Homeland Security
Science and Technology

Homeland Security Science and Technology Advisory Committee (HSSTAC): Quadrennial Homeland Security Review Subcommittee

Cybersecurity White Paper

March 10, 2017

This publication is presented on behalf of the Homeland Security Science and Technology Advisory Committee, Quadrennial Homeland Security Review Subcommittee, Cybersecurity, chaired by Dr. Vincent Chan with contributions from Mr. Byron Collie, Mr. John Sims, Mr. William Crowell, Lt. General Harry Raduege, USAF (Ret), and Dr. Ted Willke as part of recommendations to the Department of Homeland Security, Under Secretary for Science and Technology, Robert Griffin (*Acting*).

<Signature on File>

____

Vincent W.S. Chan
The Joan and Irwin Jacobs Professor of EECS
Massachusetts Institute of Technology

HSSTAC Staff: Michel Kareis, HSSTAC Executive Director/DFO and Gretchen Cullenberg, QHSR Subcommittee support.

CYBERSECURITY AND HOMELAND SECURITY

Dr. Vincent Chan, Subcommittee Chair; Mr. Byron Collie, Mr. John Sims, Mr. William Crowell, Lt. General Harry Raduege, USAF (Ret), and Dr. Ted Wilke

White Paper for HSSTAC Quadrennial Homeland Security Review (QHSR) Subcommittee in support of the 2018 QHSR

Introduction

Cyber security is a very serious and ubiquitous issue affecting public safety and infrastructure protection. Some potential vulnerability areas will be flagged here without detailed articulation of threat surfaces, assessment of capability of adversaries, detection and mitigation techniques and gaps in protection tools and techniques. An adequate treatment will need discussions and expositions at the classified level. For the DHS mission it is clear that any adequate safeguards will need the collaboration of industry and especially partner agencies both in the technologies they have and will develop/ed and also their in-place capabilities in the field. DHS only has been and will be able to work on a small subset of these security technologies and deploy limited infrastructures.

Inherent tradeoffs between privacy and performance and between security and cost limit the financial incentive for commercial entities to devote full attention to the issue. As a result, there is need for academic and government development of industry-wide security standards[1]. Research in this area is largely focused on device and/or user authentication and resource-constrained encryption, along with some research on the physical layer security of the expanding Internet of Things (IoT). The IoT presents a rapidly expanding societal attack surface that while offering massive benefits in accessibility, convenience, functionality and efficiency, also provides a significant entry point into systems and infrastructures which were previously physically segregated and difficult to compromise. Having a huge number of objects on the network substantively increases the risks of insider attacks and constant presence of compromised nodes. A new security paradigm that allows good operations in the presence of compromised nodes and constant insider attacks is a major shift from previous models assumed.

Missions and goals

Before any decisions on R&D investment DHS needs to develop a set of security goals and outcomes for DHS missions as derived from its mandate. This is essential since the field of cyber security is so vast, clear articulation of missions and goals will help focus limited R&D resources on the most critical problems. The following are possible goals for DHS:

[1] An example of academic and government development of industry-wide security standards is the National Institute of Standards and Technology (NIST) Cyber security Framework (NIST-CF).

1. Provide or help acquire cyber security systems (includes providing guidance and advice) for U.S. Federal Government departments and agencies (excluding DoD, IC,..) as developed by DHS.
2. Help acquire cyber security systems (includes providing support, guidance and advice) for cities and their infrastructures and services
3. Provide cyber security for DHS departments' operations and their coordination with outside entities
4. Provide cyber security partnerships, information and in some cases operational support to state, local, tribal and territorial governments and the 16 critical infrastructure sectors.

Within a set of well-articulated goals, the Science and Technology Directorate should identify critical technology areas and shortfalls for DHS investment. Attention must be paid to the timing to fruition of these R&D investments and ascertain that these technologies will be there when the threats arrive. It would be impossible for DHS to develop all the necessary protection technologies by itself; thus DHS must identify US and allied government agencies that can augment its expertise. As much as 90% of the technologies can be obtained from the outside either from the industry or from other government agencies, Figure 1.

Mission span

Entities that can be protected under a DHS cyber security umbrella (but not limited to) are: sensors, information inflight and at rest, computing and storage elements, networks and infrastructures e.g. power grid, IoT and Smart City infrastructures. It is imperative to first create an overall architecture that integrates internal and external protection mechanisms which is not a common practice in government systems. This architecture must have the following attributes:

1. Quantifiable performance metrics and a system design that is measured against real life service quality outcomes (not some internal technical parameters not directly related to QoS)
2. The ability to detect, localize and isolate attacks
3. The ability to maintain critical services
4. The ability to reconstitute impaired system e.g. post Fukushima restoration of communication[2]
5. Capabilities for attribution and counter actions such as adversary disruption

[2] In this case it took almost 30 days which is much too slow for first responders.

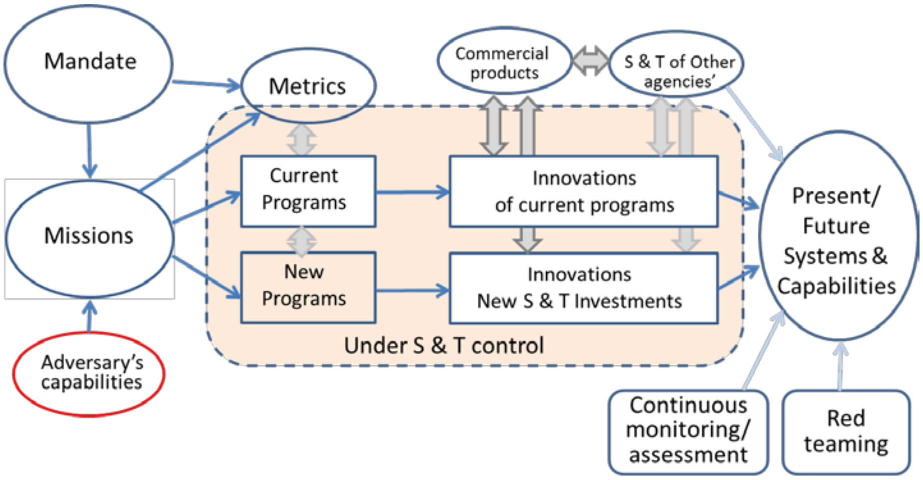

Figure 1. Investment flow.

It is not clear that defense alone will be sufficient to defend critical infrastructures. The last item is an offensive move to take down the adversaries' assets. These types of actions have ramifications on investigative, legal, diplomatic and military matters related to jurisdictions pertaining to other departments such as State, DoD, Commerce, etc. These departments need to be consulted and a holistic counter-measure plan should be created ahead of any crisis.

Creating a cyber defense system for the US Federal government

To fulfil its missions and goals DHS should create a cyber defense system for some parts of the federal government, including departments and agencies[3][4]. An effective cyber defense system should be made up of overlapping, redundant, layered, pervasive, and rapidly updated defenses. The following are some necessary steps to be taken to create a mission architecture:

1. Government should create an overall security strategy and architecture that reflect known best practices[5]
2. Create an outcome-oriented plan with a set of security goals and outcome metrics
3. Effective systems must have a comprehensive list of features and excellent coordination between components
4. This system must be dynamic and quickly adaptive since static (quasi-static) systems are unlikely to be effective against a significant fraction of the threat eco-system

Necessary characteristics of a cyber defense system for the US federal government

[3] DHS currently has a National Cybersecurity Protection System (NCPS, as described by the Comprehensive National Cybersecurity Initiative (CNCI) - https://www.dhs.gov/national-cybersecurity-protection-system-ncps

[4] DHS cyber division has provided leadership to Information Sharing and Analysis Organizations ISAOs, see www.dhs.gov/isao in response to EO 13691. This ranges from automated methods of threat sharing, automated vulnerability detection, risk measurement and mitigation, etc. Important research needs to address human/social issues such as building trust within and across sectors, and also economic issues, such as measuring and incentivizing investments in Cyber.

[5] NIST has created a Cybersecurity Framework for improving critical infrastructure, however it is not an architecture in the sense that is described here; www.nist.gov/cyberframework

An effective cyber defense system should be made up of overlapping, redundant, layered, pervasive, rapidly updated defenses. A significant adversary will attack over a range of domains that include physical attacks, electronic warfare, communications, and psychological means and will not simply be content with being confined to remote Internet attacks. Even if we were limited to cyber aspects alone, there is a litany of attack vectors that do not typically appear in the field of view, see list in item 3 below. Adversaries will choose the least costly of tools that accomplish their goals. Measuring the effectiveness of the system after developing countermeasures to a particular threat is not likely a good indicator of the effectiveness against the adversary's complete capability. We should expect that there are more stealthy and comprehensive threats such as zero-day attacks being held in reserve for just this occasion. The following are some necessary characteristics the mission architecture must have and maintain:

1. An overall architecture that integrates internal and external protection mechanisms:
    a. Based on current complete threat models
    b. Use of outcome oriented security metrics (see Appendix 1), and plan for continuous assessment, updating hygiene standards, with ability to prioritize attack flags or exploitation indicators
2. Effective security, since perimeter-defense-only security systems are inadequate and must be augmented by other techniques. It is useful only for known, well-defined signatures and indicators but will not be effective against zero-day attacks especially when updates are performed with delays longer than minutes
3. Protection beyond eroding perimeter defenses that typically have the following vulnerabilities (list not exhaustive):
    a. Theft of legitimate credentials
    b. Various form of privilege escalation
    c. Supply chain interdiction
    d. Cloud infrastructure
    e. Social media
    f. Wireless and mobile devices
    g. Bring your own device (e.g. USB sticks)
    h. Guest devices
    i. Channels to peers and trusted partners that are less secure than protected external connections
4. Analytics that are implemented simultaneously with the deployment of security tools
5. Incorporation of the human dimension of cyber security protection mechanisms, including insider threat, human factors, organizational behavior (e.g. "political" compromises that lead to unsafe system design) and an emphasis on behavioral science.

Despite the publication of the "Enabling Distributed Security in Cyberspace" paper[6] by DHS in 2011, there has been little progress in achieving a shared information architecture supporting

[6] https://www.dhs.gov/xlibrary/assets/nppd-cyber-ecosystem-white-paper-03-23-2011.pdf

mutual defense across connected entities. The DHS Automated Indicator Sharing (AIS) platform[7] has only achieved limited success despite the signing into law of the Cybersecurity Information Sharing Act (CISA) of 2015. Any successful, evolutionary cybersecurity platform will require interconnectedness to other similar mature systems to support identification of new adversary Tactics, Techniques and Procedures (TTPs) and assessment of control measures ability to provide protective, detective and reactive coverage. Smart sensors, data lakes, advanced data analysis techniques and machine learning all offer opportunities for integrating behavioral modeling with known signature based techniques to identify anomalous behaviors and activities that may be indicative of the presence of advanced adversaries within a defended infrastructure.

Recommendations

There should be an over-arching mission security architecture detailing how policies, capabilities and components pieces should be integrated to provide an adaptive, resilient infrastructure. This architecture must be supported by a comprehensive residual risk assessment, informed by a realistic threat model (realizing that there will be a variety of threat actors and models targeting the landscape of various agencies and mission segments). Effective cyber defense requires redundant overlapping layers of defenses distributed pervasively throughout the organization's networks. Redundancy and overlap would seem undesirable and inefficient, but anything less is guaranteed to be inadequate.

When looking outside fixed government and corporate environments there are several types of security capabilities that must be considered. Vehicle safety is an extreme example; since communication between vehicles and road-side units about local road information must be accurate and timely. For driverless vehicles, the threat of denial-of-service or jamming attacks is of particular concern. For large data networks, the integrity of link state data will be important for network control and management functions. With the growth of software defined networks (SDN) and perhaps, network function virtualization (NFV), network control plane security becomes critical. If learning algorithms are used in support of network operations, then data contamination can be especially dangerous, impacting not only immediate actions, but also future decisions.

Securing the IoT in the Smart City context should be within the preview of DHS. In this case, the network is developing quickly at massive scale. Security must be addressed in the context of the huge and highly dynamic future network. Network protocols – including security – must therefore scale to support billions of nodes and to respond rapidly to changes in traffic and link states. Because of the large number of resource-constrained devices entering and leaving the network, it cannot be assumed that all nodes are non-malicious. In fact, the network should be designed under the assumption that some fraction of nodes is compromised, and there should be graceful performance degradation as the size of the compromised fraction grows. There should be a ubiquitous sensing function to assess the integrity of nodes and active query techniques to further vet node integrity. One possibility is to maintain satellite connectivity to most nodes for

[7] https://www.dhs.gov/ais

queries and communicate with the "good" nodes and periodically rekey them.

The following is a list of specific recommendations for DHS to pay attention to in its quest to develop a mission security architecture:

1. Develop a set of security goals and outcome metrics for DHS missions
2. Develop a strategy, and architecture and establish an outcome oriented plan moving forward.
    a. Create a formal cybersecurity strategy
    b. Immediate development of an overall architecture for the system
        i. Interview best of breed commercial implementers
        ii. Engage partners and outside experts in the creation and upkeep of the architecture
    c. Conduct continuous measurement of system performance and frequent red team evaluations
3. Implement rapid acquisition processes
4. Create realistic expectations
    a. Prevent what you can, and rapidly mitigate what you did not expect
    b. Prioritize the importance of the data that needs to be protected and provide appropriate protection
5. Cyber security is too dynamic for Government processes alone. It is essential to set goals and outcome measures and then rely on private sector government partners implementation and rapid upgrades
6. Automate existing manual processes in operations; implement machine speed updates of signatures, indicators, actions and reactions and minimize humans in the loop
7. Empower people to update system at the lowest working level possible
8. Conduct continuous measurement of system performance including basic Receiver Operating Characteristics curves and overall characterization of cybersecurity posture and risk
9. Ensure qualified experts vet approaches and results
10. Incorporate in a timely fashion (which means very fast compared to time scales of typical government processes) useful new features/functionalities from commercial sources and partners into system
11. Continuously assess user performance needs
12. Consider implementing rapid acquisition processes
13. Supply chain integrity must be assured[8]
14. Procurement contracts should be outcome-measure oriented instead of prescriptive: describe desired outcomes; do not prescribe the solution
15. Enable choices from best-of-breed and always consider changing possible solutions
16. To manage the significant sources of risk to the integrity of the nation's complex cyber systems of systems, DHS should address the interconnectedness and interdependencies

[8] DHS should partner with other agencies such as the DoD that already have program in this area.

that exist between the cyber infrastructure and other safety-critical cyber-physical infrastructure systems of systems.

Technologies to invest in

There are only limited resources that DHS can use to invest in cyber security technologies. A large fraction of deployed infrastructure by DHS must use both commercial technologies and tools and techniques developed and deployed by other agencies such as the ICs, DoD and FBI. The following is a list of technologies that will impact cyber defense. DHS should invest in the R&D of these technologies only if they are not already available from outside the Department (a rough estimate has over 90% of the technologies available from the commercial sector and other US and allied government agencies):

1. Network and cyber perimeter defense
2. Data protection
3. Trusted computer architecture beyond Von Neumann
4. Monitoring of internal elements and incorporation of external sensor reports
5. Behavioral monitoring and anomaly detection
6. Data analytics
7. Cognitive decision making on automated mitigation actions
8. Partnership with industry/government-agencies to protect against zero-day attacks
9. Post attack mitigation strategies: fault localization/isolation, attribution, reconstitution, data recovery, and offensive measures,

The last two items in particular require a proactive posture in reaching out to other agencies. It is not sufficient merely to seek consultations or opinions; they must be engaged as fully functional partners.

Deterrent beyond cyber technologies

The best scenario is when the cyber security system in place serves to deter attacks. A potential attacker must believe that the defender can identify the source of an attack. Thus, attribution techniques are very important tools. The range of countermeasures should be rich enough to afford a broad spectrum of proportional responses. Some of these responses can be outside the cyber domain ranging from those that are within the purview of the departments under Commerce, State and the DoD. This type of deterrent is most effective when the nation announces that it considers certain infrastructure to be vital and critical and that an attack on their integrity will result in countermeasures on entities with the same importance for the offending nation or organization but not limited to the cyber domain. For example, an attack on U.S. critical infrastructures such as the power grid may draw physical attack on the key infrastructure of the offending nation or organization. It is important that such a deterrent message be credible in the sense that potential adversaries understands that the U.S. has both the capability and the will to respond to an attack once identified.

Path forward

Going forward DHS should take the following necessary steps:

1. Derive missions from mandates
2. Identify necessary capabilities
3. Review system performance against adversaries’ capabilities
4. Consider and incorporate science and technologies from other agencies
5. Assess technical capabilities of existing programs and their reasonable expectations in the near future
6. Identify gaps in existing programs and initiate new programs if the necessary science and technologies are not available from other agencies; form alliances where-ever possible
7. Cost execution of programs and reprioritize with financial considerations
8. Create maturation process and transitioning plans to operations

The cyber threat is clear, present and continues to become more formidable. Our nations’ critical infrastructures and ability to conduct vital business are at risk. Immediate response with a credible timely program is needed. DHS should fulfil its part of the responsibility.

Appendix 1

Some examples of metrics that can be used:

Definitions (examples only):

1. Serious event {SE}
2. At least one serious injury
3. Significant financial loss
4. Serious infrastructure impairment
5. Mid-level event{MLE}
6. Minor event {ME}

Metrics (examples only):

1. Prob {SE} < ^{2}
2. Prob {early detection: before event; followed by mitigation}
3. Prob {detection: after occurrence without opportunity to mitigate}
4. Prob {attribution}
5. Prob {resolution: attribution + neutralization}