University of Innsbruck
School of Management
Information Systems

To Invest or Not to Invest?

Assessing the Economic Viability of a Policy and Security Configuration Management Tool

11th Annual Workshop on the Economics of Information Security
(WEIS 2012)
Berlin, Germany

Lukas Demetz and Daniel Bachlechner
University of Innsbruck
Austria

Policy and security configuration management

- Organizations face numerous regulatory and contractual requirements they need to comply with
- Expenditures for compliance are increasing, especially for service providers offering services to multiple customers
- Managing requirements and the configuration of IT landscape components is cumbersome and error-prone
- A tool partially automating policy and security configuration management may help to
  - reduce the costs associated with policy and security configuration management
  - increase the trustworthiness through higher levels of security and compliance

PoSecCo – A policy and security configuration management tool

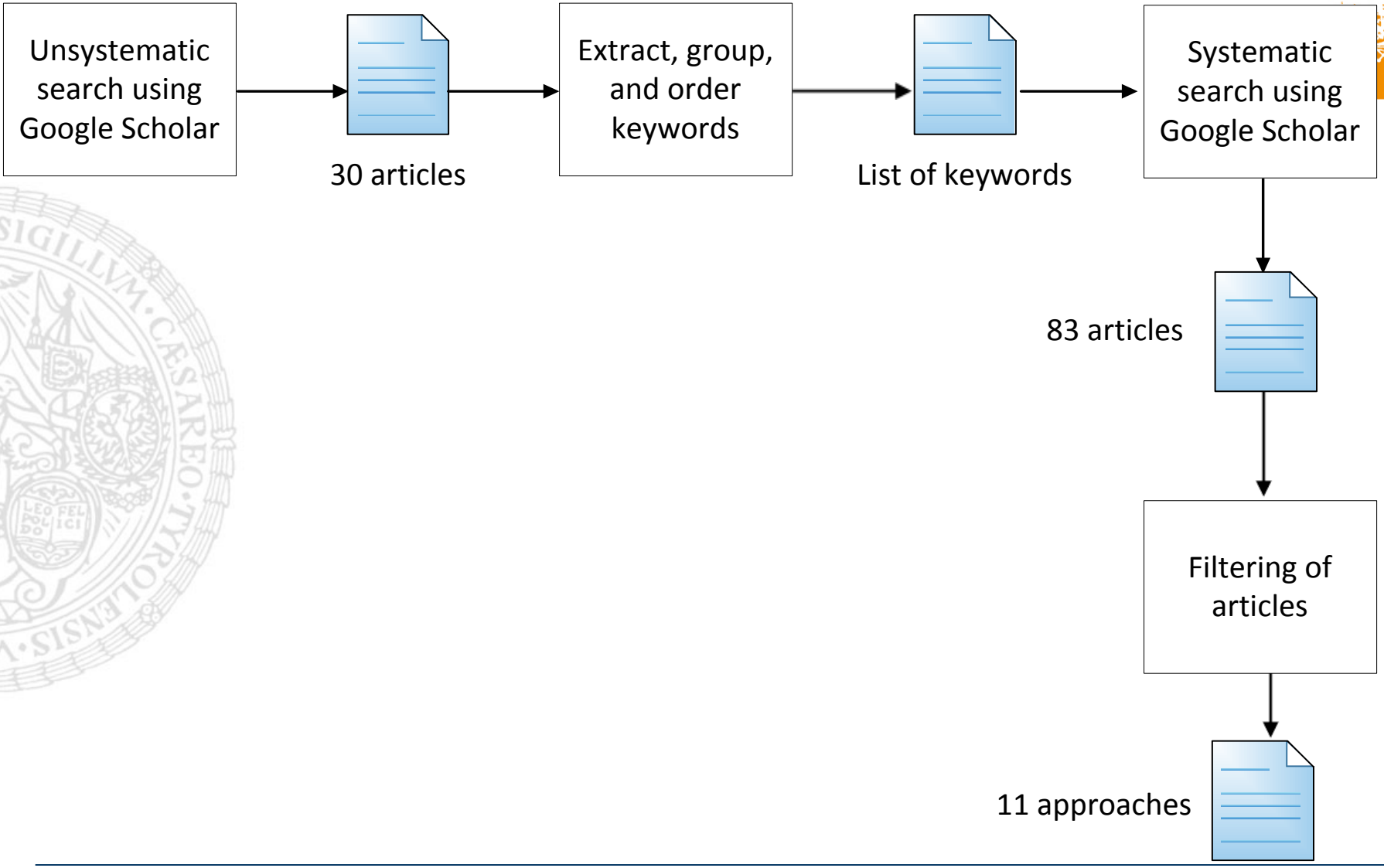
- Aims at policy and security configuration management
- Aims to support reducing costs and increasing trustworthiness
- Establishes link between business requirements and security configuration of IT landscape components
- Can be operated in two modes:
  - Planning mode
  - Running mode
- Offered as a whole
- Ideally run not only at one organization but also at its suppliers and customers to increase overall benefits

Requirements for investment approaches for such a tool

The approach

- *must* support investment decisions regarding security products bought as a whole
- *must* consider financial measures
- *should* consider non-financial measures
- *must* support one-time costs and benefits
- *should* support running costs and benefits
- *must* be applicable without explicitly considering attacks
- *should* consider network effects

Identification of approaches



Results

Authors	Bought as a whole	Financial	*Non- financial*	One-time costs	*Running costs*	Attacks	*Network effects*
Gordon & Loeb [1]	X	X		X		X	
Mizzi [2]	X	X		X	~	~	
Al-Humaigani & Dunn [3]	X	X		X		X	
Sonnenreich et al. [4]	X	X		X		X	
Cremonini & Martini [5]	X	X		X		~	
Huang et al. [6]	X	X		X		X	
Tallau et al. [7]	X	X	X	X	~	X	~
Wang et al. [8]	X	X		X		X	
Gordon et al. [9]	X	X		X		X	
Bodin et al. [10]	X	X	X	X	~	X	~
Butler [11]	X	X	X	X		X	

Findings and conclusion

- The approaches by Bodin et al. [10] and Tallau et al. [7] at least partially fulfill all requirements defined for a policy and security configuration management tool
- Both are not completely suitable as both are primarily suited for comparative analyses
- These two approaches could be combined with useful features of the other approaches

THANK YOU!

Contact

Lukas Demetz
Lukas.Demetz@uibk.ac.at

University of Innsbruck
School of Management
Information Systems
Universitätsstraße 15
A-6020 Innsbruck

Acknowledgments

The research leading to these results was partially funded by the European Union 7th Framework Programme (FP7) through the PoSecCo project (project no. 257129).

PoSecCo
Policy and Security Configuration Management

http://www.posecco.eu

References

[1] Gordon L. A. and Loeb M. P. The economics of information security investment. ACM Transactions on Information and System Security, 5(4):438-457, 2002.

[2] Mizzi A. Return on information security investment-the viability of an antispam solution in a wireless environment. International Journal of Network Security, 10(1): 18-24, 2010.

[3] Al-Humaigani M. and Dunn D. B. A model of return on investment for information systems security. In Proceedings of the 46th IEEE International Midwest Symposium on Circuits & Systems, Vols 1-3, pp. 483-485, 2003.

[4] Sonnenreich W., Albanese J., and Stout B. Return On Security Investment (ROSI) { A Practical Quantitative Modell. Journal of Research and Practice in Information Technology, 38(1):55-66, 2006.

[5] Cremonini M. and Martini P. Evaluating Information Security Investments from Attackers Perspective: the Return-On-Attack (ROA). In Proceedings of the 4th Workshop on the Economics of Information Security (WEIS 2005), 2005.

[6] Huang C. D., Hu Q., and Behara R. S. An economic analysis of the optimal information security investment in the case of a risk-averse firm. International Journal of Production Economics, 114(2):793-804, 2008.

[7] Tallau L. J., Gupta M., and Sharman R. Information security investment decisions: evaluating the Balanced Scorecard method. International Journal of Business Information Systems, 5(1):34-57, Jan. 2010.

[8] Wang J., Chaudhury A., and Rao H. R. A value-at-risk approach to information security investment. Information Systems Research, 19(1):106-120, Mar. 2008.

[9] Gordon L., Loeb M., and Lucyshyn W. Information security expenditures and real options: A wait-and-see approach. Computer Security Journal, 19(2):1-7, 2003.

[10] Bodin L. D., Gordon L. A., and Loeb M. P. Evaluating information security investments using the analytic hierarchy process. Communications of the ACM, 48(2):78-83, 2005.

[11] Butler S. A. Security attribute evaluation method: a cost-benefit approach. In Proceedings of the 24th International Conference on Software Engineering, pp. 232-240, Orlando, Florida, 2002.