515 E Cleveland, Suite C
Monett, MO 65708

"Vulture" - A Broadband CALEA Solution
Preliminary

April 10, 2007

"Vulture" is a software implementation of the T1.IAS (ATIS-PP-1000013.2007) CALEA standard protocol for broadband data interception. Vulture is designed to run as a command-line utility under the Linux operating system. We will be providing software-only and pre-configured hardware/software packages.

Current Features:

- Runs under Linux - currently CentOS 4.4
- Licensed per-host not per-intercept or per-intercept per-LEA. Pricing is going to be $2995 per host with a 20% per year support/update maintenance fee. The first years maintenance is included in the purchase price. Pricing for pre-configured systems is being developed.
- Extremely simple; a text file is used to configure each intercept and one process runs for each intercept allowing multiple captures to run with different intercept types and/or to different law enforcement agencies.
- Each intercept can capture headers only, full content, or both headers and content.
- Uses libpcap to capture traffic from specified IP address or IP subnet.

Requirements:

- Your network must be able to assign a static IP address to the intercept target.
- You must be able to mirror all traffic or just the intercept target traffic to a span-port Vulture is connected to.

Status and Availability:

- Finishing touches are being put on the utility. Load testing needs to be done to determine guidelines for computer size versus intercept bandwidth/simultaneous captures.
- We are on the FBI's waiting list for interop testing. This is not a certification and is not required to have a standard solution giving "safe harbor".
- We expect to have a deliverable release 1.0 the week of April 30. A release candidate for anyone wanting to test will be available the week of April 23.
- Some of the standards are still evolving, particularly the short-term storage of T1.IAS in pcap format for LE to collect via SFTP and/or HTTPS and may or may not be fully standardized by the May deadline. We expect that there will be several releases of the software short-term.

Future Additions:

- Radius and DHCP support - intercept target will still need to have a static IP but this will allow CmII messages for access attempts, rejects, etc.
- Possible support for Cisco SII to allow intercept directly from Cisco routers.

What it doesn't (and probably never will) do:

- T1.678 or J-STD-025-B voice intercepts. This handles voice captures and is done by the Metaswitch directly. It is strictly to comply with the broadband data requirement.

Configuration Sample:

```
caseid = "FBI-1234";
iapsystemid = "MTI 123";
interface = "eth1";
subjectip = "10.100.0.11";
subjectmask = "/32";
subjectiptype = "static";# static, radius, dhcp -- only static supported
subjectaccessmethod = "dsl"; # dsl, dialup, lan, cable, wifi, wimax, other
subjectidentity = "someusername"; # username, e-mail address, etc.
startdate = "2007-04-07 19:30:15";
enddate = "2007-05-07 19:30:15";
deliverymode = "realtime"; # realtime, store
intercept = "headers";  # headers, content, headers+content
cmiiaddress = "udp:10.0.0.1:1000"; # udp:ipaddress, tcp:ipaddress, file:path
cmccaddress = "udp:10.0.0.1:1001"; # udp:ipaddress, tcp:ipaddress, file:path
```

Contact Info:

Kevin Wormington
Missouri Telecom, Inc.
417-489-0860
kworm@missouri-telecom.com

Note: Vulture is a tentative name and is subject to change.