United States House of Representatives
House Armed Services Committee
Terrorism and Unconventional Threats
and Capabilities Subcommittee

Hearing on:
Private Sector Perspectives on Department of Defense Information Technology and Cybersecurity Activities

Dr. Fred B. Schneider
fbs@cs.cornell.edu
(607) 255-9221

Samuel B. Eckert Professor of Computer Science
Cornell University
4115C Upson Hall
Ithaca, New York 14853

February 19, 2010

Testimony of Fred B. Schneider
Samuel B. Eckert Professor of Computer Science
Cornell University, Ithaca, New York
February 19, 2010

Good afternoon Chairwoman Sanchez, Ranking Member Miller, and distinguished members of the Committee. I appreciate this opportunity to comment on cyber security research and education. I am Fred B. Schneider, a Computer Science professor at Cornell University and Chief Scientist of the NSF-funded TRUST[1] Science and Technology Center, a collaboration involving researchers at U.C. Berkeley, Carnegie-Mellon University, Cornell University, Stanford University, and Vanderbilt University.
Today, I come before you as a representative of the Computing Research Association, an organization devoted to the mission of strengthening research and advanced education in computing, and comprised of more than 200 academic departments of computer science, computer engineering, and schools of information; 20 industrial computing research labs; and 6 affiliated professional societies.

I have been a Computer Science faculty member since 1978, actively involved in research, education, and in various advisory capacities for both the private and public sectors. Besides teaching and doing research at Cornell, I am a member of the DoD Defense Science Board (DSB), the Dept. of Commerce Information Security and Privacy Advisory Board (ISPAB), the Computing Research Association's board of directors (where I chair of the CRA Government Affairs committee), and a council member of the Computing Community Consortium. I also co-chair Microsoft's TCAAB external advisory board on trustworthy computing.

Our nation's increasing dependence on computing systems that are not trustworthy puts individuals, commercial enterprises, the public sector, and our military at risk. Increased data on-line, increased networking, and increased computing all mean increased exposure. These computing systems need to work as we expect—to operate despite failures and despite attacks. They need to be *trustworthy*.

The risk is particularly problematic for our armed forces, where computing systems have become integral to the success of virtually all aspects of peace-time and war-time operations, ranging from situational awareness and logistics management all the way to command and control of weapons systems. We thus unwittingly are creating new and weakly-defended targets for our adversaries to exploit. Moreover, users of our cyber-enabled systems are often unaware of just how dependent they have become on computing and just how vulnerable they are to attack.

[1] Team for Research in Ubiquitous Secure Technology.

In addition, computer systems and networks are increasingly being interconnected in subtle and unexpected ways, resulting in surprising and hidden dependencies of one system on another. Cyber-security of military systems often depends on the trustworthiness of private-sector and/or public-sector systems. The success of military operations then becomes hostage to the security of these other systems. For example, mission-critical functionality could depend on the Internet or could co-exist on computers that also host mundane administrative functions. These interdependencies create paths that enable attackers to compromise some system that is not seen as critical, and thus is not well protected, as a means to reach a critical asset that might actually be well protected. The recent trend towards outsourcing computation in third-party "clouds" will only make the problems worse.

The growth in attacks we witness today should not be surprising. The more we depend on a system, the more attractive a target it becomes to somebody intent on causing disruption; and the more value that is controlled by a system, the more attractive a target it becomes to somebody seeking illicit gain. But more disturbing than the growth in attacks is that our defenses can't keep up. The core of this problem is the asymmetric nature of cyber-security:

- **Defenders are reactive; attackers are proactive.** Defenders must defend all places at all times, against all possible attacks (including those not known about by the defender); attackers need only find one vulnerability, and they have the luxury of inventing and testing new attacks in private as well as selecting the place and time of attack at their convenience.

- **New defenses are expensive to develop and deploy; new attacks are cheap.** Defenders have significant investments in their approaches and business models, while attackers have minimal sunk costs and thus can be quite agile.

- **The effectiveness of defenses cannot be measured; attacks can.** Since we cannot currently quantify how a given security technology or approach reduces risk from attack, there are few strong competitive pressures to develop defenses. So vendors frequently compete and are evaluated on the basis of ancillary factors (e.g., speed, integration, brand development, etc.). Attackers see their return-on-investment and have strong incentives to improve their offerings.

The result has been a cyber-security mentality and industry built around defending against known attacks. Our defenses improve *only* after they have been successfully penetrated. And this is a recipe to ensure some attackers succeed—not a recipe for achieving system trustworthiness and not an acceptable state of affairs for military systems. We must move beyond reacting to yesterday's attacks (or what attacks we predict for tomorrow) and instead start building systems whose trustworthiness derives from first principles.

Yet today we lack the understanding to adopt that proactive approach; we lack a "science base" for trustworthiness. We understand that the landscape includes attacks, defense mechanisms, and security properties. But we are only now starting to characterize the lay of the land in terms of how these features relate—answers to questions like: What security properties can be preserved by a given defense mechanism? What attacks are resisted by a given mechanism? How can we overcome the inevitable imperfections in anything we might build, yet still resist attacks by, for example, forcing attackers to work too hard for their expected pay-off. Having a science base should not be equated with implementing absolute security or even concluding that security requires perfection in design and implementation. Rather, a science base should provide—independent of specific systems— a principled account for techniques that work, including assumptions they require and ways one set of assumptions can be transformed or discharged by another. It would articulate and organize a set of abstractions, principles, and trade-offs for building trustworthy systems, given the realities of the threats, of our security needs, and of a broad new collection of defense mechanisms and doctrines. And it would provide scientific laws, like the laws of physics and mathematics, for trustworthiness.

An analogy with medicine can be instructive here. Some maladies are best dealt with in a reactive manner. We know what to do when somebody breaks a finger, and each year we create a new influenza vaccine. But only after significant investments in basic medical sciences are we starting to understand the mechanisms by which cancers grow, and developing a cure seems to require that kind of deep understanding. Moreover, nobody believes that disease will some day be a "solved problem." We make enormous strides in medical research yet new threats emerge and old defenses (e.g., antibiotics) are seen to lose their effectiveness.

Like medicine and disease, system trustworthiness is never going to be a "solved problem". There will be no "magic bullet" trustworthiness solution, just as there is not going to be a miracle cure for all that ails you. We must plan to make continuing investments, because the problem will continue evolving:

- **The sophistication of attackers is ever growing, so if a system has vulnerabilities then they will find it**. Any assumption made when building a system does, in fact, constitute a vulnerability, so every system will have vulnerabilities of one sort of another. And with enough study, attackers will find these vulnerabilities and find ways to exploit them.

- **The technology base used by our systems is rapidly changing.** Systems are replaced on a 3-5 year time span, not because computers or software wear out but because newer software and hardware offers improved functionality or better performance (which is then leveraged into new functionality). New systems will work differently, will involve different assumptions, and therefore will require new defenses.

- **The settings in which our computing systems are deployed and the functionality they provide is not static.** With new settings come new opportunities for attack and disruption, whether it is creating a blackout by attacking the “smart grid” or predicting the target destination for a Predator UAV by monitoring the (unencrypted) video stream it broadcasts while en route.

We can expect to transcend the constant evolution only through the understanding that a science base provides. A science base is also our only hope for developing a suite of sound quantitative trustworthiness measures, which in turn could enable intelligent risk-management decisions, comparisons of different defenses, and incentivize investments in new solutions.

A science base for trustworthiness would not distinguish between classified and unclassified systems, nor would it distinguish between government and private-sector systems. The threats and trade-offs might be different; the principles are going to be the same. But even an understanding of how to build trustworthy systems for the private sector would by itself be useful in military and government settings, simply because so-called COTS (commercial off the shelf) technologies that are developed by the private sector for the private sector are widely used within the military too.

Many equate cyber-security research with investigations solely into technical matters. This oversimplifies. Achieving system trustworthiness is not purely a technology problem. It also involves policy (economic and regulatory). Technological solutions that ignore policy questions risk irrelevance, as do policy initiatives that ignore the limits and capabilities of technology. So besides investing in developing a science base for trustworthiness, we must also invest in research that bridges the technical and the non-technical. We need to understand when we might get more traction for trustworthiness from a policy solution than from a technology one. For example, identifiers—your mother’s maiden name, your credit card number, your bank account number, and your social security number—are not a good basis for authentication because they will be known to many. So regulation that prohibits the use of identifiers as authenticators might more effectively defend against identity theft than new technology could.

As another example, there is much talk now about making the Internet more secure by adding the means to trace packets back to their senders and the software that generated the packets. With this *doctrine of accountability*, unacceptable actions aren’t prevented but simply attributed, which in turn brings repercussions for the perpetrator—trial, conviction, and penalties in the civilian setting or some sort of sanctions or military retaliation in the international setting. Of course, suitable evidence must be available, and the accuracy of claims being made about accountability is crucial.

But there is a tension between accountability and anonymity, so a doctrine of accountability if not instantiated with great care could impinge on our societal values, our culture, and our laws. Such changes may be feasible in the military setting; but they are unlikely to be embraced in Internet, and the military will have to depend on the Internet for some time come. Thus, we need to understand what effects proposed technological changes could have; forgoing social values like anonymity and privacy (in some sense, analogous to freedom of speech and assembly) in order to make the Internet more-trustworthy might significantly limit the Internet's utility to some, and thus not be seen as progress.

Moreover, a doctrine of accountability in networked systems isn't something that can be enforced locally. When network traffic crosses international borders, accountability for originating a packet can be preserved only if all countries carrying that traffic cooperate. Some countries will see mandates for cooperation as mandates to cede autonomy, and they will resist. Various cultures resolve tension between anonymity and accountability in different ways, perhaps even selecting different trade-offs for their own traffic than for outsiders' traffic. In short, there is no universal agreement on mandates for accountability. Yet without either having such agreement or limiting places with which we are willing to communicate, our attempts to implement a doctrine of accountability cannot succeed.

Finally, beyond system and legal support for accountability, we will need analysis methods that can be used to identify a perpetrator after an offense has occurred. Classical techniques for criminal investigations in the physical world—the fingerprint on the wine glass, the fiber sample from the rug, DNA matching—aren't much use on data packets. Bits are bits, and they don't travel with detritus that can help identify their source, intent, or trajectories. Thus, the relatively new field of computer forensics faces some tough challenges, especially when there's scant system support for accountability, as is the case today. The DARPA "Cyber Genome Project" announced in January is intended to support research that addresses this problem, and thus this DoD initiative is a step in the right direction at the right time.

Question: *What research agenda should the DoD be pursuing related to IT and cybersecurity?*

The Department of Homeland Security recently posted a list of studies[2] that each give research agendas for cyber security and trustworthiness. That list of studies includes 19 entries, including two National Research Council (NRC) volumes and one Defense Science Board study. And the list is limited only to recent work. It, for example, omits a 1991 NRC Computer Science and Telecommunications Board study "*Computers at Risk: Safe Computing in the Information Age,*"[3] which, rather presciently begins:

> "The modern thief can steal more with a computer than with a gun. Tomorrow's terrorist may be able to do more damage with a keyboard than with a bomb."

It also omits mentioning the 1999 NRC study "*Realizing the Potential of C4I: Fundamental Challenges*,"[4] which focused on three key areas—interoperability, information system security, and DoD process and culture—in the command, control,

[2] See http://www.cyber.st.dhs.gov/documents.html.

[3] http://www.nap.edu/catalog.php?record_id=1581#toc

[4] http://www.nap.edu/catalog.php?record_id=6457

communications, computers, and intelligence programs in the military. The start of the security recommendations section of the report states that

> "The same military diligence and wisdom that the U.S. military uses to defend physical space can and must be applied to defend the cyberspace in which C4I systems operate."

What is perhaps more impressive than the number of government-supported studies that elucidate cyber-security research agendas is that these cyber-security research agendas all are in agreement about research needs. The requirements of the military are not all that different, here, than the cyber-security needs for other sectors. The policy options available in a military setting might be different, but the basic outlines of the technological options are probably not. In short, there is little to be gained in constructing yet one more research agenda and there is a considerable cost: constructing another research agenda would take valuable time, causing a further delay before our nation's researchers can turn their attention to making progress on solutions.

I would, however, like to take this opportunity to provide a lens through which the space of research might be viewed, giving what I see as key principles for defining the scope and direction of DoD trustworthiness research investments, going forward.

- **We must not let short-term needs derail the research investments that are the only way to obtain long-term and long-lasting solutions.** Too much federal funding—especially DoD funding—in the recent past has been focused on developing near-term solutions to immediate problems. Funding short-term solutions is consistent with the reactive approach to cyber security. We can no longer afford to be reactive. Instead of putting our thumb in the dike, we need to look into the future and think proactively.

- **Researchers must consider the real attackers we face today and those we expect to encounter tomorrow—not just hypothetical attackers.** This requires access to real data about how the systems and networks that are to be protected are being used. There is a tension here, as the military is reluctant to release operational data about its systems and networks, even in a sanitized form.

- **We must embrace research that bridges policy (regulation and economics) with technology.** As discussed above, to do research in technology without knowledge of policy or vice versa risks irrelevance. With the monetization of hacking, understanding the economics of the underground cyber criminals is critical to defending against them and /or disrupting their criminal activities.

- **We must continue to invest broadly in research concerned with building software systems: operating systems, networks, programming languages, formal methods, database systems, etc.** Ultimately, the things that undermine a system's trustworthiness will be traced to errors in design, implementation, requirements, or assumptions.

Federal Funding for Research. A list of research problems is just a start. Somebody needs to do the research listed on any research agenda. Faculty at our nation's universities are the engines of innovation. Not only do faculty drive basic research in the U.S., but university researchers also have a strong track record of transitioning that work to practice, This means that the funding climate for cyber-security research at universities is critically important for making progress on any cyber-security research agenda. Faculty are attracted by hard problems (and cyber-security provides plenty of those), but faculty are only attracted to research areas where resources are available to work on solutions.

DoD supports cyber security research through DARPA, through the MURI program, and through the services (AFOSR, ARO, and ONR). Over the last 30 years, this has been a critical source of funding for those of us in the research community who are concerned with topics most relevant to trustworthiness.

NSF recently has become a significant source of research funding, but this was partly offset by DARPA's decision under former Director Tether not to fund unclassified work in trustworthiness at universities. Other agencies, such as DHS and IARPA picked up some of the slack when DARPA stopped providing funding. However, DHS's cyber security funding tends to be more short-term and at a much lower level. IARPA has funded some trustworthiness research, but again it leans towards short-term projects.

Long-term stable funding in trustworthy computing is crucial for progress. The President's Information Technology Advisory Committee's independent report *Cyber Security: A Crisis of Prioritization*[5] points out that a lack of continuity in cyber security funding discourages younger faculty and graduate students from entering fields where future funding is uncertain. This prevents researchers from undertaking the kind of long-term exploration that is so needed to rise above our reactive approach. It also leads to a shortage of cyber security expertise, as researchers exit the field for better-funded areas of inquiry.

The overall level of funding for cyber security research is generally seen as dangerously low. The PITAC report makes this point quite explicitly. IT security expenditures are estimated to reach $79 billion annually by 2010[6]. According to the NITRD *Networking and Information Technology Research and Development Program*[7], $342.5M was being requested for FY2010 "Cyber Security & Information Assurance." This means Federal budget requests for unclassified research in system trustworthiness total roughly .4% of the expenditures that might be leveraged by the research. Moreover, anecdotal information about specific funding programs at various key Federal agencies suggests

[5] *Cyber Security: A Crisis of Prioritization*. President's Information Technology Advisory Committee, Feb. 2005. http://www.nitrd.gov/pitac/reports/20050301_cybersecurity/cybersecurity.pdf

[6] *Information Security Products & Services – Global Strategic Business Report*, Global Industry Analysts, Inc, July 2007.

[7] *The Networking and Information Technology Research and Development Program*. Report by the Subcommittee on Networking and Information Technology Research and Development, May 2009. page 21, http://www.nitrd.gov/Pubs/2010supplement/FY10Supp-FINAL-Preprint-Web.pdf

that only a portion of the $342.5M is spent on academic research in cyber-security. It then comes as no surprise to find the recent National Research Council CSTB report *Toward a Safer and More Secure Cyberspace*[8] stating that funding levels for cyber-security research are low, preventing researchers from pursuing their promising research ideas. And this echoes the findings in the PITAC report[9] which stated that (i) cyber-security solutions would emerge only from a vigorous and well funded program of research and (ii) that levels of funding were dangerously low to solve problems or to sustain a community of researchers.

Finally, note that having an ecology of Federal agencies that fund cyber-security research—and indeed, computing research broadly—is quite valuable. And there once was such a diverse ecology of funding sources for the various styles and topics that trustworthiness research spans. But that ecosystem has been eroding, as funding agencies have redefined their priorities. Inter-agency coordination that has been voluntary and tight budgets have prompted some of the Federal funding-agencies to reduce their IT and cyber-security research investments and/or to focus those expenditures on short-term work, which they see as better suited for their missions. Some of these decisions are difficult to defend, given the central role that system trustworthiness plays in the missions these agencies are supposed to support. DoD, which involves a number of distinct units that fund IT and cyber-security research, is thus missing an opportunity when it allows these to function as isolated and independent agencies.

Question: *What are we doing as a nation to ensure we have a future pipeline of IT professionals (including supporting K-12 educational activities)?*

Cyber-security professionals are today not adequate in number and not being adequately trained to meet the needs of either the military or civilian sectors.

- **Part of the problem is resources**. University Computer Science (CS) departments lack the faculty to offer the relevant courses. Few faculty members have the necessary expertise to offer courses in this area. And even if a CS department has managed to hire a few cyber-security specialists, they will likely also be involved in teaching the large complement of other classes that need to be covered by a department giving undergraduate and graduate CS degrees.

- **Part of the problem is content**. The field is relatively young and fast moving. There is not yet widespread agreement about what technical content must be covered, which makes this an exciting time to be teaching cyber-security at the university level. But it also means that textbooks and other teaching materials have short lives unless they are frequently revised, which is a disincentive to some

[8] *Toward a Safer and More Secure Cyberspace*. S Goodman and H. Lin (eds), National Academies Press, Washington, DC, 2007. Appendix B.6. http://books.nap.edu/catalog.php?record_id=11925

[9] *Cyber Security: A Crisis of Prioritization*. President's Information Technology Advisory Committee, Feb. 2005. http://www.nitrd.gov/pitac/reports/20050301_cybersecurity/cybersecurity.pdf

> authors. So there are fewer good textbooks than would be found in a more mature subject. Yet, creating agreement on content by legislating a curriculum would be a serious mistake at this point, because it would retard the dissemination of new ideas to students and it would discourage faculty from writing texts that reflect improvements in our understanding of the field.

Some institutions have been able to distinguish themselves by offering particularly strong programs in trustworthiness and in cyber-security. Little is gained by giving that list here. However, I would be remiss if I failed to mention two DoD programs that have been leaders in cyber-security education, not only within DoD but at the national level: West Point and the Naval Postgraduate School. DoD investments in these programs have been highly leveraged both (i) in producing military personnel who are well educated and (ii) in helping other universities design their courses and curricula in cyber-security.

Outside of DoD educational institutions, the problem of undergraduate education in cyber-security is complicated by the broad clientele that Computer Science departments serve. Some have argued that all undergraduates should be trained in cyber-security; and this might be a reasonable strategy for our nation's service academies. But not all undergraduate Computer Science majors in public or private universities are headed for system-building careers, and students destined for other careers need to master other content. Also, not all system developers were computer science majors as undergraduates. Thus, it just doesn't make sense to impose a cyber-security requirement on all students in University Computer Science departments.

University Curriculum. I believe that the more sensible approach is for our nation's universities to offer specializations in system trustworthiness. Students will choose this specialization, in part to make them attractive to employers and in part because the subject matter is so engaging. A well trained cyber-security professional needs to have exposure to a broad variety of topics. One would expect to see courses that cover technical topics, such as computer security principles, distributed systems and networking, systems reliability, software engineering, cryptography, and user interfaces and human factors. But I also strongly advocate exposure to non-technical topics, including cyber-law (intellectual property law, communications law, privacy law), ethics, economics of computing and networking, business strategy, and human relations (i.e., management of people). This broad education would enable a cyber-security professional to use all conceivable technical and policy tools for achieving trustworthiness. It would also ensure that solutions could be evaluated in a broader societal context, so that risk-management and trade-offs between different social values (such as privacy versus accountability) can be contemplated.

There is likely more than 1 year's worth of content past today's CS BS degree, but there is probably less than 3 years of course material. This would argue for creating some sort of graduate, professional degree program. It would be designed so that its students would learn both the technical and the non-technical topics needed to define and develop trustworthy computing systems, manage them, and oversee their deployment, use, and evolution.

A Cybersecurity Credential. Most professions expect their practitioners to have a credential before they are allowed to practice. But I believe that credentials by themselves are not the solution. At best, they are a symptom of a solution. For example, you might hope that a credentialed individual would engage in best practices. But hope is all you can do. Possession of a credential does not by itself compel the use of best practices, and it is easy to imagine credentialed system builders cutting corners by choice (such as out of laziness) or by mandate (such as from management trying to cut costs). Also, the value of a credential depends on the institutions that define what content must be mastered to obtain the label. To whom should society be willing to vest that responsibility? How do we ensure that the content and standards enshrined by the credential have been selected based entirely on society's best interests rather than financial gain or commercial advantage?

In a fast moving field, content will change rapidly. The credentialing process must keep up, as must credential holders. Otherwise, credentials impede the spread of innovation because people who employ practices learned for a credential are soon engaging in outdated methods. So a credentialing scheme must take this into account.

We are not the first group of professionals to face these problems. Credentialing schemes that the legal and medical professions use, for example, seem to serve society well. Therefore, it would be wise to understand the particulars of those credentialing processes before endeavoring to create one for producers of trustworthy systems. I see three elements as being crucial to the success of these extant schemes:

- Obtaining a credential requires far more than passing an examination. To earn a credential, a candidate undertakes years of post-bachelors education, in which the curriculum has been set by the most respected thinkers and practitioners in the field.

- Credential holders are required to stay current with the latest developments in the field by continuing their education through courses sanctioned by the institution that issues credentials.

- The threat of legal action to individuals (including malpractice litigation) incentivizes professionals to engage in best practices.

In sum, using exams to create labels for our workforce might sound like a way to get more trustworthy systems, but it's not. To have the desired effect, a credential must bestow obligations and responsibilities on practitioners. Moreover, curriculum and educational programs—not an exam—are central to the enterprise.

The Overall IT Workforce. Beyond concerns about the supply of cyber-security professionals, there is considerable concern within the IT community about the adequacy of the overall IT workforce—particularly in light of recent Bureau of Labor Statistics' projections of the increasing demand for computing and mathematical science graduates in the U.S. and recent enrollment and degree production statistics. The most recent BLS ten-year projections (from 2008-2018) predict computing and mathematical occupations will grow by 22 percent, the fastest of any "professional" occupations in the survey. That's about 150,000 new job openings requiring a computer science or mathematical background over the next decade—an amount that significantly outstrips current degree production.[10] In fact, during the period from 2002–2007, the number of undergraduate degrees in computer science actually dropped by 34 percent.

The statistics at the K-12 level, further up the pipeline, are not particularly encouraging either. While the number of high school students taking Advanced Placement science and math exams has roughly doubled over the past decade, the number of students taking the AP computer science exam has declined in recent years.[11] Participation rates among women and underrepresented minorities in computing at the K-12 level are also troubling. In 2008, only 17 percent of AP computer science test-takers were women, although women represented 55 percent of all AP test-takers. While AP CS participation rates among underrepresented groups has increased the past 10 years, it remains low at 11 percent for the AP CS test, compared to 19 percent for all AP test-takers.

Addressing these issues will require action from federal, state and local policy makers, as well as from the high-tech industry and scientific and education societies like CRA and its affiliates. It is encouraging to see that DARPA, recognizing these pipeline issues are "an issue of national importance," has released a solicitation aimed at garnering innovative new ideas to encourage students to major in computer science and pursue careers as engineers and scientists.[12] Similar efforts at the National Science Foundation aimed at increase participation rates among underrepresented populations, particularly its Broadening Participation in Computing program, have shown positive results. While the root causes of these problems are probably beyond federal agencies' ability to address, efforts like DARPA's CS-STEM program and NSF's BPC can help mobilize communities that have impact. The most recent student data seem to indicate that enrollment in CS programs is once again on the increase, although still way off its peak.[13]

[10] http://www.acm.org/public-policy/08-18%20chart.jpg

[11] http://www.acm.org/public-policy/AP.jpg

[12] https://www.fbo.gov/utils/view?id=69c81b4b7f892d4e0e0d8a7bec0eba29

[13] http://www.cra.org//resources/crn-archive-view-detail/upward_trend_in_undergraduate_cs_enrollment/

Biographical Sketch

Fred B. Schneider is Samuel B. Eckert Professor of Computer Science at Cornell University. He joined the Cornell faculty in Fall 1978, having completing a Ph.D. at Stony Brook University, preceded by a B.S. in Engineering from Cornell in 1975. Schneider currently also serves as the Chief Scientist for the NSF-funded TRUST Science and Technology Center, which brings together researchers at U.C. Berkeley, Carnegie-Mellon University, Cornell University, Stanford University, and Vanderbilt University.

Schneider's research has focused on various aspects of trustworthy systems—systems that perform as expected, despite failures and attacks. His early work concerned formal methods to aid in the design and implementation of concurrent and distributed systems that satisfy their specifications; he is author of two texts on that subject: *On Concurrent Programming* and *A Logical Approach to Discrete Mathematics* (co-authored with D. Gries). He is also known for his research in theory and algorithms for building fault-tolerant distributed systems. And his paper on the "state machine approach" for managing replication brought an SOSP "Hall of Fame" award for seminal research.

More recently, his interests have turned to system security. His work characterizing what policies can be enforced with various classes of defenses is widely cited, and it is seen as advancing the nascent science base for security. He is also engaged in research concerning legal and economic measures for improving system trustworthiness.

Schneider was elected Fellow of the American Association for the Advancement of Science in 1992, the Association of Computing Machinery in 1995, and the Institute of Electrical and Electronics Engineers in 2008. He was named Professor-at-Large at the University of Tromso (Norway) in 1996, and was awarded a Doctor of Science *honoris causa* by the University of NewCastle-upon-Tyne in 2003 for his work in computer dependability and security.

Schneider has served since Sept 2006 as a member of the Information Security and Privacy Advisory Board (ISPAB), which advises NIST, the Secretary of Commerce, and the Director of OMB on information security and privacy issues pertaining to Federal Government Information Systems. He was appointed to the Defense Science Board in January 2010. He chaired the National Academies Computer Science and Telecommunications Board study on information systems trustworthiness that produced the 1999 volume *Trust in Cyberspace*. He also served as a member of CSTB from 2002-2008 and served from 2004-2007 on the CSTB study committee for improving cyber-security research. Schneider was a member of the NSF Computer and Information Science and Engineering advisory committee 2002-2006. And in Fall 2001, he chaired the United Kingdom's pentennial external review of research funding for academic Computer Science.

In 2007, Schneider was elected to the board of directors of the Computing Research Association (CRA) and appointed to the steering committee of CRA's Computing Community Consortium. He currently chairs CRA's Government Affairs Committee.

Schneider is a frequent consultant to industry, believing this to be an efficient means of implementing technology transfer as well as learning about the real problems. He is co-chair of Microsoft's Trustworthy Computing Academic Advisory Board, which comprises outside technology and policy experts who meet periodically to advise Microsoft about products and strategy. He also provides technical expertise in computer security as well as more broadly to a variety of firms, including: BAE Systems, Fortify Software, and Microsoft.