SIPFIX: Use Cases and Problem Statement for VoIP Monitoring and Exporting

draft-huici-ipfix-sipfix-00

Felipe Huici, Saverio Niccolini, Sven Anderson
Presented by Thomas Dietz
Motivation and use cases

• Motivation: distributed monitoring and operations of VoIP networks
  – Live monitoring of control plane (e.g., SIP) and media plane (e.g., RTP)
    ➢ E.g., a voice-only call can be seen as two flows
      ✓ SIP flow
      ✓ RTP flow

• Use cases, i.e., why do we need to monitor VoIP networks
  – QoS, SLAs, Traffic Engineering, Troubleshooting, Security, Billing, Law enforcement, etc.

• Requirements (or challenges)
  – Distributed measurements (multiple observation points)
    ➢ From (multiple) probes to (less and optional) mediators to (one) collector
  – Application layer semantics (Deep Protocol Inspection)
    ➢ SIP, SDP, RTP, RTCP, etc.
  – Flexible exporting format to accommodate future changes in protocols
    ➢ SIP defines a new one every day 😊
  – Correlation of control plane and media plane flows

• We need a standardize way to make probes, (mediators) and collectors talk to each other
What is our contribution?

• **Now**
  – Enumerate use cases
  – Define requirements of what we would need

• **In the future**
  – Just define some Information Elements (IEs)
    using IE template (RFC 5102)

• **Flow type definitions (main ones)**
  – SIP Flow
    – “sipDialogId” composed of (sipFrom, sipTo, sipCallId)
    – May include other SIP header IEs
  – Media Flow
    – “sipMediald”: a unique identifier for a media stream description of a SIP dialog
  – Media Flow Descriptor
    – "Virtual" flow to correlate SIP and Media Flows (can be extracted from SIP Header or from SIP Payload, i.e., SDP)
      ✓ Contains “sipDialogId” and “sipMediald”

• **Paper reference (for additional details)**
  – Anderson, Niccolini, Hogrefe, “SIPFIX: A Scheme For Distributed SIP Monitoring”
    – IEEE International Symposium on Integrated Network Management (IM) 2009
Why IPFIX?

• To re-use what is there already
  – Build on existing standards instead of inventing new ones
  – Reduce development costs by making usage of many IPFIX libraries available

• Even more…
  – SIP and RTP are indeed flows
    ➢ Just not at IP layer (something similar to IPFIX for other layers…)

• Even more…
  – A lot of IPFIX extensions re-used
    ➢ Mediation concepts
      ✓ fundamental for distributed monitoring scenarios
    ➢ Bidirectional Flows (RFC 5103)
      ✓ merging SIP request and responses still keeping per-direction counters
    ➢ Common Properties (RFC 5473)
      ✓ Defining a commonPropertiesID with fields common to many reports (sipFrom, sipTo, sipCallId), e.g., a long lasting call
Example of how SIPFIX makes usage of Mediation

- Example: monitoring and operations of a VoIP call (UA1 ↔ UA2)
  - Receiving call flows from two locations: can compute e2e delay

- Receiving SIP IEs and RTP IEs from SBC2
  - Exports the whole call flow

- Receiving SIP IEs from MGW1 and RTP IEs from SBC1
  - Correlates, merge and exports a single flow (the call)
Related work

- The Common Log File (CLF) format for the Session Initiation Protocol (SIP)
  - draft-gurbani-sipping-clf-01
- Binary Syntax for SIP Common Log Format
  - draft-roach-sipping-clf-syntax-01

- Similarities
  - IPFIX is being considered as a candidate for CLF
  - IEs to be defined would probably overlap (need to talk)
    - E.g., from, to, callid, etc.

- Differences
  - focused on particular use case
    - interpreting the state of SIP transactions
  - not using mediation concepts (correlating & merging)
  - only focused on control plane
Is there an home for this work?

• Just defining a bunch of Information Elements (IEs)
  – IPFIX supports this either by defining enterprise-specific IEs or by registering new IEs at the IANA registry

• Where to go? What to do?
  – Operations and Management Area 😊
    ➢ we are talking about operations and management, we are talking about flows, we are highly re-using IPFIX concepts (mediation, biflow, common properties)
  – Real-time Applications and Infrastructure Area
    ➢ SIP knowledge would be there
  – Just allocate the IEs and use them in products? 😞