
Science of Cyber-Security

Contact: D, McMorrow - dmcorrow@mitre.org

November 2010

JSR-10-102

Approved for public release; distribution unlimited

JASON
The MITRE Corporation
7515 Colshire Drive
McLean, Virginia 22102-7508
(703) 983-6997

REPORT DOCUMENTATION PAGE

Form Approved
OMB No. 0704-0188

Public reporting burden for this collection of information is estimated to average 1 hour per response, including the time for reviewing instructions, searching existing data sources, gathering and maintaining the data needed, and completing and reviewing this collection of information. Send comments regarding this burden estimate or any other aspect of this collection of information, including suggestions for reducing this burden to Department of Defense, Washington Headquarters Services, Directorate for Information Operations and Reports (0704-0188), 1215 Jefferson Davis Highway, Suite 1204, Arlington, VA 22202-4302. Respondents should be aware that notwithstanding any other provision of law, no person shall be subject to any penalty for failing to comply with a collection of information if it does not display a currently valid OMB control number. **PLEASE DO NOT RETURN YOUR FORM TO THE ABOVE ADDRESS.**

1. REPORT DATE (DD-MM-YYYY) November 19, 2010	2. REPORT TYPE Technical	3. DATES COVERED (From - To)	
4. TITLE AND SUBTITLE Science of Cyber-Security		5a. CONTRACT NUMBER	
		5b. GRANT NUMBER	
		5c. PROGRAM ELEMENT NUMBER	
6. AUTHOR(S)		5d. PROJECT NUMBER 13109022	
		5e. TASK NUMBER PS	
		5f. WORK UNIT NUMBER	
7. PERFORMING ORGANIZATION NAME(S) AND ADDRESS(ES) The MITRE Corporation JASON Program Office 7515 Colshire Drive McLean, Virginia 22102		8. PERFORMING ORGANIZATION REPORT NUMBER JSR-10-102	
9. SPONSORING / MONITORING AGENCY NAME(S) AND ADDRESS(ES) ODUSD (AT&L)/RD /IS 1777 North Kent Street, Suite 9030 Rosslyn, Virginia 22209		10. SPONSOR/MONITOR'S ACRONYM(S)	
		11. SPONSOR/MONITOR'S REPORT NUMBER(S)	
12. DISTRIBUTION / AVAILABILITY STATEMENT Approved or public release; distribution unlimited.			
13. SUPPLEMENTARY NOTES			
14. ABSTRACT JASON was requested by the DoD to examine the theory and practice of cyber-security, and evaluate whether there are underlying fundamental principles that would make it possible to adopt a more scientific approach, identify what is needed in creating a science of cyber-security, and recommend specific ways in which scientific methods can be applied. Our study identified several sub-fields of computer science that are specifically relevant and also provides some recommendations on further developing the science of cyber-security.			
15. SUBJECT TERMS			
16. SECURITY CLASSIFICATION OF:			17. LIMITATION OF ABSTRACT UL
a. REPORT UNCL	b. ABSTRACT UNCL	c. THIS PAGE UNCL	
			18. NUMBER OF PAGES
			19a. NAME OF RESPONSIBLE PERSON Steven E. King
			19b. TELEPHONE NUMBER (include area code) 703-588-7414

Contents

1	EXECUTIVE SUMMARY	1
2	PROBLEM STATEMENT AND INTRODUCTION	9
3	CYBER-SECURITY AS SCIENCE – An Overview	13
3.1	Attributes for Cyber-Security	14
3.2	Guidance from other Sciences	15
3.2.1	Economics	16
3.2.2	Meteorology	16
3.2.3	Medicine	17
3.2.4	Astronomy	17
3.2.5	Agriculture	18
3.3	Security Degrades Over Time	18
3.3.1	Unix passwords	18
3.3.2	Lock bumping	19
3.4	The Role of Secrecy	20
3.5	Aspects of the Science of Cyber-Security	22
3.6	Some Science	23
3.6.1	Trust	23
3.6.2	Cryptography	23
3.6.3	Game theory	24
3.6.4	Model checking	26
3.6.5	Obfuscation	26
3.6.6	Machine learning	27
3.6.7	Composition of components	27
3.7	Applying the Fruits of Science	28
3.8	Metrics	31
3.9	The Opportunities of New Technologies	32
3.10	Experiments and Data	34
4	MODEL CHECKING	37
4.1	Brief Introduction to Spin and Promela	38
4.2	Application to Security	42
4.2.1	The Needham-Schroeder Protocol	43
4.2.2	Promela model of the protocol	45
4.3	Scaling Issues	49

4.4	Extracting Models from Code	52
4.5	Relationship to Hyper-Properties	53
5	THE IMMUNE SYSTEM ANALOGY	65
5.1	Basic Biology	65
5.2	Learning from the Analogy	68
5.2.1	The need for adaptive response	69
5.2.2	A mix of sensing modalities	70
5.2.3	The need for controlled experiments	71
5.2.4	Time scale differences	73
5.2.5	Responses to detection	74
5.2.6	Final points	75
6	CONCLUSIONS AND RECOMMENDATIONS	77
A	APPENDIX: Briefers	85

Abstract

JASON was requested by the DoD to examine the theory and practice of cyber-security, and evaluate whether there are underlying fundamental principles that would make it possible to adopt a more scientific approach, identify what is needed in creating a science of cyber-security, and recommend specific ways in which scientific methods can be applied. Our study identified several sub-fields of computer science that are specifically relevant and also provides some recommendations on further developing the science of cyber-security.

[Click here to download full PDF material](#)