



University of Maryland University College

**Making Intrusion Detection
Systems and Intrusion
Prevention Systems Intelligent:
Hands-On Laboratory Exercises**

**Dr. Jim Q. Chen, John Smet, Barry
Williams, Victor Tsao, John R. P. Dittamo,
Irfan Mohammed, Lamin Kamara, Alkalifa A.
Samake, Zhuqing Jiang, and Jim Street**

March 2008

Acknowledgements

- Special thanks to other participants of this project: Nicole Regobert, Joseph Sudassy, Zhenqiang Yi, Michael Hughes, David Vigna, Sharon A. Archer, Marcelle S. Owens, and Khalid Bendidi

Objectives

- Discuss what is necessarily needed in performing intrusion detection and intrusion prevention
- Show what is available in the alert logs of the Snort Intrusion Detection System
- Discuss what is missing in the picture
- Propose a solution
- Design corresponding hands-on laboratory exercises
- Discuss pedagogical lessons learned

Reality

- Not just deal with computers and networks
- Deal with humans who are using computers and networks

Interdisciplinary Approach

- Intrusion detection
- Intrusion prevention
- Data mining
- Artificial intelligence
- Psychology
- Sociology
- Criminology
- Etc.

What Is Necessarily Needed?

- Who is the intruder?
- What has been done?
- When does it occur?
- Where does the intruder come from? Where does the intruder go?
- How does the intruder carry out the intrusion?
- Why does the intruder carry out the intrusion?

Available Items in the Snort Alert Logs

- See demo logs

Available Items in the Snort Alert Logs

- Time
- Alert message
- Protocol
- Source IP address
- Traffic direction
- Destination address

Available Items in the Snort Alert Logs

- Source port number
- Destination port number
- Number of total alerts
- Number of unique alerts
- Time of first occurrence
- Time of last occurrence
- Signature
- Intrusion classification / severity

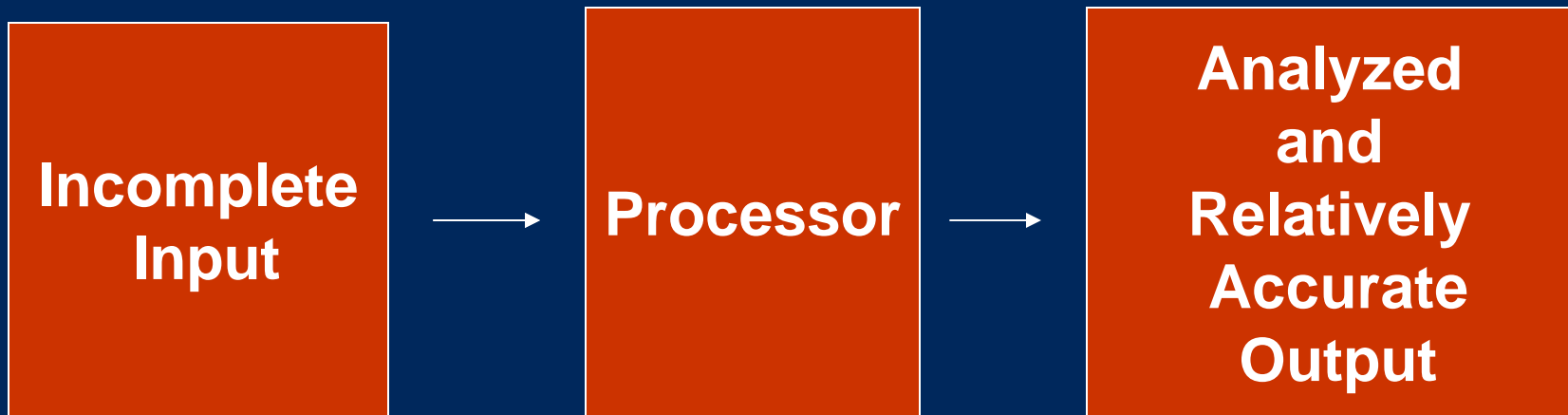
What Is Missing?

- Do we really know who is the intruder?
- Do we really know what has happened?
- Do we really have the timeline of the intrusion?
- Do we really know where the intrusion traffic was initiated?
- Do we really know how this intrusion is carried out?
- Do we really know the intention of the intrusion?

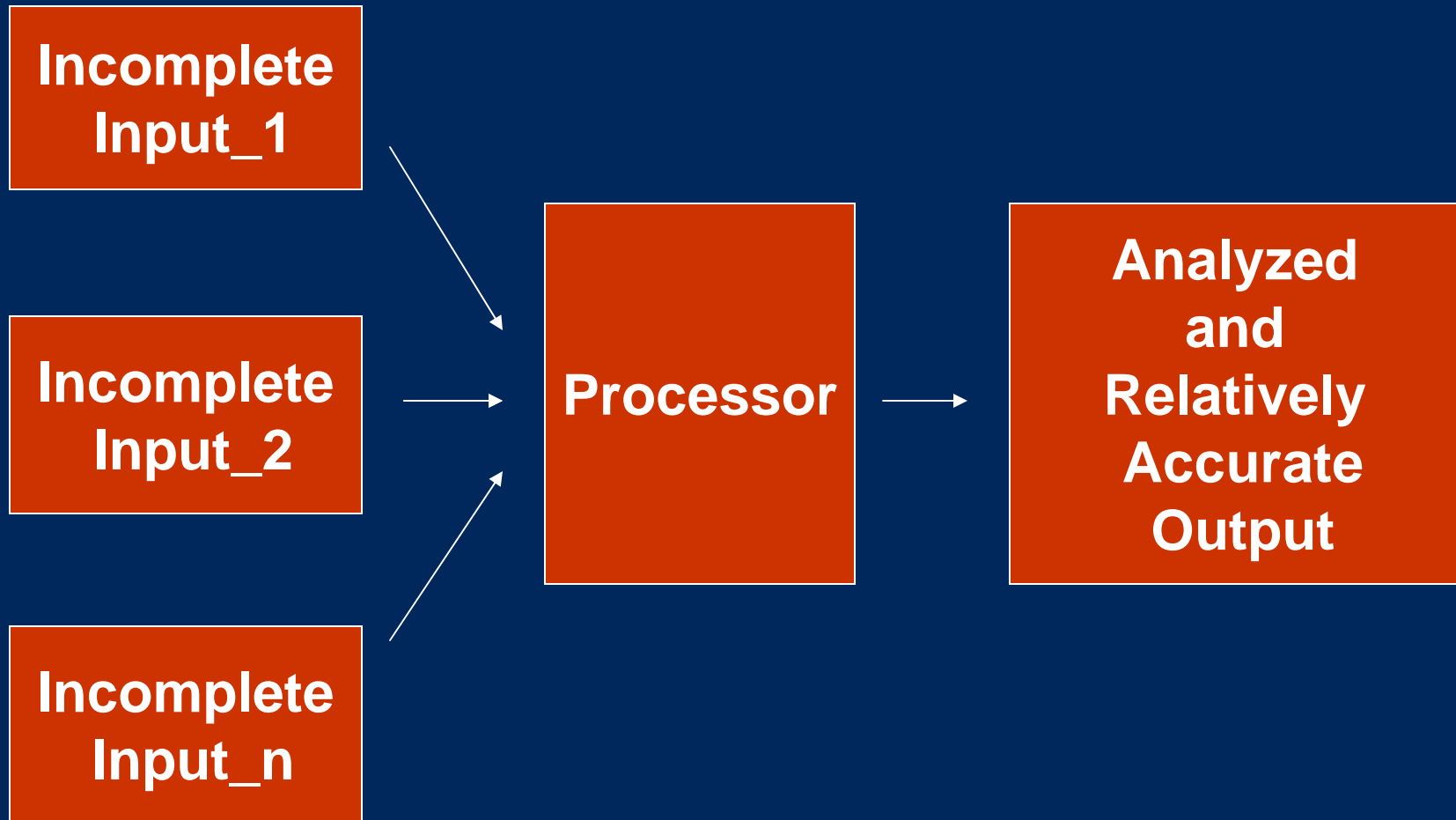
Issues

- No crystal-clear answers to these questions in many occasions
- No decisive conclusion

Challenge [see Chen(2008a)]



Solution [see Chen(2008a)]



Condition [see Chen(2008a)]

- All these incomplete inputs are gathered at the same period of time within the same network segment

Examples

- Input_1: Snort alert log file
- Input_2: WireShark capture file
- Input_3: tcpdump file

New Challenges

- How do we incorporate different log files into one database?
- How do we create different views with different requirements?
- How do we identify new patterns?

3 Lab Exercises

- Lab 1: Load different types of log files into one database
- Lab 2: Create different views with different requirements
- Lab 3: Identify new patterns

Lab 1: Loading Log Files

- Read in a Snort alert log file, i.e. "alert.ids"
- Read in a WireShark capture file
- Read in a tcpdump log file

Loading Log Files

- Demo

Lab 1: Lesson Learned

- There are different types of log file formats.
- Some file formats need to be converted before the file is loaded as an input.
- There are different ways of handling the unique fields in different log files.

Lab 2: Creating Different Views

- Create a view that displays when and what
- Create a view that displays when, what, and where
- Create a view that displays when, who, and what
- Output different views

Creating Different Views

- Demo

Lab 2: Lesson Learned

- Relevant pieces of Information are grouped together for display.
- Different perspectives can be provided.
- New and interesting patterns can be identified.
- These patterns can be used to create new identities.

Lab 3: Identifying New Patterns

- Answer the questions about who, what, when, and where
- Compare the information provided by different views with the answers provided by the alert log file "alert.ids" in Snort
- Discuss the new patterns identified

Identifying New Patterns

- Demo

Lab 3: Lesson Learned

- More information about who, what, when, where, and how is provided.
- New patterns may be identified.

Pedagogical Implication

- Put students into the real-life scenarios
- Challenge students with the real-life problems
- Promote interdisciplinary approach
- Encourage students to think out of the box
- Enhance learning with hands-on exercises
- Make the learning experience more interesting

Summary

- Multiple incomplete inputs may help us to arrive at a relatively accurate conclusion.
- Having different combinations of categories may generate new views and perspectives.
- Different views may help us to gain a better understanding of the intrusion.
- Challenging students with real-life issues may enhance their learning and motivate new creative solutions.

References

- Beale, J., Baker, A., Esler, J., and others. (2007). *Snort IDS and IPS Toolkit*. Rockland, MA: Syngress Publishing, Inc.
- Chen, J. Q. (2008a). "Building Intelligence for Intrusion Detection and Intrusion Prevention". Manuscript. Graduate School of Management & Technology, University of Maryland University College
- Cox, K. & Gerg, C. (2004). *Managing Security with Snort and IDS Tools*. Sebastopol, CA: O'Reilly Media, Inc.
- Giuseppini, B. and Burnett, M. (2004). *Microsoft Log Parser Toolkit*. Rockland, MA: Syngress Publishing, Inc.
- Kasabov, N. (1998). *Foundations of Neural Networks, Fuzzy Systems, and Knowledge Engineering*. Cambridge, MA: The MIT Press
- Provos, N. and Holz, T. (2008). *Virtual Honeypots: From Botnets Tracking to Intrusion Detection*. Upper Saddle River, NJ: Addison-Wesley, Pearson Education
- Singer, A. and Bird, T. (2004). *Building a Logging Infrastructure*. Berkeley, CA: The USENIX Association
- Snort, <http://www.snort.org>
- Tcpdump, <http://www.tcpdump.org>
- WireShark, <http://www.wireshark.org>