NISTIR 8192

Enhancing Resilience of the Internet and Communications Ecosystem

A NIST Workshop Proceedings

Tim Polk

This publication is available free of charge from:
https://doi.org/10.6028/NIST.IR.8192

National Institute of
Standards and Technology
U.S. Department of Commerce

NISTIR 8192

Enhancing Resilience of the Internet and Communications Ecosystem

A NIST Workshop Proceedings

Tim Polk
Applied Cybersecurity Division
Information Technology Laboratory

This publication is available free of charge from:
https://doi.org/10.6028/NIST.IR.8192

September 2017

U.S. Department of Commerce
Wilbur L. Ross, Jr., Secretary

National Institute of Standards and Technology
Kent Rochford, Acting NIST Director and Under Secretary of Commerce for Standards and Technology

National Institute of Standards and Technology Internal Report 8192
33 pages (September 2017)

This publication is available free of charge from:
https://doi.org/10.6028/NIST.IR.8192

Comments on this topic may be submitted through February 5, 2018 to:

National Institute of Standards and Technology
Attn: Applied Cybersecurity Division, Information Technology Laboratory
100 Bureau Drive (Mail Stop 2000) Gaithersburg, MD 20899-2000
Email: distributed.threats@nist.gov

See Section 5 of this document for additional details.

Reports on Computer Systems Technology

The Information Technology Laboratory (ITL) at the National Institute of Standards and Technology (NIST) promotes the U.S. economy and public welfare by providing technical leadership for the Nation's measurement and standards infrastructure. ITL develops tests, test methods, reference data, proof of concept implementations, and technical analyses to advance the development and productive use of information technology. ITL's responsibilities include the development of management, administrative, technical, and physical standards and guidelines for the cost-effective security and privacy of other than national security-related information in federal information systems.

Abstract

These proceedings document the July 11-12, 2017 "Enhancing Resilience of the Internet and Communications Ecosystem" workshop led by the National Institute of Standards and Technology. Executive Order 13800, "Strengthening the Cybersecurity of Federal Networks and Critical Infrastructure" required the Secretaries of Commerce and Homeland Security to "jointly lead an open and transparent process to identify and promote action by appropriate stakeholders to improve the resilience of the internet and communications ecosystem and to encourage collaboration with the goal of dramatically reducing threats perpetrated by automated and distributed attacks (e.g., botnets)." The workshop was designed to allow stakeholders to explore a range of current and emerging solutions addressing automated, distributed threats in an open and transparent manner. The workshop attracted 150 participants from diverse stakeholder communities and was conducted under Chatham House Rules.

Keywords

Botnet; distributed threat; distributed denial of service attack (DDoS); Internet of Things; resilience; root of trust; secure update

Acknowledgments

While the National Institute of Standards and Technology (NIST) convened this workshop, its success was due to the insightful contributions offered by the 150 participants from industry, academia, standards organizations, nongovernmental organizations, and government agencies. We particularly appreciate the contributions of our panel chairs and panelists; their thought provoking discussions were critical to the success of the breakout sessions that followed.

Finally, this workshop report would not have been possible without the extraordinary support we received from NIST's National Cybersecurity Center of Excellence (NCCoE) and The MITRE Corporation, the operator of the NCCoE. The NCCoE is a public-private collaboration for accelerating the widespread adoption of integrated cybersecurity tools and technologies, and is co-sponsored by the State of Maryland and Montgomery County, Md. The NCCoE and MITRE provided subject matter experts to capture the contributions from our participants and performed a detailed analysis after the workshop, identifying key areas of interest and concern. The subject matter experts that supported this process were:

- Brian Abe (NCCoE)
- Drew Allensworth (NCCoE)
- Brittany Biondo (Mitre)
- David Dandar (Mitre)
- Lura Danley (Mitre)
- Zachary Furness (NCCoE)
- Diane Khula (Mitre)
- Susan Prince (NCCoE)
- Julie Steinke (NCCoE)
- Caroline Tan (NCCoE)
- Aaron Temin (NCCoE)
- Teresa Thomas (NCCoE)
- Mary Yang (NCCoE)

Executive Summary

Executive Order 13800, "Strengthening the Cybersecurity of Federal Networks and Critical Infrastructure" was issued May 11, 2017. In Section 2 (d), the executive order requires the Secretaries of Commerce and Homeland Security to "jointly lead an open and transparent process to identify and promote action by appropriate stakeholders to improve the resilience of the internet and communications ecosystem and to encourage collaboration with the goal of dramatically reducing threats perpetrated by automated and distributed attacks (e.g., botnets)." The Executive Order directs the Departments to publish a preliminary report in January 2018 and submit the final report to the President by May 11, 2018.[1]

These proceedings document the July 11-12, 2017 "Enhancing Resilience of the Internet and Communications Ecosystem" workshop led by the National Institute of Standards and Technology. The workshop was one of several work streams pursued concurrently by various components of the departments to engage stakeholders and identify appropriate actions. The workshop attracted 150 participants from diverse stakeholder communities and was conducted under Chatham House Rules.

Six overarching themes emerged during the workshop discussions:

1. The global nature of the problem: The majority of the compromised devices that make up botnets are geographically located outside the United States. Coordinated action with international partners will be required to increase the resilience of the ecosystem against these threats.
2. The availability of effective tools: The tools, processes, and practices required to significantly enhance the resilience of the ecosystem are widely available, and routinely applied in selected market sectors, but generally under-utilized.
3. The importance of securing products throughout the full lifecycle: Devices that are vulnerable at time of deployment, lack facilities to patch vulnerabilities after discovery, or remain in service after vendor support ends, make assembling botnets and distributed threats far too easy.
4. The impact of gaps in education and awareness: Knowledge gaps in home and enterprise customers, product developers, and infrastructure operators impede the deployment of the tools, processes, and practices that would make the ecosystem more resilient. In particular, customer-friendly mechanisms to identify more secure choices analogous to the Energy Star program or vehicle crash ratings are needed to inform procurement decisions.
5. Conflicts between market incentives and resiliency goals: Perceived market incentives do not align with the goal of "dramatically reducing threats perpetrated by automated and distributed attacks." Market incentives motivate product developers and vendors to minimize cost and time to market, rather than build in security or offer efficient security updates.

[1] The full text of the Executive Order is available at https://www.gpo.gov/fdsys/pkg/FR-2017-05-16/pdf/2017-10004.pdf.

6. The need for coordinated cross-sector action: No single stakeholder community is positioned to address the problem in isolation. Contributions from all sectors will be required to significantly increase the resiliency of the ecosystem against botnets and automated distributed threats.

The workshop provided critical input that, along with the public input received in response to the National Telecommunication and Information Administration's Request for Comments and a report from the National Security Telecommunications Advisory Committee, will inform the development of the draft report. Implications for the January 2018 report include:

- Actions proposed in the report will address each of the overarching themes gleaned from workshop participants.
- The report will recommend one or more proposed actions for each of the stakeholder groups (i.e., infrastructure providers, product developers, enterprises, home users, academia, and government).
- Non-government stakeholders expect the Federal government to lead by example and promote actions by other stakeholders through incentives rather than regulation.
- Many actions will have dependencies upon actions assigned to other stakeholders, so collaborative mechanisms will need to be identified in the report as well.
- Recommendations will likely include immediate actions to increase awareness and deployment of currently available technologies, mid-term actions to create market incentives (especially to secure the full product lifecycle) and promote international coordination and collaboration, and long-term actions to develop new technologies.

Further public contributions on this topic are welcomed and may be submitted to distributed.threats@nist.gov. Contributions submitted by October 15, 2017 will be considered for inclusion in the preliminary report, which will be shared with the community on or before January 5, 2018.

Public contributions and comments on the preliminary report will be accepted through February 5, 2018. After the comment period has closed, a public workshop will be held in February to discuss the planned resolution of comments. Based on the public comments and discussions held at the second workshop, the Departments will complete the report for submission to the President on or before May 11, 2018.

Table of Contents

List of Appendices

List of Figures

1. Introduction

Executive Order 13800, "Strengthening the Cybersecurity of Federal Networks and Critical Infrastructure" was issued May 11, 2017. In Section 2 (d), the executive order requires the Secretaries of Commerce and Homeland Security to "jointly lead an open and transparent process to identify and promote action by appropriate stakeholders to improve the resilience of the internet and communications ecosystem and to encourage collaboration with the goal of dramatically reducing threats perpetrated by automated and distributed attacks (e.g., botnets)." The Executive Order directs the Departments to publish a preliminary report in January 2018 and submit the final report to the President by May 11, 2018.[2]

These proceedings describe the July 11-12, 2017 "Enhancing Resilience of the Internet and Communications Ecosystem" workshop led by the National Institute of Standards and Technology (NIST) as an initial step in this process. The workshop was conducted under Chatham House Rules. Participants were encouraged to share the opinions and information presented at the workshop, but were asked to refrain from identifying speakers or their affiliation. In keeping with the rules, this report does not associate issues raised within the workshop with organizations or industry sectors.

The workshop complemented several work streams pursued concurrently by various components of the departments to engage stakeholders and identify appropriate actions, including a Request for Comments published by the National Telecommunications and Information Administration (NTIA)[3] and Department of Homeland Security (DHS) tasking for the National Security and Telecommunications Advisory Council (NSTAC).[4]

The Proceedings is composed of five main components: this introduction; a brief recounting of the process employed to organize the workshop and develop the proceedings; a workshop summary highlighting common themes from the workshop; anticipated impacts by the information obtained from the workshop participants on the public draft of the report that Commerce and DHS will issue in January 2018; and opportunities for continued engagement on this topic.

[2] The full text of the Executive Order is available at https://www.gpo.gov/fdsys/pkg/FR-2017-05-16/pdf/2017-10004.pdf.

[3] The National Telecommunications and Information Administration (NTIA) published the "Request for Comments on Promoting Stakeholder Action Against Botnets and Other Automated Threats" on June 8. Additional information, including the public comments received by NTIA are available at https://www.ntia.doc.gov/federal-register-notice/2017/rfc-promoting-stakeholder-action-against-botnets-and-other-automated-threats.

[4] For additional information on NSTAC, please see https://www.dhs.gov/national-security-telecommunications-advisory-committee.

2. Workshop Planning, Execution, and Analysis

Workshop Planning

Immediately following the issuance of E.O. 13800, and concurrent with these efforts, NIST began planning a public workshop, in conjunction with our partners from NTIA and DHS, as an initial step towards engaging stakeholders in the development of the report. The workshop was designed to allow stakeholders to openly and transparently explore a range of current and emerging solutions to enhance the resilience of the Internet and communications ecosystem (the ecosystem) against automated, distributed threats. The workshop was announced on June 6, 2017 with just five weeks lead time to ensure that contributions could be reflected in the January public draft. Despite the lead time, the workshop quickly achieved full registration of 150 participants representing diverse stakeholder communities. The workshop planning team particularly appreciates the many accommodations made by our panelists, speakers, and facilitators to participate given the short lead time and unexpected disruptions of air travel.[5]

Overview of Workshop

The agenda was structured as a series of moderated panels and breakout sessions exploring the potential contributions of five key stakeholder communities: communications infrastructure providers; product developers; customers; researchers; and governments. In addition to offering subject matter expertise, the panels were intended to stimulate discussion in the breakout sessions. Breakout facilitators were directed to guide discussion towards identification of a broad range of options for a specific stakeholder community (e.g., infrastructure providers, product developers, or network owners) to enhance the resilience of the ecosystem against automated distributed threats. Facilitators were asked to defer discussion of options specific to other communities to the appropriate session, but discussion highlighting dependencies between possible actions by different stakeholder communities was encouraged. Facilitators were instructed that breakout participants need not achieve consensus with respect to a particular option, or establish an ordering or prioritization of these options.

Analysis and Preparation of Proceedings

NIST's National Cybersecurity Center of Excellence (NCCoE) provided cybersecurity subject matter experts (SMEs) to serve as scribes for the breakout sessions and performed the initial technical analysis of the collected inputs. Approximately 787 contributions were categorized into ten major categories; 313 contributions were also categorized as fitting into one of five orthogonal minor categories.

[5] See https://www.washingtonpost.com/news/dr-gridlock/wp/2017/07/10/hazmat-incident-at-air-traffic-control-center-delays-flights-around-the-washington-region/?utm_term=.d009260f400e.

The major categories were:

- Awareness
- Business Challenges
- Product Development & Lifecycle
- Complexity of Ecosystem
- Consumer Role
- Governance
- Information Sharing, Collaboration & Privacy
- Data
- Metrics
- Fundamental and Emerging Technologies

Scribes categorized the discussion topics raised in their breakout sessions according to these categories, and aggregated percentages were developed. The distribution of the 787 contributions is depicted in Figure 1, below. Nearly half of the contributions were characterized as business challenges or governance issues.

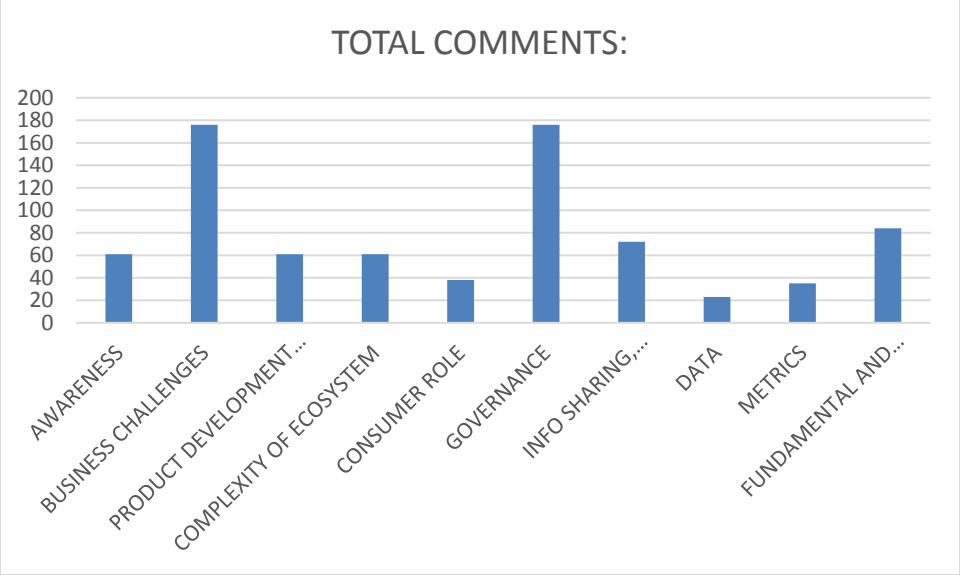

Figure 1. Distribution of Contributions as Characterized by Scribes

The minor categories were:

- Adversaries
- Communication
- Cybersecurity
- Lessons & Best Practices
- Standards

Scribes categorized the discussion topics raised in their breakout sessions according to these minor categories, and aggregated percentages were developed. The distribution of the 313 contributions is depicted in Figure 2 below. More than half of the comments assigned to minor categories were deemed cybersecurity issues, with lessons learned, communication, and standards getting the bulk of the remaining comments.

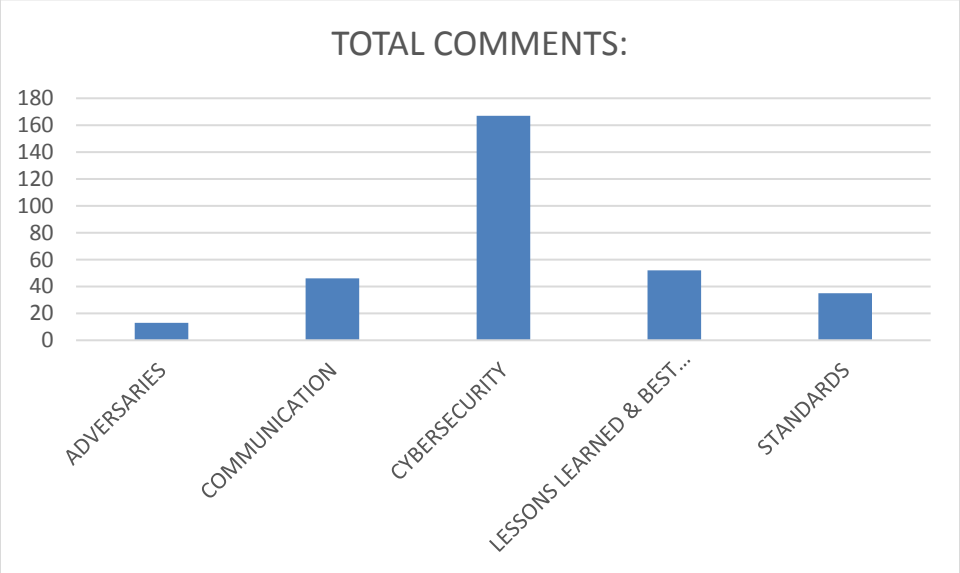

Figure 2. Characterization of Contributions According to Minor Topic Areas

NIST subject matter experts based this proceedings on the raw notes provided by the NCCoE scribes, bulleted lists of highlights prepared by the scribes, and the NCCoE supplied analysis, as well as the NIST SMEs' own personal notes.

3. Workshop Summary

This section summarizes the issues raised by presenters and workshop participants over the course of the workshop and is presented in two subsections.

- The first subsection presents six overarching themes that emerged from the discussions. These themes apply across multiple sectors, and were raised by different participants on multiple occasions. While consensus was not judged and should not be assumed, few spoke against these concepts.

- The second subsection offers sector-specific (i.e., specific to a stakeholder community) issues and observations. In some cases, this represents a more detailed view of the overarching themes, but in others the concepts are simply unique to that sector. The sector-specific observations are organized by workshop panel.

While the workshop scope included the full range of automated distributed threats, it should be noted that conversation frequently focused on the Internet of Things. It was clear that the Mirai botnet was "top of mind" for many participants, and provided a shared context for discussions on securing the product lifecycle, education and awareness, and many other topics. The IoT context is only reiterated in the summaries that follow where the issues or observations were specific to IoT (as opposed to illustrative framing.)

As noted previously, the workshop was conducted under Chatham House Rules, and facilitators were directed to focus on surfacing options for action rather than reaching consensus or obtaining objective measures of support. This summary uses the phrases "several participants," "a number of participants," and "many participants" to denote our subjective assessment of increasing levels of support or interest beyond the normal baseline.

Overarching Themes

Six overarching themes were encountered throughout the workshop discussions[6]:

1. The global nature of the problem;
2. The availability of effective tools;
3. The importance of securing products throughout the full lifecycle;
4. The impact of gaps in education and awareness;
5. Conflicts between market incentives and resilience goals; and
6. The need for coordinated cross-sector action.

Workshop participants noted repeatedly that botnets and distributed threats are a global problem. While there are exceptions, the majority of the compromised devices that make up botnets are geographically located outside the United States. Actions that increase the security of devices sold in the United States, or that protect against threats from domestic telecommunications

[6] Note that the workshop participants did not agree to these or establish a priority. Accordingly, the ordering of the six themes is not significant.

traffic, can only address a portion of the problem. Coordinated action with international partners will be required to increase the resilience of the ecosystem against these threats. While resolution will require a global approach, there was broad agreement that the United States could and should lead the way in the fight against these threats, acting by example and promoting appropriate norms of behavior.

There was also broad agreement that opportunities for immediate action were available. To quote one speaker, "We are not starting from a blank sheet of paper." By applying a suite of well-known and effective tools, processes, and practices, we can significantly enhance the resilience of the ecosystem. These tools have proven their value in the personal computing domain. However, these technologies and processes are not included in the common practices for product development and deployment in many other sectors. A set (or sets) of minimum standards or requirements needs to be established, although perhaps not formally, to ensure that best practices are applied across all sectors.

Addressing the entire product/network lifecycle with these tools, processes, and practices was another overarching theme. The importance of building security in from the beginning, rather than bolting it on later, was a widely shared belief. Far too many products are shipped with known vulnerabilities; these products may be detected, attacked, and compromised within minutes of deployment. Secure update mechanisms are needed to address vulnerabilities discovered during the normal product lifetime. Clear and effective processes to address end-of-life issues are also needed, as vulnerabilities in obsolete products cannot be addressed, ensuring that adversaries have a reliable starting point when penetrating an enterprise or establishing a botnet.

Participants noted a systemic education and awareness problem. Almost 6 % of the recommendations/comments during workshop breakout sessions focused on the importance of education and awareness. Many attendees cited transportation safety, where seatbelt usage and crash test ratings have led to better outcomes, as an education and awareness success story. Others cited the same sector as a cautionary tale, with long lead times before widespread acceptance of seat belts and other technological improvements. Energy Star was also the subject of repeated discussion, with simple metrics for consumers. An independent body to test and certify security-relevant features, and offer a more accessible rating scheme, was frequently cited as an important step towards consumer identification of products with strong security features.

Perceived market incentives do not align with our security and resilience goals, according to many workshop participants. Product developers and vendors minimize cost and time to market, rather than build in security or offer efficient security updates. Much of the discussion focused on techniques to create market incentives, such as independent product certification, but some felt that more active government intervention (e.g., regulation) would eventually be needed to overcome market failures. However, participants noted that regulatory compliance can also be at odds with our security and resilience goals.[7]

[7] For example, a number of attendees cited a historical reluctance within the health care sector to patch medical devices to avoid re-certification by the Food and Drug Administration. Note that current FDA guidance addresses this issue, allowing patching without requiring re-certification in some cases. See "Postmarket Management of Cybersecurity in Medical

Another theme was the inability of any particular sector to impact the resiliency of the ecosystem in isolation. Infrastructure providers can improve the efficacy of anti-DDoS mechanisms, but they can always be overcome by larger numbers of devices. Device manufacturers can improve the quality of their products, but we do not have the technology required to build perfect products, so some devices will always be vulnerable to compromise. Similarly, enterprise owners can increase their investments in security but some of their systems will be vulnerable, and adversaries have the entire Internet to launch attacks upon the enterprise. Researchers can develop better technologies, but security improvements are only realized if vendors include these technologies in products, customers purchase these products, and appropriately deploy them. Contributions from all sectors will be required to significantly increase the resilience of the ecosystem against botnets and automated distributed threats.

Sector Specific Summaries

This section reviews issues and observations from the workshop from the perspective of each stakeholder community in turn. In some cases, this represents a more detailed or nuanced view of the overarching themes, but in others the concepts are simply unique to that sector.

Infrastructure

The infrastructure provider sector was the subject of the first workshop panel and the following breakout session. The panel focused on the current state of the infrastructure, trends, and current and promising approaches to mitigate automated distributed threats such as DDoS, with particular focus on botnets and IoT.

Several participants noted that the Internet infrastructure is far more resilient today, and withstands DDoS attacks of previously unthinkable magnitude on a near-daily basis. This demonstrates both the effectiveness of current tools and the arms race nature of DDoS protection.

Participants explicitly identified a number of tools and techniques for DDoS protection; these are listed below with a brief discussion of strengths and limitations. (Order of presentation has no significance.)

- Ingress/Egress filtering: Many participants referred to the Internet Engineering Task Force (IETF) Best Current Practice (BCP) 38, “Network Ingress Filtering,” and BCP 84, “Ingress Filtering for Multi-Homed Networks.” Historically, DDoS attacks have relied on network address spoofing, where compromised systems assert source addresses that do not exist on the local network, to hide the location of the attackers’ resources.[8] By traffic filtering at enterprise boundaries and discarding traffic that is clearly illegitimate, it is possible to limit the effectiveness and scope of these attacks.

Devices”, https://www.fda.gov/downloads/medicaldevices/deviceregulationandguidance/guidancedocuments/ucm482022.pdf

[8] Some recent DDoS attacks, such as Mirai, have asserted legitimate source addresses.

BCP 38 and BCP 84 were published in 2000 and 2004, respectively, but adoption and deployment has been slow and uneven. While the level of current support was debated at the workshop, there was widespread support for ubiquitous deployment of traffic filtering for edge networks. There was brief discussion of the limitations of filtering within the Internet backbone, where asymmetric routing (where traffic between two endpoints follows separate paths in each direction) complicates differentiation of legitimate traffic from that with spoofed network addresses.

- Off-premise DDoS protection services: ISPs are offering off-premise DDoS protection services for customers, where traffic is rerouted and filtered before delivery to the customer network. DDoS protection services require provisioning significant additional resources (in terms of specialized systems and extra bandwidth) to absorb and process the projected additional traffic. These services have proven effective in numerous cases, but service providers are continually forced to increase the level of additional resources as botnets grow larger and total bandwidth of attacks increases.

  The effectiveness of these services is limited in part by customer awareness. DDoS protection services require provisioning significant additional resources (in terms of specialized systems and extra bandwidth) so they are not featured in basic network service offerings. Customers may not be aware of the risks presented by DDoS attacks until they become a victim, or that these services are even available. Even where an enterprise has the knowledge of and desire to procure anti-DDoS services, architectural changes may be required to optimize the level of security achieved.

  (Note: Communications between customers and service providers presents another challenge to the effectiveness of Off-Premise DDoS Protection services. See Realtime signaling, below.)

- On-Premise DDoS Protection: Where DDoS attacks are tailored to target an enterprise's critical resources, such as key applications or corporate firewall, local protection mechanisms may be more effective. These "On-Premise" services are now available as a supplement to the traditional service provider (off-premise) DDoS protection services offered by ISPs. As above, customer awareness of risks and available technologies is required as a precursor to enhancing resilience through these technologies.

- Realtime Signaling: As noted above, communications with DDoS protection services and devices during attacks can be problematic. Several attendees highlighted the Internet Engineering Task Force's DDoS Open Threat Signaling (DOTS) Working Group as a promising source for solutions in the near future. DOTS is currently developing a suite of standards for the realtime signaling of DDoS related telemetry and threat handling requests over links that may be congested by attack traffic.

Participants also highlighted a number of specific challenges for infrastructure-based approaches to enhancing the resiliency of the ecosystem.

- Global Coordination: The Internet is a global infrastructure, as is the threat. Infrastructure-based approaches demand close cooperation and coordination. Participants

indicated that cooperation amongst domestic peers has become fairly robust, but the international communication and cooperation has been uneven. There are efforts to establish norms and codify practices, but these efforts are lagging the problem.

Participants noted that almost fifty companies have agreed to the Mutually Agreed Norms for Routing Security (MANRS), and this agreement could be considered a model for a botnet-specific effort. Others pointed to the U.S. Anti-Bot Code of Conduct for Internet Service Providers (ABCs for ISPs) developed by the Federal Communications Commission's Communications Security, Reliability, and Interoperability Council ("CSRIC").[9]

- Complexity: Infrastructure issues are exacerbated by increasing complexity of the Internet – not just the advent of IoT, but also the expansion of multi-tenant infrastructure. The standards and practices that are widely applied to PCs and servers have not been uniformly applied to the IoT space, with unfortunate consequences, and smaller ISPs do not have the capacity to implement the same standards and practices as the large ISPs. Even where an enterprise has the knowledge of and desire to procure anti-DDoS services, architectural changes may be required to optimize the level of security achieved.

- Metrics: Usable metrics to characterize attacks and document their severity are lacking. One participant noted that the Federal Bureau of Investigation had developed a 75 attribute framework to describe distributed attacks, but that completing this description took so long that attacks were often over. Usable and widely recognized metrics are needed to facilitate coordination and cooperation.

- Inter-dependencies: Participants noted a number of dependencies with other sectors. Poor security attributes of edge devices, and especially of IoT devices, make it extremely difficult for the infrastructure to protect against these attacks.

- Education and Awareness: Customer education and awareness is urgently needed; when ISPs contact enterprises to alert them to problems, the enterprises are often ill-equipped to comprehend the problem or execute their own responsibilities. They generally assume that their ISP "was going to handle that", whatever "that" might be.

- Education and awareness for operational staff was also considered problematic. In particular, some felt that weak deployment of BCP 38 filtering at foreign ISPs, smaller domestic ISPs, and enterprise maintained BGP routers was largely a result of skills gaps within those organizations.

Product Manufacturer

The second panel and breakout session explored current efforts and future opportunities for

[9] Communications Security Reliability and Interoperability Council (CSRIC) III, U.S. Anti- Bot Code of Conduct (ABCs) for Internet Service Providers (ISPs), Final Report, WG 7 (Mar. 2012), http://transition.fcc.gov/bureaus/pshs/advisory/csric3/CSRIC-III-WG7-Final-Report.pdf

network component and device manufacturers (including IoT solution providers) to address the root causes of recent botnets (unconstrained network access, hard coded passwords, and buggy software). The discussion included products developed for both enterprise and home use.

There were two general characterizations of the product development problem. The most prevalent characterization indicated the number of vulnerabilities in products must be significantly reduced to make it harder to compromise devices en masse and launch large attacks. On the other hand, products will never be perfect, so some participants felt we should concentrate on technologies that limit the damage from compromised devices. The two characterizations are not in conflict, and most seemed to think both avenues should be pursued.

With respect to making it harder to compromise systems, many participants emphasized that this was a product lifecycle issue. It is critical, in their opinion, to manage the vulnerability of devices from initial product shipment, through use, to end-of-life. A number of techniques that reduce the vulnerability of products were discussed:

- To reduce the vulnerability in products at initial deployment, participants suggested increased application of a number of complementary tools and best practices. For example, secure by design development processes are more likely to result in default settings that are generally secure and avoid hard-coded administrative passwords and other common pitfalls. Security-sensitive software development toolchains can eliminate common coding errors, such as most buffer overflows.

- Even when developed using secure-by-design methodologies and security-focused toolchains, vulnerabilities in software are likely to be detected, continuing for months or years after the product is first deployed. Malware targeting these vulnerabilities is often widely available in days or weeks after detection. To manage the vulnerability of these products, many participants asserted that secure and preferably automatic update is absolutely essential. Additionally, they asserted that manufacturers should commit to patching security vulnerabilities for some minimum period after deployment.

- Roots of trust are a complementary technology that was cited by numerous participants. By providing a set of basic and highly trusted functions, we can increase assurance that software and firmware are unchanged or were only changed through secure update mechanisms. The Trusted Platform Module (TPM) is a widely available example, but may be too costly for inexpensive devices. New efforts, such as the Trusted Computing Group (TCG) Device Identity Composition Engine (DICE) may expand the scope of products that incorporate these technologies by providing a basis for device identity and verifying software updates have been installed. Devices need an identity issued by the manufacturer so there is a way to know what kind of device it is and what configuration, software and patches are intended for the device. The draft NIST SP 800-193 publication from May 30, 2017 describes roots of trust for protection, detection and recovery that could be applied in the IoT space as building blocks to remotely recover devices. People are unlikely to individually manage IoT devices, so automated recovery is needed.

- End-of-Life Issues and Unlicensed Software: Participants also highlighted the vulnerabilities associated with devices that are not supported by their manufacturer. In

such cases, updates are no longer being released (or perhaps never were) so vulnerabilities persist indefinitely. This has parallels with unlicensed software, where security updates are generally unavailable.

Participants lauded Microsoft's decision to update Windows XP to mitigate the WannaCry exploit, in spite of ending support three years earlier, but felt this was an exceptional case. Participants regarded past proposals for general solutions to end-of-life problems, such as releasing software for unsupported products to the open source community, as impractical.

Participants noted that the techniques above are widely known and well understood. They are applied broadly in some sectors (e.g., operating systems) but almost never in others (e.g., the Internet of Things). A number of impediments and root causes were suggested, including:

- Consumer Education and Awareness: Product manufacturers are motivated by sales, and consumers do not have the perspective required to prioritize security or the ability to identify the products with higher assurance. Consumers may not be naturally motivated to choose such products, given that compromised products often continue to perform their given function while participating in distributed attacks. Consumer education should focus on potential security implications and performance impacts rather than botnet prevention – users may not care if their nanny cam attacks a large bank, but they will care about strangers invading their family's privacy.

  Once motivated, consumers will still need assistance to select products that are likely to have less vulnerabilities throughout the deployment lifecycle. No satisfactory mechanism for conveying information to consumers regarding the security of products exists today. Energy Star for energy efficiency and the National Highway Traffic Safety Administration's (NHTSA's) 5-Star Safety Ratings for vehicle safety were cited as important and successful examples.

- Product Developer Education and Awareness: As the space between IT and traditional product lines blur, educating product developers about security has become an urgent need. Designers of household appliances understand how to keep foods at a safe temperature, clean fabrics, or toast bread. As these products become part of the ecosystem, we are asking these designers to incorporate new security requirements that are foreign to them. In particular, industry needs to recognize that secure update mechanisms are a requirement for "everything."

- Misalignment with Market Incentives: Many product developers are afraid that investing in security will make their products more expensive and delay rollout of the innovative new features that build market share. Larger vendors have more robust development processes, but startups and smaller companies often rely on less mature processes.

- Unclear responsibility: There was also discussion with respect to responsibility – who should be responsible for the security of products? Owners? Vendors? For home users and small businesses, it seems impractical to hold them responsible if their home DVR or the security camera in their convenience store is compromised and added to a botnet. For

industrial users, we may be able to have higher expectations, but as IoT devices multiply there may be limitations there as well. In both environments, protocols such as the Manufacturer's Usage Description (MUD, see Virtual Network Segmentation below) may help shift some of the responsibility to the manufacturers in a scalable fashion.

The second viewpoint was that products will never be perfect, and the incentives simply don't focus on security. This reinforces the idea that secure update is a foundational security requirement, but we also need to find ways to limit the damage from compromised devices. Several directions forward were proposed, including:

- Virtual Network Segmentation: Historically, Internet-connected systems have enjoyed full connectivity at the network and transport layers.[10] The needs of human users are unpredictable, so significantly constraining traffic would be unmanageable. The security implications of full connectivity are significant: any device on the Internet can be used to launch an attack on any other device; once compromised, the device becomes a launching pad for lateral movement both within the enterprise and attacks on other Internet-connected devices. With the emergence of the Internet of Things (IoT,) communications needs for many devices become more predictable and the security implications of full connectivity unacceptable. For example, an IoT thermostat may need to communicate with the manufacturer's website for updates but probably does not need to communicate with a stock exchange.

  The MUD standard currently under development in the IETF offered one potential path forward. When devices join the network, they request an IP address through the Dynamic Host Configuration Protocol (DHCP). When using MUD, the device also indicates how to securely obtain a description of the device's communications requirements from the manufacturer. Networking equipment vendors leverage the MUD file and their existing capability to enforce packet filtering on a per device basis. If compromised, the attacker could not use the IoT thermostat to move laterally through the coffee maker or attack the stock exchange.

- Threat signaling offers an alternative approach for constraining network access. Third party services identify host systems or domains that present a relative threat to the ecosystem (or some sector of industry). This information is passed to subscribing enterprise networks, which establish appropriate route filters and discard potentially harmful traffic. While MUD is tailored to support devices with well–defined communications requirements, threat signaling enhances the security of personal computing devices with user-driven (and unpredictable) communications needs.

Customers: Enterprises, Home Users, and Government

The third panel and breakout session explored how customers, particularly in the enterprise, can both protect themselves from distributed attacks--including DDoS, attacks on critical

[10] Later, network administrators could constrain access through firewall rules that applied across the enterprise, but there were generally no limitations within the enterprise.

applications, and fraud--and avoid being part of the problem. Participants were asked to highlight the capabilities and limitations of best current practices and emerging technologies, and consider the potential for cross-sector collaboration.

Many participants differentiated customers into three broad classes: home users; enterprises; and government. Enterprises were further differentiated by size in some discussions – either as large versus small and medium sized businesses (SMBs), or startups versus established companies. Participants had vastly different expectations for different classes of customers in terms of awareness, best practices, applicability of technologies, and collaboration.

Participants identified a number of current and emerging best practices:

- As noted earlier, many participants identified secure update for all networked devices, including both an appropriate update mechanism and a vendor commitment to provide patches, as the most important best current practice. The details of an "appropriate" update mechanism depended upon the intended customer. For example, participants suggested that home users would only benefit from secure update if the mechanism was automatic and unattended. Large enterprises would demand a higher level of control through centralized management tools. The needs and expectations of SMBs could vary depending upon network architecture and expertise.

- Real-time information sharing was identified as a best current practice for government and larger enterprises. Sharing information, both within the enterprise and across the ecosystem, will allow enterprises to better protect resources. Participants observed that malicious actors are better at this than we are.

  However, information must be shared in an actionable form, rather than as unformatted text. There are multiple solutions currently available for general cybersecurity information sharing. In particular, participants identified the Structured Threat Information eXpression (STIX™) and Trusted Automated eXchange of Indicator Information (TAXII™) as current best practice. The DDoS Open Threat Signaling (DOTS) standards currently under development in the IETF will provide a DDoS specific solution.

- Network architectures that constrain traffic flows to limit potential attack vectors and constrain attacks that can be launched from compromised systems were also discussed. Emerging technologies that establish virtual segmented networks, such as the MUD protocol (see Product Manufacturer, above) would provide actionable information to home and enterprise networks in a scalable manner. For legacy devices, network equipment could leverage "threat signaling" (e.g., information sharing to identify local compromised systems and suspicious external systems or domains) and constrain traffic appropriately.

Since much of the necessary technology is widely understood, significant discussion was devoted to perceived impediments to and potential drivers for adoption.

- The current and potential impact of cyber insurance was widely debated. Experience from other sectors demonstrates that insurance can drive adoption of technologies. For example, automotive insurance discounts for anti-lock brakes and air bags encouraged consumers to prioritize these features. Insurance for buildings often requires smoke detectors and may provide discounts for sprinklers or other active measures. However, cyber insurance offerings are often inconsistent and were judged to have had minimal impact to date on cybersecurity technology deployment.

- Some participants suggested that additional actuarial data will be required to positively impact the market. Once data is available to impose uniform requirements and offer discounts for beneficial options, cyber insurance could positively influence enterprise owners.

- Education and awareness is a systemic problem, especially for SMBs and home users. On average, government and large enterprises were expected to have significant awareness and relatively deep knowledge of security requirements to support product selection and implementation of best practices. On the other hand, the national pool of cybersecurity experts is insufficient to impose these expectation on SMBs, and home users cannot be expected to become cybersecurity experts.

  While drowning in information, customers have no way to differentiate snake oil from effective technologies. For example, one participant received 32 emails for products that claimed to protect against WannaCry the day after that attack was launched. Few customers would have the ability to evaluate their claims so most take no action.

  To facilitate productive procurement and deployment decisions, customers need accessible data. Participants highlighted the importance of certification of products and debated the impact of various certification regimes. The NHTSA 5-Star Safety Rating and DOE's ENERGY STAR scorecard were cited as examples of packaging certification data in an accessible form. Participants have high hopes for ongoing initiatives at Underwriters' Laboratories and Consumer Reports, although the criteria for those efforts was unclear. Demonstration projects at the NCCoE and their associated practice guides offer another promising option.

- Participants espoused a range of views regarding the possibilities of strictly voluntary adoption. While all participants expressed a preference for voluntary measures, there was concern that slow adoption would force the government to step in, particularly in sectors that are already regulated. The prospect of regulations at a state level was particularly concerning to participants. The possibility of 50 slightly different sets of regulations would be counterproductive, complicating the offering of products and services. However, imposition of increased requirements upon government entities themselves, to lead by example and create an initial market, was frequently recommended.

- Clarity of regulations (if imposed) was considered essential to avoiding unexpected consequences. When forced to infer, regulatory hurdles are often imagined that constrain or prevent implementation of appropriate security mechanisms.

- Participants also expressed concerns about cost. Without government incentives, costs for enhancing cybersecurity must be passed on to consumers. In a globally economic environment, imposition of requirements domestically can hamper the competitiveness of businesses abroad.

In summary, participants agreed that cultural changes will be required before home users and American enterprises maximize their contribution to the resilience of the ecosystem.

Research and Academia

The second day of the workshop began with the Research Directions panel, and the topic was also addressed as part of the sole Day 2 breakout session later that morning. The goal of these discussions was to identify and explore gap areas with respect to providing network resilience, and highlight opportunities to address those gaps.

Participants identified a broad range of research directions that could positively impact the resilience of the ecosystem, including:

- Metrics and classification: Metrics and classification methodologies for automated distributed threats could improve prioritization of resources for mitigation efforts and law enforcement actions.

- Botnet/DDoS modeling: Robust models for botnets and other automated threats that encompass detection, passing data, and enforcement could enable more comprehensive and coordinated responses.

- Malicious actor behavior: Changes in DDoS actors behavior will negatively impact the efficacy of many current techniques. These changes include the nationalization of state mafias and cyber criminal organizations; the shift from "stolen resources" to "criminal infrastructure"; and the shift from user-driven traffic to automated systems/IoT. Research is needed to predict the impact of these changes on current anti-DDoS technologies.

- Socio-technical issues: Resilience, like many aspects of cybersecurity, has social dimensions and cannot be addressed through technology alone. Participants highlighted the importance of research approaches that consider human, social, organizational, economic and technical factors, and their impact on deployment and operation of a resilient infrastructure. Human-machine interfaces (see below) were a specific focus. Research is also needed to understand how to design organizations that are more resilient in the face of cyberattack and more efficient in their incident or disaster recovery processes.

- Human machine interfaces: Given our workforce challenges in cybersecurity, improvements in human-machine interfaces are urgently needed. The relationship between operational technologies (e.g., SCADA components) and their operators was of particular interest. Automation potentially offers numerous security benefits, but operators will need greater transparency into the algorithms before they will trust machine decisions.

Home users provide another machine interface challenge. Engineering to user behavior, rather than assuming unlikely changes, may increase the efficacy of current technologies.

- Machine Learning/Artificial Intelligence (AI): Machine learning and AI techniques may offer new avenues for early detection of and adaption to stresses, including distributed threats. Additional research in machine decision making, modeling of what-if scenarios, and the use of big data (from network and system sensors) to establish normal baselines could potentially contribute to the resilience of the ecosystem.

- Attribution: Attribution of computer security incidents is problematic, and is arguably more difficult for botnets and distributed threats. Identifying the malicious actor and the compromised systems would contribute positively to mitigation during attacks, and enable law enforcement actions that could deter subsequent actors.

- Evidence of Efficacy: As with other aspects of computer security, evidence that tools and techniques are effective is needed to justify continued investment.

- Remediation: After detecting compromise, users are often faced with unpalatable options: attempt to clean the system; or discard the device. Cleaning the system is often unreliable; remediation processes can be complex, and advanced persistent threats (APTs) are designed to survive remediation. Discarding devices is expensive and impractical in most scenarios. Research that makes remediation simpler and more reliable for users would clarify these choices and increase resilience after a detected compromise.

- Architecting networks for resilience: Network designs can impact resilience, and limit options for anti-DDoS mechanisms. Research into network design to maximize resilience and preserve options is needed.

- Much of the recent research in network resilience has focused on increasing visibility into edge networks, but opportunities may exist to leverage new sensors and make the Internet "smarter" in its core. To enable these next generation architectures, research is needed that identifies the types of sensors, where to locate them, which information should be shared, and with whom.

Participants also noted several impediments to research-focused efforts to enhance the resilience of the network, including:

- Education and Awareness: Physics, chemistry, and other scientific fields are introduced much earlier in the United States' education system than computer science in general and cybersecurity in particular. Late exposure to the field limits interest, as many students have identified a field of study before heading to college. Attracting more of the best and brightest would likely have a ripple effect in terms of the aggregate intellectual property.

- Lack of Monetary Resources: Budgets for research are shrinking across both public and private sectors. The National Science Foundation underwrites a significant portion of both basic and applied research in the field, but the total dollars available are insufficient to fund all the promising research efforts.

Government and Public Policy

Day 2's second panel addressed government and public policy options to enhance the resilience of the ecosystem. The topic was also addressed, along with research directions, as part of the Day 2 breakout session later that morning.

As with the other sectors, participants noted that many ongoing activities in government and public policy are already underway to enhance the resilience of the ecosystem, including:

- Law enforcement actions: Law enforcement agencies at all levels are pursuing more cybersecurity related crimes, including those involving automated distributed threats. In particular, participants noted that the Federal Bureau of Investigation has taken down a number of high-profile botnets in recent years. These successes provide a foundation for future cases and create a measure of deterrence.

- Regulatory enforcement: Regulatory agencies are developing and enforcing policies for cybersecurity within their traditional scope. For example, the Food and Drug Administration has established guidelines for medical devices that decouple basic security updates from existing product certification regimes, and the Federal Trade Commission (FTC) has taken action in numerous privacy and security-related cases. IoT devices have figured in some of these enforcement actions.

- Policy initiatives: Privacy and data security issues for IoT devices have been the focus of policy initiatives in several departments and agencies. The FTC's IoT workshop series focusing on specific IoT devices (e.g., drones, smart TVs) and the FTC public competition "IoT Home Inspector Challenge" were two prominent examples from a long list of activities.

- Education and awareness: The Federal government is working to bridge education gaps on the national scale through the National Initiative for Cybersecurity Education (NICE), which includes many government agencies. Regulatory agencies are independently pursuing complementary education activities, such as publication of guidance and blog posts, that are targeted towards their stakeholders.

- International coordination and collaboration: Other governments are also responding to automated distributed threats to the ecosystem, and are reaching out to their traditional partners and allies to coordinate and exchange information.

As in other sectors, these efforts are significant but more is needed to mitigate the evolving threat. Participants identified several different vectors for government to impact the resilience of the network, including:

- Procurement: While recognizing the Federal government's purchasing power is no longer the dominant force in the information technology market, participants encouraged government to use the power of the purse in concert with well-specified technical requirements as a step towards key goals and to lead the private sector. For example, by requiring vendors to support automated security updates, the government could increase

the resilience of the Federally owned and managed components of the ecosystem and expand the range of options available to security-focused private sector entities.

- Basic research: Participants noted that the Federal government remains the primary funding source for basic research in most scientific disciplines. Industry is understandably focused on later stage R&D, so the Federal government must ensure that funding is both sufficient and well-directed.

- International Cooperation and Coordination: As noted earlier, the ecosystem is global, and effectively combatting distributed threats will require cooperation by and coordination with non-US service providers, manufacturers, and enterprise users. In some cases, these entities are tightly coupled with nation states. The federal government is uniquely positioned to promote and facilitate cooperation and coordination with such entities.

- Law Enforcement: Law enforcement efforts to takedown botnets and mitigate these threats had broad support amongst participants. Cautious support for reviewing and revising policies that impede prosecution was expressed, with the caveat that revisions must balance law enforcement concerns with privacy and property rights.

- Creating Market Incentives: Several participants identified the draft document Communicating IoT Device Security Update Capability to Improve Transparency for Consumers, developed through NTIA's multistakeholder process on Internet of Things Security Upgradability and Patching, as an example that could create market incentives for security upgrades.[11]

- Regulation and Market Incentives: Participants preferred market incentives to broad regulatory initiatives, but expressed a degree of pessimism given past market failures. Participants noted that new cybersecurity-focused regulations in currently regulated sectors could be appropriate and have a positive impact if carefully considered. Medical devices were highlighted as one such industry sector, and FDA's recent statements regarding patching were cited as an example of thoughtful and balanced regulation. Regulations could also have a positive impact by clarifying liabilities and accountability at different stages in the product lifecycle or incident response process.

    - It was suggested that following a model like that used by the International Telecommunications Union – Radio Sector (ITU-R) for managing radio spectrum internationally might be a good approach to establishing how to cooperate in cyberspace internationally.

[11] For the draft document, see https://www.ntia.doc.gov/files/ntia/publications/draft_communicating_iot_security_update_capability_-_jul_14_2017_-_ntia_multistakeholder_process.pdf. For more on the NTIA-led IoT effort, see https://www.ntia.doc.gov/category/internet-things.

- Education and Awareness: There is a lot of defensive cybersecurity guidance already available and either not known or being ignored. Perhaps more emphasis should be put on getting more pervasive implementation of basic protections.
    - If we are going to rely on consumers to handle cybersecurity, we need to both make it easier and provide more education, much earlier than currently delivered, on models to help people understand cybersecurity.

- Streamlining Remediation: Perhaps Government can do more to make remediation easier after a breach. Can citizens get assistance in recovering from breaches, such as making it easier to notify people and organizations that new accounts are being established and old accounts are void.

- Establishing Guidance: Participants suggested that the Federal government in general, and NIST in particular, could assist industry through additional guidance to support voluntary action. A number of participants cited the process NIST used to develop the Framework for Improving Critical Infrastructure Cybersecurity (Cybersecurity Framework) as a model of consensus building towards useful and accepted guidance. Participants explicitly suggested extending the Cybersecurity Framework to address IoT.[12]

- Lead by Example: Participants noted that relatively few devices in recent botnets were located in the U.S, validating domestic security approaches. This success story is largely overlooked and is not replicated. To create incentives for those outside the U.S. to take security measures, we must prove our success and then advertise it internationally, sharing our solution. Through this success, we, as a community, could convince the right people to act and to make cybersecurity spending decisions.

- Incentivizing Non-Market Actions: From an ISP perspective, there are costs associated with certain tasks that increase the resilience of the network but do not directly benefit either the customer or ISP. (Quarantining and notifying customers was cited as an example.) Government could incentivize these non-market actions by providing funding or otherwise allowing businesses to recoup costs.

[12] Extending the CSF to IoT would most likely entail developing an IoT sector profile, much like the CSRIC IV effort for the communications sector. See CSRIC IV, Cybersecurity Risk Management and Best Practices, Final Report, WG 4 (Mar. 2015),

https://transition.fcc.gov/pshs/advisory/csric4/CSRIC_IV_WG4_Final_Report_031815.pdf.

4. Conclusions & Implications

Executive Order 13800 directed the Departments of Commerce and Homeland Security to submit a report to the President that will "identify and promote action by appropriate stakeholders to improve the resilience of the Internet and communications ecosystem and to encourage collaboration with the goal of dramatically reducing threats perpetrated by automated and distributed attacks (e.g., botnets)."

The workshop provided critical input that, along with the NTIA Request for Comments and NSTAC report, will inform the development of the draft report. Implications for the January report include:

- Actions proposed in the report will address each of the overarching themes gleaned from workshop participants.
- The report will recommend one or more proposed actions for each of the stakeholder groups (i.e., infrastructure providers, product developers, enterprises, home users, academia, and government).
- Non-government stakeholders expect the Federal government to lead by example and promote actions by other stakeholders through incentives rather than regulation.
- Many actions will have dependencies upon actions assigned to other stakeholders, so collaborative mechanisms will need to be identified in the report as well.
- Recommendations will likely include immediate actions to increase awareness and deployment of currently available technologies, mid-term actions to create market incentives (especially to secure the full product lifecycle) and promote international coordination and collaboration, and long-term actions to develop new technologies.

5. Next Steps & Opportunities for Engagement

Concurrently with publication of this report, NTIA will publish a summary of statements submitted in response to the June 2017 Request for Comments.[13] Commerce and Homeland Security will commence development of the report based on the public feedback provided to date, incorporating additional input as received. In parallel, the NSTAC will continue work on its report for publication October 31, 2017.

Further public contributions on this topic are welcomed and may be submitted to distributed.threats@nist.gov. Comments submitted by October 15, 2017 will be considered for inclusion in the preliminary report, which will be shared with the community on or before January 5, 2018.

Public contributions and comments on the preliminary report will be accepted through February 5, 2018. After the comment period has closed, a public workshop will be held in February to discuss the planned resolution of comments. Based on the public comments and discussions held at the workshop, the Departments will complete the report for submission to the President on or before May 11, 2018.

[13] See https://www.ntia.doc.gov/federal-register-notice/2017/report-responses-ntia-s-request-comments-promoting-stakeholder-action

A. Agenda

The following pages present the public agenda for the workshop as posted before the workshop.

There were two "day-of" agenda changes: Carlos Morales from Arbor Networks participated in the first panel (Communications Infrastructure) on behalf of Arabella Harrington; and Craig Hyps from Cisco participated in the second panel (Products) in Eric Wenger's stead.

Enhancing Resilience of the Internet and Communications Ecosystem

NIST National Cybersecurity Center of Excellence, Rockville MD

July 11-12, 2017

Workshop Purpose: The purpose of this workshop is to explore a range of current and emerging solutions to enhance the resilience of the Internet against automated distributed threats, such as botnets. Deployment of these solutions will depend upon the ability and willingness of various parties to take action. Depending upon the specific solution, actions may be required by infrastructure providers, device manufacturers, system and network owners, research community, government, and/or standards developers. By exploring the solution space with a broad cross-section of participants, NIST hopes to identify promising avenues for all parties to enhance the resilience of the Internet.

Workshop Output: NIST will produce a workshop proceedings document that summarizes the session discussions, captures findings, and identifies opportunities for next steps. Outputs of this workshop will also serve as input to implementation activities related to Executive Order 13800, *Strengthening the Cybersecurity of Federal Networks and Critical Infrastructure*.

Agenda

Tuesday July 11, 2017

7:30	**Registrant Check-In**
8:30	**Welcome and Workshop Overview**
8:45	**Setting the Stage** *This plenary session will summarize the problem space (e.g., the botnet ecosystem), identify stakeholders (standards/protocol developers, infrastructure providers, consumers, manufacturers, regulators) in botnet mitigation, and review past approaches and outputs.* **Ari Schwartz, Venable**
9:30	**Infrastructure Provider's Perspective: Current and Emerging Standards, Best Practices, and Technologies (Panel 1)** *This plenary session will explore current efforts and future opportunities to enhance the resilience of the infrastructure (e.g., the Internet). This panel will discuss current state, trends, and current and promising approaches to mitigate automated distributed threats such as DDOS, with particular focus on botnets and IoT.* **Russ Housley, Vigil Security (moderator)** **Richard Barnes, Cisco** **Arabella Hallawell, Arbor Networks** **Danny McPherson, VeriSign** **Brian Rexroad, AT&T**

10:15	**Break**
10:30	**Session 1 Breakout (assigned)**
12:00	**Lunch**
1:00	**Product Development (Panel 2)** *This plenary session will explore current efforts and future opportunities for network component and device manufacturers (including IoT solution providers) to address the root causes of recent botnets (unconstrained network access, hard coded passwords, and buggy software). Session scope includes both enterprise and home use.* **Yolonda Smith, Pwnie Express (moderator)** **Anura S. Fernando, Underwriters Laboratory** **Jeff Greene, Symantec** **Rob Spiger, Microsoft** **Eric Wenger, Cisco**
1:45	**Session 2 Breakout (assigned)**
3:00	**Break**
3:15	**Customer Perspective: Current Approaches (Panel 3)** *This plenary session will explore how Internet users, particularly in the enterprise, can protect themselves, and avoid being part of the problem. Panelists will begin with an overview of the challenges an enterprise might face from distributed attacks, including DDoS, web applications, and fraud. Discussion will highlight the capabilities and limitations of best current practices and emerging technologies, and the potential for cross-sector collaboration.* **Nadya Bartol, Boston Consulting Group (moderator)** **Steve Curren, HHS Office of the Assistant Secretary for Preparedness and Response** **Matt Eggers, US Chamber of Commerce** **Bradley Nix, Deputy Director for US-CERT at the NCCIC, DHS** **Spencer Wilcox, Exelon**
4:00	**Session 3 Breakout (assigned)**
5:00	**Adjourn Day 1**

July 12, 2017

7:30	**Registrant Check-In**
8:30	**Welcome and Opening Remarks**
8:45	**Research Directions** *This panel will identify and explore gap areas in approaches to mitigating botnets, and highlight opportunities to address those gaps.* **Pat Muoio, Cybertech Consulting (moderator)** **David Dagon, Ga Tech** **Keith Marzullo, Univ. of MD** **Phil Reitinger, Global Cyber Alliance**
9:30	**The Government Role** *This plenary session will discuss current efforts and future opportunities for governments to enhance the resilience of the infrastructure, which may include policy and regulatory approaches, incentives and market motivators, economic impacts, and international considerations.* **Grace Koh, NEC (moderator)** **Andi Arias, FTC** **Tom Grasso, FBI** **John Nicholson, UK Embassy** **Malikah (Mikki) Smith, HHS/ONC**
10:15	**Break**
10:30	**Research & Government Role Breakouts**
11:15	**Break**
11:30	**Summary of Day 1 Breakout Sessions**
12:00	**Open Discussion**
12:30	**Closing and Next Steps (DOC/DHS)**
12:45	**Adjourn**

National Security Archive,

Suite 701, Gelman Library, The George Washington University,

2130 H Street, NW, Washington, D.C., 20037,

Phone: 202/994-7000, Fax: 202/994-7005, nsarchiv@gwu.edu