;login:

THE MAGAZINE OF USENIX & SAGE
April 2003 • volume 28 • number 2

inside:

USENIX & SAGE
The Advanced Computing Systems Association &
The System Administrators Guild

comments on the national strategy to secure cyberspace

by Dan Geer

Dan Geer is a USENIX Past President and is Chief Technology Officer at @Stake, Inc.

geer@world.std.com

The Critical Infrastructure Protection Board (CIPB) released the Draft National Strategy to Secure Cyberspace for comment last November. The strategic shift it proposed was to focus on vulnerabilities rather than opponents. While to a *;login:* audience it may well seem trite to note that on the Internet every sociopath might be your next-door neighbor, in endorsing this idea the National Strategy broke new ground for audiences other than ours. As the critical infrastructure of this and any other free nation will be dominatedly in private hands, policy at the national level will flow through people like us whether we are design-side or operations-side, USENIX or SAGE. To give one view on what this will take, what it will mean, what it will demand, below you will find my own formal response to the National Strategy, as is and as delivered. Formal responses such as this have not yet been made publicly available and so I cannot directly point to the body of responses in full. I can say that all of us here have a role to play one way or another in a world where what we do is already critically necessary. I urge all of you to be involved at whatever limit of skill and wisdom you possess.

Provable security is never affordable while affordable security is never provable

Note that the situation is moving faster than *;login:*'s publication schedule can handle–as of this writing (early March) the final draft of the Strategy came out and the CIPB was disbanded shortly thereafter, leaving lobbyists torn between how-wonderful-no-regulator and how-terrible-no-grant-money emotions.

To: Richard Clarke, Howard Schmidt, et al.

From: Dan Geer, CTO @stake, and other affiliations

Date: 18 November 2002

Re: Primum non nocere – National Strategy to Secure Cyberspace

Because (1) the cost of duplication of electronic information is zero and (2) the Internet is a commons where distance in space and time is irrelevant, it is therefore absolutely necessary to replace a military style doctrine of security (focused assessment of hostile parties and their capabilities) with a market style doctrine of security (focused risk management of one's own vulnerabilities). In this we concur with the Draft National Strategy.

Provable security is never affordable while affordable security is never provable; tradeoffs are therefore natural and inevitable. Such tradeoffs are preferably based on market forces except where market failure is intolerable. Such market failure is likely whenever risk is diffuse and deferrable. Risk will seem diffuse and deferrable in an absence of adequate visibility to the sharable risk information we collectively do have or where whether to act or not is based only on qualitative argument. The Draft speaks to an

The single most fundamental enemy of security in cyberspace is complexity.

"information deficit" and indeed there is one. The top priority going forward is to share data that is already in hand and to share it in a way that provides coherent, quantitative decision support. Unless and until there are quantitative measures, a market failure is unavoidable. The need for legislative relief in this area, e.g., the Bennett-Kyl "Critical Infrastructure Information Security Act," is real.

The information technology woven through our critical infrastructure is what in a military setting would be called a force multiplier–it adds significant power to its user out of all proportion to its cost, ergo, it is about productivity. When a force multiplier is developed by and for an elite, it will be used in whatever way the goals and the constraints, the culture if you will, of that elite would imply. When that force multiplier is made available to everyone regardless of their goals and their constraints, it should come as no surprise that goals and constraints may well have to be injected – through the rule of law, one should hope. That there is a need for a National Strategy to Secure Cyberspace at all confirms this observation.

The single most fundamental enemy of security in cyberspace is complexity. Any solution in the name of security that increases complexity is asking for trouble; any solution that costs more in productivity than it produces will consume wealth. As such, security solutions must be simple or they will be unsustainable – security's accumulating costs will grow in visibility as security's deliverables will shrink in visibility when recent events inevitably recede in group memory.

Networked communications are increasing in type, kind, and capacity to the point that the perimeter of every entity, public or private, is dissolving. When perimeters cannot be defined they cannot be defended, and when they cannot be defended there is no practical difference between the "inside" and the "outside" of the organization or society. Plainly put, perimeter defense strategies are trending sharply toward the diseconomic and will eventually fail. The effective blurring of inside and outside, exaggerated by the cost trend made above, makes security in the form of "access control" long-term unsustainable. When access control is unsustainable, the only alternative is accountability.

Accountability for actions taken is the hallmark of a free society. Accountability requires records. When the nature of offenses to security can be enumerated a priori, the records on which accountability will be based can be minimal and their handling can be procedural. When the nature of the offenses to security cannot be enumerated a priori, neither can the records that would otherwise be required to enforce accountability a posteriori.

The form of accountability most consistent with existing private sector structure and habit is that of liability. Just as the Draft National Strategy calls on all levels of society to do their part, the need for accountability must extend to all levels of society. That includes accountability in the form of liability, but if and only if that accountability is built on the calculus of risk rather than the calculus of influence. The two principal areas where the lack of teeth in the Draft must be addressed are both of this sort: product and service vendors who sell insecure products must shoulder the liability therefrom while companies and persons whose property is used for attacks on others must shoulder the liability therefrom. The easily confirmed persistence of known, fixable security flaws in the field already proves that the present regime of information-push without liability-based accountability simply will not work. Conclusions include but are not limited to:

- Software vendors can make security claims their customers are in no position to confirm. Hence, software vendors must not make security claims without either assuming the liability for those claims or by seeking, for the claims, the confirmation of a third party audit.
- Computer network operators are already well motivated to police and repulse inbound attacks. Hence, computer network operators must become liable for attacks outbound from their networks.
- When infrastructures, fail they do so in cascade. Management of large computing infrastructures is made easier by homogeneity within that infrastructure but the only defense against common mode cascade failure is heterogeneity. Hence, infrastructures that choose homogeneity must separately correct for the added risk burden they thereby impose on those who depend upon them.
- Security is a means; it is not an end. With rapid technical change, means cannot be durable. Only ends can be durable. Security-centric "procedural correctness" without a concrete description of goal state(s) makes any risk worse by soaking up the resources that might actually have gone to genuine repair and by comforting the ill-informed. Hence, whatever regulation is created or augmented in support of the National Strategy must be about ends and not means.
- The critical infrastructure of the United States of America obviously includes private sector firms that are not US-based. Hence, the National Strategy will not complete so long as it is bound to US-based firms only and the National Strategy must be so modified.
- Because the price of bandwidth falls faster than the price of storage which falls faster than the price of computation, long-term economic pressures favor capturing observable events to multiple locations for later analysis when and if needed. Because a linear growth in network end-points creates a geometric growth in network complexity, any entity charged with security must never fall behind in data collection even if it assumes analysis of that data may never occur or occur much delayed. As observability in the electronic sphere vastly exceeds observability in the physical sphere, hence the phrase "expectation of privacy" must be based on cultural norms as it cannot be any longer based on what is within the realm of the possible.

In sum, details, quantitative details, matter. We, all of us, must share data on occurrence of risk and countermeasures to risk, we must share it in a setting of sticks and carrots that harness self-interest rather than work against it, and national policy can only stress quantifiable ends that must be met or liability be assessed, assuming that the National Strategy to Secure Cyberspace wishes to itself reach a goal rather than merely look good.

Security is a means; it is not an end.