Responses to RFI for the 2015 Federal Cybersecurity R&D Strategic Plan

Ehab Al-Shaer,
College of Computing and Informatics
University of North Carolina Charlotte
Director of CyberDNA and NSF CCAA
ealshaer@uncc.edu

1. Section 201 (a)(1) of the Act identifies a number of cybersecurity objectives. What scientific, technological, or implementation gaps are indicated by those objectives? What research goals, for both basic and applied research, could serve as guidance for a federally-funded, multi-agency portfolio of R&D activities to close those gaps?

There are number of gaps that exist in the cybersecurity objectives in Section 201 (a)(1) of the act. First, a new objective that merits consideration is that the system needs to be resilient. Addressing **resiliency** both proactively and reactively with provable guarantees will facilitate automation and decision making in cyber defense. Moreover resilience architectures will allow for metric-driven automated synthesis of security controls and counter-measures to resist and mitigate attacks in a way that is scalable. It is important for resiliency to be built in the design phase rather than retrofitted. Second, **automation** is important in order to address both cyber-security challenges like fast detection and mitigation as well workforce shortage as cybersecurity today requires an army of professionals even in midsize enterprises. The current cyber-security workforce cannot sustain the growing needs of the industry. The current objectives also lack provision for tailored and predictive techniques to address challenges to the security of critical infrastructures such as the Smart Grid especially against threats from state-sponsored attacks.

2. What innovative, transformational technologies have the potential to enhance the security, reliability, resiliency, and trustworthiness of the digital infrastructure, and to protect consumer privacy?

After decades of deploying cyber security systems, it is well-known that the static and predictable behavior of cyber-systems from the view of attackers creates a fundamental design vulnerability that allows adversaries to not only plan and launch attacks effectively but also learn and evade detection easily. Furthermore, adversaries' strategies become much more sophisticated and highly unpredictable. As a result, attacks take less time to execute and a longer time to mitigate. Transformational technologies are a need of the hour to reverse this asymmetry in cyber warfare by embedding *agility* into cyber systems. Cyber agility is a system property that allows cyber systems to proactively defend against unknown threats by dynamically changing the system parameters and defense strategies in a timely and cost-

effective fashion in order to resist attack occurrences and mitigate consequences without degrading the quality of service. One defense technique for cyber agility is Moving Target Defense (MTD). This technique allows proactive defense against attacks by randomizing or mutating the system configuration to invalidate the attackers' goal.

Cyber agility aims to provide robust proactive defense by disrupting attacker plans via changing adversarial behaviors, and deterring them by prohibitively increasing the attack cost. It also aims at minimizing the time for mitigating the attack and its impact through built-in evolving resistance against attack propagation and escalation in a timely manner.

3. Discuss how the Federal government can foster the rapid transfer of R&D results into new cybersecurity technologies and applications for the timely benefit of society and the national interest.

- Increase in research funding is required for technologies that allow for continuous defense via constant monitoring and detection and automating decision-making.
- It is important to create new and specialized funding sources to stimulate large-scale collaboration between academia and the industry.
- Funding grants to build virtual and physical cyber infrastructure for developing and experimenting and evaluating novel cyber defense ideas and technologies.

4. Discuss how the current research infrastructure for creating, testing, and evaluating the next generation of secure networking and information technology systems could be improved, including how the access by academic researchers to this infrastructure and related data could be improved.

The current research infrastructure like PlanetLab, GENI, DETER and PREDICT are very limited in supporting innovative research such as cyber-agility, MTD and resiliency for the following reasons: (1) their interfaces are limited, (2) they are not scalable, (3) they are poorly maintained, (4) they limit the kind of experiments that can be run, (5) they are inflexible in adopting disruptive technologies in that it is not possible to easily modify the protocols and agility parameters etc.
The research community currently does not have an infrastructure for testing/evaluating collaborative information sharing. An infrastructure which caters to the above mentioned needs will help in improving R&D activities for the next generation of secure networking and IT systems.

5. What areas of research or topics of the 2011 Strategic Plan do not need to be prioritized anymore for federally-funded research (because, for example, solutions are now sufficiently mature, or the private sector is now significantly invested in addressing the deficiencies)?

Tailored Trustworthy Spaces and Economic Incentives may not be the most cross-cutting areas since they appear in almost all topics in cyber security. So it may be appropriate to consider them to be secondary areas.

6. What areas of research or topics of the 2011 Strategic Plan should continue to be a priority for federally-funded research and need continued federal R&D investments?

We found that the research in the area is very promising. People are beginning to adopt the ideas and methodologies of Moving Target Defense (MTD) and there are a number of products based on MTD. In our research in the AFRL-ACS project on Moving Target we found that the Random Host Mutation (RHM) and Random Route Mutation are effective in defending reconnaissance, worm, and DoS attacks [1,2].

However the area is still not mature and there are many challenges need to be addressed. For example there is no clear framework for Science of Security (SoS) and there lacks standard metrics for agility and resilience. The composition and verification of agility techniques is also an open problem.

7. What challenges or objectives not included in the 2011 Strategic Plan should be a strategic priority for federally-funded R&D in cybersecurity? Discuss what new capabilities would be desired, what objectives should guide such research, and why those objectives should be a strategic priority.

(1) Resilience-by-construction, to fundamentally change the basic assumption of the cyber system. Building the cyber system with support for agility from design, and automation of the configuration.
(2) Mutable systems, which are dynamic and agile to evolve and learn from history, optimize the strategy, and proactively disrupt and deceive the attackers. One way of achieving this is with the use of bio-inspired engineering.
(3) Collaborative defense, scalable analytics for information sharing and processing.

[1] E. Al-Shaer, Q. Duan, and J. H. Jafarian. Random host mutation for moving target defense. In Proceedings of Int. Conference on Security and Privacy Communications (SecureComm'12), 2012

[2] Q. Duan, E. Al-Shaer, and J. H. Jafarian. Efficient random route mutation considering flow and network constraints. In IEEE CNS13, 2013