



ARL-TR-9707 • JUNE 2023



Multidisciplinary University Research Initiative: Adversarial and Uncertain Reasoning for Adaptive Cyber Defense (Summary Technical Report, 2013–2021)

by Paul L Yu

Approved for public release: distribution unlimited.

NOTICES

Disclaimers

The findings in this report are not to be construed as an official Department of the Army position unless so designated by other authorized documents.

Citation of manufacturer's or trade names does not constitute an official endorsement or approval of the use thereof.

Destroy this report when it is no longer needed. Do not return it to the originator.



Multidisciplinary University Research Initiative: Adversarial and Uncertain Reasoning for Adaptive Cyber Defense (Summary Technical Report, 2013–2021)

Paul L Yu

DEVCOM Army Research Laboratory

REPORT DOCUMENTATION PAGE

1. REPORT DATE		2. REPORT TYPE		3. DATES COVERED	
June 2023		Summary Technical Report		START DATE 9/02/2013	END DATE 9/30/2021
4. TITLE AND SUBTITLE Multidisciplinary University Research Initiative: Adversarial and Uncertain Reasoning for Adaptive Cyber Defense (Summary Technical Report, 2013–2021)					
5a. CONTRACT NUMBER		5b. GRANT NUMBER		5c. PROGRAM ELEMENT NUMBER	
5d. PROJECT NUMBER W911NF1310421		5e. TASK NUMBER		5f. WORK UNIT NUMBER	
6. AUTHOR(S) Paul L Yu					
7. PERFORMING ORGANIZATION NAME(S) AND ADDRESS(ES) DEVCOM Army Research Laboratory ATTN: FCDD-RLR-EN 800 Park Office Drive Durham, NC 27703				8. PERFORMING ORGANIZATION REPORT NUMBER ARL-TR-9707	
9. SPONSORING/MONITORING AGENCY NAME(S) AND ADDRESS(ES)		10. SPONSOR/MONITOR'S ACRONYM(S)		11. SPONSOR/MONITOR'S REPORT NUMBER(S)	
12. DISTRIBUTION/AVAILABILITY STATEMENT Approved for public release: distribution unlimited.					
13. SUPPLEMENTARY NOTES ORCID ID: Paul L Yu, 0000-0003-1577-3914					
14. ABSTRACT This Summary Technical Report concerns the FY13 Multidisciplinary University Research Initiative effort titled “Adversarial and Uncertain Reasoning for Adaptive Cyber Defense: Building the Scientific Foundations,” led by Professor Sushil Jajodia at George Mason University, which was active from 1 September 2013 to 30 September 2021. The objective of the effort was to establish scientific foundations of adaptive systems that are robust, resilient, and survivable against cyber attacks and to create proactive multilevel cyber defense strategies that will minimize an attacker’s ability to understand, and to attack such systems.					
15. SUBJECT TERMS autonomous adaptive cyber defense; cyber resilience; vulnerability management; analyst scheduling; Military Information Sciences; Network, Cyber, and Computational Sciences; Summary Technical Report; STR					
16. SECURITY CLASSIFICATION OF:				17. LIMITATION OF ABSTRACT	18. NUMBER OF PAGES
a. REPORT UNCLASSIFIED	b. ABSTRACT UNCLASSIFIED	c. THIS PAGE UNCLASSIFIED			
				UU	14
19a. NAME OF RESPONSIBLE PERSON Paul L Yu				19b. PHONE NUMBER (Include area code) (301) 394-1722	

STANDARD FORM 298 (REV. 5/2020)

Prescribed by ANSI Std. Z39.18

Contents

1. Summary	1
2. Overview of Results	2
3. Knowledge Transitions and Next Steps	4
4. References	5
Appendix. Research Performance Progress Report (RPPR) Final Report	6
List of Symbols, Abbreviations, and Acronyms	7
Distribution List	8

1. Executive Summary

The Multidisciplinary University Research Initiative (MURI) effort titled “Adversarial and Uncertain Reasoning for Adaptive Cyber Defense: Building the Scientific Foundations,” led by Professor Sushil Jajodia at George Mason University, was active from 1 September 2013 to 30 September 2021. The objective of the effort was to establish scientific foundations of adaptive systems that are robust, resilient, and survivable against cyber attacks and to create proactive multilevel cyber defense strategies that will minimize an attacker’s ability to understand and to attack such systems. This topic was selected to address the MURI topic “Reduced Cyber-system Signature Observability by Intelligent and Stochastic Adaptation,” which was created to solicit multidisciplinary approaches by experts in information assurance, machine learning, adversarial modeling, game theory, control theory, behavioral science, and operations research.

The overarching contribution of this research is a new class of technologies called Adaptive Cyber Defense (ACD). The team advanced the state of the art in autonomous adaptive cyber defense by developing the scientific foundations and associated understanding of autonomous cyber operations. Specifically, the improved understanding of the role of adaptive cyber defenses paved the way for the development of next-generation autonomous cyber operations. The team developed several novel ACD mechanisms based on reinforcement learning and deep learning, advanced our understating of how stealthy attackers establish and expand their foothold within target systems, and developed the capability to ensure a predetermined level of operational effectiveness in Cyber Security Operations Centers under all adverse conditions.

The research objectives were accomplished through disciplined focus on two active but separate research areas over the course of the research program. The first area is Adaptation Techniques (ATs). The team’s research has yielded a rich repertoire of AT methods for introducing diversity and uncertainty into networks, applications, and hosts. Moreover, we have investigated the criteria for deciding where, when, and how to best employ available AT options. Such management decisions are complex due to the performance and security tradeoffs inherent in AT approaches.

The second research area is Adversarial Reasoning (AR). To address the complexity of deciding AT options, this project has harnessed a broad array of AR techniques to identify effective and stable strategies for deploying AT options in operational systems. AR combines machine learning, behavioral science,

operations research, control theory, and game theory to address the goal of computing effective strategies in dynamic, adversarial environments.

The Reduced Cyber-system Signature Observability by Intelligent and Stochastic Adaptation MURI team was led by Professor Sushil Jajodia at George Mason University with the following team members: Professor Massimiliano Albanese at George Mason University; Professor George Cybenko at Dartmouth College; Professors Peng Liu and Minghui Zhu at Pennsylvania State University; and Professors Michael Wellman, Satinder Singh Baveja, and Demosthenis Teneketzis at the University of Michigan, Ann Arbor.

During the research, the MURI team discovered two new research topics that had the potential to substantially benefit US Army cyber defense. Additional funding of \$1.0 million was provided for the team to pursue the autonomy aspects of adaptive cyber defenses and the augmentation of human cyber defenders with autonomous cyber agents. Total funding for this effort was \$7.25 million.

2. Overview of Results

From 2013 through 2021 the MURI project made efforts to advance autonomous and adaptive cyber defense to overcome the limitations of today's static cyber defenses; namely, that they are governed by slow deliberative processes involving testing, security patch deployment, and human-in-the-loop monitoring. As a result, adversaries can systematically probe target networks, preplan their attacks, and ultimately persist for long times inside compromised networks and hosts. The research objectives were accomplished through disciplined focus on two areas: AT and AR.

With AT the team developed a framework for modeling, evaluating, and countering an attacker's reconnaissance effort. Analysis of defensive strategies that control how the attacker perceives the attack surface of the target system shows that moving target defenses (MTDs) are the most effective defenses against well-designed botnets. Building on this result, the team then developed a framework to quantify MTDs and model how different MTD techniques can affect the information an attacker needs to exploit a system's vulnerability, introduce uncertainty, and reduce the likelihood of successful attacks. This framework can be used to compare sets of MTDs and to select an optimal set of MTDs that maximize security within a given budget. Address Space Layout Randomization (ASLR) is one of the most successful MTD techniques, but recent exploits have circumvented their effective application. The MURI team developed adaptive ASLR to perform direct obfuscation and block the recent exploit. Similarly, the team has developed another MTD, adaptive Data Structure Layout Randomization, that improves upon prior

work by automatically determining and applying data structure randomization to prevent adversarial manipulation and circumvention.

AR combines machine learning, behavioral science, operations research, control theory, and game theory to address the goal of computing effective strategies in dynamic, adversarial environments. The core idea is to develop a vulnerability management strategy to dynamically prioritize remediation efforts based on available resources and severity of the exposed vulnerabilities. The team developed models to optimize static and dynamic scheduling of cybersecurity analysts. The models allow managed risk under a predetermined upper bound. The team then developed a vulnerability management strategy to dynamically prioritize defensive remediation efforts based on available resources and severity of the exposed vulnerabilities. The team also developed adaptive cyber defenses based on reinforcement learning and deep learning approaches that push the boundary of existing autonomous cyber defense capabilities, including algorithms for autonomous cyber defense where attacker and defender are both adapting or where adversaries perform multistage attacks.

Key Discoveries and Accomplishments

1. The team developed a framework for modeling, evaluating, and countering an attacker's reconnaissance effort enables the assessment of defensive measures against intelligent attackers for cost and efficacy.¹
2. The team developed a framework to model how different MTD techniques can affect the information an attacker needs to exploit a system's vulnerability, introduce uncertainty, and reduce the likelihood of successful attacks.²
3. The team developed and analyzed models to optimize scheduling of cybersecurity analysts and compute the right mix of analyst expertise and assignments to improve the effectiveness of cyber defense.³
4. The team devised a vulnerability management strategy to dynamically prioritize defense mechanisms based on available resources and severity of the exposed vulnerabilities.⁴

3. Knowledge Transitions and Next Steps

The MURI team has produced more than 180 peer-reviewed journal articles, conference presentations, and books, with three best-paper awards; trained 18 new PhDs, with one dissertation award; and engaged in numerous Army programs, including the US Army Combat Capabilities Development Command (DEVCOM) Army Research Laboratory's (ARL's) Cyber Security Collaborative Research Alliance, ARL's International Technology Alliance, and internal ARL projects with numerous joint publications with ARL scientists.

The fundamental discoveries from this MURI will provide the basis for potential future cyber defenses that autonomously adapt to changing environments and intelligent attackers. Through further study, these frameworks and models for limiting attacker knowledge and improving defensive strategies could be adapted to applications in security operation centers (SOCs) to deliver dominant and robust cyberspace defensive capabilities.

This MURI and its investigators laid the foundation for autonomous adaptive cyber defense. The improved understanding of the role of adaptive cyber defenses paved the way for the development of next-generation autonomous cyber operations to ensure SOC effectiveness under all adverse conditions. Another enduring outcome of this MURI is the notion of cyber resiliency that quantifies the ability of a cyber system to return to some level of desired performance after a degradation of that performance (e.g., through adverse conditions effected by the adversary). ARL, the US Army Corps of Engineers (USACE), and the Office of the Under Secretary of Defense for Research and Engineering have been maturing this notion to develop operationally measurable and meaningful resilience concepts that can be empirically determined in an objective manner. In 2023, authors from ARL and USACE wrote the report, *Cyber Efficiency and Cyber Resilience* to highlight recent progress.⁵

4. References

The following are references cited in this STR; a complete list of publications from this project appears in the Appendix.

1. Sugrim S, Venkatesan S, Youzwak JA, Chiang C-YJ, Chadha R, Albanese M, Cam H. Measuring the effectiveness of network deception. Proceedings of the IEEE International Conference on Intelligence and Security Informatics; 2018. p. 142–147. doi: 10.1109/ISI.2018.8587326.
2. Xu J, Guo P, Zhao M, Erbacher RF, Zhu M, Liu P. Comparing different moving target defense techniques. Proceedings of the First ACM Workshop on Moving Target Defense (MTD '14); 2014. Assoc for Comput Mach. p. 97–107. doi: 10.1145/2663474.2663486.
3. Ganesan R, Jajodia S, Shah A, Cam H. Dynamic scheduling of cybersecurity analysts for minimizing risk using reinforcement learning. ACM Trans Intel Sys Technol. 2016;8:1–21. doi: 10.1145/2882969.
4. Farris KA, Shah A, Cybenko G, Ganesan R, Jajodia S. VULCON: a system for vulnerability prioritization, mitigation, and management. ACM Trans Priv Secur. 2018 Nov;21(4):1–28. doi: 10.1145/3196884.
5. Linkov I, Ligo A, Stoddard K, Perez B, Strelzoffx A, Bellini E, Kott A. Cyber efficiency and cyber resilience. Commun ACM. 2023 Apr;66(4):33–37. doi: 10.1145/3549073.

Appendix. Research Performance Progress Report (RPPR) Final Report

This appendix appears in its original form, without editorial change.

List of Symbols, Abbreviations, and Acronyms

ACD	Adaptive Cyber Defense
AR	Adversarial Reasoning
ARL	Army Research Laboratory
ASLR	Address Space Layout Randomization
AT	Adaptation Technique
DEVCOM	US Army Combat Capabilities Development Command
MTD	moving target defense
MURI	Multidisciplinary University Research Initiative
RPPR	Research Performance Progress Report
SOC	security operation center
STR	Summary Technical Report
USACE	US Army Corps of Engineers

1 DEFENSE TECHNICAL
(PDF) INFORMATION CTR
DTIC OCA

1 DEVCOM ARL
(PDF) FCDD RLB CI
TECH LIB

1 DA HQ
(PDF) DASA(R&T)

8 USARMY AFC
(PDF) L BROUSSEAU
A LINZ
K WADE
S BRADY
J REGO
T KELLY
E JOSEPH
B SESSLER

2 DEVCOM HQ
(PDF) FCDD ST
C SAMMS
M HUBBARD

81 DEVCOM ARL
(PDF) FCDD RLA
C BEDELL
B SADLER
A SWAMI
M GOVONI
M WRABACK
H EVERITT
J CHEN
P FRANASZCZUK
C TEETER
A SCHOFIELD
J LANE
FCDD RLA A
S KARNA
J NEWILL
AM RAWLETT
SE SCHOENFELD
FCDD RLA B
A WEST
FCDD RLA C
C OLIVER
G BRILL
G LARKIN
FCDD RLA CA
J FOSSACECA
FCDD RLA CB
P GILLICH
FCDD RLA CC

C KRONINGER
FCDD RLA CD
J ROBINETTE
FCDD RLA CL
F FRESCONI
FCDD RLA CG
D STRATIS-CULLUM
FCDD RLA CH
B PERELMAN
FCDD RLA CV
M KWEON
FCC RLA D
J ALEXANDER
FCDD RLA F
J GASTON
FCDD RLA G
ML REED
FCDD RLA H
J SUMNER
FCDD RLA I
D WIEGMANN
FCDD RLA J
B PIEKARSKI
FCDD RLA L
RD DEL ROSARIO
FCDD RLA N
BM RIVERA
FCDD RLA P
WL BENARD
FCDD RLA PD
F FATEMI
FCDD RLA T
RZ FRANCART
FCDD RLA V
S SILTON
FCDD RLA W
T SHEPPARD
FCDD RLB
J ZABINSKI
FCDD RLB R
S STRANK
FCDD RLB RN
C QUIGLEY
FCDD RLB RW
P KHOOSHABEH
FCDD RLB S
K KAPPRA
J VETTEL
FCDD RLD
PJ BAKER
A KOTT
K JACOBS
FCDD RLD A
A MOGRO

FCDD RLD C
T KINES
FCDD RLD D
T ROSENBERGER
FCDD RLD I
A FINCH
A LLOPIS-JEPSEN
D ROLL
S SHIDFAR
D KELLEY
FCDD RLD M
N ZANDER
R MURRAY
FCDD RLR
B HALPERN
S LEE
P REYNOLDS
K RASMUSSEN
FCDD RLR A
D STEPP
FCDD RLR C
LL TROYER
FCDD RLR D
R ZACHERY
FCDD RLR DS
R FREED
FCDD RLR E
RA MANTZ
FCDD RLR EF
F GREGORY
FCDD RLR EG
H DE LONG
FCDD RLR EH
V MARTINDALE
FCDD RLR EI
SP IYER
FCDD RLR EL
J QIU
FCDD RLR EM
C VARANASI
FCDD RLR EN
JM COYLE
P YU
FCDD RLR EP
PM BAKER
FCDD RLR ET
B ASHFORD
FCDD RLR EW
JD MYERS
FCDD RLR G
A SCRUGGS