vmware

VMware Response for:

National Science Foundation Cyber Security Research and Development Strategic Plan RFI

June 15th, 2015

Legal Notice

The contents of this document constitute valuable proprietary and confidential property of VMware Corporation and are provided subject to specific obligations of confidentiality set forth in one or more binding legal agreements. Any use of this material is limited strictly to the uses specifically authorized in the applicable license agreement(s) pursuant to which such material has been furnished. In the event there are no applicable license agreement(s) governing the use of this material, please be advised that any use, dissemination, distribution, copying or disclosure of all or any part of this material not specifically authorized in writing by VMware Corporation in advance is strictly prohibited.

This is not a legally binding document and is submitted for information purposes only. Due to the forward-looking nature of this document, VMware's response may include information about products that may be in the planning stage of development or that may represent custom features or product enhancements. Feature and functionality cited in this document that is not publicly available or generally available today is discussed within the context of the strategic evolution of the proposed products. Future functionality estimated release dates and product roadmaps that may be included are for informational purposes only and should not be considered firm commitments on the part of VMware. VMware is under no obligation to provide such future functionality.

vmware

TABLE OF CONENT

Executive Summary

Cybersecurity threats to digital infrastructure are increasing and pose real risks to government as more agencies undergo digital transformation. The Cybersecurity Enhancement Act of 2014 coordinates efforts across several federal agencies in the development of a cybersecurity R&D strategic plan. This plan will outline cybersecurity research objectives that will require government funding. As a trusted technology partner to government, VMware is pleased to respond to the request for public input on the research objectives for the strategic plan.

The National Science Foundation (NSF) has a requirement to identify gaps, learn about innovative technologies, foster rapid transfer of R&D results and improve current research infrastructure and access. Cybersecurity is an ever-changing threat landscape; as soon as vulnerability is mitigated, another threat vector arises. Actors are diverse, creative and have a persistent motivation to harm our digital infrastructure. Federal government needs to approach these challenges differently than they have in the past. Even with growing spend on IT security, we're seeing more security breaches and it's growing at an alarming rate. VMware's Software-Defined Data Center architecture enables secure, resilient and agile IT infrastructure to address these challenges.

VMware virtualization technology has helped Federal agencies optimize and manage their data center infrastructure for over 14 years and is used in over 80% of the government today. VMware virtualization software is in the data centers for all 15 Cabinet level agencies, the Department of Defense, all Military services, and the Legislative and Judicial branches of the Federal Government. The Software-Defined Data Center (SDDC) architecture applies the principles of abstraction to deliver an entire data center construct in software, decoupling service delivery from the underlying physical infrastructure.

VMware has identified some suggestions that will address the issues and concerns in response to NSF's RFI below including:

Improved Security Through Automation – Policy-based automation is a core capability of SDDC and reduces manual tasks and errors, resulting in more consistent configurations and operations.

Network Security Inherent to the Platform – This security capability – referred to as micro-segmentation – is an architectural approach that follows the notion of the "zero trust model" for least privilege access and granular security controls. This integrated capability in the platform provides greater visibility and security for the infrastructure.

Secure Desktop Computing Platform – The SDDC is the platform that enables centralized and managed virtual desktops that provide secure end user access to the digital infrastructure.

The SDDC is industry's preferred architectural approach for agility and flexibility in the data center. It's security benefits have emerged as the key business driver for accelerated market adoption. VMware with its proven track record of innovation will continually strive to solve today's toughest IT challenges.

Our Response to the RFI

Questions Related to the Cyber Security Enhancement Act of 2014

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

a) how to design and build complex software-intensive systems that are secure and reliable when first deployed

There is an implementation gap in the way software-intensive systems are designed and built. A Security Development Lifecycle program should be institutionalized as part of agencies' software development lifecycle to identify and mitigate security risks during the development phase of products. The goal is to remediate issues early in the lifecycle.

b) how to test and verify that software and hardware, whether developed locally or obtained from a third party, is free of significant known security flaws

There is an implementation gap during the test and verification phases. Product validation that leverages automated vulnerability scanning processes and 3rd party penetration testing conducted by outside consultants should be a consistent part of the development lifecycle.

c) how to test and verify that software and hardware obtained from a third party correctly implements stated functionality, and only that functionality

We recommend a repeatable process to clearly identify the functional scope of the product. A repeatable testing and verification strategy that clearly documents the test plan, encompasses multiple types of tests, and uses automated testing tools.

d) how to guarantee the privacy of an individual, including that individual's identity, information, and lawful transactions when stored in distributed systems or transmitted over networks

We recommend research around how to compute over encrypted data (client stores encrypted data in cloud and cloud provider computes over encrypted data), how to store and transmit encrypted data without provider knowing what parts are accessed and how to maintain encryption keys securely, potentially by never storing keys with data. We also recommend research on how to distribute an encryption key, potentially by spreading keys between several independent entities.

e) how to build new protocols to enable the Internet to have robust security as one of the key capabilities of the Internet

VMware utilizes industries leading edge partners to address internet protocols when faced with requirements as this.

f) how to determine the origin of a message transmitted over the Internet

VMware utilizes industries leading edge partners to address internet protocols when faced with requirements as this.

g) how to support privacy in conjunction with improved security

There is an implementation gap around privacy and product development. Privacy should be an integral part of the product development lifecycle. A Privacy Program that utilizes a "privacy by design" framework should be instituted to promote the consideration of privacy and transparency as part of products that are developed. A privacy team can work with engineers during product development to evaluate where security and privacy risks may emerge and to provide guidance for making critical privacy changes in a timely fashion. By reviewing privacy implications early in the development process, the agency helps promote a privacy-conscious approach and culture.

h) how to address the problem of insider threats

We recommend increased research around improving behavioral analytics to identify anomalous activities in the network. We also recommend research around automating the enforcement of segmentation at the compute, storage and network level when suspected threats are identified or when breaches occur.

i) how improved consumer education and digital literacy initiatives can address human factors that contribute to cyber-security

We recommend the development of a Central Security Engineering Function that provides deep expertise for federal agencies' IT security groups, collaborates w/ industry and conducts awareness campaigns on security best practices. This group can develop reference architecture frameworks that could be standardized for use across government to address compliance and security regulations.

j) how to protect information processed, transmitted, or stored using cloud computing or transmitted through wireless services; and any additional objectives the heads of the applicable agencies and departments, in coordination with the head of any relevant Federal agency and with input from stakeholders, including appropriate national laboratories, industry, and academia, determine appropriate

We recommend a multi-layer approach to protecting information in cloud services. This includes: physical security, information security, network security, security, monitoring, patching, and vulnerability management. Use of industry certifications and standards such as ISO, FedRAMP, PCI, etc. should be required of cloud service providers. There should also be continuous monitoring of compliance through independent 3rd party auditors.

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

The Software Defined Data Center

The Software Defined Data Center (SDDC) is a transformational technology that enhances the security, reliability and resiliency of the infrastructure through policy-based automation (vs. error-prone, manual tasks) and fine-grained network segmentation.

SDDC is an architectural approach driven by software where all the domains of the data center –servers, storage and networking –are virtualized. Policy-based automation is a core capability of SDDC and drives operational efficiencies. In contrast to manual tasks or script-based automation, policy-based automation utilizes defined rules (policies) to ensure consistent deployment of services. This increases the reliability and resiliency of infrastructure by reducing manual tasks and the potential of human errors. Complex

processes can be simplified and manual/labor-intensive tasks that are prone to error can be entirely automated in software.

In contrast to hardware-based, traditional "stacks" of data center infrastructure, software defined data centers leverage the power of virtualization to abstract the underlying physical infrastructure to create logical pools of resources that can be managed and secured more efficiently. Since resources such as compute, networks and storage are created in software, they can be created, backed up, replicated more easily, thus improving the resiliency of the infrastructure. Logical network constructs such as firewalls are faithfully reproduced in software and can be easily deployed at a very granular level, typically on a per virtual machine basis. This dramatically improves the security posture and provides new capabilities to secure the east-west network traffic in data centers.

SDDC and Data Center Micro Segmentation

This innovative approach of fine-grained network segmentation – also known as micro-segmentation – transforms how we can design and secure our digital infrastructure. VMware's SDDC architecture increases operational security using VMware's network virtualization (NSX) platform and its native micro-segmentation capabilities "baked-in" to the platform. As organizations try to move to an increasingly fine-grained network segmentation approach (e.g., Forrester Research's Zero-Trust Network Architecture) for their data center networks in response to the increasing incidence of attackers moving freely within the enterprise data center perimeter, the NSX platform provides a viable solution to these threats.

NSX wraps security controls around much smaller groups of resources – often down to a small group of virtualized resources or individual VMs. This approach known as micro-segmentation has been understood to be a best practice approach from a security perspective, but difficult to apply in traditional environments. The inherent security and automation capabilities of the NSX platform are making micro-segmentation operationally feasible in the enterprise data center for the first time. VMware NSX deploys three modes of security for data center networks – fully isolated virtual networks, segmented virtual networks (via high-performance, fully automated firewalling native to the NSX platform), and segmentation with advanced security services with our security partners. Examples of partner integration include Palo Alto Networks for network segmentation with next-generation firewalls or Rapid7 for vulnerability scanning. When it comes to the business case, network micro-segmentation is not only operationally feasible using VMware NSX, but cost-effective, enabling the deployment of security controls inside the data center network for a fraction of the hardware cost. Many large data centers are using security as one of the big first benefits of the software-defined data center. In the very near future, this approach to data center security will become the new normal.

SDDC and Network Virtualization

Network virtualization with SDDC is a transformational technology that increases service availability and resiliency. Network virtualization abstracts the underlying physical network hardware and allows organization to reproduce networking constructs more easily. A flatter, simplified leaf-spine fabric can be employed utilizing equal-cost multi path routing between any point on the network. This leads to a more resilient network topology. VMware NSX can run on top of these resilient networks and reproduce simple to complex network topologies, while providing the advanced networking services that organizations need. With network virtualization, provisioning of network services can be automated greatly reducing variations in deployment. This streamlines and de-risks infrastructure moves, adds, and changes leading to a more reliable infrastructure.

Organizations are also using NSX to complement their existing disaster recovery solutions to enhance the resiliency of their infrastructure. NSX is helping them to reduce their recovery time objective (RTO) by upwards of 80%, considerably minimizing downtime and cost to the business. Enterprises use NSX to replicate the entire network and its security environment. They periodically snapshot the network construct, along with its applications and services, and maintain it at a recovery site. IT does not need to change IP addresses because the virtual network construct is decoupled from the underlying hardware and topology. The disaster recovery site is identical to the primary site, with no tradeoffs in functionality or performance. The copy sits at the recovery site in standby mode for push-button activation in the event of a disaster. Any changes made to the source network are automatically replicated to the copy at the recovery site.

Secure Desktop

A centralized secure virtual desktop solution is an innovative technology that increases the security and trustworthiness of the digital infrastructure. This solution accomplishes this by simplifying desktop management, streamlining application updates, centralizing data and supporting multi-factor authentication for secure, trusted access to resources.

Today's dynamic workforce is no longer tethered to traditional stationary desktops. Due to the "consumerization" of technology, end users want to use mobile devices such as tablets and smartphones as well as laptops and traditional PCs to access information, no matter where they are located. This introduces a level of complexity and potentially increases the threat vectors to infrastructure. While end users are embracing these trends, IT teams—faced with tight budgets—are struggling with how to best support and manage these new devices and new capabilities while protecting sensitive information as it is accessed across networks and locations.

A secure virtual desktop solution supports this need for device diversity by delivering high- fidelity virtual desktops and applications to traditional desktops, laptops, thin clients and a vast majority of the mobile devices in the market today. This solution provides IT with a way to securely manage this growing need for mobility Validated solution architectures such as VMware's Secure Desktop is specifically built to meet the needs of agencies looking for reliable, secure end user access across devices and locations. The solution supports smart card authentication (CAC/PIV/SIPRnet token) and RSA tokens enabling secure and trusted access to data. The solution is compliant with FIPS 140-2. The Secure Desktop solution is tightly integrated with the SDDC and its network micro segmentation capabilities allowing for an end-to-end automation of desktops in a secure, virtual network.

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

These recommendations foster the rapid transfer of R&D results into new technologies and applications:

Rapid Innovations Programs – Institute or expand programs whereby agencies have the resources and capabilities to quickly test out ideas and solutions for current and emerging problems

Streamline Acquisitions – Look for ways to onboard new technologies on government acquisition contracts for the constantly adapting cyber security threats

Public/Private Partnerships – Develop policies that foster collaboration between and public and private sectors on projects where there's mutual interests

Reduce Barriers to Entry – Incentivize new entrants into the government market and make it so that it is easier to conduct business with government

Community Cloud Computing – Institute policies that promote the use of community clouds for collaboration across agencies as well as the private sector

Patents and Trademarks – Continue to invest in programs to reduce the time it takes to obtain patents and trademarks to accelerate innovation

Centers of Excellence – Promote the idea of government-wide centers of excellence to innovate and develop common standards/best practices to accelerate innovation

Reevaluate Requirements and Certifications – reduce unnecessary burden of requirements and certifications where it clearly is of no value and not applicable to a given technology

Industry Researchers in Government Programs – facilitate greater interaction between industry and government funded research programs especially in the early stages of the program to improve visibility and speed up adoption of results.

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

Improvement of Current Research Infrastructure

The current research infrastructure to evaluate the next generation of secure networking and systems could be improved through the broader use of cloud computing. Historically, organizations have increasingly adopted private cloud models as a next step from server virtualization, but adoption of other cloud models (public, community), particularly the hybrid cloud can further enhance the current infrastructure.

Hybrid cloud allows organizations to extend the same operating environment (operating systems, applications, networking, management, operations, and tools) both on- and off-premise. The hybrid cloud approach ensures workload mobility without the need for recoding, minimizing both the risk and cost of development and A&A. This provides an agile platform for migration and collaboration across various research programs in government.

Virtualization and the Software Defined Data Center enable the hybrid cloud and simplify the creation, testing and evaluation of the secure networking and systems. For example, VMware's Hybrid Cloud solution supports NSX network virtualization, which extends the capabilities for secure networking from on premise to the public cloud. Network virtualization allows for complex network topologies with advanced networking services to be spun up, torn down, replicated and backed up with ease. This accelerates testing even when complex network scenarios are required.

Network virtualization also enables logical segregation of user test environments even in cases of shared research infrastructure. With physical networks, it's cumbersome to replicate, segment and ensure consistency of networks to support dozens or hundreds of these test environments. With network virtualization, these networks are easily created on top of the physical network and the applications will operate in the same way that it would in the physical network. This is especially useful in cases where multiple test scenarios need to be evaluated with a common baseline.

Improving Access by Academic Researchers and Related Data

Cloud computing improves access to resources by providing a self-service catalog. Through a self-service catalog, academic researchers can deploy, test and evaluate systems without having to wait hours or days. This provides autonomy and dramatically increases the efficiency of researchers and IT. Furthermore, the automation of service deployment ensures consistency in research.

The combination of self-service automation with network virtualization streamlines the creation and access to these environments. A researcher can create a complete virtual data center (compute, storage and network resources) that's logically separated from other researchers. This virtual data center can be accessed internally or externally with networking services such as VPN, firewalls, etc.

Advanced Data Services running on public cloud platform is another example of how data access by academic researchers could be enhanced. VMware's partnership with Google enables data services such as cloud storage, real-time analytics services, and NoSQL database services to run on the VMware Hybrid Cloud. Researchers are able to quickly utilize these data services for their applications without the need for complex setup or configuration.

Questions Related to the 2011 "Trustworthy Cyberspace: Strategic Plan for the Federal Cyber Security Research and Development Program"

The 2011 Strategic Plan defined five promising areas where research could make fundamental, game-changing advances in improving the security and trustworthiness of cyberspace: **Tailored Trustworthy Spaces**, **Moving Target**, **Cyber Economic Incentives**, **Designed-In Security**, and **Science of Security**.

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

The cyber threat landscape continues to evolve and poses serious challenges now more than ever. As government continues with digital transformation, there are more opportunities for innovation in government but at the same time, attackers can potentially have more opportunities to infiltrate our networks. The areas of research identified in the 2011 Strategic Plan are still relevant and federally funded research in these areas will greatly contribute to securing government information technology.

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

More focus needs to be directed toward inducing change to develop security solutions that can be implemented in a relatively short time period. In addition, we need to accelerate the adoption of these newly developed solutions. In the *Moving Target* area of research, we should highlight technologies and techniques that can reduce the threat landscape by segmenting the IT fabric and providing adaptable security that is automatically changing given the current scenario. We should research how to reduce the attack vector of a compromised network through the use of micro-segmentation and reducing the ratio of machines to networks. Today, the ratio of machines to networks is 1:100's or 1:1000's. By reducing this ratio to 1:1 or 1:10's, we reduce the impact of breaches dramatically. Once a network is infiltrated, there is often easy and unfettered lateral access to resources on the network. The typical network secures the perimeter through the use of traditional physical firewalls to keep attackers out, but generally don't monitor east-west traffic once inside the network. By utilizing distributed logical firewalls to complement traditional firewalls, the security posture is enhanced as organizations now have better visibility and control of east-west network traffic which is the vast majority of traffic in our networks

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

A high-level objective that we believe should be a strategic priority for cyber security R&D is how we can leverage software defined constructs and it's flexibility to increase infrastructure agility and enhance security posture. Software defined networks and the ability to improve security through segmentation is emerging, but a desired capability of automating an end-to-end process of network threat isolation through SDN in response to a suspected breach is still lacking. This autonomous capability should be prioritized as we find that attackers continually adapt their techniques and our defenses need to be adaptable as well. This will improve government's ability to adapt to the changing threat landscape and if a breach does occur, limit its impact.

A software-defined, platform centric approach to infrastructure such as networks should also be an objective to guide research. Software-defined platforms for infrastructure, with open and extensible APIs where industry can readily integrate industry proven solutions is best practice and further enhances security. Service insertion to an extensible platform from the broad ecosystem of technology vendors provides government with the choice of technologies that best meet their cyber security requirements. This provides flexibility and potential cost savings for government.

Summary

VMware believes that our customer security and safety is of paramount importance and runs the most mission critical workloads of our customers, we believe that we have a duty to ensure that our products remain secure at all times. We have well-established programs and practices to continually identify, remediate and mitigate security risks in this ever-changing threat landscape. We are encouraged to see a concerted effort in government to tackle the growing challenges with cyber security and have responded to the questions within the RFI. We look forward to continued partnership with the National Science and Technology Council (NSTC) and the Networking and Information Technology R&D (NITRD) program to develop a comprehensive approach to Cyber Security Research and Development.

Appendix: Sources

VMware Software Defined Data Center Capabilities and Outcomes:
http://www.vmware.com/files/pdf/techpaper/Technical-whitepaper-SDDC-Capabilities-IToutcomes.pdf

VMware Product Security White Paper: http://www.vmware.com/files/pdf/VMware-Product-Security.pdf

VMware Data Center Micro-Segmentation White Paper:
http://blogs.vmware.com/networkvirtualization/files/2014/06/VMware-SDDC-Micro-Segmentation-White-Paper.pdf

VMware Secure Desktop Solution for Federal Government Solutions Brief:
https://www.vmware.com/files/pdf/view/VMware_View_5_Federal_Solution_Brief.pdf

VMware vCloud Air Security Technical White Paper

https://www.vmware.com/files/pdf/vcloud-air/vmware-vcloud-air-security-technical-whitepaper.pdf