CYBER SECURITY: WHO IS WORRYING ABOUT T&E?

Test & Evaluation to Meet the Advanced Persistent Threat
International Test and Evaluation Association

John B. Foulkes, Ph.D.
(Teacher/Consultant/Grandfather/(Very Recent) Great Grandfather)
November 29, 2012

Cyber Security: The Problem

- *This country's critical infrastructure (power plants, bridges, hospitals, financial institutions) are at risk to exploitation, disruption and even destruction by our adversaries through cyber-attacks.*
- *Our systems are easily penetrated; once penetrated, cleanup is expensive and time consuming; and if one system can be penetrated, all can be.*
- *Stuxnet, Flame, Duqu, etc., etc., etc.*
- *Etc.*
- *Etc.*

OK, we get the message

The Prevailing Philosophy

- "Defense in Depth": A common approach to deterrence
  - Pile on layers and layers of defenses (sometimes making things worse), in the hope that any and all types of penetration can be prevented.
    - This is more like "Failure in Depth".
  - ***As one DARPA program manager put it recently: "Our current mentality is P^{4}I: "Perimeter Protection, Patch, and Pray"***
    - *The "I" stands for the intrusion that always follows"!*

- Any solution short of complete denial of intrusion is not acceptable.

The testing of any "solution", whatever it may be, has not been given adequate attention.

Message

- **We need to seriously start thinking about testing in the Cyber Domain**
  - **Policy**
    - We have a lot of policy already……
    - ***Kratznicki's Law: Compliance with policy is inversely proportional to the amount of policy to be complied with.***
  - **Methodology**
    - Adapt/translate from the traditional domains into the Cyber Domain, but…….
    - Operations in Cyber Space do not translate well from conventional operations.
      - The avenues of approach for an adversary are wide.
      - In conventional operations, we can study the terrain and know where the enemy can and can't go.
      - Not so in Cyber Space: if the terrain exists, it is passable.
  - **Infrastructure**

Zero Day: "A virtual battleground for Pentagon's cyber warriors" Washington Post, November 27, 2012 (Robert O'Harrow Jr.)

- Researchers use virtual cities to develop cyber defenses
  - CyberCity
    - *"One of **hundreds** of virtual environments – often known as cyber ranges" or test beds – launched in recent years by military, corporate , and academic researchers to confront the mind-bending security challenges posed by cyberspace……"*
  - DARPA's "National Cyber Range"
  - DoD's "Information Assurance Range"
  - Cyber range at Eastern Michigan University – Merit Network, Inc.
  - Cyber ranges run by Northrup Grumman
  - Defense Technology Experimental Research (DETER) project

Efforts are primarily research-focused, using Constructive and Virtual environments

Navigating a Way Forward……

- Academia and industry provide the inertia
- Feasible products emerge
- Understanding the operational environment
- Characterizing and replicating the threat(s)
- Building the right “sand box”
  - The proliferation of “cyber ranges” is astounding
    - The term cyber range is misapplied
    - Rather, range (or ranges) that can test system capabilities within the cyber domain….
  - Research, development, testing, training, and operations should be interwoven
  - Distributed L-V-C capabilities: reconfigurable; persistent
- Use cases
- Goal: Conducting no-kidding test/training events in a realistic than support acquisition decisions

The Academic Contribution: Understanding the "physics" of system/network intrusion

- Behavior of systems (hardware software, people) in networks has a rich mathematical foundation.
  - Modeling the human
  - Statistical techniques applied to stochastic processes
  - Current University-level research using:
    - Variable Length Markov Models (VLMMs)
    - Hidden Markov Models (HMM)s
    - Partially Observable Markov Decision Processes (POMDPs)
    - Bayesian Networks
  - All help provide better insight into pattern recognition; in predicting attacks and their outcomes, assessing the probability of penetration and determining the risk of disruption or destruction of the system.

Recently Published Research

- *"Projecting Cyber-attacks Through Variable-Length Markov Models";* Daniel S. Fava, Stephen R. Byers*, Student Member, IEEE*, and Shanchieh Jay Yang*, Member, IEEE*
  - Presents a VLMM that captures the sequential properties of attack tracks, allowing for the prediction of likely future actions on ongoing attacks; it is able to adapt to newly observed attack sequences without requiring specific network information.

- *"Robustness of the Markov-Chain Model for Cyber-Attack Detection";* Nong Ye*, Senior Member, IEEE*, Yebin Zhang, and Connie M. Borror
  - Presents a cyber-attack detection technique through anomaly-detection, and discusses the robustness of the modeling technique employed. In this technique, a Markov-chain model represents a profile of computer-event transitions in a normal/usual operating condition of a computer and network system (a norm profile).

Recently Published Research

- *"Methods to Window Data to Differentiate Between Markov Models"*; Jason M. Schwier, Richard R. Brooks, *Senior Member, IEEE*, and Christopher Griffin, *Member, IEE*
  - Uses statistical pattern matching calculations performed on a sliding window of data samples to detect changes between behaviors.

- *"Behavior Detection Using Confidence Intervals of Hidden Markov Models";* Richard R. Brooks, *Senior Member, IEEE*, Jason M. Schwier, and Christopher Griffin, *Member, IEEE*
  - Uses confidence intervals for HMM analysis; enables consideration of the number of data samples available when comparing an HMM model with a sensor data stream; uses a novel approach in applying receiver operating characteristic (ROC) curves to find detection thresholds when confidence intervals are used.

Summary

Bottom Line:

- Efforts to completely deny adversarial intrusion are resource prohibitive.
- Attention must be given to testing cyber products in a realistic, operational environments.

Next Steps:

- Identify the key, critical components of infrastructure (starting with DoD networks and architectures
- Use Markov model theory (HMMs, VMMs) to develop algorithms for understanding and bounding the probabilities of adversarial intrusion.
- Soliciting product developers.
- Adapting the existing L-V-C capabilities to serve as operational research and testing “sand boxes”.