

System for integration of tools for full content verification on multiple sensors

Tommy Steensnæs
08.06.2010



Outline

- Problem description
- Research questions
- Methods
- The system
- Testresults
- Conclusion and summary
- Questions

Problem description

- Lack of tools designed for Computer Network Defense
- Existing tools; not to the point
 - Perceived usefulness is not optimal
- Solution: simple command line based tools
- Problem: No scalability for use on multiple sensors

Research questions

- To what extent is it possible to integrate the use of packet capture tools in a way that minimizes the added effort of starting a packet capture when expanding the number of sensors?

Research questions cont.

- Can the data from the captures be organized in a way that makes them accessible for the analyst?

Research questions cont.

- If so, can this integration also be used to document the process in such a way that it reduces the need for administrative documentation?

Methods

- Develop prototype
- Keystroke-level modeling
- Perceived effectiveness and usefulness survey

Prototype

- Input interface
 - Transparent communication with arbitrary number of sensors
 - Secure communication with SSH
 - Force description and authorization
 - All captures are logged in database

Add capture

Time: 14:54:19

[Ongoing captures](#) [Add capture](#) [Inactive captures](#) [Capture directory](#)

Command: Description: Authorized:

Sign: Dfile: Active: Sensors:

Hold down "Control", or "Command" on a Mac, to select more than one.

- Sensor4
- Sensor3
- Sensor2
- Sensor1



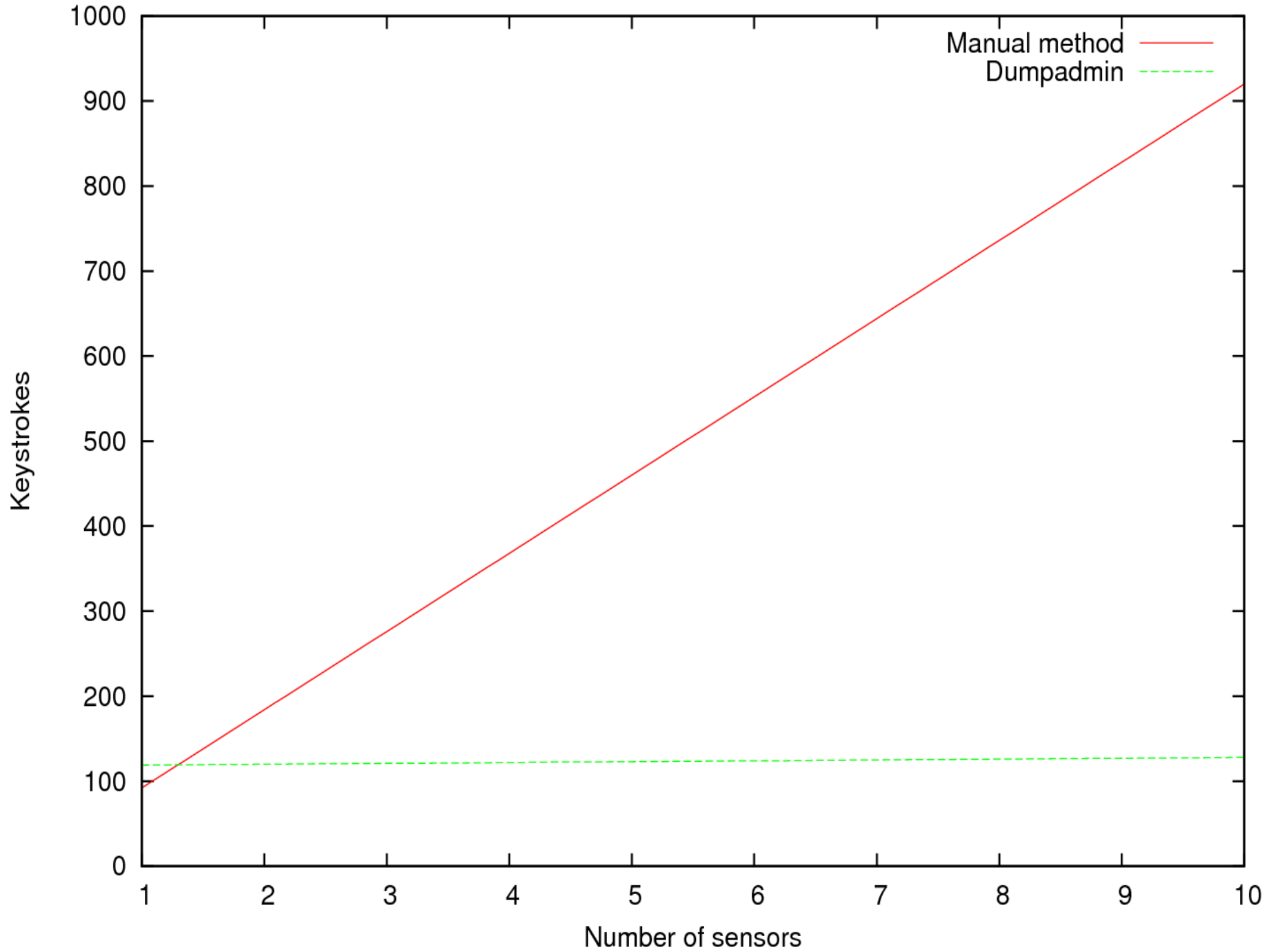
Prototype cont.

- Status
 - All ongoing capture listed
 - Changes to captures immediately presented
- Stopped captures
 - List inactive captures from database
 - Export to PDF

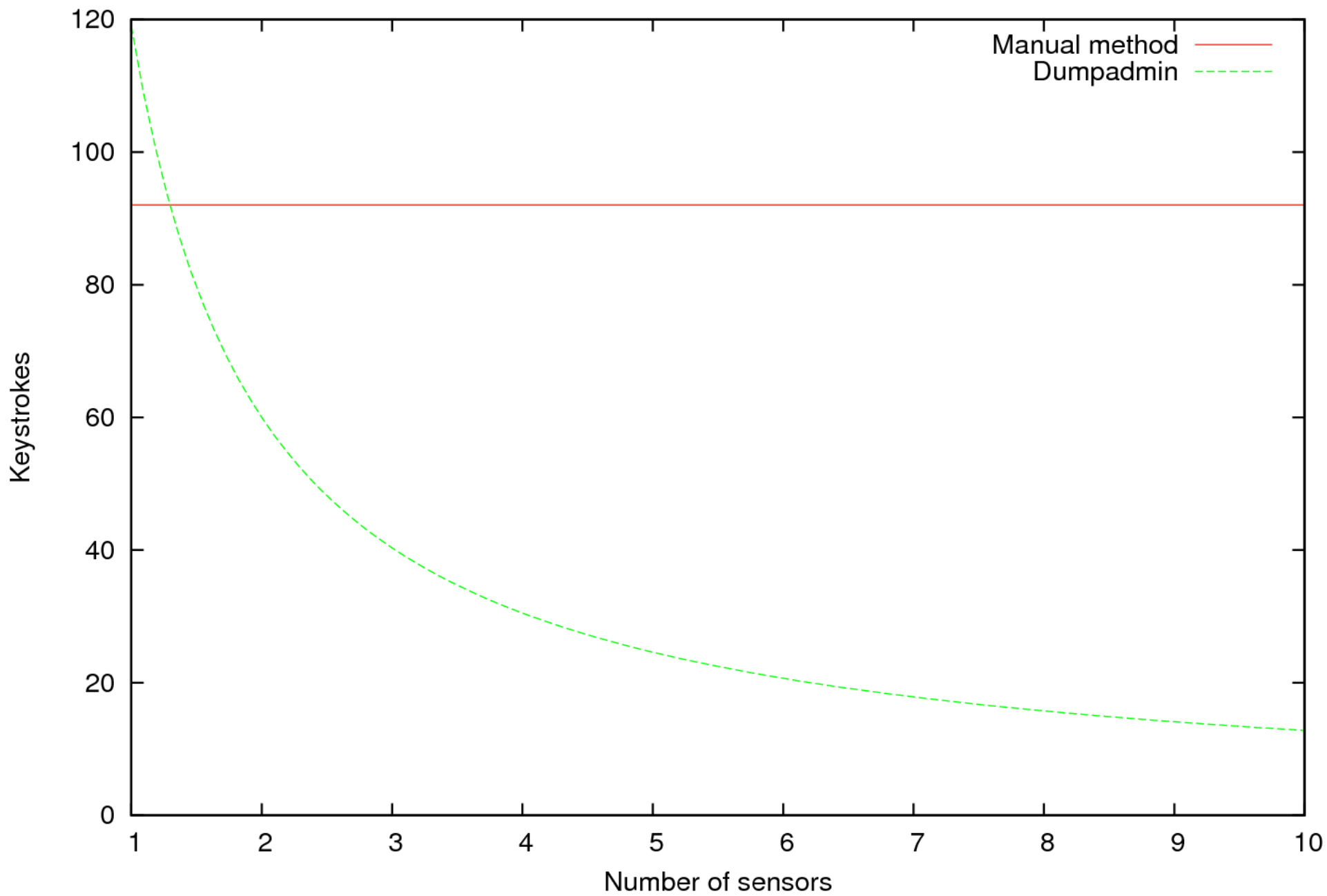
Testresults, KLM

- Keystroke-level modeling shows substantial increase in efficiency
- Does not account for extra operations such as logging and documentation and added complexity of multiple terminals

Example 2



Example 2, average



Testresults, perceived effectiveness

- Survey shows:
 - The system increases effectiveness and will be useful
 - Interface is easy to learn and use
 - Needs extra features to be optimal

Question(statement)	Mean	Median	Mode
The system would help me be more effective	5	5	5
It would be useful in my daily job	5	5	5
Both occasional and regular users would benefit from it	5.3	5	7
I can use it successfully every time	5.8	6.5	7
The system is easy to use	5	5	5
The system was easy to learn	6	6	7
I easily remember how to use it	6.3	7	7
The system makes it easier to monitor packet captures	5.6	6	5
I prefer this system over the manual method for starting and monitoring packet captures	5.9	6	6

Conclusion and Summary

- The prototype shows that increased efficiency and effectiveness can be achieved by the proposed system
- Future work:
 - Support filters from file, add functionality to inspect content of capture files
 - Broader surveys to investigate applicability in other environments

Questions?