

Merit Network, Inc.
CALEA Compliance Test Architecture

OVERVIEW

Merit must respond to the CALEA rulings with a document describing how Merit will comply. The date for the compliance document to be submitted is not yet final, but it is assumed that the date will be sometime in early 2007. Technical/physical compliance with the CALEA rulings is required by May 2007.

This briefing document is a preliminary perspective for discussion on how Merit will *technically* comply with CALEA. Important compliance details to be developed but which are not addressed in this document include methods and procedures for accepting a wiretap request, processing it, timing for action, communication around it and many other topics. These topics will be further clarified in the coming months.

ASSUMPTIONS

At this time, it is assumed that Merit will be required to be “Gateway Compliant.” This means that Merit’s border devices where traffic flows in or out of our network will require modification, and/or new technologies will need to be deployed at these points to assist law enforcement in court-ordered wiretaps. The simplest ‘test’ to identify where the gateways requiring compliance are, is answering the following question affirmatively: “Does traffic leave or enter AS-237 at this point?”

These locations for gateway compliance include those where we purchase commodity Internet services (Equinix and Detroit) but also would include at least eight private peering locations. Merit derives much value from our open peering policy from a performance, cost and cultural perspective. CALEA will not diminish our efforts to establish peering, but will add an additional layer of cost and management.

It is also assumed that Merit does not want to break new ground or lead the industry in this compliance technology. However, we do not want to be led by a vendor community with a costly solution that is imposed. The CALEA environment continues to be vague, particularly in terms of how compliance will be accomplished. Ultimately we believe it will be time and case law that will refine the definition. In the meantime, we intend to have a response to CALEA that we believe is reasonable and cost effective.

TECHNICAL COMPONENTS

Merit is in the process of prototyping and testing an architecture that we feel meets CALEA requirements for gateway compliance. The goal of the prototyping is to determine the hardware and software feasibility of the proposed architecture.

Merit’s potential CALEA compliance architecture is depicted in the attached diagram and described below. The diagram reflects Merit’s 10G core network of routers, some of our

currently deployed 10G switches, and the two new devices described below. These two new devices sit beyond the 10G switches, and have the following functionality:

1. A Dell 2850 computer, which will be deployed at each ingress/egress point on the network to collect traffic only when a wiretap order is received. This device will be connected to the 10G or 1G switches in the network. We refer to this device as the “collector”. Software on this computer will include filters, which will be written by Merit R&D to sort data based on the wiretap order, i.e., to extract traffic from/to a particular IP address from the mirrored data stream. Each collector will have two interfaces. The first interface receives mirrored data from the 10Gig or 1G switch while the second interface is used as a management interface for communicating with the collector. The collected data is stored locally on this collector until the management software issues a transfer request. While the collection task itself is performed by commonly used packet capture software, the goal of the additional management layer that Merit intends to add is to ensure that sufficient logs are maintained regarding the use of the collector which can alert us to potential unauthorized use of this facility.
2. The second new device in the network is also a Dell 2850 which will be used as the management console for the entire set of deployed collectors. We refer to this device as the “controller”. There would likely be one of these devices in the network, not considering spares or backup devices. This device is responsible for issuing collection commands to the Dell collector machine that is collecting the traffic. This controller device will control any traffic collection activity, e.g., specifying the IP address for which to collect data. It is responsible for starting or stopping the collection of data, as well as the transfer of collected data from the collectors to an exit computer from which an LEA can collect the data. This device will take all the collected traffic from all the collectors. All activity initiated by this controller will be logged in a secure way to ensure against possible misuse.

A third device required is the computer that the Law Enforcement Agency (LEA) will use to receive and store the data that Merit sends. Merit believes that this device will be the responsibility of the Law Enforcement Agency to procure and manage, although for end-to-end functionality of the architecture, it is feasible that Merit would prefer to procure and manage it. We refer to this device as the “Law Enforcement Agency (LEA) machine.” For the purposes of our prototyping work, this device is specified as follows although it is understood that the Law Enforcement Agencies may have other plans not yet communicated with us:

A standard COTS workstation or server with at least 0.5 Terabytes of available disk space, using a UNIX based operating system. This device will be implemented with strict firewall policies that only permit secure access from specific LEA hosts, and the Merit controller as described above.

FUNCTIONALITY OF THE ARCHITECTURE

When Merit receives a wiretap order, it is assumed it will be for all traffic on an IP address or a set of IP addresses. Thus Merit will first determine the institutional user of the IP address. If specific port numbers are specified, these will also be in the filters to ensure only the appropriate traffic is collected.

Merit Engineers will then configure the controller to send the appropriate command to *every* collector. In addition, they will ensure that appropriate traffic is mirrored towards the collectors. All collectors must be enabled to collect data because all traffic from and to a particular IP address is collected, and this traffic could come through any of Merit's border devices.

The collectors will run appropriate packet captures to capture traffic for the particular IP address for which the wiretap order was issued, and store this data locally for the duration of the capture. Collected data may be transferred to the controller or the Law Enforcement Agency machine designated to receive it by issuing the appropriate command.

Merit will provide full packet captures of data in standard packet capture (PCAP) format. Any embedded data will not be further processed to generate MP3 or WAV or VoIP format files. Merit views this additional activity as moving into the forensics of the wiretap event, and thus not part of its role. Additionally it should be noted that the proposed architecture cannot provide any historical data prior to the initiation of the collection activity.

STATUS OF PROTOTYPING EFFORT

We have started to build the software tools for the controller and the collector, including the filters, controller commands and management interfaces. We have also verified individual components of the architecture such as the data collection and transfer capability by capturing local test traffic and storing it. The next phase of prototyping will include the following:

- Development of secure login capability;
- Deployment of functional components at test collection points;
- Testing the complete system architecture.

We anticipate this phase of the prototyping to be complete, and a report available by late October.

OTHER

We believe this architecture serves the gateway compliance requirement of CALEA. Traffic staying within Merit Network will not be captured, e.g., traffic between CMU and WMU.

Merit plans to share this architecture description with our peer networks, and work with them as they desire to test and implement. At this juncture, we do not see any revenue potential for our development efforts, and believe that any ROI would be minimal and thus not worth pursuing.

Merit will interview Members and Affiliates in the coming weeks to determine if it is desirable for Merit to be the “trusted third party” for these entities when they receive wiretap orders. This effort would indeed require consulting fee reimbursement from the Member or Affiliate. In addition, a fee structure for this ongoing trusted third-party role would need to be developed.

CALEA ARCHITECTURE PROTOTYPE TEST ENVIRONMENT MERIT NETWORK

