Identifying Cyber Ecosystem Security Capabilities

Peter M. Fonash, Ph.D., DHS

Abstract. Strengthening the security and resilience of the cyber ecosystem requires reducing the number of vulnerabilities and the ability to automatically mitigate attack methodologies. This article draws from various research reports to categorize the underlying attack methodologies and summarizes current perspectives on the capabilities needed within the cyber ecosystem to strengthen its security and resilience, while protecting the privacy of the authorized users of the ecosystem.

Introduction

A general consensus has been forming in the cybersecurity community that cybersecurity defenses must become more automated, less reactive, distributed, and better informed. There have been a number of proposals and ongoing activities to enable automated collective action to strengthen the resilience and security of the cyber ecosystem[1] in the face of the advanced cyber threat. These proposals and activities support a range of automated collective actions, including the sharing of indicators and information, the selection of courses of action, and the coordination of responses. This article uses a three-step process to identify capabilities needed in the future cyber ecosystem to make these automated collective actions possible.

The first step was to understand the types of cyber attacks being faced by today's computer systems. Drawing from reports that help categorize today's attacks, an attack categorization is proposed. The second step was to review recent papers on cyber ecosystem security, including industry and academic comments on a cyber ecosystem paper [1] published by DHS. From these sources, a set of cyber ecosystem security capabilities was proposed. The third step was to analyze the collective cyber ecosystem capabilities and their ability to counter the proposed attack categories. This analysis resulted in a mapping of the cyber ecosystem capabilities against the attack categories.

Categories of Cyber Attacks

Using data from NIST, "Computer Security Incident Handling Guide" [2] and the "2012 Data breach Investigations Report" [3], a list of cyber attack categories was created. The attack categories are attrition, malware, hacking, social tactics, improper use (insider threat), loss or theft of equipment, physical action, and attacks that consist of multiple components. Table 1 provides a description for each cyber attack category, and includes the category "other" for completeness.

To cover current and future attacks, the attack categories have been made very general. For example, hacking is a very broad category of attack, but seems to be sufficient for the purposes of this article. Although other categories of attack can be created, this list is useful for helping to identify capabilities needed within the future cyber ecosystem to improve resilience and security.

The following section briefly discusses recent articles and papers that have proposed automated collective action in the future cyber ecosystem. These proposals will form the basis for the desired capabilities that are identified in a subsequent section.

Proposals for Collective Action in the Future Cyber Ecosystem

DHS has been working with industry, other government agencies, and the research and development community to develop a consensus on desirable future cyber ecosystem capabilities. The DHS National Protection and Programs Directorate (NPPD) published a paper "Enabling Distributed Security in Cyberspace: Building a Healthy and Resilient

Table 1. Categories of Cyber Attack

Attack Category	Description of Attack
Attrition [2]	Use of brute force methods to compromise, degrade, or destroy systems, networks, or services. Includes distributed denial of service attacks intended to impair or deny access to a service or application and resource depletion attacks [4].
Malware [2,3]	Any malicious software, script, or code developed or used for the purpose of compromising or harming information assets without the owner's informed consent, regardless of delivery method. Includes Web and email attacks and attacks executed from removable media or a peripheral device.
Hacking [3,4]	An attempt to intentionally access or harm information assets without authorization or in excess of authorization, usually conducted remotely. Includes data leakage attacks, injection attacks and abuse of functionality, spoofing, time and state attacks, buffer and data structure attacks, resource manipulation, use of stolen credentials, backdoors, brute force and dictionary attacks on passwords, and exploitation of authentication.
Social Tactics [3]	Use of social tactics such as deception, manipulation, and intimidation to obtain access to data, systems or controls. Includes pretexting (fake surveys), solicitation phishing, and elicitation of information through conversation.
Improper Usage (Insider Threat) [2]	Inappropriate use of privileges or inappropriate logical or physical access to data, systems, or controls by a person or persons associated with an organization. Any incident that would violate an organization's acceptable usage policies by an authorized user. Includes installation of unauthorized software and removal of sensitive data.
Physical Action [3]/Loss or Theft of Equipment [2]	Human Driven attacks that employ physical actions and/or require physical proximity. Examples are: stolen identity tokens and credit cards, tampering with or replacing card readers and point of sale terminals, and tampering with sensors. The loss or theft of a computing device or media used by the organization, such as a laptop or smart phone.
Multiple Component [3]	A single attack that encompasses the use of multiple techniques. Advanced attacks would often fall into this category, with various attack components occurring at different steps in the cyber kill chain [5,6].
Other [2]	An attack that does not fit into any of the other categories, such as supply chain attacks and network reconnaissance [4].

Cyber Ecosystem with Automated Collective Action" [1] to encourage a discussion of the cyber ecosystem capabilities. Additionally, the DHS cybersecurity strategy is outlined in the "Blueprint for a Secure Cyber Future" [7].

Two recent Microsoft security documents discuss collective options for improving the security "health" of computer systems. In the first, Scott Charney, Corporate Vice President for Trustworthy Computing, presents [8] a spectrum of computer defense. The computer defense spectrum includes collective defense. Charney recommends that "society needs to explore ways to implement collective defenses to help protect consumers who may be unaware that their computers have been compromised, and to reduce the risk that these compromised devices present to the ecosystem as a whole." In a subsequent Microsoft document, Kevin Sullivan, Senior Security Strategist for Trustworthy Computing, discusses [9] collaboration to secure consumer computers. Sullivan's strategy recognizes that, "As no single entity can defeat global cybercrime by itself, members of the internet ecosystem must take collective action."

Two IBM articles likewise present a case for cybersecurity improvements as a result of information exchange and collaboration. An early IBM Systems Journal article [10] recommends autonomic computing to provide security. The article asserts that computing systems, "like the biological systems that keep our hearts beating and our body chemistry balanced, can take care of routine and even exceptional functions without human intervention." A more recent IBM report [11] makes a similar recommendation, based on a public health and safety model for cybersecurity. "Effective response requires continuous research, open information exchange, and transparency among a wide range of actors. This allows responses to be better individualized to confront the particular nature of the threat and its risk of spreading more widely."

The previously mentioned DHS cyber ecosystem paper [1] discusses automated collaboration to help strengthen the resilience and security of the cyber ecosystem. Drawing a parallel from the practice of continuous monitoring, the DHS NPPD paper proposes to automate collaborative identification, analysis, and responses to strengthen protections against the advanced cyber threat. The DHS cyber ecosystem paper describes a future cyber ecosystem in which computing systems, "work together in near—real time to anticipate and prevent cyber attacks, limit the spread of attacks across participating devices, minimize the consequences of attacks, and recover to a trusted state. In this future cyber ecosystem, security capabilities are built into cyber devices in a way that allows preventive and defensive courses of action to be coordinated within and among communities of devices. Power is distributed among participants, and near—real time coordination is enabled by combining the innate and interoperable capabilities of individual devices with trusted information exchanges and shared, configurable policies." The paper envisions a future in which authentication, automation, and interoperability are the building blocks that enable cyber components to work together.

Based on this understanding of the future cyber ecosystem, the next section identifies capabilities desired in the future cyber ecosystem. The goal is a cyber ecosystem that helps mitigate all categories of cyber attack rather than defending against only known attacks.

Desired Cyber Ecosystem Capabilities

All nine attack categories can benefit from three common capabilities, called cyber ecosystem "building blocks" in the DHS NPPD ecosystem paper [1]. These capabilities are:

- **Automation** – allows the speed of response to approach the speed of attack.
- **Interoperability** – permits dynamic and seamless collaboration by removing technical constraints and barriers.
- **Authentication** – enables trusted online decisions between resources and actors at a distance, preferably in a way that enhances privacy.

The attack categories have additional commonalities, including the need for attack detection and situational awareness [7] and the ability to take advantage of shared information. For the cyber ecosystem to respond to an attack, the attack must be detected. As attacks become more sophisticated, identification of attacks, whether attempted or successful, will become more difficult. Furthermore, to minimize the consequences of an attack, detection should anticipate an attack as early as possible in the cyber attack lifecycle, commonly called the cyber kill chain [5,6]. Once an attempted or successful attack has been detected, the participants in the cyber ecosystem must be able to share and make use of that information. A key value of collective action is the ability to inform other systems of an attack before those systems come under attack. Additionally, a security management system can correlate inputs from various sensors to refine what is known about the attack.

A secure and resilient cyber ecosystem needs to do more than just share information about attacks. Security management systems can use the shared information to develop, evaluate, and implement alternative courses of action, as well as assess the effectiveness of the actions as the actions occur. Risk-based data management [12] will help support these capabilities. The effectiveness assessment can provide inputs for a range of subsequent actions, such as sensor reconfiguration, tightening security configurations, alerts and warnings, and the development of new courses of action. NIST Special Publication 800-61 recommends [2] the capability to document the attack, response and recovery. This is more than just an audit trail. It includes forensics-quality images and records that can subsequently be used to analyze the attack, identify undiscovered attack techniques, and support criminal investigation.

Not all attacks are alike, so the cyber ecosystem must include capabilities that are able to respond to the individual attack categories as well. This includes the capability to:

- Identify and respond to attrition attacks that did not necessarily gain access to an information system. Responses could require action by external participants.
- Identify malware that has no known signature, heuristics, or actions.
- Identify when the performance of systems or components is degraded, preferably before the systems or components fail.
- Perform near-real time risk-based management, so that automated responses are feasible.
- Filter out authorized activity so as to identify unauthorized hacking or insider activity, based on behavior monitoring that incorporates business rules [12].
- Employ actions that will not tip off an adversary, such as (but not limited to) monitoring the attack or using tailored trustworthy spaces [12], moving target [12], or containment (quarantine or honey-pot) to limit the scope of an attack.

The cyber ecosystem will always include well-known existing cybersecurity capabilities. These include user education to increase awareness of the sophisticated attacks, including social and physical attacks; cybersecurity education and training for the IT staff; and the need for secondary capabilities such as reserve power and cooling, backup communications, spare systems, and alternate sites.

The cyber ecosystem must include capabilities that will protect privacy and civil liberties.

Charney wrote, "Privacy concerns must be carefully considered in any effort to promote Internet security by focusing on device health. In that regard, examining health is not the same as examining content; communicating health is not the same as communicating identity; and consumers can be protected in privacy-centric ways that do not adversely impact freedom of expression and freedom of association." [8] The DHS cybersecurity strategy envisions that, "collaboration principles will foster the transfer of specific, actionable cybersecurity information using approved methods to those who need it, while protecting the privacy and civil liberties of the public." [7] Conversely, information systems within the cyber ecosystem will store, but not inappropriately share, data needed by authorized law enforcement officials to perform their duties.

Continued operations and recovery are key resiliency capabilities for the cyber ecosystem. A MITRE report [6] presents the following cyber resiliency goals:

- **Withstand an attack** – continue essential mission/business functions despite successful execution of an attack.
- **Recover from an attack** – restore mission/business functions to the maximum extent possible subsequent to successful execution of an attack.
- **Evolve** – minimize adverse impacts by changing missions/business functions, as well as perhaps changing the supporting cyber capabilities.

In 2011, DHS published the "Blueprint for a Secure Cyber Future: The Cybersecurity Strategy for the Homeland Security Enterprise" [7]. The Blueprint lists a number of objectives to strengthen the cyber ecosystem and enable success against current and future threats:

- **Develop the Cyber Workforce in the Public and Private Sectors:** Maintain a strong cadre of cybersecurity professionals to design, operate, and research cyber technologies.
- **Build a Base for Distributed Security:** Provide individuals with tools, tips, education, training, awareness, and other resources appropriate to their positions that enable them to implement existing cybersecurity features and configurations in protocols, products, and services.
- **Reduce Vulnerabilities:** Design, build and operate information and communication technology to specifically reduce the occurrence of exploitable weaknesses. Enable technology to sense, react to, and communicate changes in its security or its surroundings in a way that preserves or enhances its security posture.

Assess effectiveness
Authentication
Interoperability
Automated Defense Identification, Selection, and Assessment
Build Security In
Business Rules-Based Behavior Monitoring
General Awareness and Education
Moving Target
Privacy
Risk-Based Data Management
Situational Awareness
Tailored Trustworthy Spaces

Table 2. Desired Cyber Ecosystem Capabilities

- **Improve Usability:** Design trusted technology that is easy to use, easy to administer, rapidly customizable, and performs as expected.
- **Appropriately Validate Identities in Cyberspace:** Use risk-based decision making for authentication, raising the level of trust associated with the identities of individuals, organizations, networks, services, and devices involved in online transactions and communication.
- **Increase Technical and Policy Interoperability Across Devices:** On a device-to-device level, strengthen collaboration, create new intelligence, hasten learning, and improve situational awareness.
- **Automate Security Processes:** Employ automated mechanisms for acting collectively in near real-time to anticipate and prevent incidents, limit the spread of incidents across participating devices, and minimize consequences.

The various capabilities discussed above can be combined into a list that takes into consideration similarities and differences. For example, a number of capabilities are related to automation, information sharing, collaboration, and assessment of results. Table 2 presents an alphabetical list of the major capabilities discussed above that are desirable in the future cyber ecosystem.

Mapping Desired Cyber Ecosystem Capabilities Against Attack Categories

The following table (Table 3) maps the desired cyber ecosystem capabilities against the attack categories. It reflects a combination of the recommendations in the literature, the recommendations of the research community [13] and industry review [12] of the DHS cyber Ecosystem paper [1]. It is noted that almost all

Table 3. Compare Attack Categories against Desired Cyber Ecosystem Capabilities

	Categories of Cyber Attack							
Desired Cyber Ecosystem Capabilities	Attrition	Malware	Hacking	Social Tactics	Improper Usage (Insider)	Physical Action; Loss or Theft	Multiple Component	Other
Automation	x	x	x	x	x	x	x	x
Authentication	x	x	x	x		x	x	x
Interoperability	x	x	x	x			x	
Automated Defense Identification, Selection, and Assessment	x	x	x	x	x	x	x	x
Build Security In	x	x	x	x		x	x	x
Business Rules-Based Behavior Monitoring	x	x	x	x	x	x	x	x
General Awareness and Education	x	x	x	x	x	x	x	x
Moving Target	x	x	x	x			x	x
Privacy	x	x	x	x	x	x	x	x
Risk-Based Data Management	x	x	x	x	x	x	x	x
Situational Awareness	x	x	x	x	x	x	x	x
Tailored Trustworthy Spaces	x	x	x	x			x	x

the boxes are filled in. This reflects the thought that the capabilities work together as a system and the probability that a particular capability will help in some way to either help detect or mitigate an attack.

DHS has a number of ongoing efforts that help achieve some of the desired future capabilities. Examples of some of these activities include:

- Early detection of attacks, preferably before an attacker has begun to exploit the attack.
  - Trusted Automated Exchange of Indicator Information (TAXII)
  - National Cyber Protection System
  - Continuous Monitoring activities
- Interoperability that permits maximum collaboration and information sharing by removing technical constraints and barriers.
  - Various Security Content Automation Protocol (SCAP) activities
  - Continuous Monitoring Activities
  - TAXII
  - The National Cybersecurity and Communications Integration Center (NCCIC)
- Authentication that enables trusted collective actions to occur automatically.
  - Support to the National Strategy for Trusted Identities in Cyberspace
- Automation to rapidly share indicators and warnings, possible courses of action, configuration settings and policy updates, and other useful information.
  - TAXII, SCAP, Common Vulnerabilities and Exposures (CVE), Open Vulnerability Assessment Language (OVAL), Malware Attribute Enumeration and Characterization
  - Federal Information Security Management Act
  - Continuous Monitoring
- Develop collaborative courses of action, given available information, policies, tools, procedures, and capabilities.
  - National Cyber Incident Response Plan
  - NCCIC and US-CERT
- Build security into products and components, so that they are able to participate properly and effectively in the future cyber ecosystem.
  - Software Assurance Program
  - Education and Training
  - CVE, OVAL
- Utilize shared information via systems and components that have the ability to produce and consume near-real-time indications and collaborative response information.
  - Dynamic Defense, and Defense-in Depth [12]
  - SCAP
  - TAXII
- Increase awareness of people by providing alerts, tools, tips, guidelines, and resources that are appropriate to a given situation; and of unauthorized activity by business- and operations-based behavioral analysis tools.
  - Education and Outreach Programs
  - NCCIC
- Transparency and Privacy that protects the rights of citizens and system users by sharing data that focuses on the event.
  - DHS Privacy Advocate

Summary and Recommendations

This article presents a categorization of cyber attacks and proposes a set of future cyber ecosystem capabilities to mitigate those attacks. These cybersecurity capabilities, when built into the future cyber ecosystem components and systems, will help strengthen the security and resilience of the cyber ecosystem.

The list of desired capabilities is not expected to change as a result of changes in threats, attack methods, technologies, and processes. This is because our approach is based on broad attack categories, not the specific technical details of those cyber attacks that will change as technology evolves. Although the paper's list of capabilities is not guaranteed to be complete, it does not include characteristics that will become unnecessary in the future. The cyber ecosystem itself is continuously evolving. Recent major evolutional trends are toward mobility and cloud computing. The cyber ecosystem capabilities must be able to adapt to support new environments, such as cloud and mobile. Federal and industry research and development (R&D) are key to the development of many of the desired capabilities.

The federal government's R&D community has developed a plan [13] for the research required to support the development of future cyber ecosystem security capabilities. Among the areas of emphasis in the plan is develop improved metrics for accessing cybersecurity risk and developing cyber security economic investment incentives; tailored trustworthy spaces and moving target [13].

Charney reminds us that collective solutions require collective development and integration. "To build on the current national and industry efforts, we can identify what is working and what is not, and document both to enable more individual action and community building. We can also begin to work through international bodies to standardize what types of information on machine health should be shared and how to exchange it with appropriate security and privacy protections." [8]

Acknowledgement:

The author gratefully acknowledges the assistance of Robin A. Simmons of The MITRE Corporation in preparing this article.

ABOUT THE AUTHOR

Dr. Fonash is the Chief Technology Officer for DHS' Cybersecurity and Communications organization. Dr. Fonash has held several senior positions at the National Communications System (NCS). He was Deputy Manager and Director of the NCS. Prior to that Dr. Fonash was Chief, NCS Technology and Programs Division. He managed special Presidential and priority communications services technology development, nationwide network modeling and analysis, specialized telecommunications research and development, and the deployment of (NS/EP) priority communications services nationwide on all major commercial networks.

Before arriving at the NCS, Dr. Fonash served as the Chief of the Defense Information System's Agency Joint Combat Support Applications Division, providing technical software integration services to the functional communities and guiding functional applications' compliance with the standard common operational environment. He also worked for the Office of the Assistant Secretary of Defense for Command, Control, Communications and Intelligence, and was responsible for Defense communications infrastructure policy and program oversight. He was also Chairman of the Office of the Secretary of Defense Information Technology Architecture Council.

Dr. Fonash has a Bachelor of Science in Electrical Engineering and a Master of Science from the University of Pennsylvania, a Master of Business Administration from the University of Pennsylvania's Wharton School, and a Doctor of Philosophy in Information Technology and Engineering from George Mason University.

REFERENCES

1. "Enabling Distributed Security in Cyberspace: Building a Healthy and Resilient Cyber Ecosystem with Automated Collective Action", DHS National Protection and Programs Directorate, 23 March 2011.
2. "Computer Security Incident Handling Guide" (draft), National Institute of Standards and Technology Special Publication 800-61 Revision 2, March 2012.
3. "2012 Data Breach Investigations Report", Verizon Corporation, March 2012.
4. Common Attack Pattern Enumeration and Classification, http://capec.mitre.org
5. Eric M. Hutchins, Michael J. Cloppert, and Rohan M. Amin, "Intelligence-Driven Computer Network Defense Informed by Analysis of Adversary Campaigns and Intrusion Kill Chains", Lockheed Martin Corporation, November 2010.
6. Deborah J. Bodeau and Richard Graubart, "Cyber Resiliency Engineering Framework", MITRE Technical Report MTR11023, September 2011.
7. "Blueprint for a Secure Cyber Future: The Cybersecurity Strategy for the Homeland Security Enterprise", Department of Homeland Security, December 2011.
8. Scott Charney, "Collective Defense: Applying Public Health Models to the Internet", Microsoft Corporation, October 2010.
9. Kevin Sullivan, "Collaborating to Secure Consumer Devices: Promoting Device Health for a Safer, More Trusted Internet", Microsoft Corporation, May 2011.
10. David M. Chess, Charles C. Palmer, and Steve R. White, "Security in an Autonomic Computing Environment", IBM Systems Journal, Volume 42, Number 1, 2003.
11. "Meeting the Cybersecurity Challenge: Empowering Stakeholders and Ensuring Coordination", IBM U.S. Federal White Paper, February 2010.
12. Recommendations from the Cyber Ecosystem Working Group, a working group formed by the Cross-Sector Cyber Security Working Group, January 2012.
13. Trustworthy Cyberspace: Strategic Plan for the Federal Cybersecurity Research and Development Program, Executive Office of the President, National Science and Technology Council, December 2011.

NOTES

1. The cyber ecosystem is global, evolving and includes government and private sector information infrastructure; the interacting persons, processes, data, information and communications technologies; and the environment and conditions that influence their cybersecurity.