Lawful Interception based on Sniffers in Next Generation Networks

Andres Rojas & Philip Branch
Centre for Advanced Internet Architectures,
Swinburne University of Technology

Outline

- Lawful Interception (LI) - what is it?
- A Sniffer based LI system today
- AAA, RADIUS, DIAMETER
- Future Networks
- Possible Solutions
- Conclusion
- Questions

Outline

- Lawful Interception (LI) - what is it?
- A Sniffer based LI system today
- AAA, RADIUS, DIAMETER
- Future Networks
- Possible Solutions
- Conclusion
- Questions

SWIN BUR NE CENTRE FOR ADVANCED INTERNET ARCHITECTURES

Lawful Interception (LI)

- In Australia:
  - “Telecommunications (Interception) Act, 1979”
  - Attorney General’s Department
- Legal Warrant based interception
  - Issued by judge
  - Strict start and end date+time
  - Specifies what to intercept: content, information about the communication, or both
  - Who to send intercepted communications to
- LI & telephony: a known entity
- LI & IP communications: relatively unknown

SWIN BUR NE CENTRE FOR ADVANCED INTERNET ARCHITECTURES

Outline

- Lawful Interception (LI) - what is it?
- A Sniffer based LI system today
- AAA, RADIUS, DIAMETER
- Future Networks
- Possible Solutions
- Conclusion
- Questions

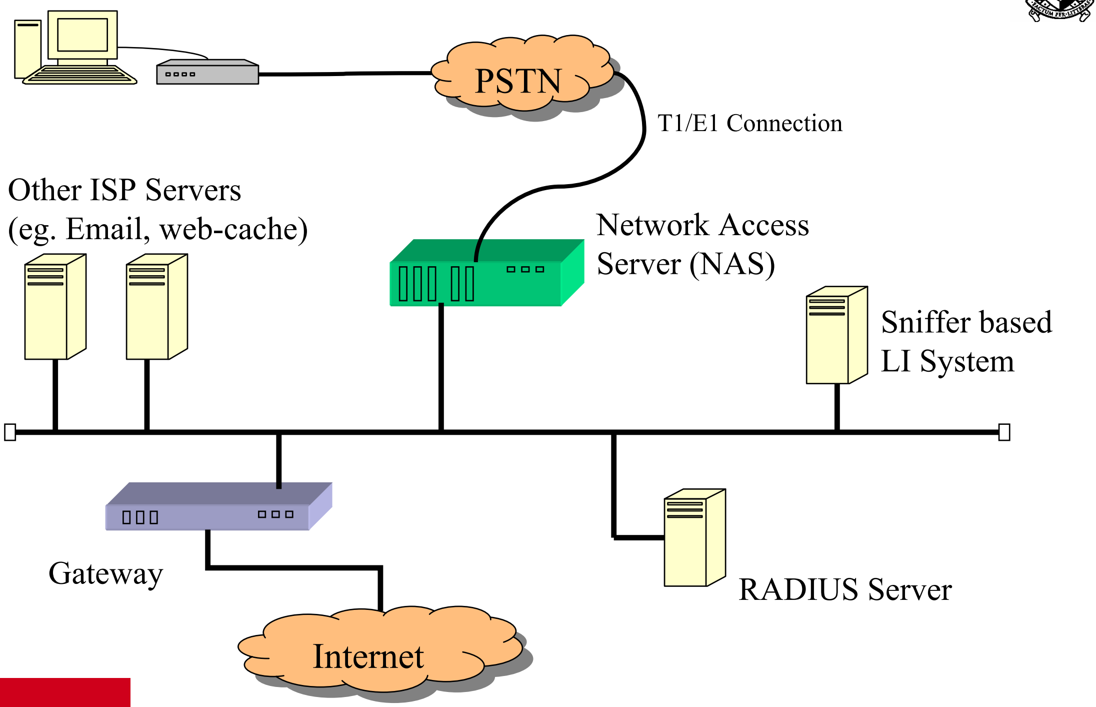
Sniffer based LI - RADIUS

- A system with access to all traffic on a network
- Methods of access:
  - Hub
  - Port mirroring
  - Optical tap/splitter

Sniffer based LI - RADIUS (2)

- Commercially available products
  - Citadel Interception Technologies
  - Aqsacom Inc.
  - Top Layer Networks Inc.
- Interception based on: IP addr, MAC addr, cable modem ID
- Also, higher level data: IM id, email address, RADIUS username
- RADIUS based interception

Sniffer based LI - RADIUS (3)



PSTN

T1/E1 Connection

Other ISP Servers
(eg. Email, web-cache)

Network Access
Server (NAS)

Sniffer based
LI System

Gateway

RADIUS Server

Internet

Outline

- Lawful Interception (LI) - what is it?
- A Sniffer based LI system today
- **AAA, RADIUS, DIAMETER**
- Future Networks
- Possible Solutions
- Conclusion
- Questions

AAA, RADIUS, DIAMETER

- AAA = Authentication, Authorization & Accounting
- RADIUS: AAA solution of choice
- DIAMETER = 2 x RADIUS
  - Base DIAMETER: common types, formats, security
  - DIAMETER Applications: eg NAS, MIPv4
- Migration away from RADIUS towards DIAMETER

AAA, RADIUS, DIAMETER (2)

- DIAMETER Security
  - DIAMETER MUST be used with a security mechanism
  - DIAMETER clients:
    - IPsec at minimum
    - ESP (Encapsulating Security Payload)
  - DIAMETER servers:
    - TLS and IPsec
- Sniffer based LI not as simple

Outline

- Lawful Interception (LI) - what is it?
- A Sniffer based LI system today
- AAA, RADIUS, DIAMETER
- **Future Networks**
- Possible Solutions
- Conclusion
- Questions

Future Networks

- IPv6 + RADIUS
  - RFC3162: must support IPsec
- IPv6 + DIAMETER
  - Adherent to Base DIAMETER security requirements
- MobileIPv6 + AAA
  - Not specified in RFCs
  - Likely to follow DIAMETER for MIPv4
  - Adherent to Base DIAMETER security requirements

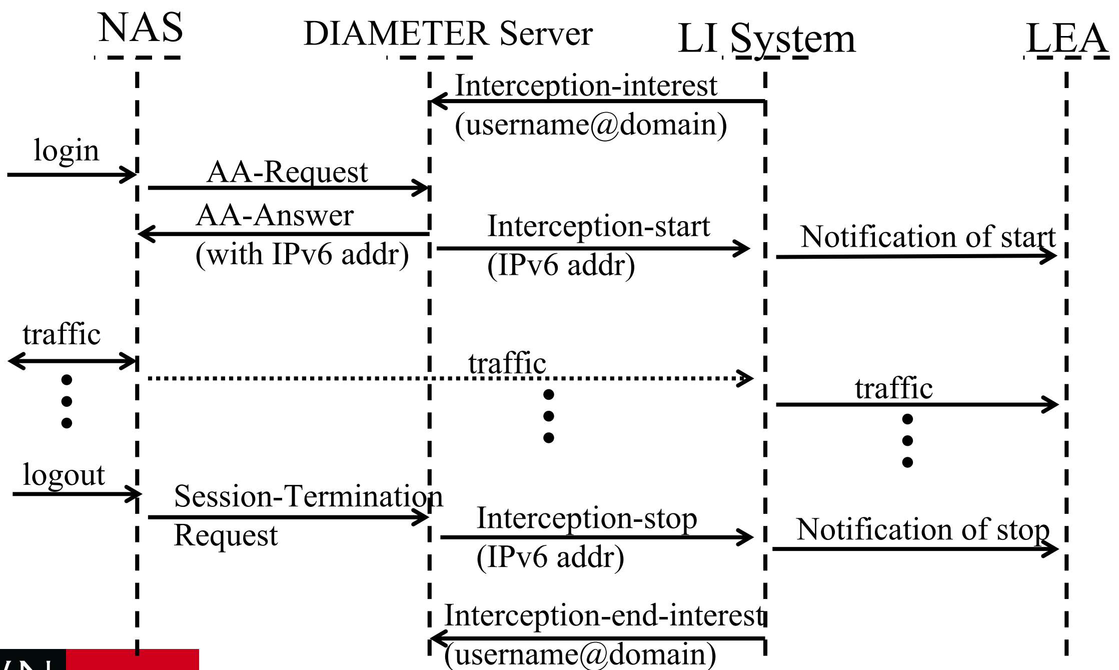
Outline

- Lawful Interception (LI) - what is it?
- A Sniffer based LI system today
- AAA, RADIUS, DIAMETER
- Future Networks
- **Possible Solutions**
- Conclusion
- Questions

Possible Solutions

- Sharing Keys
  - Encryption keys used in DIAMETER server/client communication
  - Keys also shared with LI system
  - Assumes IPsec w/ ESP
  - "Key Escrow" ?
- Dedicated LI protocol
  - Application level protocol b/w AAA server & LI system
  - Cleaner (from LI system point of view)
  - An example case for IPv6+DIAMETER

Possible Solutions (2)



Possible Solutions (3)

- Proprietary Solution
  - LI capability built into AAA server as proprietary
  - Open to scrutiny?

Outline

- Lawful Interception (LI) - what is it?
- A Sniffer based LI system today
- AAA, RADIUS, DIAMETER
- Future Networks
- Possible Solutions
- **Conclusion**
- Questions

Conclusion

- Sniffer based interception in use today
- RADIUS based
- Future networks demand security
- Lawful Interception becomes more complex
- Possible solutions
- Take home message is:
  - "as the security in the network improves, systems which relied on simple security are made more complex"

Outline

- Lawful Interception (LI) - what is it?
- A Sniffer based LI system today
- AAA, RADIUS, DIAMETER
- Future Networks
- Possible Solutions
- Conclusion
- **Questions**