MOVING TOWARD TRUSTWORTHY SYSTEMS: R&D ESSENTIALS

Frederick T. Sheldon, *Oak Ridge National Laboratory*
Claire Vishik, *Intel*

Under the game-change metaphor, strategies developed to address hard problems will potentially lead to breakthroughs in many different interrelated cybersecurity areas. For software assurance, a game change should focus on improving resiliency and hardening new technologies that implement moving-target defenses and tailored trustworthy spaces.

In February 2010, former OpenNet Intitiative Director Dennis Blair advised Congress "malicious cyberactivity is growing at an unprecedented rate," and stated that the country's efforts to defend against cyberattacks "are not strong enough." The Pentagon has since experienced an "explosion" of computer attacks, currently averaging about 5,000 per day. Indeed, with cyberthreats steadily increasing in sophistication and frequency, the need for software assurance to ensure scalable trust at all levels—personal, private, public, and national—is crucial.

Cybersecurity, which comprises numerous interrelated components, and software assurance are inextricably intermingled. The former extends the boundary of physical security to the domain of cyberspace, while the latter provides the means for delivering on the promise that we can depend on the technologies that implement cyberspace. Secure systems must be dependable, and dependable systems fail if not secured. Unreliable software is inherently insecure.

Unfortunately, cybersecurity practice and policy are largely heuristic, reactive, and increasingly cumbersome, struggling to keep pace with rapidly evolving threats. Advancing beyond this predominantly reactive posture will require a transformation in computing and communication systems architectures.[1,2] New capabilities are required that don't merely solve today's plethora of security enigmas[3,4] but enable comprehensive game-changing strategies.[5]

In this article, we seek to raise awareness about the essential issues and broad initiatives aiming at stemming the tide, changing the game, and solving the hard cybersecurity problems from novel multidisciplinary viewpoints. This will let us devise new directions in many areas, including software assurance. Our analysis targets the emerging and evolving path forward for cybersecurity R&D based on recent workshops and summits dedicated to defining new approaches to cybersecurity. Specifically, we concentrate on the outcomes of the 6th Annual Cyber Security and Information Intelligence Research Workshop (www.csiir.ornl.gov/csiirw/), and the Federal Cybersecurity R&D Themes Kickoff Event organized by Network and Information Technology Research and Development (NITRD; www.nitrd.gov/CSThemes.aspx). Both events focused strongly on approaches that can help revolutionize

0018-9162/10/$26.00 © 2010 IEEE

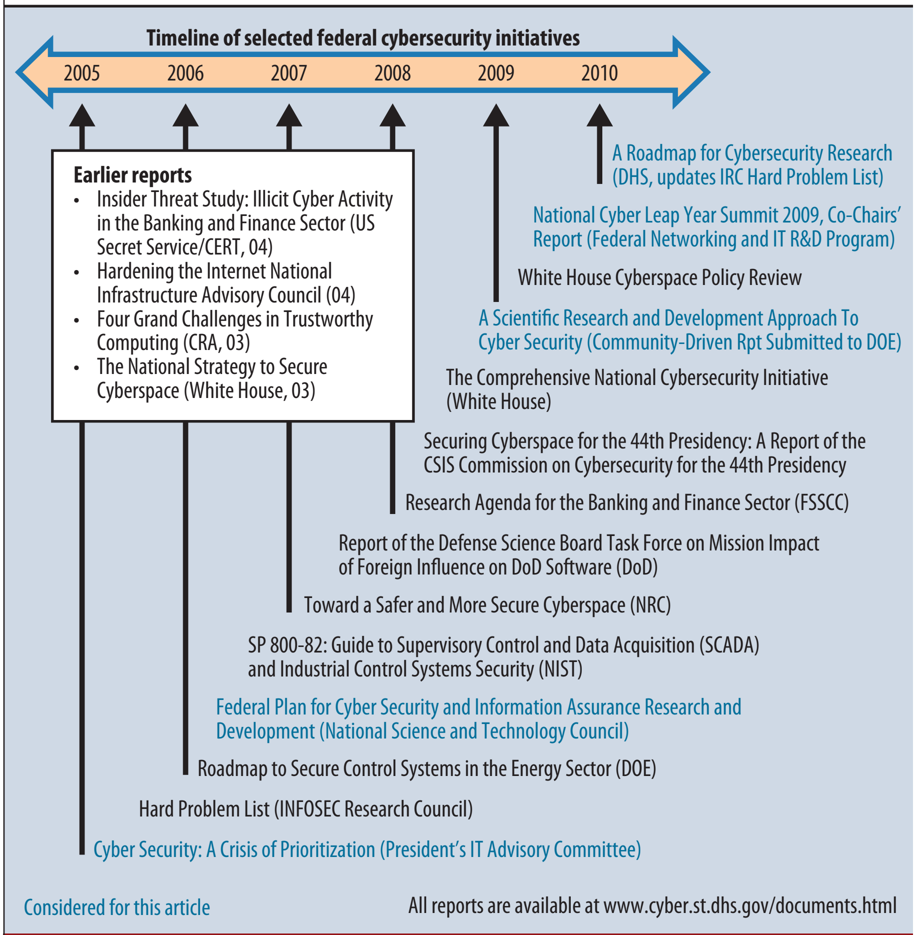
Timeline of selected federal cybersecurity initiatives
2005
2006
2007
2008
2009
2010
Earlier reports
• Insider Threat Study: Illicit Cyber Activity in the Banking and Finance Sector (US Secret Service/CERT, 04)
• Hardening the Internet National Infrastructure Advisory Council (04)
• Four Grand Challenges in Trustworthy Computing (CRA, 03)
• The National Strategy to Secure Cyberspace (White House, 03)
A Roadmap for Cybersecurity Research (DHS, updates IRC Hard Problem List)
National Cyber Leap Year Summit 2009, Co-Chairs' Report (Federal Networking and IT R&D Program)
White House Cyberspace Policy Review
A Scientific Research and Development Approach To Cyber Security (Community-Driven Rpt Submitted to DOE)
The Comprehensive National Cybersecurity Initiative (White House)
Securing Cyberspace for the 44th Presidency: A Report of the CSIS Commission on Cybersecurity for the 44th Presidency
Research Agenda for the Banking and Finance Sector (FSSCC)
Report of the Defense Science Board Task Force on Mission Impact of Foreign Influence on DoD Software (DoD)
Toward a Safer and More Secure Cyberspace (NRC)
SP 800-82: Guide to Supervisory Control and Data Acquisition (SCADA) and Industrial Control Systems Security (NIST)
Federal Plan for Cyber Security and Information Assurance Research and Development (National Science and Technology Council)
Roadmap to Secure Control Systems in the Energy Sector (DOE)
Hard Problem List (INFOSEC Research Council)
Cyber Security: A Crisis of Prioritization (President's IT Advisory Committee)
Considered for this article
All reports are available at www.cyber.st.dhs.gov/documents.html

Figure 1. Comparison overview for selected federal cybersecurity initiatives. The numbers in parentheses indicate the number of solution themes.[7]

the evolution of new ideas in cybersecurity. We believe these ideas will benefit the development of many, if not all, interrelated cybersecurity components.

DEVISING GAME-CHANGING APPROACHES TO CYBERSECURITY'S HARD PROBLEMS

Addressing the hard problems hobbling the vision of scalable trustworthy systems requires conducting game-changing R&D activities to enable a transformation in cyberspace. The NITRD subcommittee, comprising 14 member federal agencies, thus organized the National Cyber Leap Year. NCLY has proceeded on the premise that, while some progress on cybersecurity will be made by researching better solutions to today's problems, some of them might be too hard. The NCLY has pursued a complementary approach by searching for ways to bypass the intractable problems and *changing the game*, as in "if you are playing a game you can't win, change the game!" (www.nitrd.gov/NCLYBackgroundInfo.aspx).

At the 2009 NCLY Summit, more than 100 subject-matter experts developed ideas on five topics that could move the balance in cyberspace toward the defenders' favor:

- *Digital provenance*—basing trust decisions on verified assertions
- *Moving-target defense*—attacks only work once if at all
- *Hardware-enabled trust*—knowing when we've been had
- *Nature-inspired network defense*—moving from forensics to real-time diagnosis
- *Cybereconomics*—crime doesn't pay

Aneesh Chopra and Howard Schmidt described the results of the NCLY and Summit in the White House Blog (www.whitehouse.gov/blog/2010/05/19/help-change-game-cybersecurity) as follows:

> In a challenge to the research and development community, the President's Cyberspace Policy Review (near-term action item #9) called for a strategy for new, game-changing technologies that give the advantage to beneficial use. This challenge complements and extends the call in the Comprehensive National Cybersecurity Initiative (CNCI goal #9) for "leap-ahead" technologies, strategies, and programs. The National Cyber Leap Year responded to this challenge, gathering input from the community through concept papers and a national summit.

The first three game-changing concepts emerging from this process are as follows:

- *Moving target*—systems that move in multiple dimensions to the attacker's disadvantage and to increase resiliency.
- *Tailored trustworthy spaces*—security tailored to the needs of a particular transaction rather than the reverse.
- *Cybereconomic incentives*—a landscape of incentives that reward good cybersecurity and ensure that crime doesn't pay.

These broad themes aim to change the foundations of cybersecurity R&D. Foundational changes are always difficult to achieve. Taking these ideas from a high-level inspirational stage to concrete projects, technology development, implementation, deployment, processes, and incentives will require considerable effort and resources.

Table 1. Crosswalk of recent federal cybersecurity priorities.[2,5-8]

Selected federal problems characterization efforts			Solution themes(†)
PITAC 2005 cybersecurity priorities	NSTC 2006—Some of the top cybersecurity/IA R&D priorities	DHS 2009 Roadmap for Cybersecurity Research (Hard Problem List v. 2)	NITRD 2009 National Cyber Leap Year Summit
P1 Authentication (3)	N1 Authentication, authorization, trust management, and access control and privilege management (4)	D1 Scalable trustworthy systems (including system architecture and requisite development methodology) (4)	(1) Hardware-enabled trust {P1|2|3|4|5, N1-5|7|9|10, D1-3|5-7|9-11}
P2 Secure software engineering (2)	N2 Large-scale cyber situational awareness and automated attack detection, warning, and response (3)	D2 Enterprise-level security metrics (including measures of overall system trustworthiness) (3)	
P3 Holistic system security (2)	N3 Insider threat detection and mitigation and forensics, traceback, and attribution (4)	D3 System evaluation life cycle (including approaches for sufficient assurance) (2)	(2) Cybereconomics {P3|8|9|10, N1-3|6|8|11, D1|2|4|10|11}
P4 Monitoring and detection (3)	N4 Secure DNS and routing protocols and process control systems (3)	D4 Combating insider threat (3)	
P5 Secure fundamental protocols (2)	N5 Domain-specific security (such as wireless and RFID) (2)	D5 Combating malware and botnets (3)	(3) Moving-target defense {P1|4|7|9, N4-6|8-10, D1|2|5|7|9}
P6 Mitigation and recovery (1)	N6 Detection of vulnerabilities and malicious code; metrics and software testing and assessment (3)	D6 Global-scale identity management (3)	
P7 Cyberforensics (3)	N7 Secure OS and software engineering and information provenance (3)	D7 Survivability of time-critical systems (4)	(4) Digital provenance {P1|2|5|7, N1|3|4|7|11, D3|4|6|7-11}
P8 Modeling and testbeds (3)	N8 Cybersecurity and IA R&D testbeds and IT systems, and Internet modeling, simulation, visualization (3)	D8 Situational understanding and attack attribution (2)	
P9 Metrics, benchmarks, best practices (3)	N9 Trusted computing base architectures and composable, scalable, secure systems (3)	D9 Provenance (relating to information, systems, and hardware) (4)	(5) Nature-inspired cyberhealth {P3|4|6-10, N1-3|6-11, D1|4-9}
P10 Nontechnology issues (2)	N10 Inherently secure, high-assurance, and provably secure systems and architectures (3)	D10 Privacy-aware security (3)	
	N11 Trust in the Internet and privacy (3)	D11 Usable security (3)	

† Progress in a solution theme area will support advances in the other problem areas listed {P1-10, N1-11, D1-11}; (#) indicates a priority (or in the case of column 3, a hard problem). Larger numbers indicate the priority's stronger cross-cutting nature.

Yet we believe they offer a promising path to long-term comprehensive solutions that will enable novel theoretical and empirical research and help advance many topics related to cybersecurity, including software assurance.

CYBERSECURITY IS VITAL TO MODERN SOCIETY'S WELFARE

During the past decade, the breadth and complexity of cyberspace has vastly expanded. Recent federal policy documents emphasize the importance of cybersecurity to the welfare of modern society, as Figure 1 shows. Some examples include the President's "National Strategy to Secure Cyberspace in 2003," which describes national response priorities for reducing threats and vulnerabilities; awareness and training; national security and international cooperation; "Cyber Security: A Crisis of Prioritization,"[8] which describes 10 technologies needed for cybersecurity; and the "Federal Plan for Cyber Security and Information Assurance Research and Development,"[7] which addresses 49 cybersecurity and information assurance technical topics, grouped into eight major R&D areas ranked as top funding or technical priorities.

Over a two-year process the DHS Roadmap for Cybersecurity Research[2] identified 11 "hard problems," enlisting cyber researchers across the board from industry, academia, and the National Laboratories, while the NCLY Summit developed five cross-cutting solution themes.

Table 1 summarizes the problem space next to the proposed solution space based on an analysis of the R&D priority documents and the NCLY Co-Chairs' Report.[5] The nation is defining how to achieve a leap forward in cybersecurity through development of game-changing technologies, according to Aneesh Chopra, US CTO. This change is necessary, as the current approaches, though experiencing incremental improvements, failed to stem

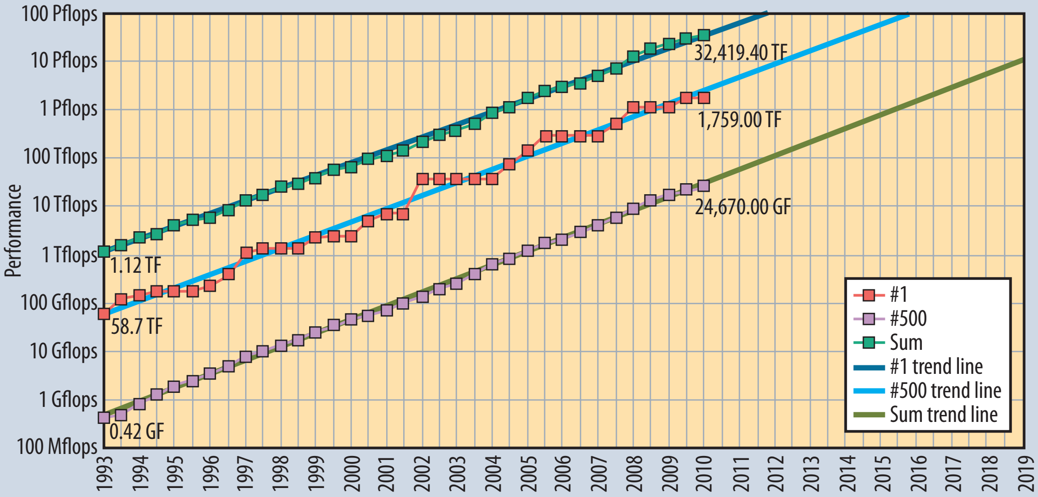

Figure 2. Computational performance versus year: (top, green) sum of the world's top 500 computers; (middle, red) fastest computer; (bottom, purple) slowest of the top 500 computers.

losses that, though no definitive report exists, have been estimated to have exceeded $1 trillion globally in 2008[9] due to cybercrime and e-fraud.

The problems in cybersecurity are more obvious than the potential solutions. The R&D community must develop innovations for addressing the long list of cybersecurity priorities[10] in a way that delivers innovative, deployable technologies and defines processes and incentives that are necessary for game-change solutions. A long-term vision for scalable trustworthy systems and computing environments requires solutions for all the priorities/problems in Table 1, as well as a viable approach to the problem of composition to ensure that today's dynamic and diverse ecosystems are addressed holistically. But what do the terms *trustworthy*, *scalable,* and *composition* really mean?

Trustworthiness is a multidimensional measure of a system's ability to satisfy each of the stated requirements' multiple aspects to achieve acceptable levels of system integrity, availability, and survivability, as well as data confidentiality, guaranteed real-time performance, accountability, attribution, usability, and other critical needs. Precise definitions and well-defined measures against which trustworthiness can be evaluated are fundamental precursors to developing and operating trustworthy systems.[2]

Scalability satisfies requirements as systems, networks, and systems of systems expand in functionality, capacity, complexity, and scope—without performance tradeoffs. Composability creates systems and applications with predictably satisfactory behavior from components, subsystems, and other systems.[2]

Currently available security features in hardware, operating systems, networks, and applications are underutilized, while approaches for securing heterogeneous environments with varying levels of protection in their elements have only begun to emerge. Now that individual security technologies are well understood, we must focus on the complete picture, placing areas of concentration such as software assurance in the context of the bigger cybersecurity problems.

Scalable trustworthy systems and environments should comprise trustworthy components and subsystems, down to the most basic level, thus avoiding the need to develop new methodologies and tools at each successively larger scale. Operationally, these trustworthy systems must function in an environment that can be trusted and provide proof of its trustworthiness as required for different process types.

One path in this direction makes greater use of already available security features, in both hardware and software. Such a set of building blocks will require an architectural framework that can preserve trustworthiness with incremental additions at any scale. Scalability is supplemental to trustworthiness. Constructive system design, meticulous use of best practices, ability to self-heal following breaches and failures, error correction to overcome unreliable communications and storage, and encryption to protect both the integrity and confidentiality of insecure communications are some approaches needed to improve security. While developers, users, and administrators must trust the systems and environments they use, we also need to ensure that developers, users, and administrators are trustworthy.

Thus, we face the following challenges: establishing a sound basis for composability that scales to large, complex, trustworthy systems; conducting evaluations of composite systems that are themselves composable and scalable; and developing components, analysis tools, business processes, metrics, and testbeds for trustworthy scalable environments.

MAINTAINING THE PACE OF CHANGE

Keeping pace with evolving modern systems and computing environments presents an important challenge for cybersecurity. As Figure 2 shows, significant increases in computing power combined with technological advances offer the potential for developing new security technologies, but they can also provide advantages to attackers.[11,12]

External malware attacks via the Internet involve deliberate infiltration or damage to a computer system without the owner's informed consent.

Internal attacks also pose a significant threat.[13] They can be introduced by malware acting on behalf of external forces, infiltrated through a variety of methods, and potentially hijacking critical cyberphysical resources. Attacks range from "low-and-slow" over a day or more to "fast-and-focused" at the millisecond level or faster.[14] Their detection is easily obscured in the sea of normal dynamic cyberactivity.

The greatest challenge is the continuous evolution of attacks. Solutions for known threats do not address the new attacks. Traditional risk methodologies provide commonsense advice and suggest security-driven assessments but usually lack specific guidelines for the evaluation of emerging threats. New approaches to defenses are needed that can reduce attackers' advantages, especially when new attacks are first deployed. These approaches can include the following:[5]

- Thwarting malicious cyberactivity through signaling, implementation of diversity, and immunogenic detection as hardware-software solutions.
- Rapidly regenerating (self-healing) survivable capabilities in mission-critical systems after a sophisticated attack.
- Evolving immunity to attacks through evolutionary computing to create new deceptions (gaming strategies) as new threats emerge.
- Self-learning while monitoring insider activity and developing profiles for appropriate and legitimate behavior (modeling).
- Assimilating the many disparate security tools using both feed-forward and feedback signaling mechanisms in a cyberdefense system to help ensure tolerance and identify attacks while minimizing false alarms.

These and other approaches will need to overcome obstacles to solving the hard problems in cybersecurity.

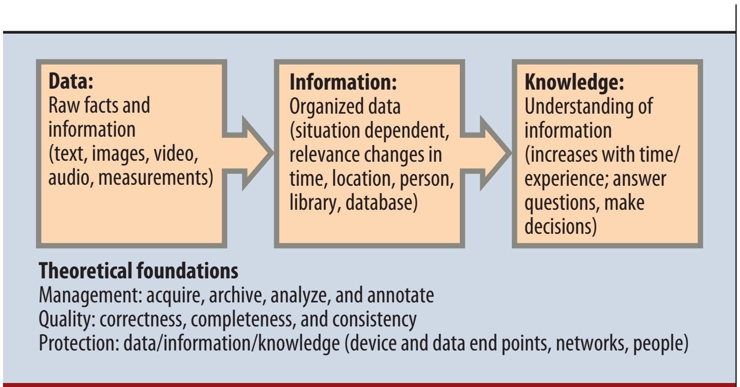
Data:
Raw facts and information
(text, images, video, audio, measurements)
Information:
Organized data
(situation dependent, relevance changes in time, location, person, library, database)
Knowledge:
Understanding of information
(increases with time/ experience; answer questions, make decisions)
Theoretical foundations
Management: acquire, archive, analyze, and annotate
Quality: correctness, completeness, and consistency
Protection: data/information/knowledge (device and data end points, networks, people)

Figure 3. Conversion of raw data into information (data in the context of other data), hence into knowledge (information in the context of other information) for understanding and prediction.

HARD PROBLEMS IN CYBERSECURITY

Complexity at all levels is the first aspect that makes cybersecurity so challenging. All modern devices are themselves networks of systems and components such as CPUs, memory, storage, and I/O devices. Likewise, software consists of complex interconnected functions. The information infrastructure is a complex system of systems involving hardware, software, operating systems, data, networks, and people.

Each component interacts in complex ways with other components and systems, sometimes producing unexpected and potentially adverse behavior. Failure in such an infrastructure can be so complex that it becomes impossible to determine the cause. Scalable trustworthy systems and environments must be designed to help cope with this complexity.

From the viewpoint of security, most processes traverse systems, environments, and applications that have different security protection levels. A user can initiate a mission-critical transaction from a phone or from a secure terminal; in both cases, the transaction will terminate in a secure server but will travel over different networks. The same device and network can be used for a variety of situations demanding varying levels of security.

The immense amount of diverse data is another reason cybersecurity is a "hard problem," involving 452 exabytes (4.52 × 1,021 bytes) or 72 Gbytes for each person on Earth.[15] "Data" is all electronic forms of information and knowledge. Scalable, trustworthy systems must be able to process this tsunami of data in near real time for attack characterization, situational understanding, attack attribution, and appropriate response.[16]

The conversion of data into information and hence into knowledge is the third reason cybersecurity is a hard problem. Data analysis in the context of other data generates information, processed in the context of other information to create knowledge, as Figure 3 shows. Current systems can't always create knowledge, and not all processes and decisions can be automated with current technology. We must rely on the decisions of humans who cannot respond at computer speeds or detect sparse anomalies. Robust cybersecurity requires a new paradigm.

Nontechnical constraints are the fourth aspect of cybersecurity that make it hard. These include

- the need to protect private information (essential for societal acceptance);
- usability and cost-effectiveness, including the need to comply with mandates of law at all levels, provide for graceful degradation of safe operation during failure, and minimally impact users' ability to do work; and
- economic concerns.

The inadequacy of perimeter defenses in our networked world provides the fifth reason that achieving cybersecurity is hard. The whole notion of a "perimeter" is becoming fuzzy. Traditional approaches focus on "layered defense" or "defense in depth" strategies in which the "crown jewels" are protected by walls and fortifications that form "air gaps" between the layers, which play a key role in protecting assets, whether physical or cyber.[1] This "Maginot Line" approach cannot protect the "inside" from the cyber "outsiders" and is inherently ineffective against malicious attacks. Rather, we must develop active and adaptable distributed security as an integral part of novel hardware-software combinations, such as

A tailored trustworthy space is a flexible, distributed trust environment that can support functional, policy, and trustworthiness requirements arising from a wide spectrum of activities in the face of an evolving range of threats.

- systems and devices that will not leak secrets or execute malware, just as we humans harbor certain viruses without ill effect;
- systems and devices that share provable and standard trust information, confirming their trustworthiness;
- generic security-assured commodity hardware solutions at all levels; and
- systems able to determine—by technically assured means such as white-listing, cataloging, or trust establishment—whether to trust a device, software package, or network based on dynamically acquired trust information rooted in hardware and user-defined security policies.

Scalable trustworthy systems must provide accountability for users, software, hardware, networks, and complex computing environments.

Cyberattacks continue to grow in number and sophistication, as the following trends show:[4]

- organized nation-state attacks against the Pentagon and other facilities in the US;
- organized nation-state attacks on Estonia and Georgia;
- rising identity theft via the Internet;
- undocumented features in open source applications code that cause software life-cycle problems;
- open source flaws, typically on the order of 1 per 103 lines of code;
- use of botnets and other organized Internet exploits;
- website and Web application exploits; and
- compromising unsecured data.

With this level of threats, one line of reasoning maintains that completely trustworthy systems are impossible. All modern systems are complex, and flaws—either malicious attacks or honest mistakes—in complex systems are difficult to detect, understand, and analyze. Thus, all systems have vulnerabilities. The dynamic nature of current computing compounds this complexity. Ubiquitous networking opens a vulnerable connected device to Web-based or network-based attacks. This logic concludes that the root cause of vulnerabilities is the always-imperfect computing environment that can never be completely secure.

GAME-CHANGING R&D THEMES

There is an element of truth in this view. R&D themes offer a perspective that focuses not on the elimination of all potential security flaws but on devising approaches that will make these potential flaws hard to exploit technically or economically. "Toward a Federal Cybersecurity Game Change Research Agenda," organized by NITRD on 19 May 2010 (http://cybersecurity.nitrd.gov), addressed this issue with government, industry, and academia panels.

The government panel provided a discussion of a coordinated effort addressing public and private partnerships regarding game changers for assuring the trustworthiness of the digital infrastructure, to include security, reliability, resiliency, privacy, and usability. The panelists discussed how we can enable risk-aware safe operations in compromised environments, minimize critical system risk while increasing adversaries' costs and exposure, and support informed trust decisions, necessitate flexible security strategies, and allow for effective risk/benefit analyses and implementations within the framework of our three research and development themes.

Tailored trustworthy spaces (TTSs)

TTS supports context-specific trust decisions. It combines the 2009 summit topics of hardware-enabled trust and digital provenance described in column four of Table 1 into one theme.

In the physical world, we operate in many spaces with varying characteristics. Different behaviors and controls are appropriate in different spaces. Today's cyberspace redefines those environments where traditional boundaries are blurred, merged, or both. A tailored trustworthy space is therefore a flexible, distributed trust environment that can support functional, policy, and trustworthiness requirements arising from a wide spectrum of activities in the face of an evolving range of threats.

We need to enable informed trust decisions to provide users with context-specific trust services, coherent policy implementation through an integrated set of security choices or defaults appropriate for the tasks at hand, and rules and attributes visible to users, providers, and systems, as well as a means to negotiate the space's boundaries and rules. Identifying the dimensions of a tailored trustworthy space will be essential to developing and assuring approaches to identification and authentication, information flow rules, strength of separation mechanisms, and levels of online monitoring and adaptation.

Policy framework and management are essential to developing and assuring concrete user-friendly specifications of a tailored trustworthy space that is verifiable, assurable, and maintainable for all devices and systems. The infrastructure must also support validation of end point device integrity and verification of the separation of spaces. The TTS concept suggests an infrastructure that pieces together integrated support for diverse trust environments, leveraging identity management, component assurance, and composition methods for the purpose of trust negotiation and trust management.

Moving-target (MT) defense for providing resilience through agility

MT systems include nature-inspired cyberhealth. These systems primarily provide controlled change across multiple dimensions to increase uncertainty and complexity, diminish the window of opportunity for attackers, and increase their costs and efforts while increasing the resilience and fault tolerance within a system. MT technologies must survive in a new paradigm where perfect security may be unattainable, but systems must be able to continue safe operations in a compromised environment.

MT systems should confound the adversary, not the user, and therefore need management and configuration capabilities that support their inherent complexity. The deployment of MT technologies requires careful cost/benefit analysis and new metrics to enable their appropriate application. Moreover, innovative decision-support mechanisms underlie their successful deployment.

MTs must be agile and could take inspiration from autonomic behavior phenomena and concepts learned from analysis of immune systems, species evolution, and other natural responses to threats, including reverse-engineering of the brain. MT mechanisms must adapt quickly to shorten adversaries' window of opportunity and reduce performance costs. Consequently, MT control mechanisms must enable real-time threat-appropriate selection of MT protections. MT systems present management challenges that must accommodate ad hoc key distribution along with rapid and resilient rekeying mechanisms that require complex high-integrity game-resistant decision logic, including enhanced capabilities to provide situational awareness, verifiable metrics to support human/machine real-time decision making, and scalable high-assurance methods and models to validate them. If successful, MT systems can establish controlled movement across multiple dimensions and shift the advantage to the defender by increasing the costs to an attacker in time and resources for reconnaissance, planning, and development.

> **We need new theories and models to deal with investments, markets, and the social dimensions of both good and bad cyberspace behavior.**

MT systems can increase the degree of uncertainty for the attacker, the apparent complexity of an individual target, and the apparent diversity across any set of targets. At the same time, the range of defense strategies available to the defender are vastly improved, assuming the MT management of keys and controls is sufficiently assured. The end state provides resiliency and fault tolerance for the target through redundant paths, resources, and configurations.

Cybereconomics (CE) for incentivizing good security

Secure practices are essential for successful cybersecurity defenses and must be incentivized for cybersecurity to become ubiquitous. Sound economic incentives need both metrics and processes that assure development and sensible, enforceable notions of liability and mature cost and risk analysis.

We need new theories and models to deal with investments, markets, and the social dimensions of both good and bad cyberspace behavior. Research in cybersecurity economics has been growing, yet we still debate fundamental issues such as whether markets can provide the essential elements of solutions for cybersecurity. The projected benefits must be quantified to demonstrate they outweigh the costs incurred by the implementation of improved cybersecurity measures. There are no sound methodologies to indicate how secure a system is, so we cannot articulate how much more secure it would be with additional investment. To move forward, we must do the following:

- define the role for economics as part of leveraging incentives, liabilities, and regulation for cybersecurity;
- create environments where security technology can be successfully deployed;
- provide incentives to engage in socially responsible behavior in cyberspace; and
- enforce deterrents for those who participate in criminal and malicious behavior.

Economic tools have been successful in defining the direction and behaviors in various markets. Many challenges lie ahead to fully harness cybereconomics in developing new security technologies and assurance models and approaches.

A moving-target defense enables controlled movements across multiple system dimensions to reduce the window of opportunity for attackers to exploit system vulnerabilities.

A plethora of legal and ethical issues exist around the collection, protection, and distribution of data. At the same time, we must ensure that all data types and categories are available to the R&D community, including international cross-border sharing.[17-19] We must incentivize data providers to encourage sharing, under well-defined circumstances, of appropriate data that supports effective economic analysis, such as cyber "insurance actuarial information."

Current incident trending information is inadequate for decision-makers. For example, we must focus on educating users about managing their personal information and behavior (PIB) and the benefits of secure practices and acceptable cyber behavior especially as service providers begin to monetize our PIB data.

The ability to assess the economic costs and benefits of protecting critical infrastructure from disruption, educating vendors about their role with respect to secure and assured software, and providing legal frameworks that let service providers be more active in the defense of their systems and services all involve establishing an allowable scope of action within the context of global legal capacities and partnerships while empowering providers to reduce abusive or criminal behavior and provide appropriate law-enforcement support.

Viable economic solutions can reduce barriers to incentivizing data gathering and information sharing and foster better metrics and models for security deployment decisions based on knowledge and proper motivations. In turn, better metrics and models will help to identify information-assurance controls and mitigation costs in assuring mission success, include different organizational mission needs for all stakeholders, and provide a comprehensive basis for choosing a course of action that has the highest risk-reduction return on investment.[20]

INDUSTRY AND ACADEMIA PANEL SUMMARY COMMENTS ON THE THEMES

The industry and academia panel shared further insights on the themes introduced in the government panel. The complexity and uneven security protections in today's cyberspace require new game-changing approaches. Although addressing narrow topics can achieve significant progress, incremental changes are no longer sufficient as the technology development cycles become shorter and all processes are digitized.

In this complex and dynamic environment, establishing trust in all components of a process is vital, but also difficult given currently available techniques. Nevertheless, we are well positioned for a game change: multidisciplinary work is flourishing, and we have a good understanding of the technology potential and new productive ideas, as well as a growing understanding that the move from ideation to deployment must be shortened.

To build TTSs, security must be end to end and top to bottom. It is necessary to define information for trust establishment that is broadly applicable. Achieving effective and deployable results requires significant resources and a shared vision. We need security technologies that can work without compromising performance and usability or increasing energy consumption and cost.

Further, we need new approaches to hardware and software architectures that allow control of security from top to bottom and help minimize the attack surface. Many unanswered research questions remain in building TTSs, including trust in heterogeneous environments and the use of untrusted systems in trustworthy environments. Promising work is being done in the area of cache protection and secure execution, but to change the game, the hard and broad research questions must be addressed.

An MT defense enables controlled movements across multiple system dimensions to reduce the window of opportunity for attackers to exploit system vulnerabilities.

Examples of this approach include dynamic networking, just-in-time compiling, and nonpersistent virtual machines. Applicable technologies include the randomization of dynamic code and instruction sets, data chunking, and decentralization or more robust cryptographic protection for credentials. Combining these approaches is game changing because it makes attacking dynamic systems harder. MT networks can obfuscate operations by varying addresses, paths, and topologies. Research challenges remain, including definitions of provable security properties and ensuring effective scalability, performance, and energy consumption.

Cybereconomics is an important part of changing the game in cyberspace. Research in cybereconomics has grown, but debate persists over misaligned incentives and externalities and asymmetric and incomplete information. These constraints can be reduced. For example, information gathering can be incentivized, enabling us to build better economic models. We can address bounded information and cognitive biases by better understanding them. We must understand that security is in part a social science. It is defined by technology, but it is also motivated by behaviors, perceptions, and many other factors outside of technology.

The economics of cyberdefense and cyberattack are different. To build efficient defenses, we must understand the cost structure of the attacks and target the most vital components in their value chain. Separate analyses of the economic factors for defenders and attackers can achieve this goal, putting the focus on creating technologies and processes that remove incentives from economically motivated attackers.

How can we achieve momentous progress? Many approaches have been devised and all have value. All must be assessed for the R&D community to move forward.

NEXT STEPS

Solving the growing list of hard problems in trustworthy systems and trusted environments requires significant resources. Addressing these problems is a long-term, multidisciplinary, and challenging effort. The game-change approach can be instrumental in helping the R&D community reassess current approaches to cybersecurity R&D that are predominantly incremental.

Scalable trustworthy systems involve needs beyond computer science and high-performance computing, including management of complexity across all scales, analyzing exabytes of data in near real time, and protection of existing infrastructure from increasingly sophisticated attacks. For example, the FURPS+ approach (http://en.wikipedia.org/wiki/FURPS) approximates this by focusing on functionality, usability, reliability, performance, and supportability. It also bolsters the design's implementation, interfaces, and physical constraints.

The requirements for trustworthy systems need to be captured in specific, quantifiable metrics based on testing, inspection, or analysis. To achieve this vision, it is necessary to abstract specific functions as a set of predictably composable, provably secure, and interoperable components that can provide reduced-instruction-set code primitives. These cyber functions avoid, detect, and deter attackers; recognize and thwart malicious users; detect and heal underlying damage; restore normal functions; and prepare for efficient resolution of future attacks. We must also secure composable elements at all levels with a better ability to thwart attacks and provide greater scalability across all devices in the cyberinfrastructure, including computers, sensors, embedded systems, routers, repeaters, firewalls, hubs, and instruments.

A long-term R&D vision focusing on hard problems and game-changing approaches is essential to address these complex cybersecurity issues more comprehensively and holistically. With cyberthreats increasing in number and sophistication, the game is ripe for change. To successfully address the hard problems toward the vision of scalable trustworthy computing, we must conduct R&D activities that will enable the transformation of current incremental approaches into game-changing initiatives that take a comprehensive view of cybersecurity and engage all stakeholders in joint efforts.[5]

Under the game-change metaphor, strategies developed to address hard problems can lead to breakthroughs in many interconnected cybersecurity areas. For software assurance, a game change focused on reducing attackers' advantages might emphasize areas that offer significant economic incentives to attackers rather than—as is the case today—on the problems most obvious to the defenders. In addition, linking software assurance activities to work in adjacent security areas will likely encourage efficiency and innovation and bring forth novel and productive viewpoints. C

Acknowledgments

The submitted manuscript was authored by a contractor of the US Government (USG) under contract DE-AC05-00OR22725. Accordingly, the USG retains a nonexclusive, royalty-free license to publish or reproduce the published form of this contribution, or allow others to do so, for USG purposes. The authors thank Susan Alexander, currently at ODNI, and Tomas Vagoun from the National Coordination Office for NITRD.

References

1. C. Catlett et al., *A Scientific Research and Development Approach to Cyber Security*; www.er.doe.gov/ascr/ProgramDocuments/Docs/CyberSecurityScienceDec2008.pdf.

2. DHS S&T, *Roadmap for Cybersecurity Research*, Jan. 2009; www.cyber.st.dhs.gov/docs/DHS-Cybersecurity-Roadmap.pdf.
3. T. Gjelten, "Does Averting Cyberwar Mean Giving Up Web Privacy?" www.npr.org/templates/story/story.php?storyId=127575960; 9 June 2010.
4. T. Gjelten, "Timeline: Major Cybersecurity Incidents Since 2007"; www.npr.org/templates/story/story.php?storyId=125518567; 5 Apr. 2010.
5. *National Cyber Leap Year Summit 2009 Co-Chairs Report*; www.qinetiq-na.com/Collateral/ Documents/English-US/InTheNews_docs/National_Cyber_Leap_Year_Summit_2009_Co-Chairs_Report.pdf.
6. L.M. Hively, F.T. Sheldon, and A. Squicciarini, "A Vision for Scalable Trustworthy Computing," *IEEE Security and Privacy*, to appear 2010.
7. National Science and Technology Council, *Federal Plan for Cyber Security and Information Assurance Research and Development*, Inter-Agency Working Group on Cyber Security and Information Assurance, Apr. 2006.
8. President's Information Technology Advisory Committee, *Cyber Security: A Crisis of Prioritization*; www.nitrd.gov/pitac/reports/20050301_cybersecurity/cybersecurity.pdf.
9. N. Kshetri, *The Global Cybercrime Industry*, Springer, 2010.
10. National Academy of Science, "Secure Cyberspace"; www.engineeringchallenges.org/cms/8996/9042.aspx.
11. M. Näf, "Ubiquitous Insecurity? How to 'Hack' IT Systems," *Information & Security 7*, 2001, pp. 104-118.
12. S.J. Prowell, R. Kraus, and M. Borkin, *Seven Deadliest Network Attacks*, Syngress, 2010.
13. M. Keeney et al., *Insider Threat Study: Computer System Sabotage in Critical Infrastructure Sectors*, Secret Service and CERT Coordination Center, Carnegie Mellon SEI, May 2005, pp. 1-45.
14. M. Arrington, "Google Defends Against Large Scale Chinese Cyber Attack: May Cease Chinese Operations;" http://techcrunch.com/2010/01/12/google-china-attacks.
15. EMC^2, "The Digital Universe Is Still Growing"; www.emc.com/leadership/digital-universe/expanding-digital-universe.htm, 2009.
16. M. Dacier, V-H. Pham, and O. Thonnard, "The WOMBAT Attack Attribution Method: Some Results," *Proc. ICISS 2009,* LNCS 5905, Springer, 2009; https://wombat-project.eu/wombat-project-description.html).
17. A. Spasova, "Tackling Cyber Crime Together"; www.guardian.co.uk/commentisfree/2009/jun/25/cyber-crime-europe.
18. K. Poulsen, "US Defends Cybercrime Treaty"; www.securityfocus.com/news/8529.
19. R. Adhikari, "Report Warns of More Cybercrime"; www.esecurityplanet.com/news/article.php/3790191/Report-Warns-of-More-Cybercrime.htm.
20. R.K. Abercrombie, F.T. Sheldon, and A. Mili, "Managing Complex IT Security Processes with Value Based Measures," *Proc. 2009 IEEE Symp. Computational Intelligence in Cyber Security*, 1 Apr. 2009, pp. 69-75.

***Frederick T. Sheldon** is a research scientist at Oak Ridge National Laboratory. His research interests include software engineering, dependability, and cybersecurity. He received a PhD in computer science from the University of Texas at Arlington. Contact him at sheldonft@ornl.gov.*

***Claire Vishik** is a trust and security technology and policy manager at Intel. Her research interests include hardware and system security, trusted computing, technical aspects of privacy, and cybereconomics. She received a PhD in computer and information science from the University of Texas at Austin. Contact her at claire.vishik@intel.com.*

The Silver Bullet Security Podcast
with Gary McGraw
Silver Bullet Security Podcast
In-depth interviews with security gurus. Hosted by Gary McGraw.
www.computer.org/security/podcasts
Sponsored by IEEE SECURITY & PRIVACY
cigital