Exploiting Lawful Intercept to Wiretap the Internet

Blackhat DC, 2010

Tom Cross

Manager, X-Force Research

The “Great Debate”

How should the information infrastructure of the future balance the individual’s desire for privacy with the state’s interest in monitoring suspected criminals?

IETF Policy on Wiretapping (RFC 2804)

The IETF will not consider requirements for wiretapping in protocol designs

- The IETF is an international body and can't address the laws of every country
- The Internet should be free from security loopholes
  - Adding a requirement for wiretapping makes protocols more complex
    - Complexity begets vulnerability
  - The interfaces that provide wiretap access could be used with authorization
- Wiretapping the Internet is either easy or its impossible
  - RFC 1984 – Development of the Internet requires wide availability of strong cryptographic technology
- "On the other hand," wiretapping technologies should be openly described
  - "The IETF believes that the publication of such mechanisms, and the publication of known weaknesses in such mechanisms, is a Good Thing."
  - In keeping with this philosophy, Cisco and the IETF published RFC 3924 – The Cisco Architecture for Lawful Intercept in IP networks

Communications Assistance for Law Enforcement Act

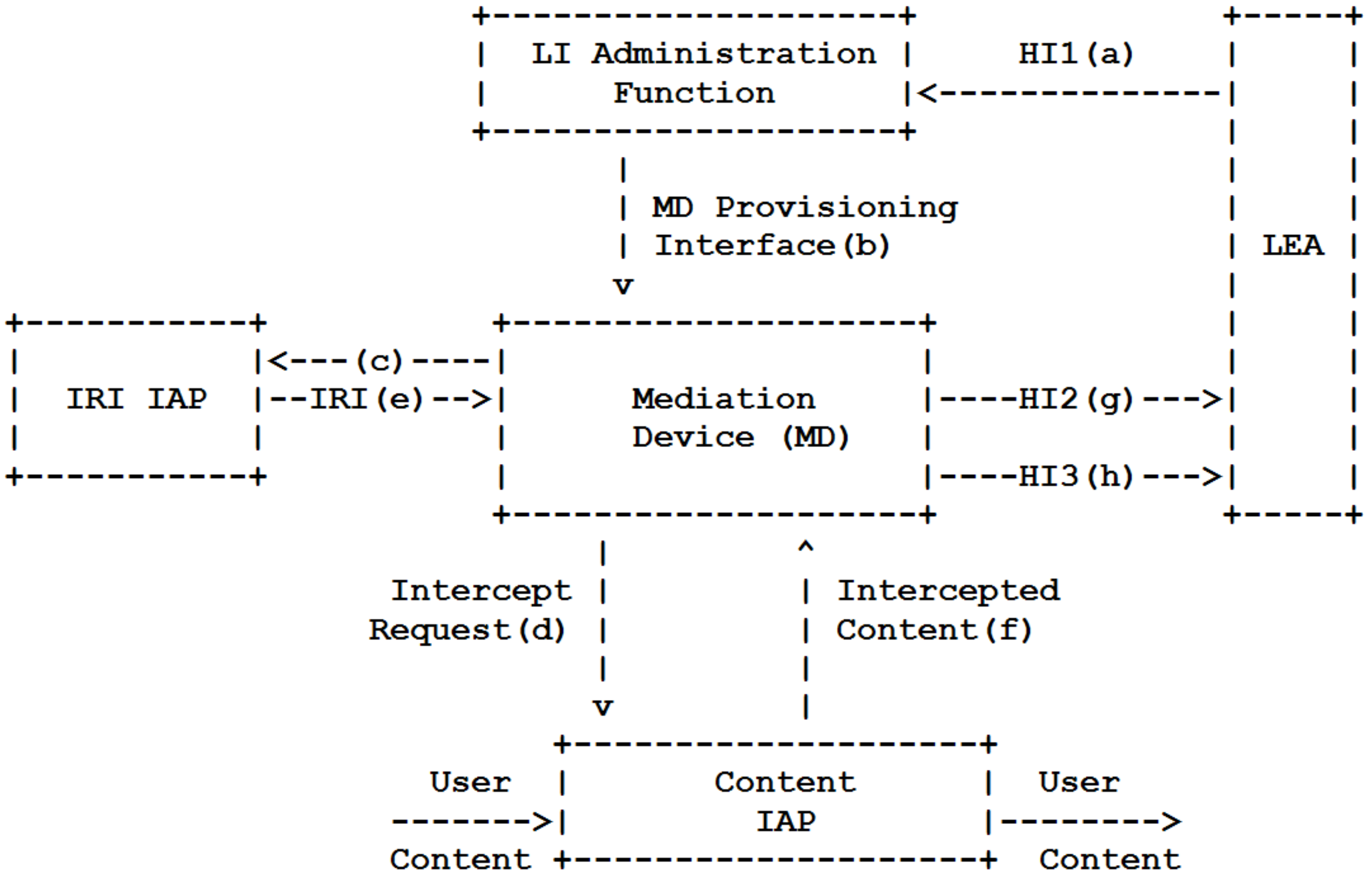
- Communications Assistance for Law Enforcement Act
  - Passed in 1994
  - Requires Telecommunications Companies to cooperate with the interception of traffic on their networks by providing technical interfaces for that purpose
  - Originally did not apply to "Information Services."

- In 2005 the FCC ruled that CALEA applies to broadband Internet providers
  - The Cisco Architecture for Lawful Intercept pre-dated this ruling
  - By 2005 Some European countries already required these interfaces for Internet networks
  - Providers may voluntarily create these interfaces even when not required to
    - The provider is going to have to grant access to the communications somehow
    - A well defined interface makes wiretapping less disruptive to network operations

The Cisco Architecture for Lawful Intercept

- The Cisco Architecture for Lawful Intercept in IP networks
  - Based on the Lawful Intercept architecture defined by the European Telecommunications Standards Institute (ETSI)
  - An SNMPv3 interface that provides the ability to wiretap IP networks
  - Described in RFC 3924 and some Internet Drafts
  - Publish in 2003/2004
  - Implemented in edge router and switch models
    - 7600/10000/12000/AS5000
  - A myriad of other companies support the same overall architecture for Lawful Intercept
  - Different vendors may supply a service provider with various interoperable components of the overall architecture for lawful intercept

The Cisco Architecture for Lawful Intercept: RFC 3924

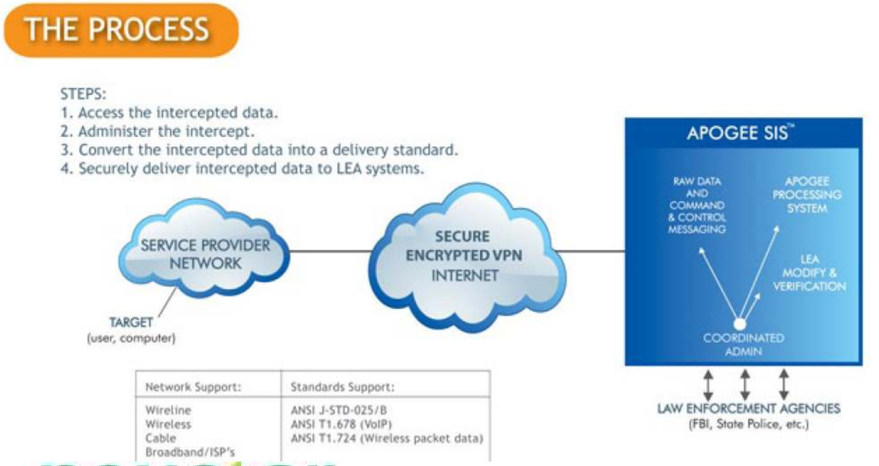


```
                       +--------------------+               +-----+
                       |  LI Administration |     HI1(a)    |     |
                       |      Function      |<--------------|     |
                       +--------------------+               |     |
                              |                             |     |
                              | MD Provisioning             |     |
                              | Interface(b)                | LEA |
                              v                             |     |
+-----------+           +--------------------+              |     |
|           |<---(c)----|                    |              |     |
|  IRI IAP  |--IRI(e)-->|      Mediation     |----HI2(g)--->|     |
|           |           |      Device  (MD)  |              |     |
+-----------+           |                    |----HI3(h)--->|     |
                        +--------------------+              +-----+
                             |         ^
                   Intercept |         | Intercepted
                  Request(d) |         | Content(f)
                             |         |
                             v         |
                           +--------------------+
                     User  |       Content      |  User
                   ------->|         IAP        |-------->
                   Content +--------------------+  Content
```

Figure 1: Intercept Architecture

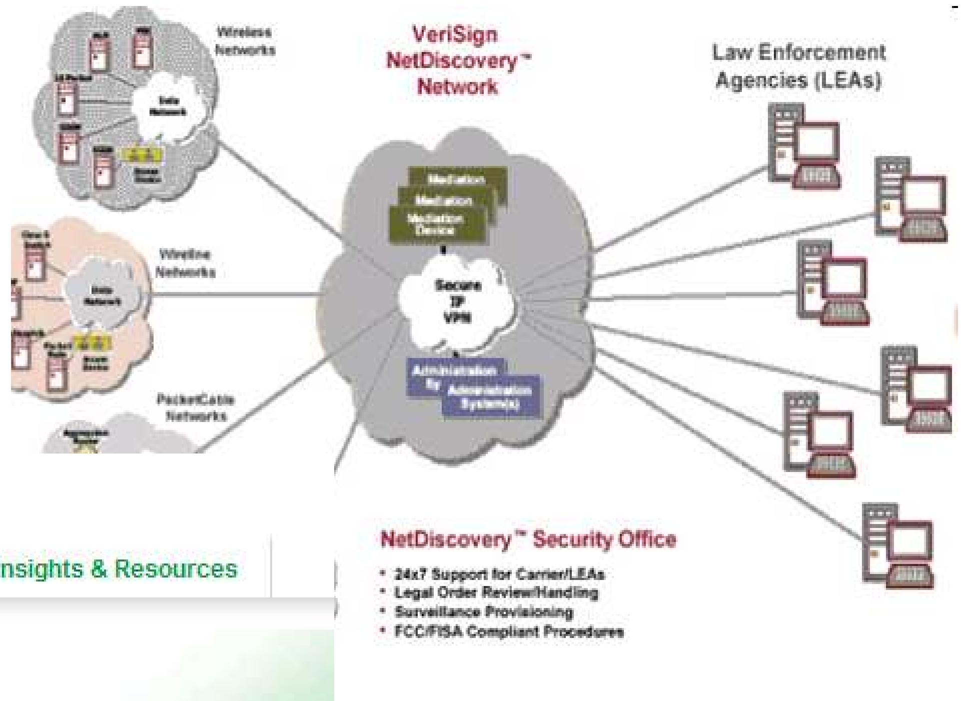
Source: RFC 3924

Lawful Intercept Administration Service Providers



STEPS:
1. Access the intercepted data.
2. Administer the intercept.
3. Convert the intercepted data into a delivery standard.
4. Securely deliver intercepted data to LEA systems.

Network Support:	Standards Support:
Wireline Wireless Cable Broadband/ISP's	ANSI J-STD-025/B ANSI T1.678 (VoIP) ANSI T1.724 (Wireless packet data)



NetDiscovery™ Security Office
- 24x7 Support for Carrier/LEAs
- Legal Order Review/Handling
- Surveillance Provisioning
- FCC/FISA Compliant Procedures

Legal Compliance Services

- Overview

Court-Ordered Records Production

LEAP

Risk Management

Technical Assistance in Lawful Interception of Communications

Why risk non-complia legal liability

Mitigate the impact of CALEA compl systems and process quickly. Just C

Legal Compliance Services (CALEA)

Solutions

CALEA Compliance Services

Looking for a comprehensive, cost effective CALEA service?

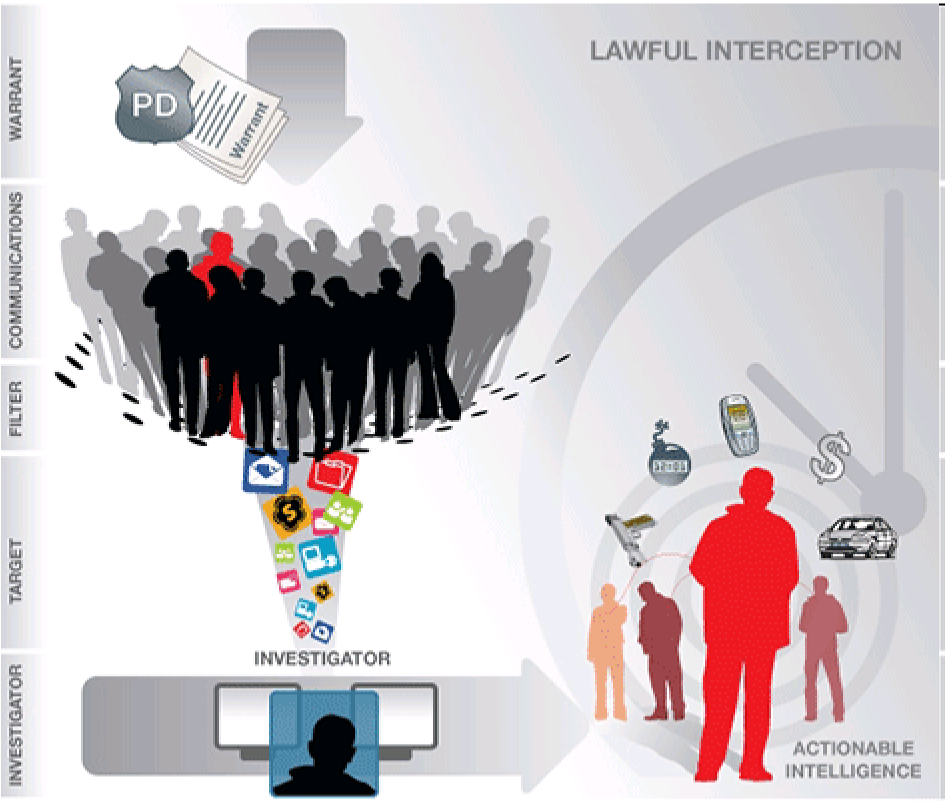
If you are, you've come to the right place! Welcome to BearHill's CALEA compliance center. This portion of our web presence is

Mediation Device Vendors

(many also make Intercept Access Points (IAPs))

Mediation device equipment suppliers include:

- Aqsacom
- ETI
- Group 2000
- Pine Digital Security
- Verint
- SS8
- SUNTECH Intelligent Solutions
- Utimaco
- Accuris
- ATIS systems
- DigiVox
- GTEN AG
- NICE Systems
- Teletron
- Urmet Group



(Verint marketing material)

The Interception Request

```
CTapStreamIpEntry ::= SEQUENCE {
  cTapStreamIpIndex Integer32,
  cTapStreamIpInterface Integer32,
  cTapStreamIpAddrType InetAddressType,
  cTapStreamIpDestinationAddress InetAddress,
  cTapStreamIpDestinationLength InetAddressPrefixLength,
  cTapStreamIpSourceAddress InetAddress,
  cTapStreamIpSourceLength InetAddressPrefixLength,
  cTapStreamIpTosByte Integer32,
  cTapStreamIpTosByteMask Integer32,
  cTapStreamIpFlowId Integer32,
  cTapStreamIpProtocol Integer32,
  cTapStreamIpDestL4PortMin InetPortNumber,
  cTapStreamIpDestL4PortMax InetPortNumber,
  cTapStreamIpSourceL4PortMin InetPortNumber,
  cTapStreamIpSourceL4PortMax InetPortNumber,
  cTapStreamIpInterceptEnable TruthValue,
  cTapStreamIpInterceptedPackets Counter32,
  cTapStreamIpInterceptDrops Counter32,
  cTapStreamIpStatus RowStatus }
```

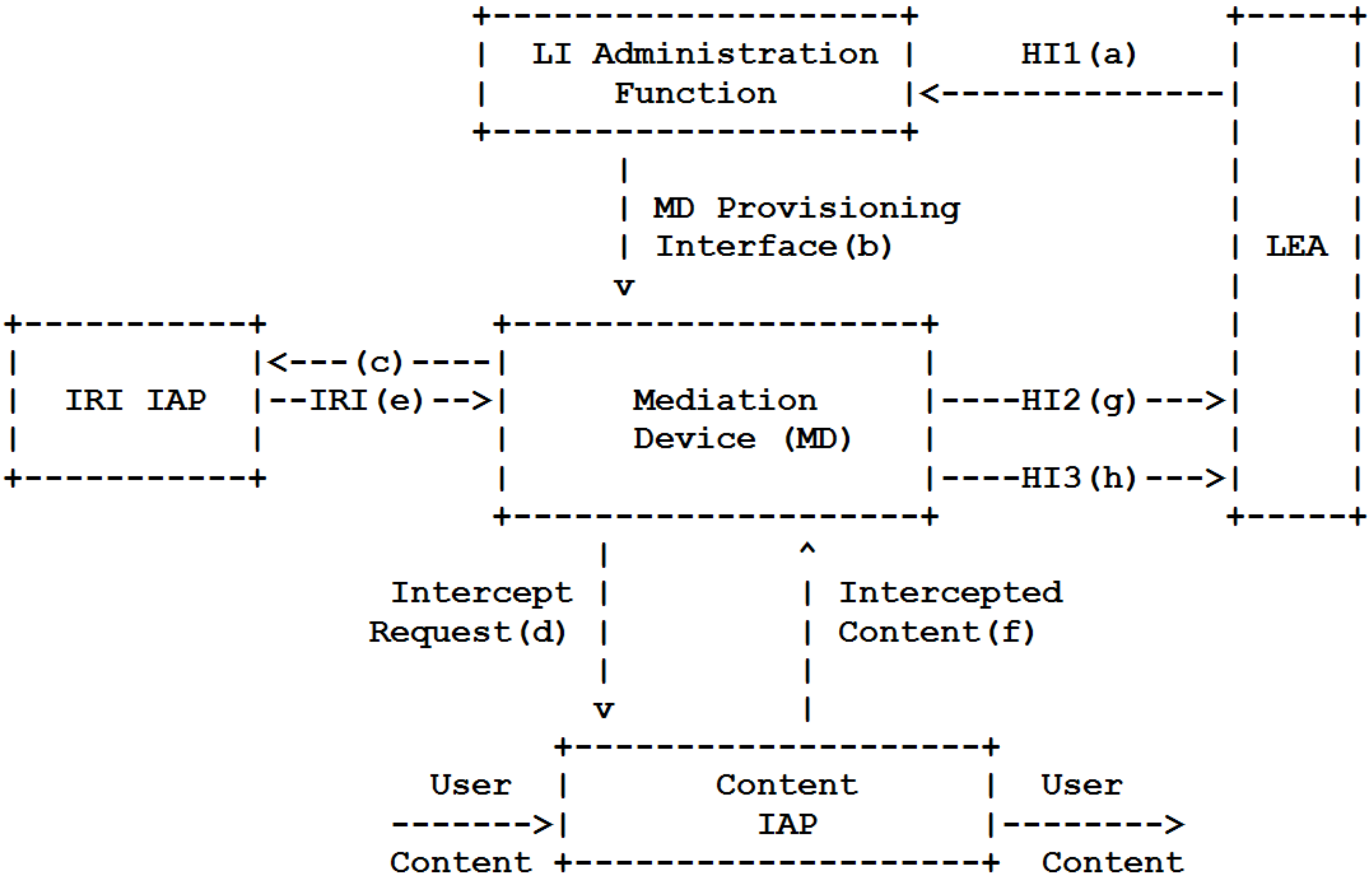
The Interception Request

```
CTapMediationEntry ::= SEQUENCE {
  cTapMediationContentId Integer32,
  cTapMediationDestAddressType InetAddressType,
  cTapMediationDestAddress InetAddress,
  cTapMediationDestPort InetPortNumber,
  cTapMediationSrcInterface InterfaceIndexOrZero,
  cTapMediationRtcpPort InetPortNumber,
  cTapMediationDscp Dscp,
  cTapMediationDataType Integer32,
  cTapMediationRetransmitType Integer32,
  cTapMediationTimeout DateAndTime,
  cTapMediationTransport INTEGER,
  cTapMediationNotificationEnable TruthValue,
  cTapMediationStatus RowStatus }
```

Security Concerns for Lawful Intercept

- Preventing the subject from discovering the surveillance
- Preventing the subject from manipulating the surveillance
  - Transmitting information that was not collected
  - Inducing the collection of information that was not transmitted
  - The Eavesdropper's Dilemma: What do you do with packets that have the wrong checksum?
- Protecting the interface from unauthorized use
  - Preventing the provisioning of unauthorized wiretaps
  - Preventing an authorized wiretap from collecting information outside the scope of the authorization

Where should minimization happen? IAP, MD, or LEA?

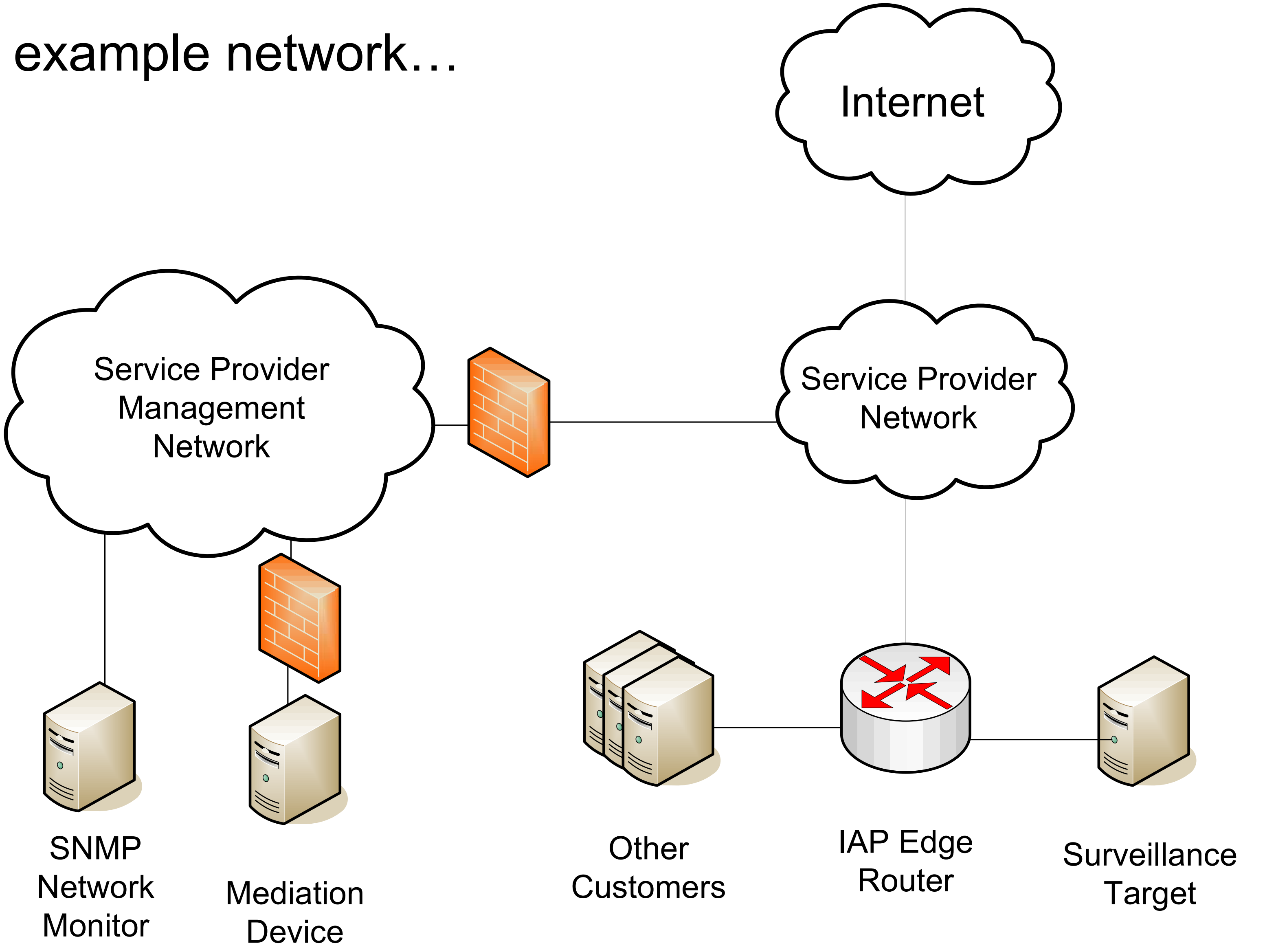


```
                       +--------------------+               +-----+
                       |  LI Administration |     HI1(a)    |     |
                       |      Function      |<--------------|     |
                       +--------------------+               |     |
                              |                             |     |
                              | MD Provisioning             |     |
                              | Interface(b)                | LEA |
                              v                             |     |
+-----------+           +--------------------+              |     |
|           |<---(c)----|                    |              |     |
|  IRI IAP  |--IRI(e)-->|      Mediation     |----HI2(g)--->|     |
|           |           |      Device (MD)   |              |     |
+-----------+           |                    |----HI3(h)--->|     |
                        +--------------------+              +-----+
                             |          ^
                   Intercept |          | Intercepted
                  Request(d) |          | Content(f)
                             |          |
                             v          |
                           +--------------------+
                     User  |       Content      |  User
                   ------->|         IAP        |-------->
                   Content +--------------------+  Content
```

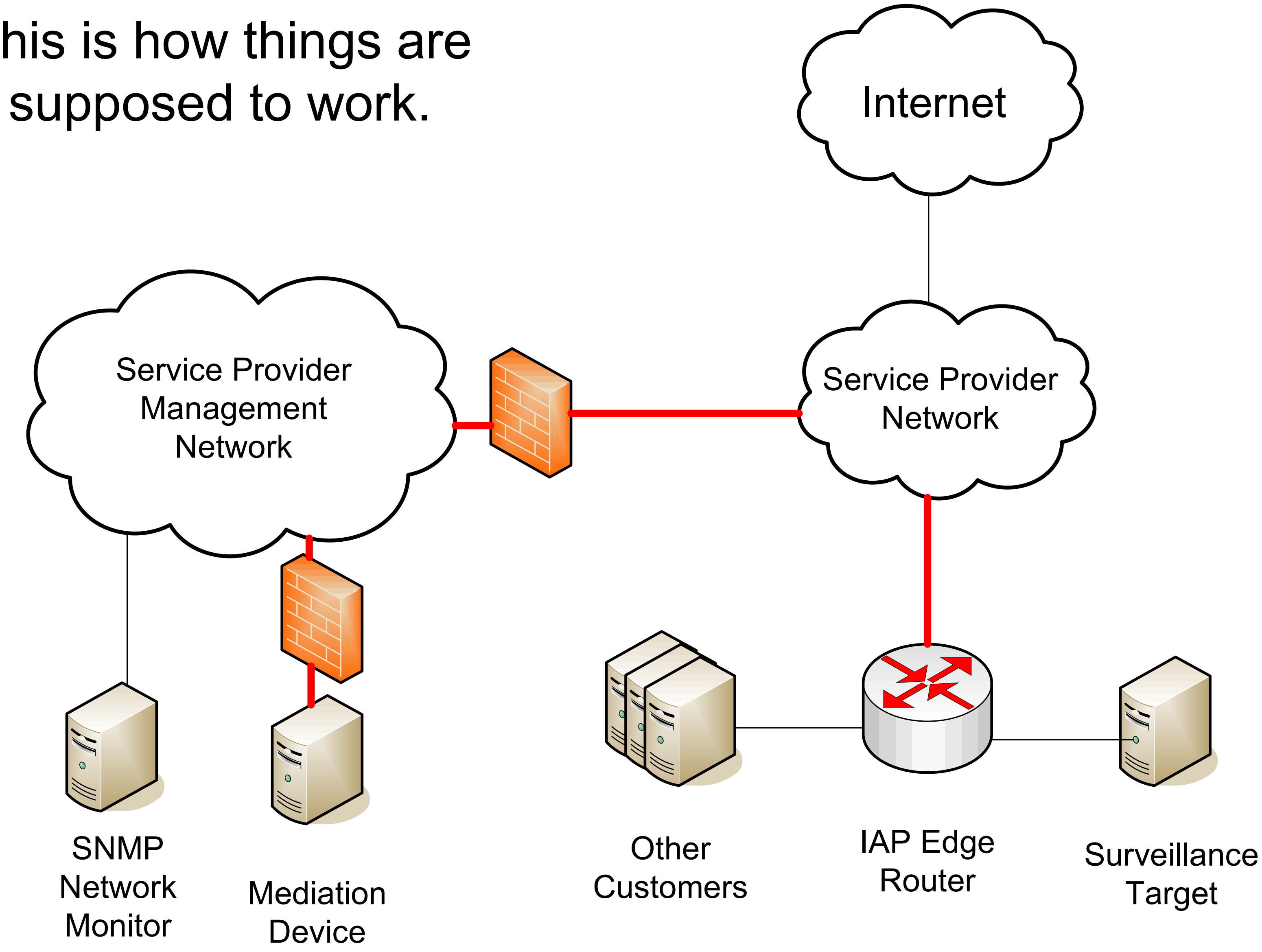
Figure 1: Intercept Architecture

Source: RFC 3924
Copyright (C) The Internet Society (2004).

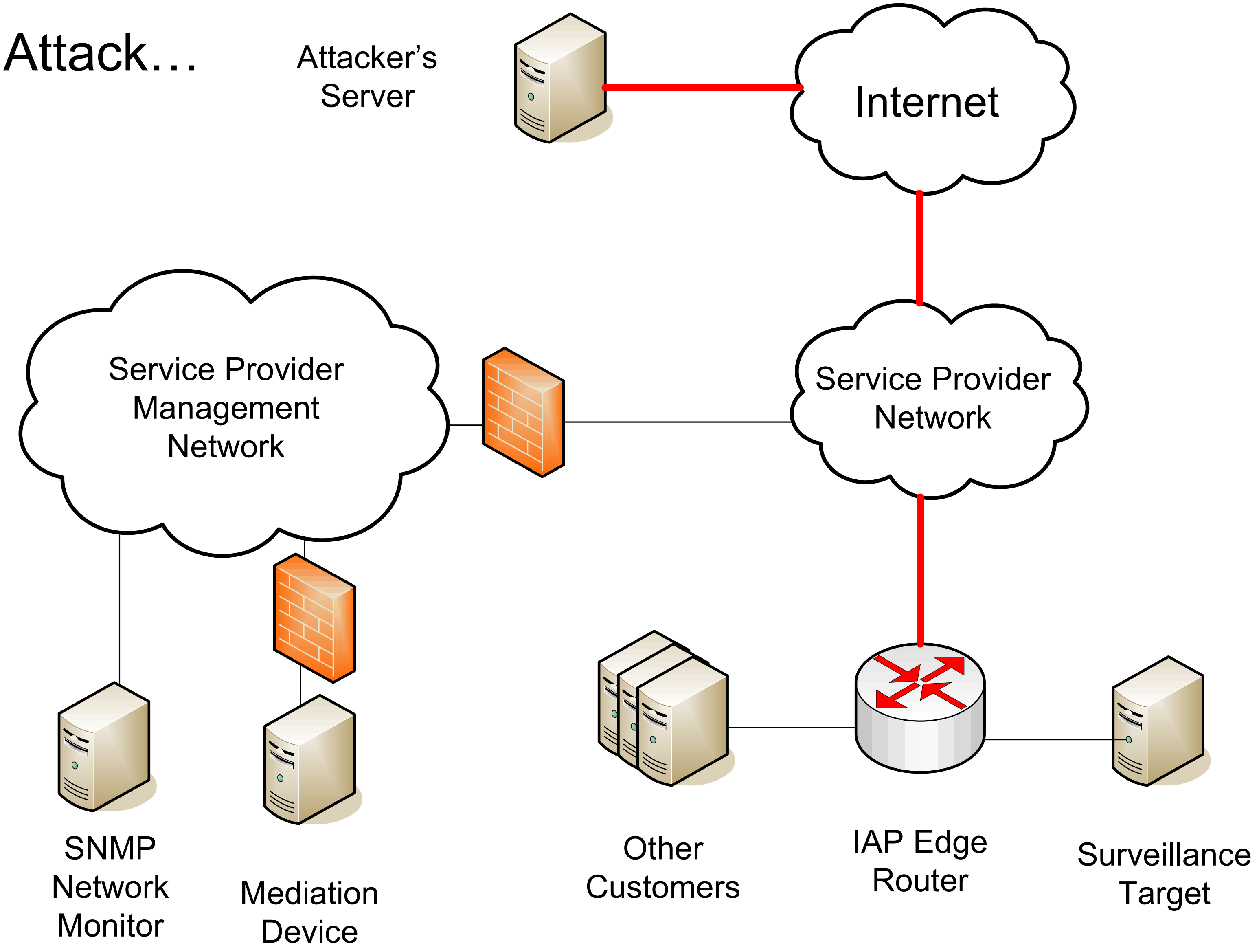
An example network…



This is how things are supposed to work.



An Attack…


Attacker's
Server
Internet
Service Provider
Management
Network
Service Provider
Network
SNMP
Network
Monitor
Mediation
Device
Other
Customers
IAP Edge
Router
Surveillance
Target

Unauthorized Interception Requests

- Single, properly authenticated SNMPv3 packet accessing the TAP-MIB
  - Attacker would need to be able to send a packet that the interface will receive.
    - Packet filtering might interfere with this.
  - Attacker would need the correct SNMPv3 EngineID, EngineBoots, and EngineTime values
    - These values are intended to prevent authenticated SNMPv3 messages from being replayed
    - They can be obtained with a single unauthenticated transaction
    - They can be shared between clients
  - The correct username and password are required
    - In some cases the password is not necessary (CVE-2008-0960)
  - Collected traffic can be sent anywhere on the Internet over any service
    - IP Access Control Lists (ACLs) do not filter outbound traffic from Cisco routers

Vulnerabilities

1. The Susceptibility of SNMPv3 to Brute Force Credential Discovery

2. The Password Implementation Vulnerability in SNMPv3

3. The Lack of Audit Trails

4. The Flexibility of the Output Stream

5. The Susceptibility of the Interface to Packet Spoofing

6. The Lack of a Requirement for Encryption

Brute Forcing SNMPv3 Usernames and Passwords

```
usmMIBBasicGroup OBJECT-GROUP OBJECTS {
  usmStatsUnsupportedSecLevels,
  usmStatsNotInTimeWindows,
  usmStatsUnknownUserNames,
  usmStatsUnknownEngineIDs,
  usmStatsWrongDigests,
  usmStatsDecryptionErrors,
  usmUserSpinLock,
  usmUserSecurityName,
  usmUserCloneFrom,
  usmUserAuthProtocol,
  usmUserAuthKeyChange,
  usmUserOwnAuthKeyChange,
  usmUserPrivProtocol,
  usmUserPrivKeyChange,
  usmUserOwnPrivKeyChange,
  usmUserPublic,
  usmUserStorageType,
  usmUserStatus }
```

CVE-2008-0960 - Why Brute Force?

- SNMPv3 Message Digests are the first 12 bytes of a cryptographic hash of the message contents combined with a secret key, which is a combination of the password and the EngineID of the SNMP service
- The RFC says message digests that aren't 12 bytes long should be thrown out but many implementations didn't.
- The result of the local HMAC calculation is going to be greater than 12 bytes, so many implementations performed this comparison operation:

```
memcmp( myHMACbuffer, packetHMACbuffer, packetHMAClength )
```

- Attacker can send 256 messages with different 1-byte HMACs and one will be accepted.

CVE-2008-0960

- Disclosed in June, 2008
- Multiple Vendors impacted (Linux, Solaris, OSX, Juniper, and Cisco)
- Some implementations were vulnerable for over 6 years
- **Most Cisco software that supports Lawful Intercept was not vulnerable**
  - IOS 12.3(7)XI before 12.3(7)XI8a
  - 12.3(7)XI supports lawful intercept in 10000 Series Routers
- Cisco 10000 series routers
  - Edge router for broadband service providers
  - Supports IP “VPNs”

Lack of Audit Trails

- Attacks on SNMPv3 authentication are noisy – it would be nice if you could monitor those attacks using traps!
- Cisco’s Configuration Guide for Lawful Intercept advises network administrators to enable SNMP trap notifications
- Cisco’s documentation implies that traps will be sent “for packets with an incorrect SHA/MD5 authentication key or for a packet that is outside the authoritative SNMP engine's window (for example, outside configured access lists or time ranges).”
- No IOS version I tested sent authentication failure traps for SNMPv3 messages with the wrong username, password, or Engine values.
  - Authentication failure traps were generated for SNMPv3 requests if they came from a source IP address that was blocked by a group access list.
  - Cisco determined that this behavior is as intended.
  - CSCsz29235: The documentation for 'snmp-server enable traps snmp' command stated that SNMPv3 authentication failure traps can be generated, which is incorrect. The documentation has been updated to indicate that SNMPv3 authentication failure traps are not generated.

TAP-MIB – The attacker can turn the audit trail off!

```
CTapMediationEntry ::= SEQUENCE {
  cTapMediationContentId Integer32,
  cTapMediationDestAddressType InetAddressType,
  cTapMediationDestAddress InetAddress,
  cTapMediationDestPort InetPortNumber,
  cTapMediationSrcInterface InterfaceIndexOrZero,
  cTapMediationRtcpPort InetPortNumber,
  cTapMediationDscp Dscp,
  cTapMediationDataType Integer32,
  cTapMediationRetransmitType Integer32,
  cTapMediationTimeout DateAndTime,
  cTapMediationTransport INTEGER,
  cTapMediationNotificationEnable TruthValue,
  cTapMediationStatus RowStatus }

cTapMediationNotificationEnable OBJECT-TYPE
        SYNTAX     TruthValue
        MAX-ACCESS read-create
        STATUS     current
        DESCRIPTION
        "This variable controls the generation of any notifications or
           informs by the MIB agent for this table entry."
        DEFVAL { true }
        ::= { cTapMediationEntry 12 }
```

TAP-MIB – Flexibility of the Output Stream

```
CTapMediationEntry ::= SEQUENCE {
   cTapMediationContentId Integer32,
   cTapMediationDestAddressType InetAddressType,
   cTapMediationDestAddress InetAddress,
   cTapMediationDestPort InetPortNumber,
   cTapMediationSrcInterface InterfaceIndexOrZero,
   cTapMediationRtcpPort InetPortNumber,
   cTapMediationDscp Dscp,
   cTapMediationDataType Integer32,
   cTapMediationRetransmitType Integer32,
   cTapMediationTimeout DateAndTime,
   cTapMediationTransport INTEGER,
   cTapMediationNotificationEnable TruthValue,
   cTapMediationStatus RowStatus }

cTapMediationTransport OBJECT-TYPE
        SYNTAX     INTEGER {
                              udp(1),
                              rtpNack(2),
                              tcp(3),
                              sctp(4)
                   }
        MAX-ACCESS read-create
        STATUS     current
        DESCRIPTION
           "The protocol used in transferring intercepted data to the
           Mediation Device. The following protocols may be supported:
                      udp:     PacketCable udp format
                      rtpNack: RTP with Nack resilience
                      tcp:     TCP with head of line blocking
                      sctp:    SCTP with head of line blocking "
        ::= { cTapMediationEntry 11 }
```

Packet Spoofing

- The Interception Request is a single UDP packet

- Many Service Providers use SNMPv3 “Infrastructure” Access Control Lists
  - This makes requesting the SNMPv3 “Engine” values difficult
  - Otherwise obtaining the “Engine” values is impractical but not impossible

- SNMPv3 User-Group Access Control Lists
  - Can be used to lock access to Lawful Intercept down to the IP address of the Mediation Device
  - Still susceptible to spoofing
  - Ultimately useful when coupled with encryption

Encryption

- “Although encryption is not necessarily a requirement, it is highly recommended…”

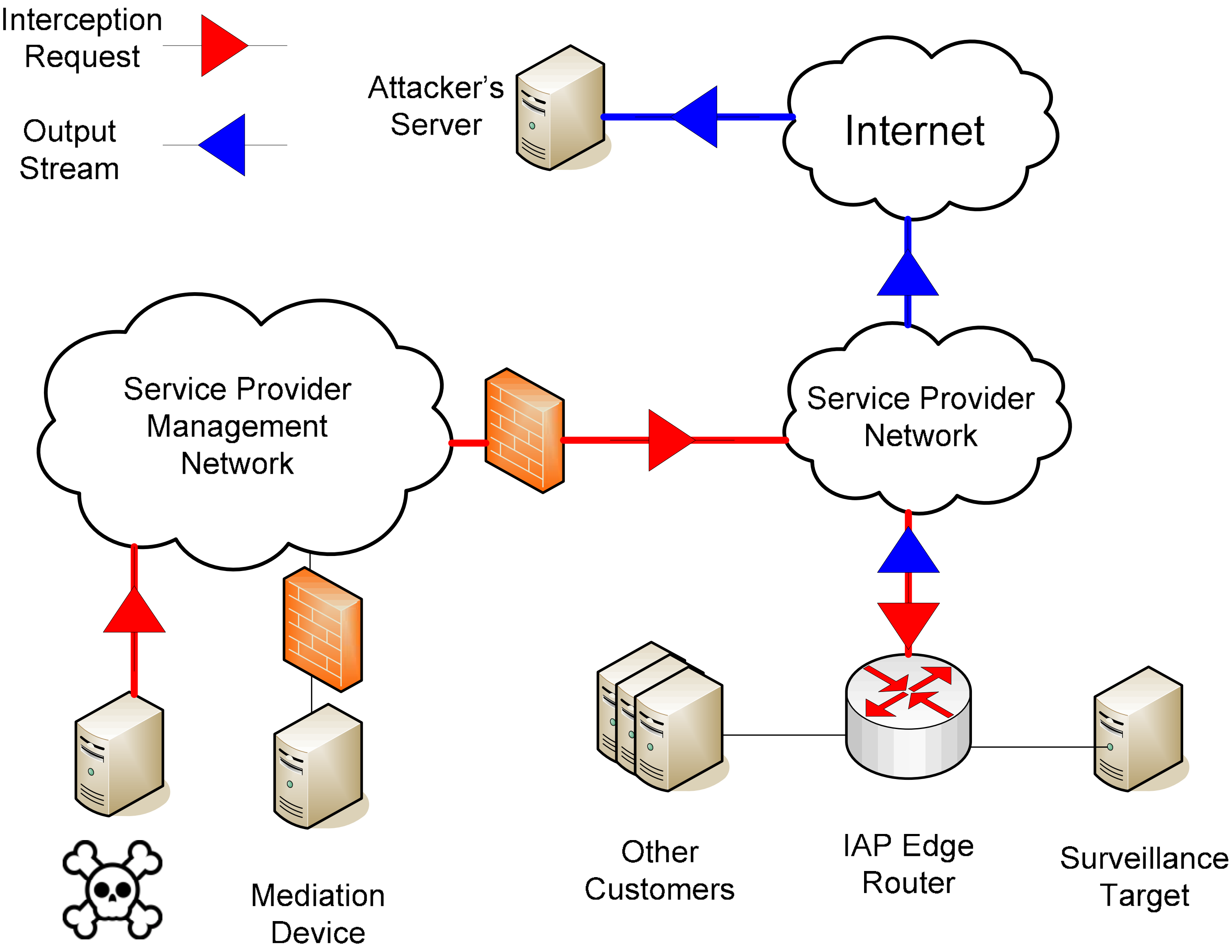
- SNMPv3 Encryption
  - Protects you from CVE-2008-0960
  - Insider attacks are a risk (spoofing, no audit trail, output stream goes anywhere)

- IP Sec ESP
  - Mentioned in the Internet Draft for the TAP-MIB
  - The only way to encrypt the output stream
  - Only effective if coupled with a User-Group access control list

How practical is this attack?

- What I think service providers are doing:
  - Most service providers are using SNMPv3 “Infrastructure” IP Access Control Lists
  - Some service providers were vulnerable to CVE-2008-0960
  - Many service providers are not using encryption
  - Few service providers are using SNMPv3 User-Group IP Access Control Lists

- What that means:
  - SNMPv3 “Engine” values are impractical to obtain from source addresses that are not in the “Infrastructure” Access Control List
  - Attacks from addresses on that list are practical in many real world deployments
  - The problem is particularly bad when coupled with CVE-2008-0960


Interception Request
Output Stream
Attacker's Server
Internet
Service Provider Management Network
Service Provider Network
Mediation Device
Other Customers
IAP Edge Router
Surveillance Target

Have Lawful Intercept technologies been attacked before?

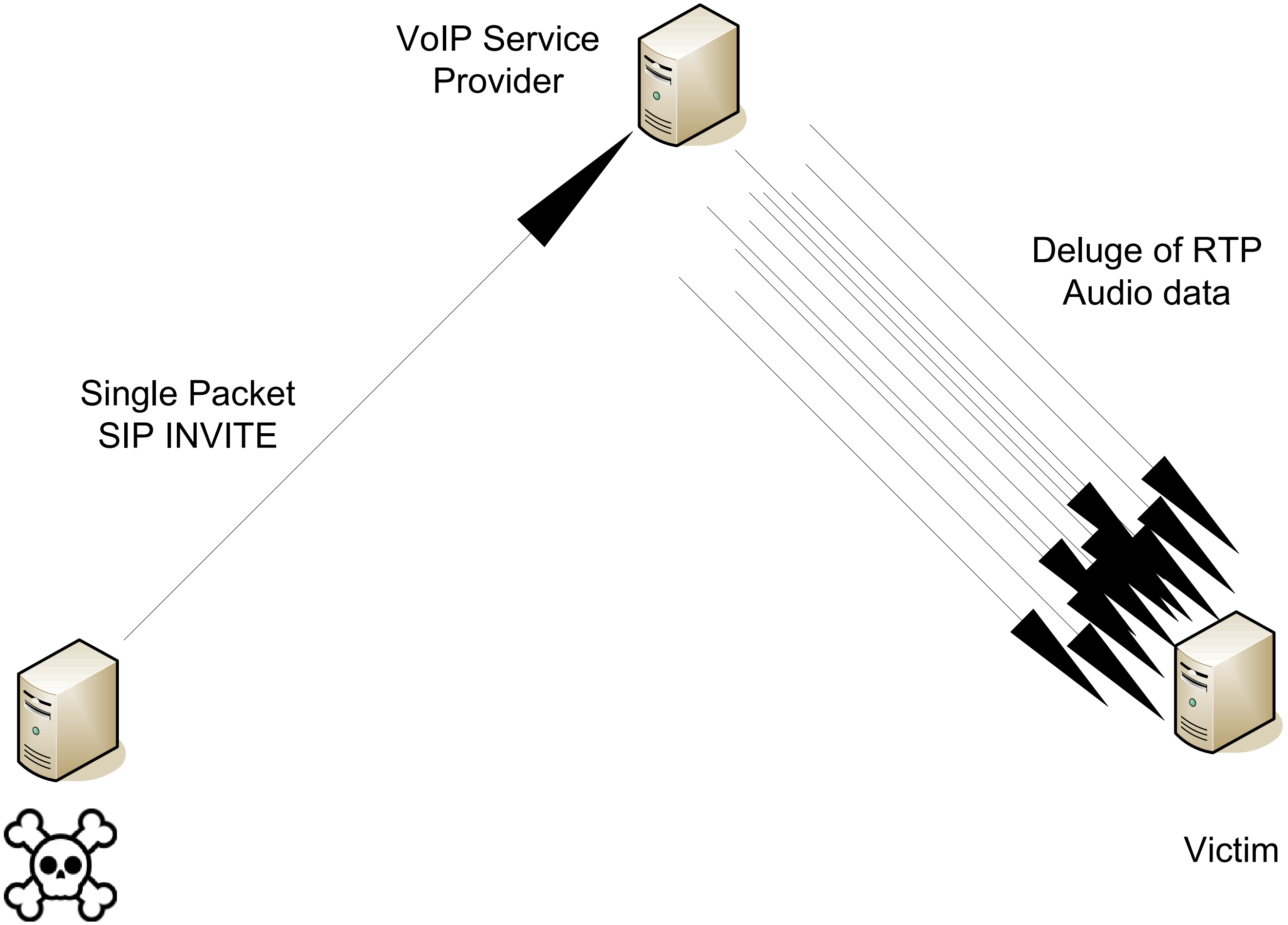
- The “Athens Affair”
  - Described in IEEE Spectrum Article – July 2007
  - Occurred in 2004/2005
  - Malware was installed on Ericsson cellular telephone switches
    - Used “rootkit” like techniques to hide from switch operators
    - Was discovered by Ericsson staff while auditing a core dump to isolate a bug
  - Malware used Lawful Intercept code in the phone switch
    - According to the IEEE article, the interface for managing intercepts was separate from the software that actually performed the intercepts
    - The logs were kept in the management interface
    - The separation of audit trails from the core functionality is a fundamental architectural flaw in a lot of Lawful Intercept technology
  - Cellphones of Greek government officials were monitored
    - At least 100 subjects
    - Included the Greek Prime Minister
  - So we’re clear, no Cisco equipment was involved in this incident

Where should these vulnerabilities be addressed?

- There are three areas where changes could be made to help make this attack on Lawful Intercept more difficult
  - Changes to the User-based Security Model for SNMPv3 (RFC 3414)
  - Changes to the Cisco Architecture for Lawful Intercept
  - Correct Deployment of Lawful Intercept

- If the vulnerabilities can be addressed through careful deployment, why bother changing the protocol specification or implementation?

A digression about SIP



A digression about SIP

- Unauthenticated SIP INVITE requests are single UDP packets – easily spoofed
- An INVITE request can cause a large stream of RTP traffic to be directed to an arbitrary destination address and port
- This situation can be abused to launch traffic amplification denial of service attacks
- If INVITE requests were harder to spoof, it would be easier for victims to convince SIP operators or their service providers to filter out the source addresses causing abuse
- The SIP authentication process creates an interactive transaction that can prevent spoofing of INVITE requests
  - The SIP RFC advises operators to create an “anonymous” account with a blank password
  - Operators rarely do this in practice – preferring single packet anonymous transactions
  - SIP systems are the conduit for traffic amplification not the victim
- Changes to the SIP protocol that solved the INVITE spoofing problem at a lower level than the configuration of a SIP server, such as in the design or implementation, would have a “trickle down” effect, making deployments on the Internet more likely to be secure across the board.

Negative Externalities

- It is the natural economic interest of protocol designers to provide implementers with maximum flexibility
- It is the natural economic interest of protocol implementers to provide users with maximum flexibility
- Sometimes an economic relationship between two parties has an unintended negative impact on a third party – this is called a negative externality
- An infrastructural security risk generated by a protocol is such an externality
- Protocol designers can address negative externalities in their designs by steering implementers and users toward secure deployment

Recommendations for the User-based Security Model for SNMPv3

- Make authentication errors less helpful to an attacker

- Make Engine Values more difficult to predict and share
  - SYN-Cookies cannot be guessed and they are tied to a source address
  - This will cut down on packet spoofing in SNMPv3

- Send traps or informs when authentication failures occur

Recommendations for Lawful Intercept

- Use a different port
  - Make it easier to filter
  - SNMP over TCP would help prevent spoofing

- Allow the router administrator to limit the addresses for the output stream

- Move notification control into the router configuration
  - Network Administrators should not be able to use notifications to monitor surveillance, nor should they be able to direct copies of the output stream to unauthorized destination addresses they control
  - Verifying notification and output stream address agreement between the router configuration and the interception request would prevent abuse by either party

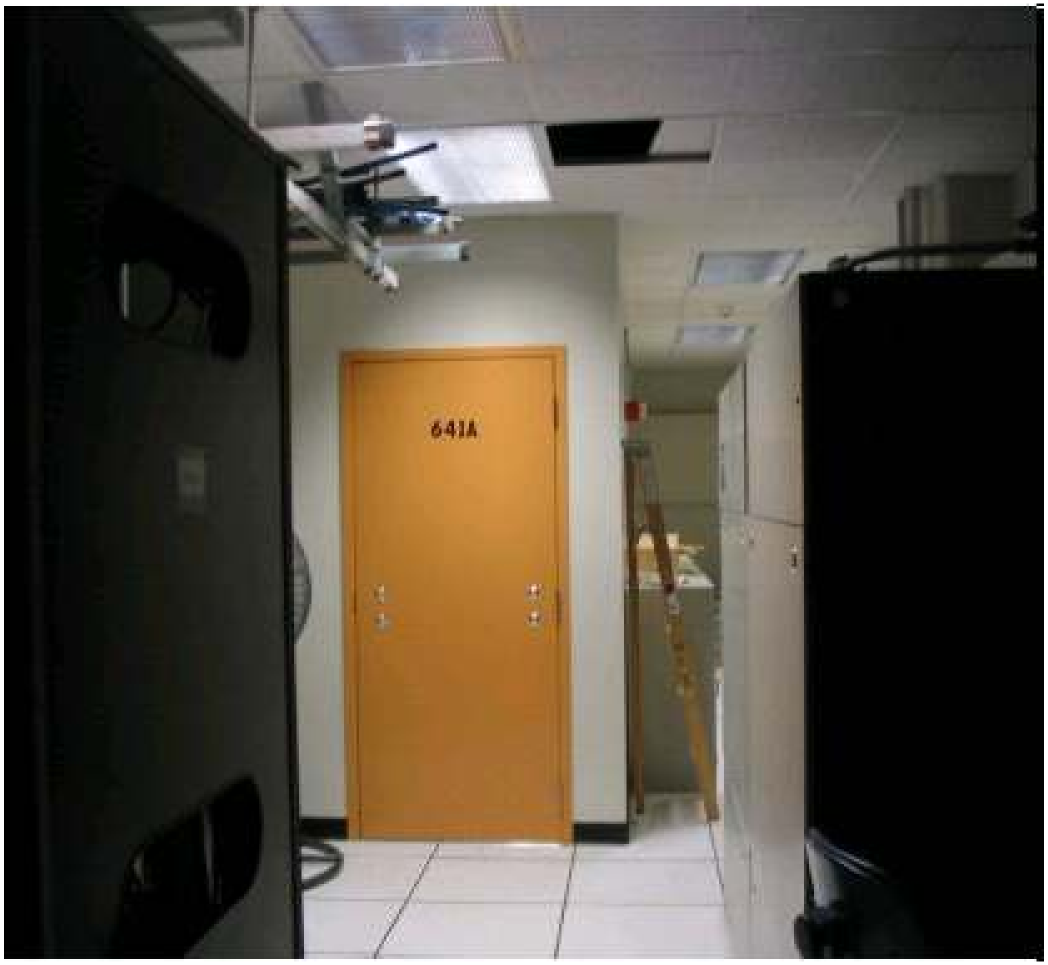
Recommendations for Proper Deployment

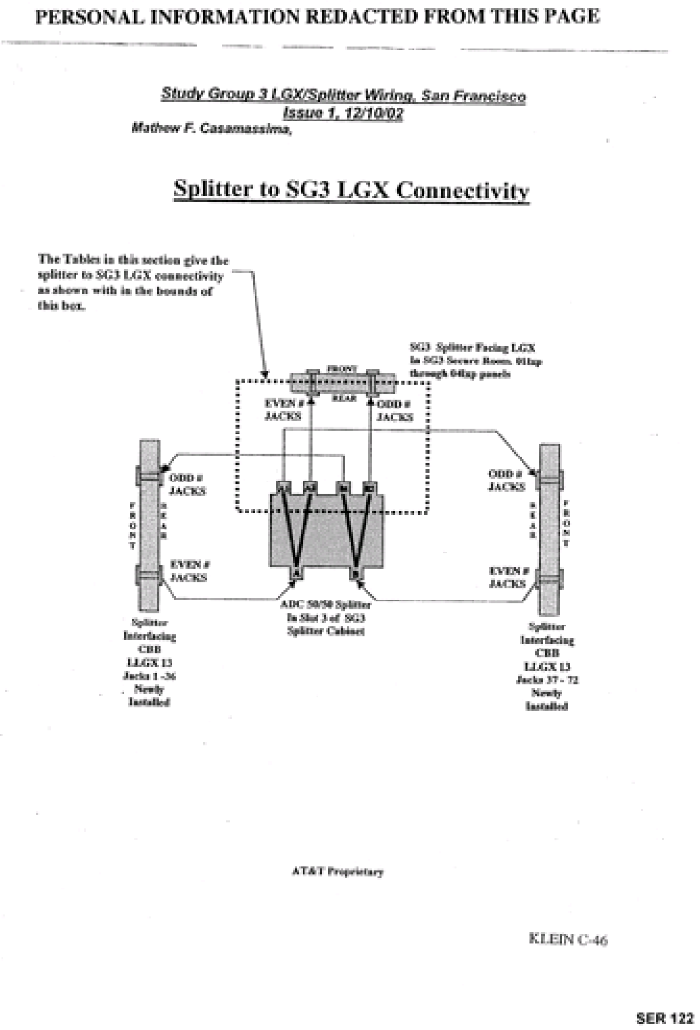
- Make sure you've patched CVE-2008-0960!
- Use Encryption – specifically IP Sec
- Use a User-Group IP Access Control List to lock the Lawful Intercept user to the IP address of the Mediation Device
- Review your overall approach to protecting network infrastructure, the mediation device, and network management systems from attack
- If possible, build out of band management networks

Peer Review Matters

- Cisco did the right thing by publishing their architecture for Lawful Intercept
- Lawful Intercept is a matter of public interest
  - It is helpful if people can see and understand how surveillance is performed
  - The way that these systems perform minimization and prevent unauthorized use is a part of the checks and balances that ensure that the surveillance being performed is legally appropriate
- Technical peer review of Lawful Intercept architectures helps ensure that they are secure
- There are many architectures and vendor solutions for Lawful Intercept that have not been described in similar public documentation and have not been subjected to peer review
- We have no reason to suspect that technology we cannot review is appropriately designed – every deployed technology has security vulnerabilities

For example: The Klein Declaration





PERSONAL INFORMATION REDACTED FROM THIS PAGE

Study Group 3 LGX/Splitter Wiring, San Francisco
Issue 1, 12/10/02
Mathew F. Casamassima,

Splitter to SG3 LGX Connectivity

The Tables in this section give the splitter to SG3 LGX connectivity as shown with in the bounds of this box.
SG3 Splitter Facing LGX In SG3 Secure Room. 01lap through 04lap panels
FRONT
REAR
EVEN # JACKS
ODD # JACKS
ODD # JACKS
FRONT
REAR
EVEN # JACKS
ODD # JACKS
REAR
FRONT
EVEN # JACKS
ADC 50/50 Splitter In Slot 3 of SG3 Splitter Cabinet
Splitter Interfacing CBB LLGX 13 Jacks 1 -36 Newly Installed
Splitter Interfacing CBB LLGX 13 Jacks 37 - 72 Newly Installed

AT&T Proprietary

KLEIN C-46

SER 122

The Klein Declaration

- In 2006 Mark Klein filed a declaration in an EFF lawsuit over warrantless wiretapping
- The Klein Declaration provides a technical description of a telecommunications monitoring system alleged to be operated by the National Security Agency
- The technical architectures are different:
  - The Klein Declaration describes the use of a fiber-optic splitter to send the entire content of backbone links to a special monitoring room for analysis
  - The Cisco Architecture for Lawful Intercept only collects the specific traffic flows requested by the LEA
    - This allows the LEA to only collect information authorized by a warrant
    - The Cisco Architecture is not a secret
    - In these respects, the Cisco Architecture may protect personal privacy better

Some personal thoughts on the “Great Debate”

- Illegal wiretapping used to be really easy
  - Telco junction boxes were easy to access
  - Frequency scanners could monitor wireless phones

- Illegal wiretapping has been getting harder
  - Wireless systems have incorporated link layer encryption
  - Tapping wired infrastructure increasingly requires expensive protocol analyzers
  - Software defined radios might make some of this cheap again in the future

- Wiretapping is therefore neither easy nor impossible
  - People aren’t broadly adopting end-to-end encryption solutions, preferring point-to-point application layer or link layer encryption that is “baked in” and seamless
  - Improving link layer encryption in wired and wireless systems will reduce illegal wiretapping
  - Law Enforcement has resisted link layer encryption where it interferes with surveillance (think GSM)

Some personal opinions (not convictions):

- Wiretapping can either be performed with temporary or permanent devices
  - Temporary devices can be installed “out doors” where no audit trail exists
  - Permanent infrastructure can take one of two forms:
    - “Klein Declaration” style systems, where minimization is performed by Law Enforcement/Intelligence
    - ETSI style systems, where minimization is performed by service providers

- The value of the service provider access control provided by ETSI style wiretapping infrastructure may be worth the risk of the sort of unauthorized access described in this talk
  - This view runs against the grain of the consensus view of security researchers
  - You cannot effectively control the use of portable protocol analyzers, but permanent infrastructure must have some kind of access control
  - That access control may improve security if it is effective:
    - We know that verification of warrants or other legal authority is taking place
    - The architecture is open to the public for peer review
    - Other avenues of access can be closed off
  - The verification of legal authority needs to be <u>credible</u>

Thank You!

Any Questions?

tcross@us.ibm.com

http://xforce.iss.net