Autonomica's DSC modification project

Carl Olsen & Lars-Johan Liman

calle@autonomica.se
liman@autonomica.se

Original DSC

- Consists of:
  - Collector – collects DNS data
    - Process near the DNS server
  - Presenter – Presents the information
    - Process near the stats consumer. ©

Original Collector

- Sniffs packet using pcap-lib.
  - Same as tcpdump
- Collects statistics
  - Writes XML files
- Sends data to the presenter using
  - HTTPS or
  - rsync/ssh
- Static configuration
  - Need restart to reread configuration

Autonomica Requirements

- Able to remotely configure each collector
  - Fast reconfiguration during deviations from normal traffic
  - Collect certain data during certain times
- More Dynamic presentation
  - (Haven't come to this yet …)

Some Internal Changes

- The internal indexing mechanism has been redesigned.
- Now each of the dataset items has its own indexing
  - Needed in threaded model …

Original DSC with fork()

- Parent Process:
  - 60 sec packet sniffing
  - Create child process to handle collected data
  - Restart
- Child Process:
  - Writes to disk
  - Dies (memory is freed)

Changes from Original DSC

- From fork() to threads
  - Advantages
    - Shared memory for interprocess communication
  - Same memory as parent
    - More flexible (two way communication)
  - Disadvantage
    - Memory management
    - Redesign of certain structures

DSC with Threads

- A Reader thread:
  - Collects packets and updates the active twodimensional array
  - Creates a reporter thread every 60 sec
    - Swaps active and passive memory structure
- A reporter thread:
  - Writes passive memory to disk
  - Clears passive memory

Why Threads?

- Obvious drawback
  - Bigger memory footprint
- Crucial advantage:
  - One stable process …
  - … that can maintain network based communication with the outside world.

DSC Configuration Parser

- Original DSC parser could not be invoked twice in same session.
  - No way to clear memory structures.
- Fixed by implementing a new parser
  - Using BNFC which uses Flex and Bison
    - Easy to configure using BNF grammar
    - Creates a C parser that can be linked into the application.

DSC with SSL Support

- Two new threads incoperated into the design:
  - SSL thread
    - Authentication based on x509_v3 certificate
    - Multi threaded … (even more threads …)
  - Main Thread
    - Handles and schedules other threads
    - Reads configuration
    - Initializes and destroys memory structures

SSL Authentication

- X.509_v3 certs
  - Collector and control box must have certs signed by same CA
  - Collector
    - SubjectAltName from client has to be configured in the collector
    - Highly configureable (using XML conf. file)
  - Control
    - Presents certificate to collector
      - Has to be signed by CA known by collector

Collector-control protocol

- Based on XML
- Two types of messages
  - Order
    - User
    - Command
    - Argument
  - Response
    - Status
      - Code
      - Info
    - Data

Typical "order" message

```
<order>
   <user> effective uid </user>
   <command> e.g reconfig </command>
   <command_info>
      <arg1>/tmp/testConfig.cnf</arg1>
      <arg2> Configuration Content </arg2>
   </command_info>
</order>
```

Typical "response" message

```
<resp>
   <status>
      <code> syslog code </code>
      <info> Textual information </info>
   </status>
   <resp_data>
      Data……..
   </resp_data>
</resp>
```

Current Status

- Collectors installed at a few Autonomica anycast nodes
  - Stockholm, Oslo, London, and Tokyo
- Collectors separate from servers
  - Passive splitters
- Gathering data and experience to see where to take it further.
- Turning our focus to presenter
- Looking for input

More Toys by Autonomica
dns2db

- Want to collect the data into a real database instead
- Takes pcap file and loads relevant data into an SQL database.
- Gives ample flexibility for backend analyzers
- Graciously financed by .SE
  - … so over to the next speaker.

Autonomica AB
Bellmansgatan 30
SE-118 47 Stockholm
Sweden

Tel: +46-8-6158570
E-mail: info@autonomica.se

http://www.autonomica.se/