No Free Lunch in Cyber Security

George Cybenko

gvc@dartmouth.edu

Jeff Hughes

jeff.hughes@tenet3.com

MTD Workshop

Scottsdale AZ

November 3, 2014

THAYER SCHOOL OF ENGINEERING AT DARTMOUTH

Acknowledgements

- Kate Farris, Ph.D. Student, Dartmouth
- Dr. Gabriel Stocco*, Microsoft
- Dr. Patrick Sweeney*, US Air Force, AFRL

- ARO, AFRL, DOD funding

* former Ph.D. students

Goals of this talk

- Identify tradeoffs among MTD's
- Encourage discussion
- Stimulate the work at the workshop

Basic Message

There are tradeoffs when using MTD's in real systems

- What are the tradeoffs?
- How can they be modeled and measured?
- How can MTD's be deployed with respect to those tradeoffs to be most useful?

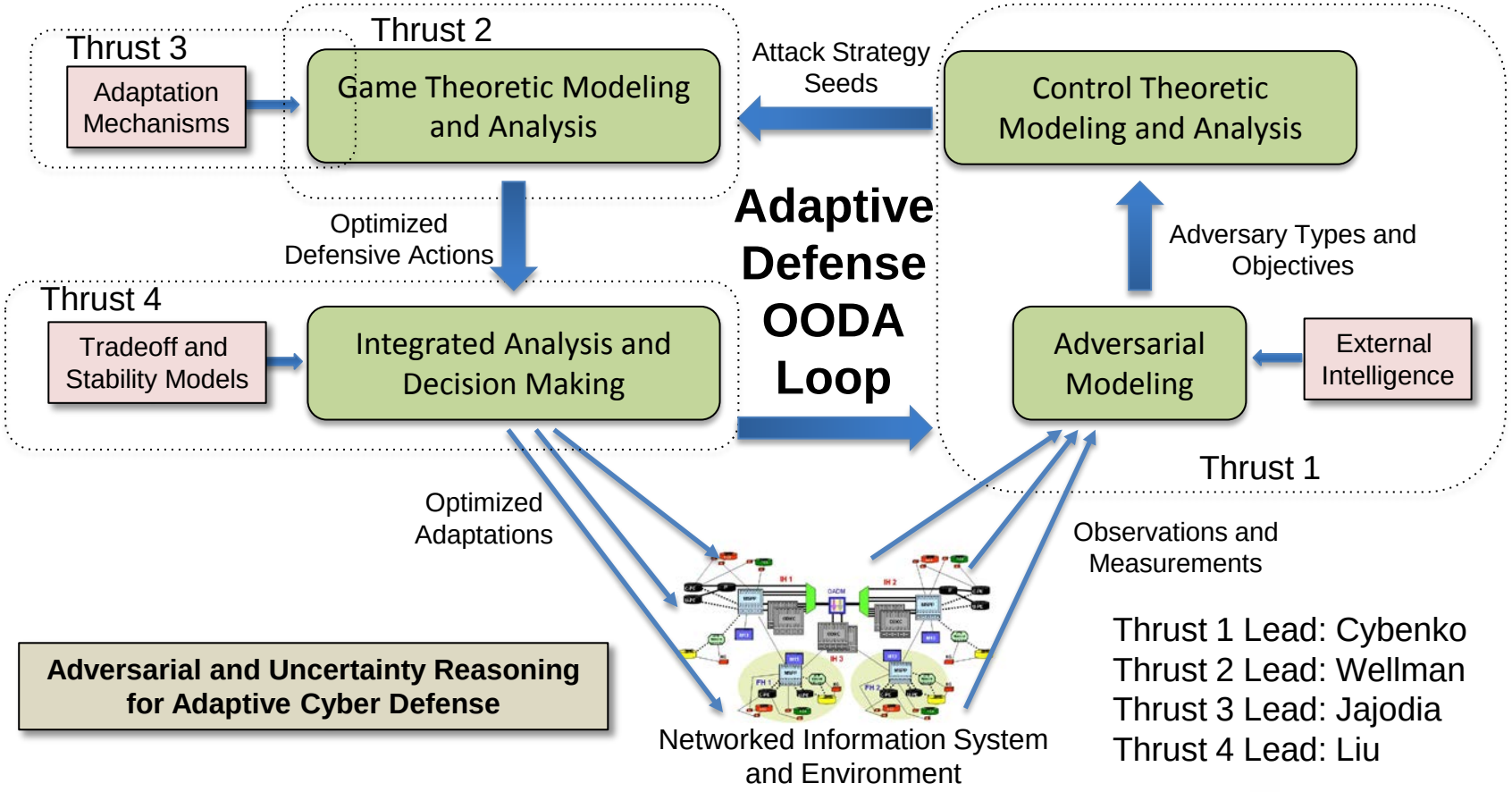
"Don't believe a weather report made by someone selling umbrellas." - This is where we are now.

Context

- MTD is a “hot” security technology
  - NITRD security focus area
  - DARPA programs (eg, CFAR)
  - MURI topics (eg 2013 ARO)
  - etc, etc
- Making MTD operationally useful/attractive
- Many good security concepts never get used

Ongoing Effort 2013 ARO MURI

Adversarial and Uncertainty Reasoning for Adaptive Cyber Defense



Thrust 1 Lead: Cybenko
Thrust 2 Lead: Wellman
Thrust 3 Lead: Jajodia
Thrust 4 Lead: Liu

George Mason, Dartmouth, Michigan, Penn State, (UMD)

"Adaptive Cyber Defense"

=

Moving Target Defense Techniques

+

Control and Game Theoretic Reasoning

THAYER SCHOOL OF ENGINEERING AT DARTMOUTH

Control and Game Theoretic Reasoning

Strategic Level: Which MTD's to develop

Operational Level: Which MTD's to use in a specific configuration/mission

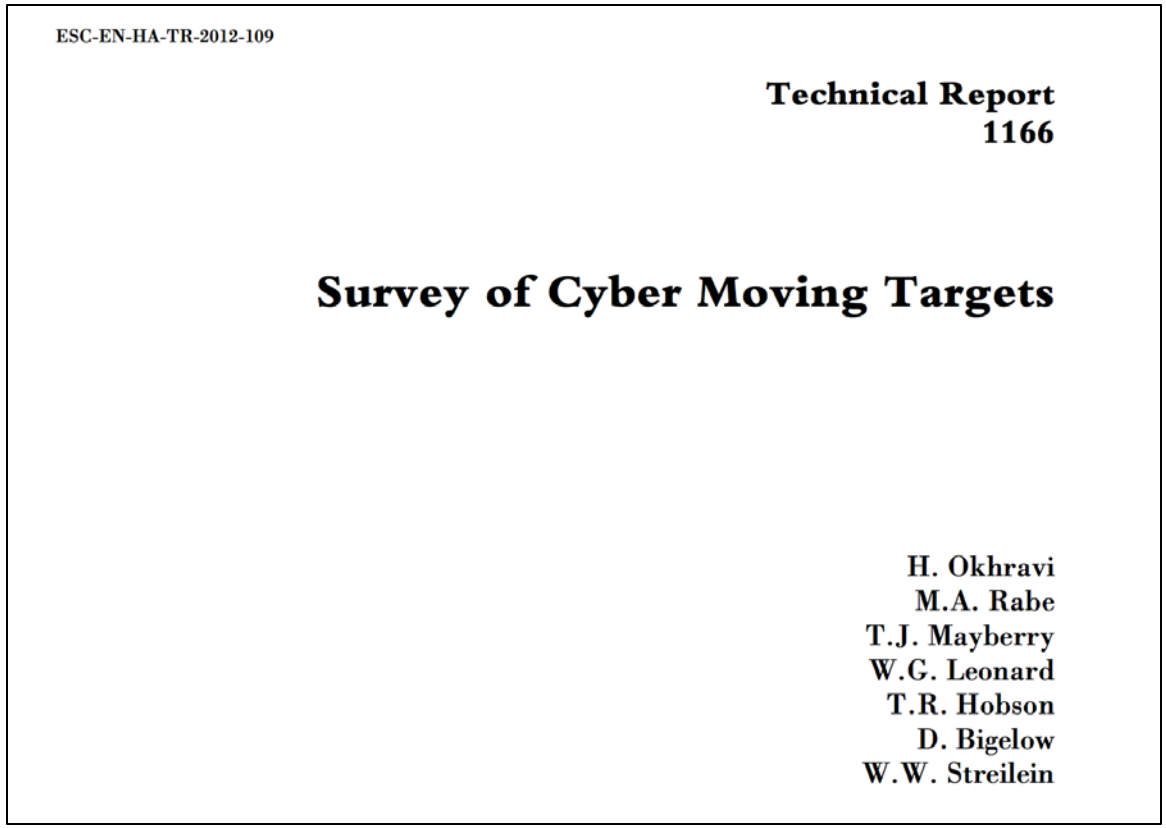
Tactical Level: How to deploy an MTD dynamically

Requires orderings of MTD costs/utilities for both attackers and defenders

Cybenko & Wellman, 2009 DARPA ISAT Study

THAYER SCHOOL OF ENGINEERING AT DARTMOUTH

There are many MTD ideas…



ESC-EN-HA-TR-2012-109

Technical Report 1166

Survey of Cyber Moving Targets

H. Okhravi
M.A. Rabe
T.J. Mayberry
W.G. Leonard
T.R. Hobson
D. Bigelow
W.W. Streilein

At least 39 documented in this 2013 MIT Lincoln Labs Report

>50 today?

How can we compare them?

THAYER SCHOOL OF ENGINEERING AT DARTMOUTH

Possible MTD Evaluation Techniques

	Analytics (Math or Data)	Testbed Network	Simulations	Red Teaming	Expert Surveys or Elicitations	Operational Network
Effectiveness	✔ M	o	o	✔	o	o
Implementation Costs	✔ M + D	o	✕	✕	o	✔
Performance Costs	✕	✔	o	✕	o	✔
Usability	✕	✕	✕	✕	o	✔
Security Priority	✔ D	✕	✕	✔	✔	✕

Good Sometimes Bad

M – Math based **D** – Data based

MTD Properties (rows)

- Effectiveness: The increase in adversary workload
- Implementation Costs: Cost to deploy in an enterprise
- Performance Costs: Host and network overhead
- Usability: Administrator and end-user effort to administer and use
- Security Priority: Importance of the attack surface addressed

Evaluation Techniques (columns)

- Analytics (Math or Data): A mathematical (M) or data analysis (D) approach to quantifying an MTD approach
- Simulations: High-level models of systems, workloads and traffic used to estimate metrics through simulation
- Testbed Network: Systems, workloads and traffic realized in an isolated network and instrumented to estimate metrics during actual runs
- Red-Teaming: Experts test cyber defenses on a operational or testbed network to find and exploit vulnerabilities
- Expert Surveys: Soliciting technical experts opinions and insights using descriptions, not simulations or testbeds
- Operational Network: Actual network used in an operational setting

THAYER SCHOOL OF ENGINEERING AT DARTMOUTH

Possible MTD Evaluation Techniques

	Analytics (Math or Data)	Testbed Network	Simulations	Red Teaming	Expert Surveys or Elicitations	Operational Network
Effectiveness	✔ M	o	o	✔	o	o
Implementation Costs	✔ M + D	o	✕	✕	o	✔
Performance Costs	✕	✔	o	✕	o	✔
Usability	✕	✕	✕	✕	o	✔
Security Priority	✔ D	✕	✕	✔	✔	✕

Good Sometimes Bad

M – Math based **D** – Data based

The Competitive Exclusion Principle

"No stable equilibrium can be attained in an ecological community in which some *r* components are limited by less than *r* limiting factors. In particular, no stable equilibrium is possible if some *r* species are limited by less than *r* factors".

S. A. Levin. Community equilibria and stability, and an extension of the competitive exclusion principle. American Naturalist, 104:413–423, 1970.

Computing Example (OS's)

Three limiting factors

- Implementation Costs
- Performance Costs
- Usability

Three species

- Windows (Implementation Costs)
- Linux (Performance Costs)
- Mac OS (Usability)

MTD Implications

What are the limiting factors?

- Implementation Costs
- Performance Costs
- Usability
- Vulnerabilities mitigated (multiple)

How many and which “species” of MTD’s?

- ASLR
- ?
- ?

Workshop Questions - 1

- How we compare MTD's against each other?
- What do we compare?
- Will it be "objective"?
- Will only a handful survive? (= number of limiting factors)

THAYER SCHOOL OF ENGINEERING AT DARTMOUTH

Types of Diversity in MTD's

Harder

Natural Diversity (Macroscale)

EG: Different communication technologies

Pseudo Diversity (Mesoscale)

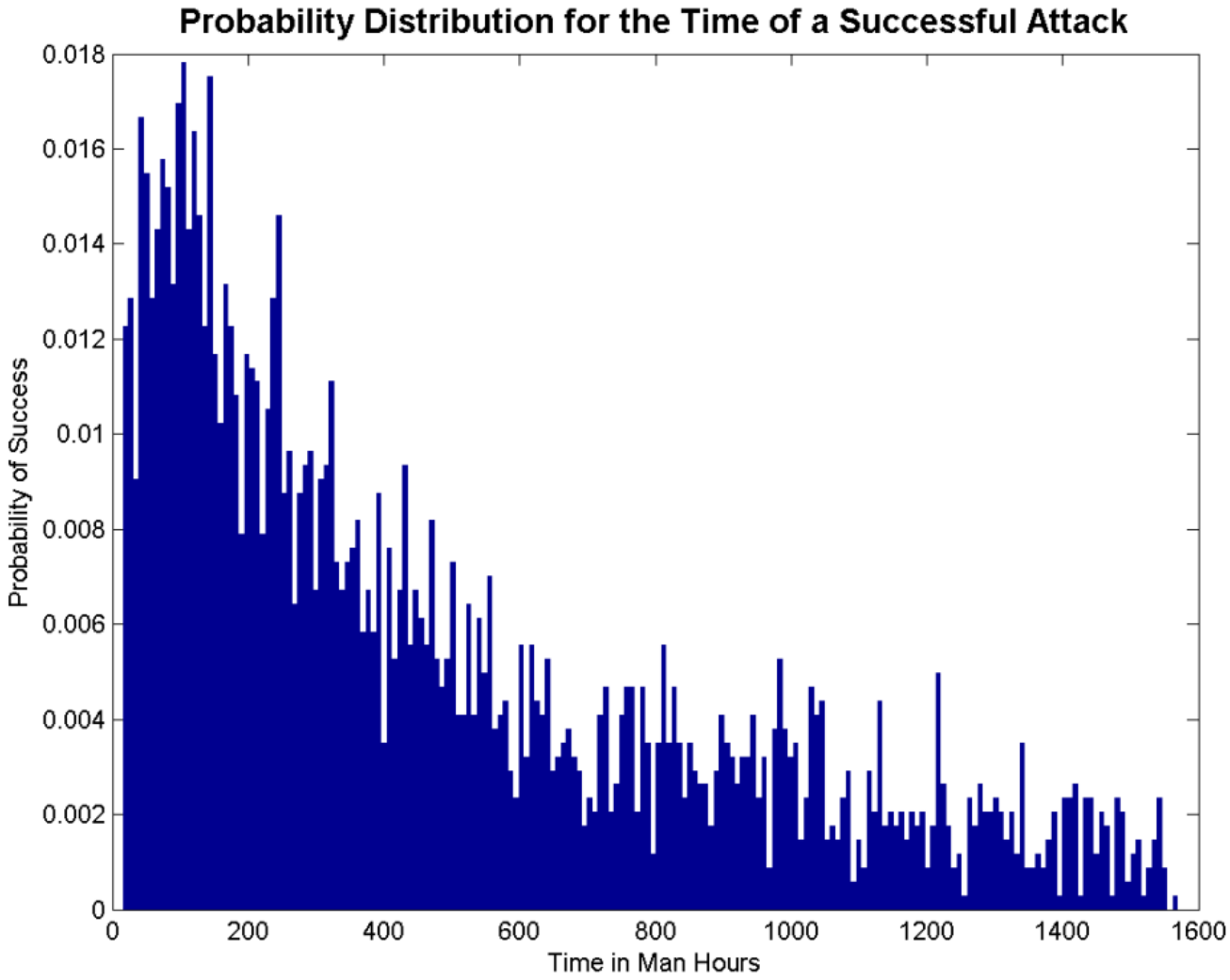
EG: Different implementations of one protocol

Artificial Diversity (Microscale)

EG: Randomization of one implementation

THAYER SCHOOL OF ENGINEERING AT DARTMOUTH

The Time-to-Compromise Metric



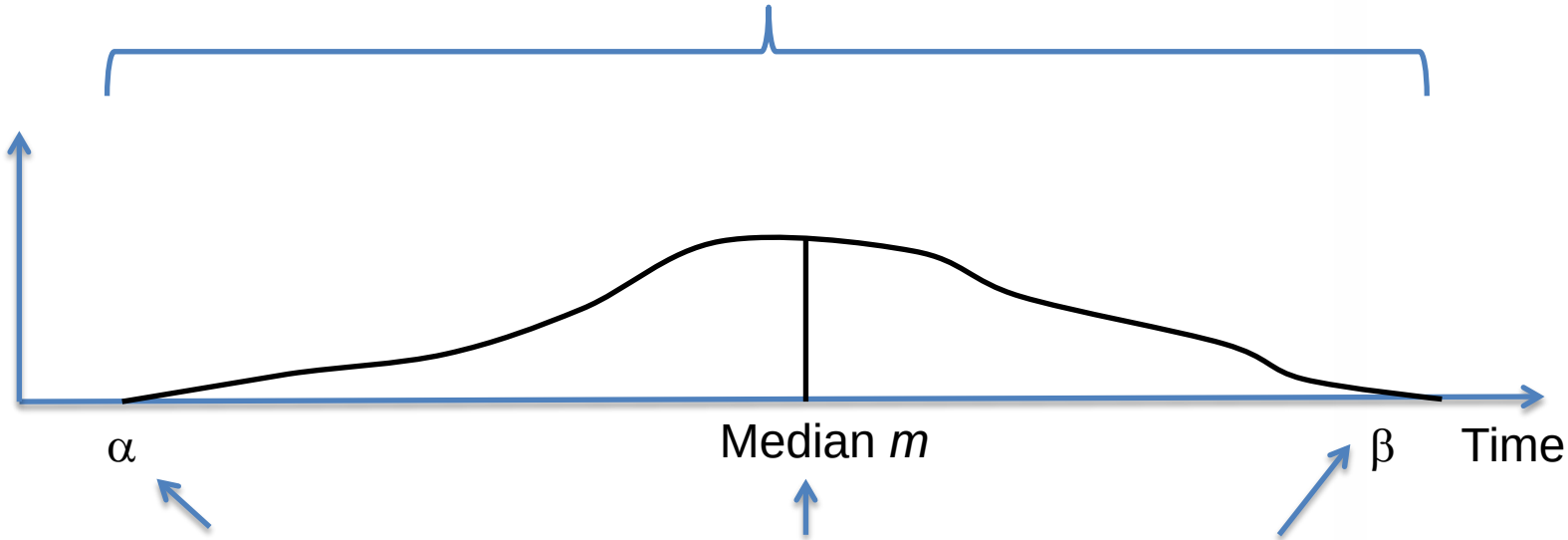
See “QuERIES”, Carin, Cybenko and Hughes, IEEE Computer, August 2008.

Cybenko, Hughes http://timreview.ca/article/712, 2013.

THAYER SCHOOL OF ENGINEERING AT DARTMOUTH

Implications for the Different CIA Security Goals

As the number of replicated Artificial Diversity components or services increases, the time to defeat the different CIA goals fills out the support of *f(t)*



Time to defeat confidentiality by *n* attackers approaches α

Time to defeat integrity by *n* attackers approaches *m*

Time to defeat availability by *n* attackers approaches β

See workshop paper, “No Free Lunch in Cyber Security”

Workshop Question - 2

- Which MTD's offer real advantages against Confidentiality attacks (a single system compromise) when there are many determined attackers?
- How fast does an MTD have to "move"?
- Do we need different types of MTD's to protect against each one of Confidentiality, Integrity and Availability attacks?

Discussion

Workshop Questions - 1

- How we compare MTD's against each other?
- What do we compare?
- Will it be "objective"?

Workshop Question - 2

- Which MTD's offer real advantages against Confidentiality attacks (a single system compromise) when there are many determined attackers?
- How fast does an MTD have to "move"?
- Do we need different types of MTD's to protect against each one of Confidentiality, Integrity and Availability attacks?