more sensors. In most situations, responses may reconfigure the network to harden it against an active attack. When hierarchical assessment is used in large networks, an assessment engine's response (output) may also provide sensor-like notifications to another assessment engine above it in the hierarchy.

3. SENSORS

Sensors detect information, anomalies, and events within an ATM network and report them to an assessment engine. Software-based sensors typically reside on the network edges and directly or indirectly examine network events or information. Hardware-based sensors are placed in the network core on high-speed links between switches and/or nodes. Initially these will be implemented with programmable logic devices (PLDs), although they could be cast into Application Specific Integrated Circuits at a later time, as conditions merit.

For the ATM Network Intrusion Detection System described herein, the sensors were designed with specific capabilities in mind.

1.) The sensors should be lightweight (meaning relatively dumb), detecting a specific condition and possibly performing a filtering function.
2.) The sensors should communicate with an assessment engine via a common protocol, although future capabilities may necessitate sensor-to-sensor communications.
3.) Sensors can be implemented in software or hardware, as appropriate.
4.) Sensors should be developed to extract information from User to Network Interface[5] (UNI) and Private Network to Network Interface[6] (PNNI) messages as appropriate.

The last consideration is significant in that the sensors need to examine network signaling information. Therefore, the sensor must implement a portion the protocol that it is watching. In order to keep the sensor implementation lightweight, the portion of the protocol that it implements must be carefully selected.

3.1 Software-based sensors

Initially, sensors for the ATM intrusion detection system were developed in software. This allowed the developers to quickly get a proof-of-concept system up and running, and allowed for experimentation with a variety of sensor types. However, software sensors are appropriate in production use, particularly in the edges of networks, where performance is not a premium, but their low cost makes them more amenable than hardware-based sensors for widespread distribution at the edge.

Two types of software-based sensors were developed and evaluated: *direct* sensors that can monitor ATM protocol exchanges and *indirect* SNMP-based sensors that monitor network devices and report device status changes. Both types of sensors use the same protocol for reporting potential intrusion events to an assessment engine. Although the use of a common protocol places some additional burden on the sensors (which may prefer their native protocols), it simplifies the implementation of the assessment engine where processing speed is precious.

3.1.1 Direct sensors

Direct sensors monitor ATM protocol messages, either as an *active* ATM node in the network (i.e., switch or end system), or as a *passive* device tapping a link using a splitter. An example of an *active direct* sensor is the PNNI sensor. This sensor implements a PNNI node, and participates in the PNNI routing protocol as if it were a switch. This allows the sensor to establish links to switches and monitor protocol traffic to detect various PNNI events, including new switches joining the network, elections of peer group leaders, and distribution of topology databases. When events occur, the event type and any supporting information (such as switch identifiers) are reported out-of-band to the assessment engine using a special reporting protocol. By reporting events using an out-of-band channel (e.g, a TCP/IP connection over Ethernet), attacks occurring on the monitored network cannot affect the reporting of attack events.

In contrast, a *passive direct* sensor is a sensor that also monitors ATM protocol traffic, but does not participate in protocol exchanges. The UNI sensor is an example of a passive direct sensor. This sensor attaches to an active UNI using a fiber-optic splitter to "tap" UNI signaling exchanges between an end system and a switch. These protocol exchanges are monitored for UNI events such as connection establishments and terminations. As with the active direct sensors, passive direct sensors report the type of event along with supporting information to an assessment engine via an out-of-band channel.

The passive direct sensor is the simplest sensor, as it does not require an entire protocol implementation to be present. Rather, it only requires a subset of the protocol decode functions to be present. Therefore, the passive direct model is the best model for high-speed implementation in hardware.

3.1.2 Indirect, SNMP-based

Indirect sensors do not monitor ATM protocol messages. Rather, they monitor ATM network devices (e.g., switches, network interfaces, etc.) for significant events that may result from protocol interactions or a low-level attack. In the proof-of-concept system, these sensors are implemented using the Simple Network Management Protocol (SNMP). SNMP trap messages, which are unsolicited notifications of network or device events, are sent to a translator which interprets the trap messages and queries the device for additional information. If the event is sufficiently noteworthy, the translator sends an event notification along with any required supporting information to the assessment engine over an out-of-band channel via the same reporting protocol that is used by the direct sensors.

3.2 Hardware-based sensors

The hardware-based sensors, patterned after the software-based passive direct sensors described above, are currently under development. Some of them will need to perform at line rates (initially 155 Mbps or 2.488 Gbps) to perform content monitoring, while others will only need to operate at signaling rates, which are a fraction of the line rates. All the sensors, whether operating at line or signaling rates, need to be scalable to higher speeds as the communication rates of switched networks increase.

However, the implementation of high-speed sensors presents some difficulties. When operating on a trunk, the sensor will likely monitor a very large number of flows simultaneously. This requires the sensor to maintain a large context lookup table to maintain state for each flow. In addition, reassembly of IP packets and/or ATM cells requires state storage, high speed lookup, storage, and copying, which will likely present implementation challenges. Finally, filtering and pattern matching functions must be performed efficiently and quickly. All of these functions (as well as other not listed here) must be performed before the next packet or cell arrival, otherwise, information (evidence) will be lost.

The platforms selected for hardware sensor development use the Altera 10K100 programmable logic device from the FLEX 10K device family and the Altera 20K400 PLD from the APEX 20K device family. The platforms support OC-3 (155 Mbps) and/or OC-48 (2.488 Gbps) communications through fiber optic interfaces.

These sensors will be placed between several switches or between switches and user nodes to examine signaling and routing messages for anomalies. When the hardware detects the specified condition, it will generate and transmit a message to another system. This message may go directly to an assessment system, or it may go to a node, specifically hosting a number of hardware sensors, to be processed, reformatted, and sent on to an assessment system.

These hardware sensors are essentially high-speed packet filters. They accept data packets, typically from an interface that has performed the optical-electrical conversion, and perform simple pattern matching against a sequence of bits stored in flip-flops or other memory devices. When a match is detected, various actions are taken. These could include raising a signal to an external interface or capturing a copy of certain information, such as the Virtual Path Identifier/Virtual Channel Identifier (VPI/VCI) for transmission to the assessment engine.

4. PUBLIC AND PRIVATE NETWORK OPERATIONS

For private networks, operational layer 2 intrusion detection requires the local site to specify filter criteria for the sensors, and attack rules for the assessment engine(s). These filter criteria and attack rules can be determined via in-house vulnerability research and/or through a commercial or public clearinghouse of attacks (akin to BugTraq). Sensors are placed at key points in the private network, such as at the connection to the public network service provider, core backbone switches, and/or at key servers, and loaded with the filtering specifications by a system administrator. Sensor events can be reported to a single assessment engine (configured by the system administrator with the appropriate attack rules) for coordinated monitoring of attacks originating either within or outside the organization. Attacks that are detected are logged and off-line responses may be generated according to site policy. Examples of responses include denial of future accesses, service cut-off, and administrative actions (e.g., reprimand, termination of employment, etc.). Because intrusion sensing, assessment, and response are all provided by a single entity, policy decisions regarding these functions require little or no coordination with others.

However, for public switched networks, administration of systems to detect attacks and abuses becomes much more difficult. Since public switched networks are implemented by more than one service provider, and the details of each provider's network implementation are considered to be proprietary, there is no central authority that is capable of monitoring the entire public network and making configuration changes or performing other responses if an attack is occurring. The provider can perform intrusion monitoring in the public network, but the location of sensors and the scope of assessment must be confined to the provider's network. The lack of coordination provided by the limited scope of intrusion assessment and response reduces the public network's effectiveness if an attack occurs across provider boundaries.

If the required level of coordination is provided by federal law enforcement, then a number of technical and political issues need to be resolved. As described by Blaze and Bellovin[7], in order to prosecute someone for network attacks, *all* evidence must be collected and stored in a manner that prevents tampering or removal. In order to collect all evidence, sensors must be placed in key aggregation points (high-speed links in particular), and must be designed so that they are not overwhelmed by the information they are viewing. These sensors must provide appropriate mechanisms (e.g., cryptographic hash functions with an appropriate key management system) that can ensure that the data that is archived as evidence is the same data that was collected by the sensor.

However, to protect the privacy of individuals who are not under investigation, these sensors must be implemented to selectively filter only those flows that are under investigation. Furthermore, the sensor must implement mechanisms to ensure that filter specs can only be loaded into the sensor when an authorized court order (warrant) has been issued. Again, cryptographic techniques are available to implement this feature.

High-speed filtering of individual layer 2 flows at presents unique challenges to the design of the sensor. Because *all* evidence must be collected, the sensor must process the filter matching very quickly, or else buffer overflows will occur and data will be lost. In addition, most of the useful identifying information may be contained in higher-layer Protocol Data Units (PDUs), and not in the Layer 2 protocol information. Therefore, the sensor must be "application aware", and be able to decode identifying information contained somewhere in the Layer 2 PDU.

Although the hardware sensors described earlier in this paper have not yet been implemented, the considerations described above are driving the requirements. Specifically, the hardware sensors will be designed with high-speed interfaces to connect on trunk lines and will implement a high-speed, multilayer pattern matching algorithm to identify Layer 2, 3, and 7 PDUs while minimizing buffer overflows. Cryptographic techniques will also be designed into the hardware sensors to implement message integrity and control access to the filter specifications. However, the impact of these cryptographic techniques on the processing speed of the filter must be determined.

5. SUMMARY AND FUTURE WORK

Switched private and public networks must be monitored to detect attacks and abuses. However, detection of network intrusions and other malicious activity in switched networks requires a new approach for intrusion detection. The intrusion detection architecture described in this paper uses sensors that are configured with specific filter criteria to report security-significant network events to an assessment engine. The assessment engine matches received events against a set of attack rules, and directs a response agent to harden the network if the assessment engine determines that an attack is underway.

The switched network intrusion detection architecture calls for active direct, passive direct, and indirect sensors for filtering of network protocol flows. These sensors may be implemented in software or hardware, depending on the required processing speed. Software-based sensors are appropriate for wide-spread distribution on low-speed links (e.g., at the network edge), whereas hardware-based sensors are more appropriate for concentration on high-speed trunks (e.g., in the network core).

Intrusion detection in the switched public network will likely use hardware-based intrusion sensors (filters), and require law enforcement access. This raises technical and policy issues associated with authorized specification of filter criteria, capture of all evidence, and preservation of evidence. Cryptographic techniques are available to address some of these issues. However, the impact of cryptography on filter performance is presently not quantified.

The ATM intrusion detection system described in this paper is currently implemented as a proof-of-concept prototype, using software-based sensors. The authors are currently developing hardware-based passive direct sensors to perform high-speed monitoring and filtering of ATM traffic. These sensors will also incorporate some of the features needed for law enforcement applications, including cryptographic mechanisms for filter specification and evidence preservation.

ACKNOWLEDGMENTS

Sandia National Laboratories is a multiprogram laboratory operated by Sandia Corp., a Lockheed Martin Company, for the U.S. Department of Energy under contract DE-AC04-94AL85000.

REFERENCES

1. Tanenbaum, Andrew S., Computer Networks, Prentice-Hall, Englewood Cliffs, New Jersey, 1981.
2. Information Processing Systems – Open Systems Interconnection – Basic Reference Model (ISO 7498), International Organization for Standardization, Geneva, Switzerland, 1984.
3. Pierson, Lyndon G., and Edward L. Witzke, "Data Encryption and the ISO Model for Open Systems Interconnection," ISE '84 Joint Proceedings, Institute of Electrical and Electronics Engineers, New York, 1984.
4. R. Smith, et al., "ATM Peer Group Leader Attack and Mitigation," *Proceedings IEEE MILCOM '99*, pp. 729-733, 1999.
5. ATM Forum Technical Committee, User to Network Signaling Specification Version 4.0, af-sig-0061.000, The ATM Forum, Mountain View, California USA, 1996.

6. ATM Forum Technical Committee, Private Network-Network Interface Version 1.0, af-pnni-0055.000, The ATM Forum, Mountain View, California USA, 1996.
7. M. Blaze and S. Bellovin, “Tapping, Tapping on My Network Door,” Inside Risks 124, *Communications of the ACM*, Vol. 43, No. 10, October, 1996.