CYBER WARFARE SIMULATION TO PREPARE TO CONTROL CYBER SPACE

Martin R. Stytz, Ph.D.

UMUC / Georgetown

mstytz@att.net , *mstytz@mstytz.com* , *mstytz@drexel.edu*

Sheila B. Banks, Ph.D.

Calculated Insight

sbanks@calculated-insight.com

Introduction

- Cyber warfare
  - Controls information flow
  - Targets information used to determine situational awareness and make decisions
- Cyber warfare simulation
  - Prepares decision-makers for information challenges
- Cyber space domination
  - Ensures accurate, trustworthy, relevant information presented to decision-maker

Background

- Cyber space
  - Data
  - Computing Technologies
  - Informational Analysis/Comprehension Technologies
  - Information Interaction/Management Technologies
- The opposing commander's mind is an important target and successfully striking it can provide a decisive advantage
- Cyber space technology requirements
  - Movement of information in the space
  - Shared Situational Assessment
  - Virtual Machine Approaches

Motivation

- Achieving cyberspace dominance is crucial, enables confident decision-making
- Must prepare decision-makers to:
  - Determine the targets of attacks
  - Operate effectively despite cyberattack
  - Determine difference between a fault and attack
  - Know the defensive techniques that are likely to be effective
- To perform properly, cyber event simulation components must exchange information about the defense, event, and response

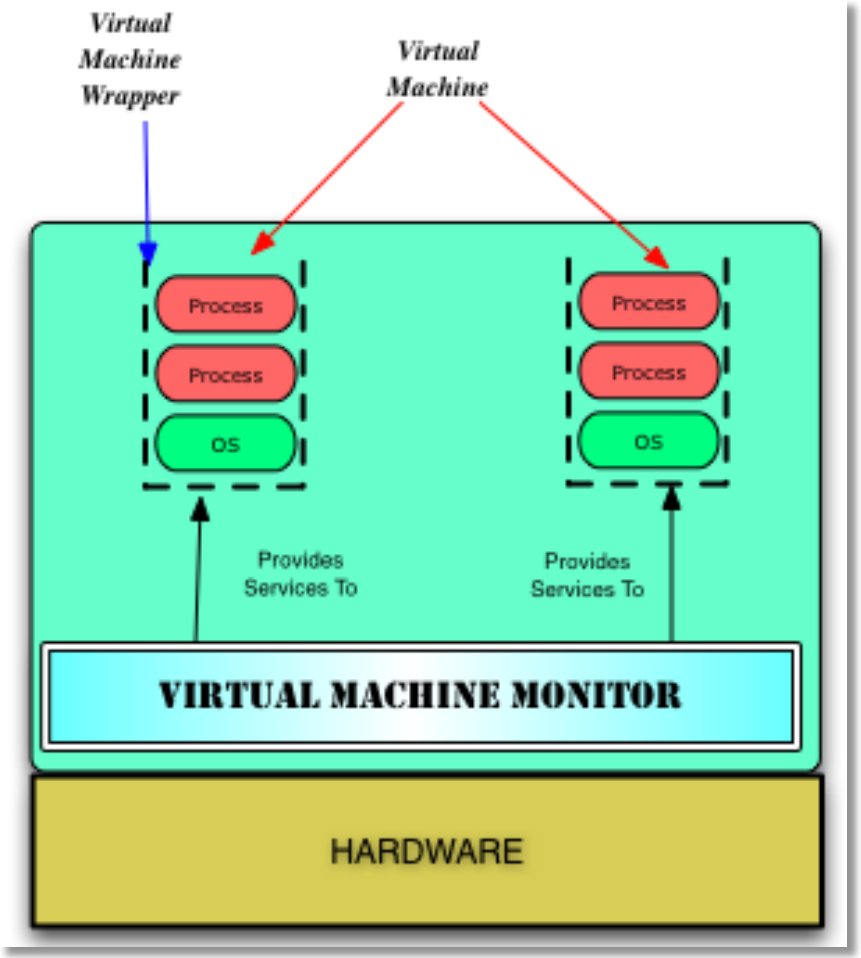
Movement of information

- Organizational information movement
  - Important in development of situational awareness
  - Network centric organizations have two sets of information:
    - Sources of data
    - Recipients of data
    - Cyberattacks target both

Shared Situational Assessment

- Definition of situational assessment (Endsley)
  - Perception
    - What are the facts
  - Comprehension
    - Understanding the facts
  - Projection
    - Anticipation based upon understanding
  - Prediction
    - Evaluation of outside forces that may act upon to effect your projections

Virtual Machine Approach



Cyber Warfare Simulation

- Simulation provides a safe and flexible teaching method
- Prepares decision-makers for cyber attacks
  - Challenges to re-assess data protection
  - Cyber warfare defenses
- Cyber warfare training goals
  - How to determine targets of attack
  - Techniques and tactics used against targets
  - Techniques and tools to use to counteract each attack and the attacks effect
  - Explicitly assessing information value to protect the highest value information in the environment

Cyber Warfare Simulation Approach

- Successful cyber warfare simulation needs only to alter the information presented to the user
- Three basic approaches
  - Increase in information presented
  - Blocking information needed by users
  - Substituting false information for actual information
- Cyber warfare simulation systems
  - Determine if a cyber attack is successful
  - Determine the effect of the cyber attack
  - Portray defensive responses

Cyber Warfare Simulation

- At each simulation step the decision-maker is provided
  - Cyber attack and defensive activities
  - Status of the attack
  - Information behaviors that mirror information delays
  - Alterations in cyber warfare environment
- Cyber simulators also communicate (machine-to-machine)
  - Types and variations of cyber attack simulated
  - Defensives that are present
  - Cyber attack success rate

Cyber Attack Effectiveness

- Protection of cyber space is the goal

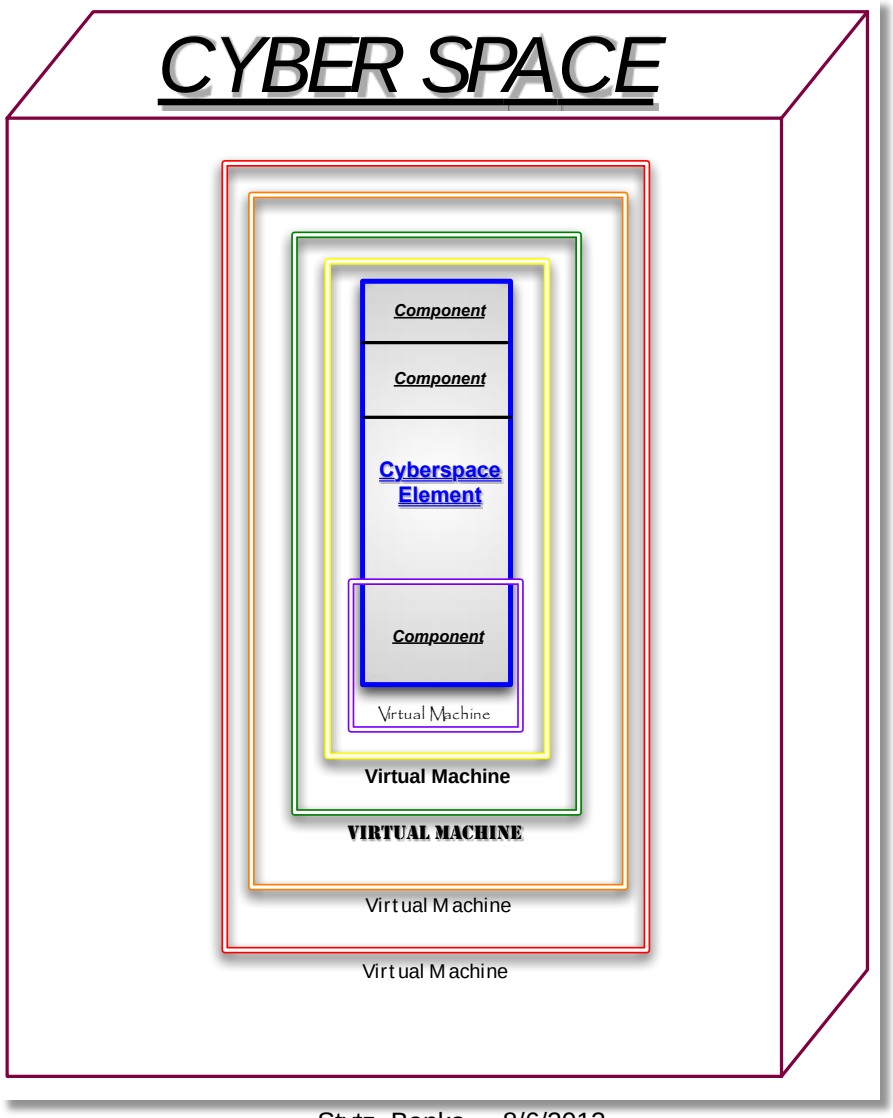
- Cyber space simulation environment allows decision-makers to protect cyber space
  - Prioritize information
  - Prioritize elements of the cyber space
  - Operate in cyber environment where elements are corrupted/compromised

Goals

- Cyber defensive goals
  - Make defeating a cyber defense difficult
  - Provide cyber defenders with dynamic defenses
  - Provide a foundation for rapid detection of cyber attacks
  - Provide successful operation despite an information breach
  - Provide rapid recovery from cyber penetration/compromise

Active Cyber Defense

- Dynamic Layered Cyber Defense



Conclusion

- Decision-makers must experience the ever increasing complexity of cyber space attacks without real-world risk
- Cyber warfare training
  - Human assessment and judgment are necessary
  - Important in situational awareness
  - Correlate disparate activities into insight with technological advancements
- Future activities
  - Advancing cyber battle understanding
  - Advancing human behavior modeling
  - Advancing decision-making and situational awareness within large-scale and high-volume data environments

Future Work

- Develop a comprehensive cyberwarfare opposing force that can be generated automatically
- Develop and test defensive strategies against bot attacks
  - The key measure is the quality of the decisions that are made
- Develop an autonomous, intelligent cyber battlespace red team for defense evaluation and attack support
  - However, need improved understanding of human behavior, reasoning, knowledge acquisition, intent reasoning, data mining, and use within a cyber battlespace

Background (2)

- **Bots are an *amalgam technology***
  - Use any technology, and change technologies at will
  - Essentially - large, distributed, secure clouds
  - Worm technology is a means for bot software to move through the internet
  - Trojan technology to hide
  - Backdoors for software updates and herder access/ exfiltration
  - Rootkits to hook and insure the bot runs at every boot-up
  - Virtualization
- **Found and developed worldwide**