The Manifesto of the Working Group on Systems Security Engineering: A Declaration of Responsibility

Rick Dove, rick.dove@incose.org; and John Wirsbinski, john.wirsbinski@incose.org

This is the manifesto of the Systems Security Engineering Working Group. At our first meeting at the 2007 International Workshop, we mapped out a general agreement on our motivation, purpose, and the necessity for collaborative work—and agreed that a manifesto was an appropriate form to articulate our sense of mission. The Manifesto of the Working Group on Systems Security Engineering:

A Declaration of Responsibility[1]

We speak here of security. Not narrowly of cyber or physical security, but of total system security—that which provides the faith and trust we want in the continued safety, service, and economic effectiveness of the systems we count on as part of life in society.

We speak here of a community of engineers responsible for that security. One that encompasses all who are involved by act or edict in the total effectiveness of systems that support or affect humankind in any and all ways. This includes of course those with the recognized duties or titles of systems engineer regardless of domain, but includes fully and equally those who function equivalently in the crafting and causing of policy, procedure, strategy, standard, law, governance, regulation and other such systems brought into existence to provide service with purpose. We view all such as systems engineers, regardless of title, and presume they are entitled to their role by studied and respected competence in the practices and principles that determine the effectiveness of the systems they cause to exist.

We speak because evidence shows a relentless deterioration in system security, because security has not been adequately embraced by system engineering as a fundamental system element, and because the systems that enable advanced societal freedoms and services are also enabling unacceptable, unpredictable, and unprecedented consequences.

We call for a new order of thought. One that breaks with the forces of de facto, reactive progress, one that consciously identifies and addresses the reality of the situation and the need for proactive, as well as reactive, engagement; one that embeds that thought and responsibility in the new best practices of systems engineering, and one that remains both vigilant and innovative as expressions and possibilities of reality continue to change.

We feel that a declaration of some strength is in order. The signs of classic denial are evident—security failures are acknowledged, yet dismissed with grudging acceptance. The techno-commercial-government juggernaut powerfully sustains continued hope in the form of new effective defense and regulation for the latest nature of violation, but nobody is addressing the systemic causes of increasing vulnerability and growing violation. Where is the machine and motivation for that?

Who is responsible?

Systems engineers have the responsibility of evaluating, establishing, and governing the objectives, interplay, and tradeoffs among the specialty engineering functions employed to create an effective system. Systems engineers accomplish this by working with the higher issues, engineering the integrated result of a complete system design and its many relationships to its environment.

We are responsible, and in so recognizing, make this declaration:

WHEN in the Course of socio-technical Evolution , it becomes necessary for an engineering community to recognize a long deteriorating situation and to assume among the powers of the practice, the responsibility and thinking that reality and the laws of nature require of them, a decent respect to the opinions of all affected requires that they should declare the causes which compel them to act.

We hold these truths to be self evident,

> that engineered systems are designed for purpose;
>
> that they are engineered by their designers to meet certain fundamental requirements;
>
> that among these are security, safety, service, and the pursuit of economic effectiveness;
>
> that to secure these requirements design principles are instituted among the community of engineers, deriving their just nature from first principles, natural laws, and best practice;
>
> that whenever such principles become inadequate to these ends, it is the responsibility of the community to abolish them, and to institute new principles that shall seem most likely to deliver security, safety, service, and effectiveness.

Prudence dictates that principles long established should not be changed for light or transient causes; and accordingly all experience has shown humankind more disposed to suffer, while inadequacy is sufferable, than to right themselves by abolishing the forms to which they are accustomed.

But when an unrelenting deterioration, no matter how incremental or diffuse, makes evident that the dominating strategy is no longer adequate, it is their right, it is their duty, to question and adjust the beliefs and behaviors that support such state of affairs, and to provide new strategy for future security.

Such has been the vocal sufferance of techno-progressive society; and such is now the necessity which constrains us to craft a new set of principles.

The history of the present situation is a history of continually increasing violation and loss, all having in direct result a continuing decrease of resources available for production, service, and innovation.

To prove this, let facts be submitted to a candid world.

> The number of malicious-code variations for active cyber attacks doubled in 2007, having taken twenty years to reach the size it was at the beginning of the year.[2]
>
> Social engineering attacks are on the rise, where criminals gain access to otherwise secured assets by tricking insiders into providing direct or indirect means for entry of outsiders with malicious intent.[3]
>
> Significant growth in the number of end-user computer vulnerabilities occurred in 2007, on multiple operating systems, and are being massively exploited.[4]

> Cyber crime has expanded from isolated attacks initiated by individuals or small rings to well-funded, well-organized operations using sophisticated technology and social engineering.[5]
>
> The cyber threat to national security is on the increase, with a current estimate of 120 countries using the Internet for political, military, and economic espionage activities.[6]
>
> A “black” cyber-economy has reached global economic sophistication, where criminals sell malware services online using the same kinds of development methods and guarantees given by legitimate software vendors.[7]
>
> Total costs of determined strategic breeches are rising dramatically.[8]
>
> Telecom fraud cost companies €42 billion in 2006 and is growing at 15% a year.[9]
>
> Security policies and regulations that are inconvenient to organizations or individuals are commonly circumvented or ignored.[10]
>
> Security that relies on rational human behavior is repeatedly shown to be ineffective.[11]
>
> Convergence of physical and cyber security multi-pronged attack gains increasing recognition, while converged counter-measures loose ground.[12]
>
> The percentage of GDP and the percentage of organizational budget applied to security measures continues to increase.[13]
>
> Systems of all kinds that are structured as networks or function as infrastructure, and are significant economic or public services, are the focal targets of the emerging “fourth generation” warfare.[14]
>
> The threat from the insider continues to grow in loss potential and incident statistics, yet security strategy remains dominated by the external threat.[15]

In every stage of these deteriorations we have responded with redress in the best reactive terms. Our repeated defenses have been answered only by new offenses. A strategy, whose character is thus marked by every act which may define ineffectiveness, is unfit to be practiced by responsible systems engineers.

Nor have these inadequacies been wanting in attentions to decision makers who establish priorities and allocate resources. They have had demonstrations from time to time of undue risk and vulnerability. We have reminded them of the circumstances of accelerating technology and social developments, and the growing uncertainties of risk. We have appealed to their common sense and motivation to do what is right, and we have invoked the common desire to avoid catastrophic embarrassment, which would inevitably interrupt our relationship of mutual enterprise. They have been deafened by the voices of established procedure and other priority. We must, therefore, bow to the necessity of outcome and satisfy their needs while accepting and dispatching our professional responsibility.

We, therefore, solemnly publish and declare, that the community of system engineers are, and of right ought to be, responsible for system security as a fundamental systems engineering practice, that they are absolved from all encroachment on responsibility assumed or claimed by others, and that all political and inertial connection with maintenance of the status quo be totally dissolved; and that as custodians of optimal system effectiveness they have full power and responsibility to develop principles and best practices that employ holistic systems thinking;

assume adversary penetration of our systems always and constantly;

define and embody resilient reactive concepts;

define and embody innovative proactive concepts;

integrate all security disciplines;

embed security within system architecture;

represent meaningful measures and heuristics of risk and security effectiveness;

identify and address the realities of the environment, including human behavior, organizational behavior, technology pace, systems complexity, globalization, agile enterprise practices, and agile adversaries; and

remain both vigilant and innovative as expressions and possibilities of reality continue to change;

and to discover, define, and address all other such things which responsible systems engineers have an obligation to do.

And for the support of this declaration, we mutually pledge to each other, as a working group, our diligence, our collaboration, and our zeal.

Endnotes

[1] Already considered a best practice in the disciplines of architecture and software design, recognition and reuse of structural patterns is gaining attention in systems engineering. Credit is given for the reuse of the pattern of thoughtful structure Thomas Jefferson crafted for *The Unanimous Declaration of the Thirteen United States of America.* Jefferson's draft manuscript is available at http://memory.loc.gov/cgi-bin/ampage?collId=mtj1&fileName=mtj1page001.db&recNum=544 (this and all other online references accessed 17 Dec. 2007).

[2] According to the Finnish company F-Secure, cited in T. Espiner, "Cracking Open the Cybercrime Economy," *ZDNet.co.uk*, 14 Dec. 2007, http://resources.zdnet.co.uk/articles/features/0,1000002000,39291463,00.htm. See also IBM Internet Security Systems, *Cyber Attacks on the Rise: IBM 2007 Midyear Report* (Somers, NY: IBM, 2007), http://www.iss.net/documents/whitepapers/x-force_threat_exec_brief.pdf.

[3] According to the Sans Institute's "Top 20 2007 Security Risks" (http://www.sans.org/top20/), cited in Ian Grant, "Social engineering attacks on the rise," *ComputerWeekly.com*, 27 November 2007, http://www.computerweekly.com/Articles/2007/11/27/228312/social-engineering-attacks-on-the-rise.htm.

[4] Sans Institute, "Top 20 2007 Security Risks."

[5] McAfee, Inc., "Virtual Criminology Report - Cybercrime: The Next Wave," http://www.mcafee.com/us/research/criminology_report/default.html . See also Internet Crime Report 2006, FBI and National White Collar Crime Center, http://www.ic3.gov/media/annualreport/2006_IC3Report.pdf . See also National White Collar Crime Center and the (U.S.) Federal Bureau of Investigation, *Internet Crime Report: January 1, 2006–December 31, 2006*, http://www.ic3.gov/media/annualreport/2006_IC3Report.pdf .

[6] McAfee, Inc., "Virtual Criminology Report."

7. Espiner, “Cracking Open the Cybercrime Economy.” See also E. Jellenc and K. Zenz, *Global Threat Research Report: Russia* (n.p.: iDefense [a VeriSign company], 2007), www.accelacomm.com/jlp/cicso_ver072707/10/80077454/ (accessed 12/17/07); and L. Greenemeier and J. N. Hoover, “The Hacker Economy,” *Information Week*, 12 Feb. 2007, http://i.cmpnet.com/informationweekdownloads/doc/0702sec_01.pdf.

8. B. Johnson, “PCI Compliance and the Cost of a Credit Card Breach,” Braintree Payment Solutions Blog, comment posted 15 Oct. 2007, http://www.braintreepaymentsolutions.com/blog/pci-compliance-and-the-cost-of-a-credit-card-breach/.

9. According to the International Forum of International Irregular Network Access, cited in J. Kennedy, “Hanging on the Telephone,” *SiliconRepublic.com*, 8 March 2007, http://www.siliconrepublic.com/news/news.nv?storyid=single7916.

10. According to a study by the Ponemon Institute, cited in J. Vijayan, “Security Policies? Workers Ignore Them, Survey Says,” *ComputerWorld*, 6 Dec. 2007, http://www.computerworld.com/action/article.do?command=viewArticleBasic&articleId=9051483&source=rss_topic17.

11. K. Erickson and P. N. Howard, “A Case of Mistaken Identity? News Accounts of Hacker, Consumer, and Organizational Responsibility for Compromised Digital Records,” *Journal of Computer-Mediated Communication* 12, no. 4 (2007), http://jcmc.indiana.edu/vol12/issue4/erickson.html.

12. L. Page, “Disgruntled Techie Attempts Californian Power Blackout,” *The Register*, 20 April 2007, http://www.theregister.co.uk/2007/04/20/terrorists_among_us_flee_flee/print.html. See also D. Goodin, “Masked Thieves Storm into Chicago Colocation (Again!),” *The Register*, 2 Nov. 2007, http://www.theregister.co.uk/2007/11/02/chicaco_datacenter_breaches/; and T. Espiner, “Burglars Plunder Verizon’s London Data Centre,” *ZDNet.co.uk*, 10 Dec. 2007, http://news.zdnet.co.uk/security/0,1000000189,39291411,00.htm.

13. A. Holmes, “The Global State of Information Security 2006,” *CSO*, 1 Sept. 2006, http://www.csoonline.com/read/090106/fea_exec_pf.html. See also Info-Tech Research Group, “Security Spending Exceeds 7% of IT Budgets,” 15 Nov. 2006, http://www.infotech.com/Research/Notes/ITAP/SecuritySpendingExceeds7PercentofITBudgets.aspx?PublicationNumber=%7B8CDEBC81-E22D-4074-AFBB-786B954B2309%7D&SubCenter=%7b0CE23E8A-D3BE-40F0-8E78-32B6309142DA%7d.

14. J. Robb, *Brave New War: The Next Stage of Terrorism and the End of Globalization* (Hoboken, NJ: Wiley, 2007).

15. CERT Program, “Survey Shows E-Crime Incidents Are declining Yet Impact is Increasing” (press release) (Pittsburgh, PA: Carnegie Mellon University, 6 Sept. 2006), http://www.cert.org/archive/pdf/ecrimesurvey06.pdf. See also R. Richardson, *CSI Survey 2007: The 12th Annual Computer Crime and Security Survey* (n.p.: Computer Security Institute, 2007), http://i.cmpnet.com/v2.gocsi.com/pdf/CSISurvey2007.pdf.