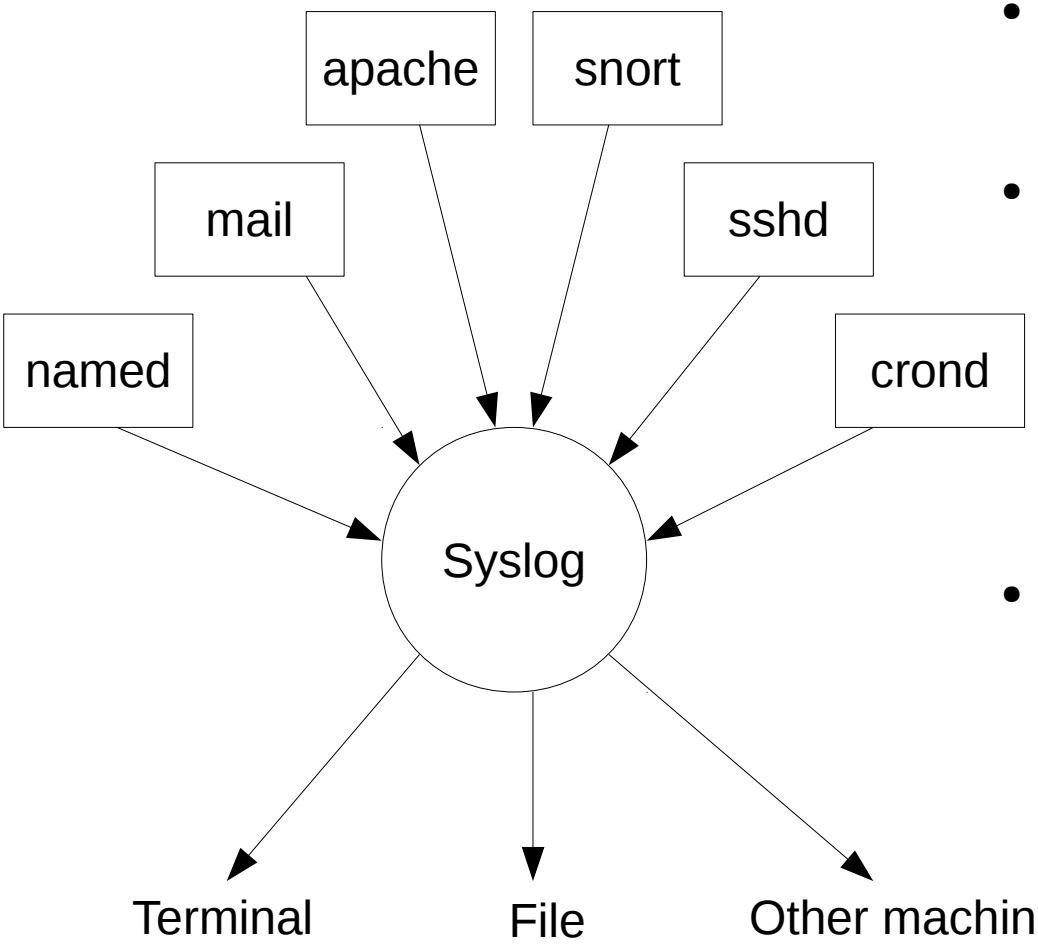
Syslog plug-in to generate LTTng trace events

Yannick Brosseau
Naser Ezzati
Michel Dagenais

Department of Computer and Software Engineering

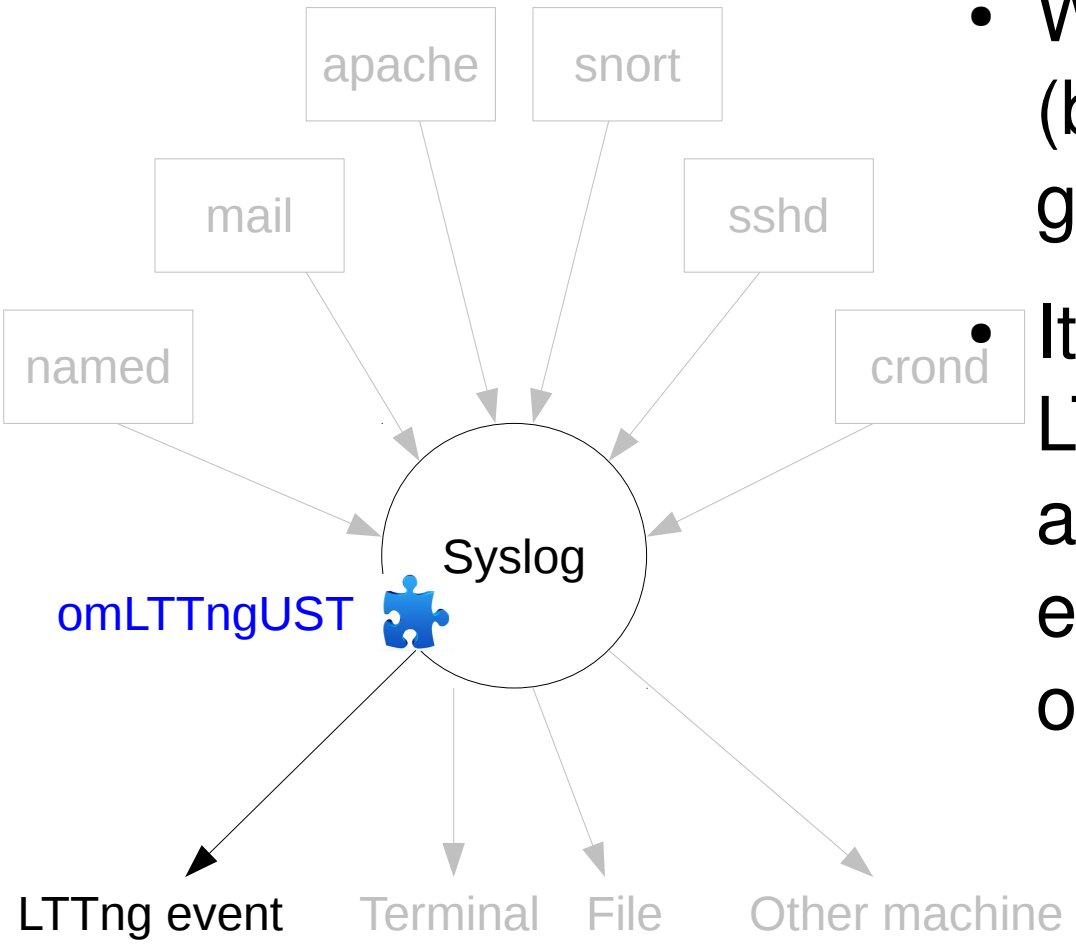
Dec 10, 2013
École Polytechnique, Montreal

Syslog



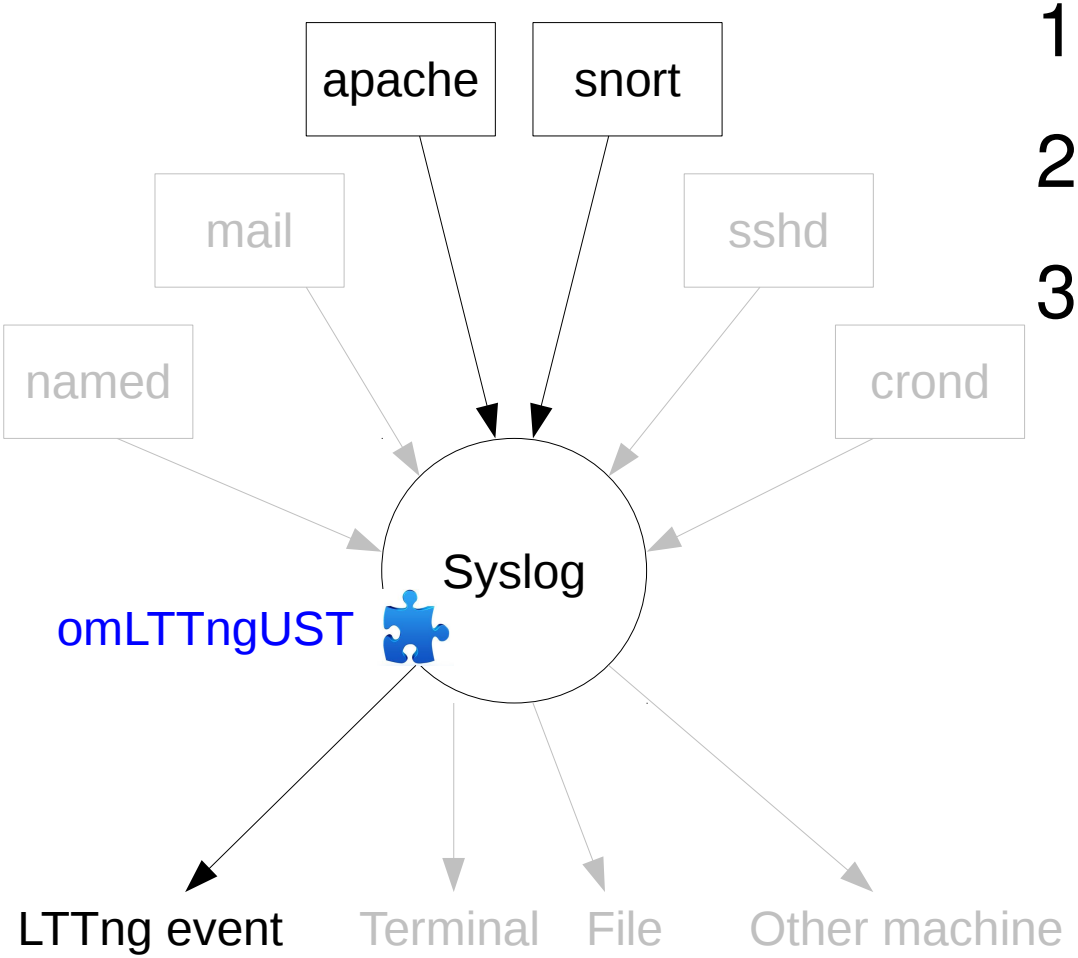
- “Syslog is a standard for computer message logging.” (wikipedia)
- Most network devices (routers and switches), can generate Syslog logs. Linux servers, apache web server, most firewalls, some printers also support Syslog.
- In Windows there is also a large number of tools that enables collecting Windows Event Log or IIS data and send it to a Syslog server.”

Syslog → Lttng



- We hooked Syslog Daemon (by adding 3 tracepoints) to generate LTTng UST events.
- It makes possible to gather LTTng trace events from any application generating syslog entries, without modifying the original application.

Demo



1. Syslog → LTTng
2. Snort → Syslog → LTTng
3. PHP → Syslog → LTTng

Thank you

Questions?