11-15-2010

CyberSMART: Cyber Scenario Modeling and Reporting Tool

Kenneth Reese

James Marshall

Dennis McGrath

Reese, Kenneth, James Marshall, and Dennis McGrath. 2012. "CyberSMART: Cyber Scenario Modeling and Reporting Tool." Paper presented at IEEE International Conference on Technologies for Homeland Security, Waltham, MA, Nov. 13-15.

CyberSMART™: Cyber Scenario Modeling and Reporting Tool

Kenneth Reese, James Marshall
Space Dynamics Laboratory
Logan, Utah
{Kenneth.Reese, Jim.Marshall}@sdl.usu.edu

Dennis McGrath
Norwich University Applied Research Institutes
Northfield, Vermont
dmcgrath@norwich.edu

***Abstract*—The Cyber Scenario Modeling and Reporting Tool (CyberSMART™) is a Web-based, scalable, collaborative tool developed under the Department of Homeland Security Science and Technology (DHS S&T) directorate that enables a cyber exercise planning team to research, organize, enter, and edit critical exercise background information. It is built specifically to address some of the unique challenges that are encountered in the design and execution of exercises containing major cyber elements. It allows the exercise planning team to develop and validate scenario elements to ensure that they are logical, that they do not conflict with each other, and that they meet the specific objectives of each exercise. The CyberSMART™ Exercise Execution Engine (EEE) provides exercise conduct teams with a mechanism for delivering individual injects from the master scenario events list (MSEL) to exercise participants. It creates an immersive environment in which participants can build situational awareness based on indicators and warnings extracted from the scenario events. Participants provide responses to threats as they are identified. Responses are based upon organizational strategies and can be analyzed in after action review.**

Keywords-cyber exercise; scenario development; conduct management

I. INTRODUCTION

Critical infrastructure providers in all public and private sectors are growing increasingly dependent upon sophisticated, interdependent information systems to provide services that are essential to the functioning of the American economy and society. These systems are more commonly being connected to larger networks and to the Internet. Each of these IT resources, while indispensable, provides a potential attack vector through which critical data and business continuity can be compromised.

Because of our nation's dependence upon critical infrastructure providers, and because of the important role cyber assets play in their respective business models, a disruption to the information infrastructure of any one of these organizations threatens the security of the United States, and requires a well-developed and thoroughly rehearsed response doctrine. Cyber incident response plans can be developed, refined, and tested through training activities and exercises similar to what has been done for traditional emergency response teams; but such preparedness exercises must reflect plausible cyber events that could occur on existing information infrastructure. These exercises should also have appropriate time dedicated to after action review (AAR) such that participants can verify whether organizational incident response plans were followed, assess whether these plans were effective, and investigate what alternative actions could have led to a more favorable outcome if applicable. Exercises following this format allow for evaluation and objective assessments of current policies and procedures, and help organizations fortify their critical infrastructure and prepare for actual cyber interruptions.

II. BACKGROUND

In Mr. Marshall's introduction of the Cyber Scenario Modeling and Reporting Tool (CyberSMART™) to the Cybersecurity Applications & Technology Conference for Homeland Security [1], the case was made that cyber exercises require a unique, detailed process for collecting, organizing, and incorporating data into a credible exercise scenario. Today's critical infrastructure is increasingly complex, inter-reliant, and controlled by information technology that is almost always connected to the Internet. In a cyber exercise, the "playing field" is a series of complex networks of information systems that control our critical infrastructures. Within those networks, a diverse collection of computers, routers, and control systems enable electronic transactions that are essential to business and government continuity. These networks, largely owned by the private sector, are difficult to characterize even by the people who keep them running on a daily basis. Because cyber exercises fundamentally involve complex, geographically dispersed IT systems, background knowledge of each participating organization's information technology assets, and the electronic transactions supported by those assets, is requisite to the creation of a compelling, meaningful exercise scenario. This technical content, which we refer to as the "gamespace" of the exercise, must be organized in a coherent way that provides value and validity to the exercise.

Additionally, unlike traditional emergency response exercises, most cyber exercises require the voluntary participation of a variety of organizations from the public, private, and academic sectors. A cyber exercise planning team must give careful consideration to the diversity of participants and their differing IT assets, monitoring methods, and response doctrines. The exercise master scenario events list (MSEL) must be developed such that it presents a clear, reasonable

DHS Science and Technology Directorate

scenario to participants, and each event can be easily mapped back to organizational and exercise objectives.

Once a cyber exercise has been planned, an immersive environment in which the exercise can be conducted is desired. This again differs from traditional emergency response exercises in that participating players need to be given an opportunity to develop situational awareness based on the indicators and warnings present in the individual MSEL injects. As occurs with genuine cyber incidents, the present danger to a participant's organization may not initially be clear or obvious. This knowledge of the threat landscape is built up over time as more data that fill in the risk picture are made available to participants.

CyberSMART was initially developed to address the difficulties experienced by exercise planning teams in national cyber exercises. It is a Web-based, scalable, collaborative tool that aids exercise planning teams in researching, organizing, creating, and editing a credible scenario for a cyber exercise. It guides exercise developers through a structured planning process, allowing members of the exercise planning team to work both collaboratively and independently behind a secure portal.

Recent development on CyberSMART has introduced an Exercise Execution Engine (EEE) as an interactive, computer-assisted environment for effective cyber exercise participation. The EEE allows an exercise controller to manage the exercise by controlling scenario time and dynamically adding, removing, or editing the MSEL injects as necessary. When a MSEL inject is ready for execution, it is delivered to the specified target organization(s) automatically. These injects arrive in player dashboards via an e-mail-like interface where players may view the observable effects of the inject and respond accordingly. The inject delivery system supports multiple media types to allow for an engaging atmosphere. Exercise players can use this e-mail-like system to respond to the injected event and to communicate with other participants. A system-wide instant chat window is also available to allow for event response and easy participant communication.

III. Cyber Exercise Planning with CyberSMART

A. *Homeland Security Exercise and Evaluation Program*

CyberSMART was developed to enhance existing guidance on exercise development created by the Department of Homeland Security. The Homeland Security Exercise and Evaluation Program (HSEEP) is a series of documents that provides guidance for state and local first responders and emergency managers to create and execute valuable and effective training exercises. HSEEP guidance is an all-hazards approach to planning, execution, and review of exercises to prepare for accidents, natural disasters, and terrorist acts across the spectrum of catastrophic events. HSEEP lays out planning timelines, exercise deliverables, conference schedules and activities, logistic support, exercise conduct, and exercise evaluation. In addition, HSEEP provides example documentation formats and guidance for building and managing a complete exercise program.

CyberSMART does not replace HSEEP guidance regarding exercise planning, documentation, evaluation, logistics planning, or project management. CyberSMART was specifically developed to address the challenge of scenario development for cyber exercises, and is considered an enhancement to HSEEP that addresses the unique nature of cyber exercises. The planning conferences suggested by HSEEP include the following:

- Concepts and Objectives Meeting (C&O)
- Initial Planning Conference (IPC)
- Mid-Term Planning Conference (MPC)
- Final Planning Conference (FPC)

The CyberSMART process is aligned with the HSEEP planning conferences and provides guidance for the discussions held during each conference, as well as the information that must be gathered between conferences. CyberSMART provides a detailed plan beginning with objectives and ending with a MSEL. In order to further clarify HSEEP concepts as they apply to cyber security exercises, the CyberSMART team drafted an annex to the HSEEP policy and guidance volumes that was submitted for consideration in 2008.

B. *The CyberSMART Three-Track Planning Approach*

Rather than build individual MSEL injects as stand-alone objects, the CyberSMART planning module uses a three-track approach (Fig. 1) to guide planners, beginning with identifying the objectives of the exercise. Both sponsors and participants identify objectives for exercise involvement. Allowing participants to define their own objectives enables their greater participation in the scenario and helps them realize the value of the exercise to their particular organizational needs.

In parallel with the development of exercise objectives, exercise designers define transactions, IT assets, and participating roles (players) for each contributing organization. This technical background information is referred to as the "gamespace" and is the key to the CyberSMART approach to exercise planning. By focusing on the transactions necessary to maintain business continuity first, then identifying information assets that support those transactions, the scenario development team can create an attack scenario that emphasizes infrastructure protection issues rather than specific cyber attack methods. The scenario events themselves are more credible, since they incorporate accurate information about the context of the attack.

The information collected from the objectives and gamespace tracks of the planning process feeds into the scenario construction. Problem sets are the cornerstone of the scenario development process. Problems sets are derived from exercise objectives, and they collectively define a series of challenges that exercise participants will face. Each problem set contains a number of event threads. Event threads define more narrowly a series of events that are bounded by a time window and focused on a subset of the exercise modules such as prevention, response, or recovery. Finally, each event thread will contain several scenario events, which are the discrete events that make up the final master scenario events list.

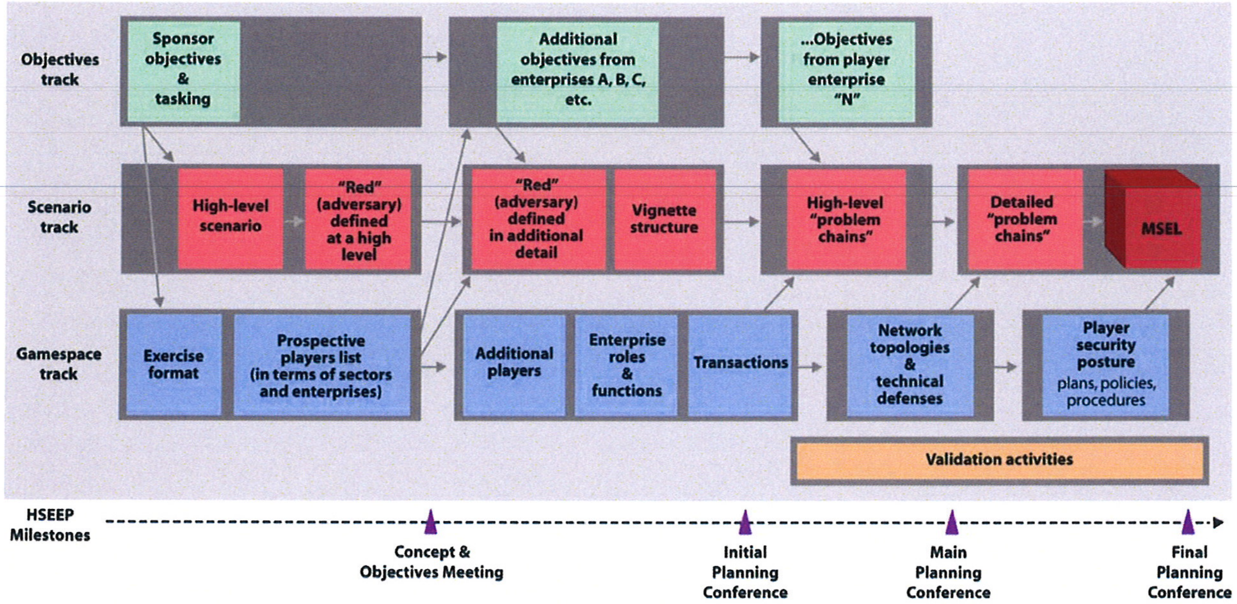
Objectives track
Sponsor objectives & tasking
Additional objectives from enterprises A, B, C, etc.
...Objectives from player enterprise "N"
Scenario track
High-level scenario
"Red" (adversary) defined at a high level
"Red" (adversary) defined in additional detail
Vignette structure
High-level "problem chains"
Detailed "problem chains"
MSEL
Gamespace track
Exercise format
Prospective players list (in terms of sectors and enterprises)
Additional players
Enterprise roles & functions
Transactions
Network topologies & technical defenses
Player security posture plans, policies, procedures
Validation activities
HSEEP Milestones
Concept & Objectives Meeting
Initial Planning Conference
Main Planning Conference
Final Planning Conference

Figure 1. Objectives track (top), scenario track (middle), and gamespace track (bottom) as they align with HSEEP milestones.

C. Exercise Planning Roles

A Cyber exercise planning team will typically employ several different levels of scenario developer. Exercise development professionals, cyber security and cyber threat subject matter experts, organizational subject matter experts, and even mid-level and high-level government policy makers may be involved in building an exercise, its scenario, objectives, and MSEL. Depending on the scope and scale of the exercise, the number of team members involved in these functions may number from a few to several dozen.

CyberSMART supports the following user types for exercise planning: exercise scenario director, exercise scenario designer, subject matter expert, and observer. The exercise scenario director is the lead person on the exercise scenario design team. The scenario director is responsible for defining the exercise objectives and the exercise description. Subject matter experts (SMEs) will construct a representation of their respective organizations, including IT assets, critical information paths and transactions, and Internet dependencies. SMEs will be able to build these representations to a much higher degree of accuracy and detail than the scenario designers, because of their knowledge and experience with their organizations. It is likely that all organizations will have provided information necessary for the exercise with an agreement that the information be strictly protected against disclosure. To account for issues of confidentiality and perceived risk on the part of participating organizations, a permissions-based hierarchy for exercise developer roles is employed. Subject matter experts will have permissions allowing them to enter information and review data only regarding their specific organization(s), but will not be allowed to see the data of other organizations, some of whom may be competitors.

D. Transition to Exercise Conduct

After the MSEL has been generated, the exercise planning team has an opportunity to finalize the MSEL at the FPC. CyberSMART provides the exercise planning team with an event review interface, where users can filter events by such parameters as status, type, planned time of execution, or sectors affected. Furthermore, team members can set the status of each event from draft or preliminary to approved or suspended to finalize the entire MSEL.

Once the scenario has been finalized, the exercise development team will have produced a complete MSEL, ground truth, and gamespace definition that can be fed into the exercise execution engine as shown in Fig. 2. The exercise director can use CyberSMART to assign exercise conduct roles, as defined below, for new or existing users. Upon initiating the transition into exercise execution in CyberSMART, a copy of the exercise is made so that it can be preserved in its completed state prior to any changes that are made to the MSEL during conduct. Changes that are made during conduct are also preserved, but in a conduct instance specific copy of the original exercise.

IV. EXERCISE CONDUCT WITH CYBERSMART

With the addition of the exercise execution engine (EEE) to CyberSMART, exercise teams can transition seamlessly into the conduct phase of the exercise and fully leverage the objectives, gamespace, and scenario that were developed in the planning phase. At a high level the EEE consists of a data store, participant interfaces, MSEL shooter, message board, and logger. The participant interfaces maintain the Web-based, simple user interface employed by the planning module to facilitate distributed, decentralized exercises.

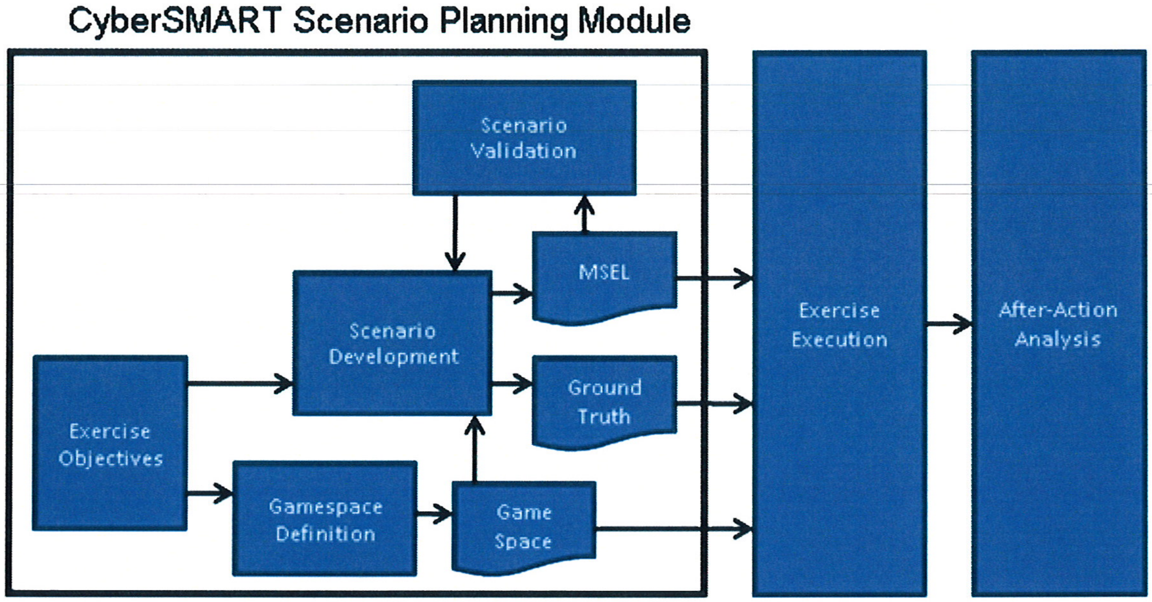

Figure 2. CyberSMART scenario planning to exercise execution process flow.

A. *Exercise Conduct Roles*

Experience indicates that differentiating participant roles is critical to the successful conduct of a cyber exercise [2]. This not only facilitates a smooth exercise execution, but also ensures a secure environment where participants may only access information associated with their role. It is critical that an organization's sensitive information be kept private and not made accessible to parties external to the organization. CyberSMART enforces these rules early in the scenario development phase, and this role separation continues through the execution and after-action analysis phases. Fig. 3 illustrates three main categories into which the roles are aligned: exercise roles, organization roles, and sim cell roles.

Under the exercise roles, the exercise controllers are responsible for the general flow and progress of the exercise. The exercise controllers manage the MSEL by ensuring that events are triggered at appropriate times and making dynamic changes to the list as required based upon the needs of exercise participants. They also have the ability to regulate scenario time—slowing or speeding the simulated passage of time as required for exercise continuity. Depending on the size of the exercise, one or more individuals may serve as exercise controllers. An exercise observer can view the same data as the exercise controller, but cannot directly change the MSEL, simulation time, or gamespace information.

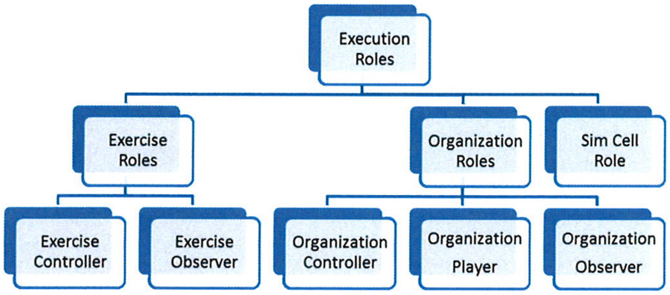

Figure 3. CyberSMART exercise execution hierarchy of roles.

Under organization roles, organization controllers see the complete list of MSEL injects assigned to their organization. They view the organization gamespace and provide situational awareness to their organization's players. The organization controllers communicate with their organization's players and the exercise controller to request dynamic changes to the MSEL injects as necessary. This helps organizations to maximize their ability to meet their objectives for the exercise. Organization players receive the delivered injects targeted for their organization. The injects contain observable effects that the players use to decide how to respond according to their organization's policies and procedures. Their actions and responses are captured by CyberSMART for after-action analysis. Organization players can use the CyberSMART chat and e-mail interfaces to communicate with other participants in an information gathering phase as they try to determine how to respond to MSEL injects. Organization observers have the same views as the organization controller, but it is a read-only display. Observers cannot directly respond to MSEL injects for their organization.

Sim cell participants act as proxies for organizations that are not participating in the exercise but that are necessary to create a complete scenario. They can access specified areas of the gamespace, and are used to provide situational awareness to organization controllers and players. They may also coordinate dynamic changes to the exercise as they deem necessary through the exercise controller.

B. *Exercise Conduct User Interface*

The user interfaces (or dashboards) provide a central location for participants to interact with the exercise and other participants. Rather than a single, all-encompassing dashboard for all participants, each role has a dashboard tailored to its unique needs and privileges. This ensures that all players have quick and easy access to the indicators and controls needed to perform their assigned role(s), while also limiting their access to data beyond the scope of their role(s).

V. Future Work

The CyberSMART scenario planning module is available for use by any organization that is preparing an exercise that includes cyber aspects, and the CyberSMART development team is seeking feedback from users of the tool. The exercise execution engine described above is in active development, and a prototype will be available in January 2013 for use in exercise conduct.

The CyberSMART team is also working with DHS S&T and FEMA on investigating a possible transition plan to eventually host the tool on the HSEEP Enterprise Platform [3]. This would allow CyberSMART to share exercise information with other applications through standardized messaging over a common enterprise service bus, and would provide more seamless integration into other tools in the HSEEP exercise support system. CyberSMART can also be transitioned for hosting on isolated networks, such as cyber test ranges, as needed.

VI. Conclusion

CyberSMART is a valuable tool for cyber exercise planning and conduct teams both in the public and private sectors, and for exercises of all sizes. It provides a robust, flexible exercise scenario development process that, when followed, ensures that exercises will effectively meet the objectives of the exercise sponsors and participant organizations. Furthermore, the CyberSMART exercise execution engine offers exercise conduct teams an immersive environment in which the objective, gamespace, and scenario development from the planning module can be fully utilized to present exercise players with a conceivable cyber incident scenario against which response doctrines can be tested and refined.

Acknowledgment

The CyberSMART team gratefully acknowledges support and guidance from Douglas Maughan, Greg Wigton and Jennifer Mekis, each representing the DHS Science and Technology Directorate; Glenn Fiedelholtz and Bridgette Walsh from the DHS National Cyber Security Division (NCSD) and the SRA NCSD contract support team; Justin Legary, Russell Clarke, Brian Weston, and Kamran Atri providing support from the FEMA National Preparedness Directorate (NPD) National Exercise Division (NED); and Steve Myers and the Seattle Emerald Down team.

References

[1] J. Marshall, “The Cyber Scenario Modeling and Reporting Tool (CyberSMART),” IEEE Conf. for Homeland Security 2009, CATCH ’09, pp. 305–309,3–4 March 2009.

[2] Space Dynamics Laboratory, “Emerald Down Cyber Exercise Final Report,” July 2010, unpublished.

[3] C. J. John et al., "New technologies and processes for the Homeland Security Exercise and Evaluation Program toolkit," 2011 IEEE International Conference on Technologies for Homeland Security (HST), pp.446–450, 15–17 November 2011.