Asymmetric Information Warfare: Cyberterrorism Critical Infrastructures

Stephen D. Wolthusen
Security Technology Department
Fraunhofer-IGD
Fraunhoferstr. 5, 64283 Darmstadt, Germany
Email: {busch, wolt}@igd.fhg.de

1 Introduction

Terrorist attacks in recent years, particularly those of October 12, 2000 and September 11, 2001, along with war games such as Millennium Challenge have demonstrated forcefully that asymmetric warfare [THO01] with conventional weapons poses a challenge to existing defense and homeland security structures that have not been addressed satisfactorily.
It appears only prudent to assume that such attacks, whether by the perpetrators of the previously mentioned acts or by new groups of non-state actors, rogue nations, or proxies for such nations will not only continue but must also be assumed to encompass further threats and to prepare accordingly where possible – a constant feature of human conflict [GOU00].

While this certainly includes CBRN (chemical, biological, radiological, nuclear) threats [COR00a, COR00b], one should not discount the probability of a massive information warfare attack on either defense or civilian systems, and given the mode of operations employed by the aforementioned terrorist groups (massive, intricately coordinated attacks) and the effectiveness of these techniques, such an attack appears likely not to be a solitary event but would be planned to coincide with a conventional or CBRN attack to achieve a maximum both in terms of destructive and in disruptive power.

Information warfare has, paradoxically, been a subject that has emerged and vanished rapidly after garnering intense interest by defense and political institutions [MOL96,NEI97], presumably in no small part because of both the amorphous nature of the conduct of conflict claimed by its advocates and the apparent lack of connection between the envisioned scenarios and the reality of minor disruptions and annoyances – indeed, most tellingly the only documented and hence often-quoted case of cyberterrorism is a 2000 case of a former employee of the Hunter Watertech utility contractor on the Australian Gold Coast manipulating the electronically controlled sewage system to release several hundred thousand gallons of untreated sludges into rivers and parkland [GRE01].

At the same time, a number of security events involving general purpose computer systems beginning in 2001 have raised the specter of massive disruptions. This apparent disconnect can arguably be traced to several developments, but most prominently to the rapidly increasing degree of internetworking among computer systems and networks as well as the bandwidth available for such interconnects. These, together with a rather homogeneous population which includes a very large pool of susceptible nodes, provide the requisite infrastructure for several categories of malware, most notably viruses such as the recent W32/Sobig.F [CER03b] and rapidly spreading worms along the lines of the recent W32/Blaster worm [CER03a], both affecting the Microsoft Windows NT family of operating systems (and also the consumer editions in case of W32/Sobig.F) with a $\rho >> 1$ [KER27,BAI75,KEP91,CHE93].

The second reason for the limits to attention paid to information warfare can be traced back to the relatively benign characteristics of the attacks themselves. While these are definitely caused in part by incompetence on the part of the authors of the malware, another possible limitation in the destructive payload can be imputed based on a desire by the malware's author's not to destroy the infrastructure on which such maladjusted individuals rely themselves.

2 Critical Infrastructures

The benignity of the attacks noted in the preceding section is, however, a decidedly relative term and is applied here only in comparison to a deliberate attack setting out to achieve maximum disruption of affected systems targeted for a tactical purpose.
It should be noted that even these comparably harmless attacks had severe repercussions in a number of areas increasingly relying on internetworked computer systems to achieve the speed and efficiency necessary for commercial competitiveness.

One example of the hazards of such internetworking is the case of the nuclear power plant Davis-Besse operated by FirstEnergy Nuclear Corp., which suffered a breach of its plant operating network (nominally separated from corporate administrative networks) on January 25, 2003. Although the plant had not been operational since 2002 because of a fault in the containment vessel detected by an earlier Nuclear Regulatory Commission inspection, the impact can be described as severe since the network overload caused by the MS SQL-Slammer worm [CER03c], which became progressively worse throughout the day without countermeasures being taken, rendered the Safety Parameter Display System inoperable for a duration of almost 5 hours before the plant process computer system was completely inoperable, this time for a duration of 6 hours.

While the connection of the plant network to the corporate network through a firewall is highly problematic in and of itself given the limited efficacy of firewall systems against advanced attacks and protocol mechanisms, the route for incursion used in this case was a separate network link between the plant network and that of a contracting company operating an application server for FirstEnergy Nuclear, which bypassed the existing firewall completely. As the contractor's server systems became infected, the bypass link permitted unhindered access to the plant network. While independent automated safeguards existed that would have provided redundant safety mechanisms even if the plant had been operational, the interconnection of SCADA systems with public networks through minimal or nonexistent security and safety mechanisms is rather troubling [NRC03].

Although the infection rates seen in the case of the MS SQL-Slammer worm were limited in the magnitude of affected computer systems compared to other recent security issues with only approximately 250'000 hosts affected, a number of critical infrastructure components were affected at the same time that the Davis-Besse incident took place.

The 13'000 automated teller machines of the Bank of America were unable to dispense cash to customers since their network connectivity to the bank's back end server systems through virtual private network connections utilizing the public Internet was severely limited by the bandwidth consumed by the attacks of the MS SQL-Slammer worm. As a result, even though the security perimeter of the bank was never breached, customers were effectively denied service on January 25, 2003. Similar issues were also reported outside banking, affecting particularly transatlantic telephone service and Internet connections [DAV03]. In addition to the aforementioned energy, banking, and telecommunications sectors, transportation was also

affected by the same attacks with ticketing of Continental Airlines impeded and flights delayed for up to 30 minutes.

Given the damage caused by the MS SQL-Slammer in spite of the harmless reinfection characteristics (the worm did not make itself resident, restarting an affected system effectively removed the worm from the system) and its nonexistent payload (the damage caused by it was solely due to network overloading, although the code executed by the worm was running with SYSTEM privileges, providing full administrative control over the entire infected server) and other recent incidents also affecting several elements of the critical infrastructure in industrialized countries, the possibilities of a malicious, structured attack purposely designed by an adversary should be obvious.

One of the primary root causes already noted above, the indiscriminate internetworking of systems and networks, particularly also of SCADA systems in critical infrastructures such as power lines, results in significant potential vulnerabilities. These become particularly exacerbated in systems where decisions are required at speeds that preclude the effective interventions by humans in decision loops and that have to rely on fully automated systems to perform such decisions and actions. Such systems, however, can be subverted or impeded with potentially disastrous effects, even assuming that they do not harbor intrinsic defects – an assumption that should not be made of systems that include highly complex COTS hardware and software systems for which no satisfactory reliability and safety information is available.

In the particular case of the energy sector, the U.S. National Security Agency had already demonstrated in 1998 during Eligible Receiver that it was possible to break into existing grid control computer systems and thereby causing massive disruptions.

As the extensive power outages of August 12, 2003 in the northeastern United States and Canada have demonstrated, the power grid can fluctuate on time-scales that do not permit adequate human reactions (the cascade of voltage collapse failures leading to the power outage lasted only nine seconds in total) [ABR03]. At the same time, a body of research is dedicated to further optimizing flows through power grids by computer-controlled systems embedded in the grid providing further avenues for potential adversaries to attack [ARM02]. It should be noted that the majority of these vulnerabilities were identified in reports dating back more than a decade [McD89] as well as in a number of national governmental analyses of critical infrastructures throughout most industrialized nations.

Even though these potential vulnerabilities are at least in general principle known, actions to remedy these issues remains limited. This is presumably largely because of the allocation of the critical infrastructure, the majority of which is owned and operated by commercial entities throughout the majority of industrialized nations that must compete with other commercial entities on cost and service provided as well as yield adequate revenue.

Since countermeasures to protect critical infrastructures frequently introduce the very redundancies and inefficiencies that the competition among the commercial entities is bound to eliminate and the returns on investments in securing the critical infrastructure that are not mandated by law or other regulations are generally not realized by the corporations operating the infrastructure but by the society at large, the commercial incentives for operators of critical infrastructures are rather limited – to the contrary, as shown by the increasing replacement of customized, highly robust components for e.g. SCADA operations or ATM devices with COTS systems running highly complex and therefore potentially vulnerable general purpose operating systems and application components.

3 Information Warfare and Cyberterrorism

While some authors have characterized information warfare as strategic in nature [MOL96], that appellation can be severely misleading in several ways. Clearly, neither current critical infrastructures including power and chemical industry sectors nor weapons systems are structured in such a way as to justify the terminology of strategic warfare [BRO59,KAH60]. At the same time, however, neither is cyberterrorism an appropriate choice in terminology for the types of attacks one is to anticipate based on the physical attacks witnessed so far since traditional "practical" terrorism is arguably primarily aimed at drawing attention to a specific cause [LAQ87].

Instead, one is confronted by a new threat dimension that can be viewed from two perspectives that need not be contradictory but have different implications for potential countermeasures.

First, as in the case of CBRN attacks, but particularly the case of biological threats that are similarly low in terms of cost of entry to information system attacks, the barriers imposed by knowledge and terminology for a well-financed group or even an individual to cause massive damage with a weapon or attack mechanism are continuously reduced [REE03]. In the case of attacks on computer systems and networks, this is further exacerbated by the already noted increases in available bandwidth, degrees of interconnection, and the latency of the interconnections, largely rendering human intervention ineffective.

This implies that a number of highly destructive (or at least disruptive in the case of most information technology systems) weapons are no longer in the purview of nation states but may at some point be deployed by even a single irrational individual. As one must assume a small but non-zero probability for each individual or group capable of such actions to perform an attack, one is faced with a continuously increasing threat as the number of individuals and groups with the knowledge and capabilities rises – which presumably cannot be limited effectively since much of the technology is dual-use or released into the open literature inadvertently [JAC01,WIM02]. This is particularly problematic since clearly the type of terrorism currently on the rise is not of the practical but rather of an apocalyptic variety that seeks destruction virtually for its own sake [PET02].

The second perspective worthy of consideration is that even though attacks already allegedly conducted particularly by the Al-Qaeda organization were aimed at destruction, a strategic objective behind the sequence of attacks cannot be dismissed outright. As such, it is perhaps appropriate to consider such actions and possible subsequent actions from the perspective of conventional warfare, i.e. to consider the adversary as an organization that wishes to subjugate one or more nations to its will using force or the threat of force. Given the proclivity particularly of the Al-Qaeda organization to coordinate operations for maximum effect and the ability of information warfare to provide amplifying effects through the disruption of communication or disinformation (e.g. for first responders or other emergency services in case of CBRN attacks) and to cause severe economic damage as a side effect, information warfare as one weapon in the arsenal of apocalyptic terrorism becomes probable.

At the same time the issues of potential disruptions to civilian infrastructure that have restrained nation states bound by the Geneva Conventions Relative to the Protection of

Civilian Persons in Time of War [GRE98] from employing information warfare where technically feasible clearly do not apply to such organizations and similar threats.
As the examples of the preceding sections have demonstrated, the effects of even comparably harmless attacks on critical infrastructure elements can be rather severe; a set of coordinated attacks by malicious entities is likely to cause significant damage in and of itself and exacerbate the effects of a concomitant attack, for all practical purposes acting as highly effective supporting fires for attacks in the physical domain.

4 Defensive Mechanisms and Triage

Given the severe restrictions imposed on potential countermeasures by largely civilian ownership of critical infrastructures discussed in section 3 and the resulting highly internetworked structure of COTS component-based systems of systems (as well as similar developments towards COTS-based network structures in the defense area, a particularly troubling development given the emphasis often placed on network-centric warfare), one of the foci for immediate action can only be the amelioration of the existing vulnerabilities and hence countering several (in part unknown) threats.

Any such mechanism must be capable of deployment over the existing heterogeneous systems found in any nontrivial organization [WOL01a] and, moreover, take into account that – given that by definition the most damaging attacks will be so-called "zero-hour attacks" where no known countermeasure exists – it will have to provide not only purely defensive mechanisms but do so both in depth and in conjunction with recovery and triage mechanisms that permit to isolate affected components and networks while providing information assurance for at least the most critical missions and objectives the information system is serving [WOL05].
In doing so, the same tight decision loops that characterize attacks must also be mastered by defensive mechanisms. This implies that at least critical parts of defensive mechanisms must be automated to an extent permitting rapid reaction commensurate with the speed of attack developments and, if possible, be able to model and predict adversaries' behavior and counteract it in time.

An obviously critical element in such a mechanism is that it must be effective for all elements constituting an information system that is required for the fulfillment of a given mission or objective, since otherwise an adversary has the opportunity to exploit such a weak link.
One way of achieving the objectives outlined above requires that the aspects of information systems relevant to information assurance be modeled mathematically (more precisely, using a first order formal theory as well as algebraic structures embedded within said theory to represent the axiomatization of the modeled systems) in the abstract and providing interpretations of the formal model onto each of the components as necessary, thereby providing a bijective mapping between a technical implementation and the mathematical model.

By formulating permitted or required operations within the formal theory, one is able to express arbitrary security models and security policies and verify the internal consistency of each policy and sets thereof. At the same time, the mathematical formulation chosen also permits the use of automated reasoning [BUN84] which can be employed to automate the predictive and reactive behavior alluded to above.

The bijective mapping onto the elements of the formal theory and the policies represented therein as well, however, must be augmented by enforcement mechanisms that permit the

control particularly over COTS components that are not by themselves capable of enforcing the information assurance properties nominally required of them. By retroactively embedding such enforcement mechanisms into COTS systems and subjugating them via an externally controlled reference monitor mechanism to the applicable security policies [WOL01b], such security policies can be enforced effectively both at the individual node (host) and network levels.

As a result, information systems can be largely protected within the confines of overall developmental assurance provided by the component COTS systems; under these constraints, however, the permitted effective behavior of components can be precisely circumscribed and modeled. In cases where the security of a given node or component network is breached or otherwise compromised, automated reaction mechanisms can quickly isolate such systems to prevent the further spread of infections or corrupted data. Moreover, security policy mechanisms can also be used to perform effective mission triage by e.g. rapidly and automatically deactivating the availability of certain vulnerable services to ensure the continued availability and information assurance of the information system for critical missions.

5 Conclusion and Outlook

Information assurance is confronted by a confluence of new and exacerbated vulnerabilities at the same time that the previously largely theoretical considerations of information warfare and cyberterrorism are becoming both viable and increasingly devastating in their potential results.

At the same time the abilities of industrialized nations to control and effectively protect the very critical infrastructures that may be a direct or intermediate supporting target of such attacks are sharply limited given the commercial imperatives under which the owners of the critical infrastructure elements are operating.

We presented and proposed a mechanism that can address the underlying constraints of existing information technology infrastructure by providing the ability to retroactively insert control mechanisms into information system components that force compliance with security policy that can be defined to provide adequate information assurance properties for given missions.

The underlying models used to represent such information assurance properties (which also include issues such as timeliness and reliability for information to be delivered) as well as issues of developmental assurance both in providing the policy enforcement and the embedding into existing systems are clearly the subject of further research and may prove relevant to improving the robustness of our information systems infrastructure.

6 References

[ABR03] U.S./Canada Power System Outage Task Force 2003: *August 14, 2003 Outage Sequence of Events*. Washington, D.C., USA, September 12, 2003.

[ARM02] Austin Armbruster and Bruce McMillin and Mariesa L. Crow: *Controlling Power Flow Using FACTS Devices and the Maximum Flow Algorithm*. In Proceedings of the 5th International Conference on Power Systems Operation and Planning, ICPSOP-2002, Abuja, Nigeria, December, 2002.

[BAI75] Norman T. J. Bailey: *The Mathematical Theory of Infectious Diseases and its Applications*, 2nd ed. Oxford University Press, Oxford, UK, 1975.

[BRO59] Bernard Brodie: *Strategy in the Missile Age*. Princeton University Press, Princeton, NJ, USA, 1959.

[BUN84] Alan Bundy: *The Computer Modeling of Mathematical Reasoning*. Academic Press, New York, NY, USA, 1984.

[CER03a] CERT Advisory CA-2003-20 W32/Blaster Worm. CERT/CC 2003.

[CER03b] CERT Incident Note IN-2003-03 W32/Sobig.F Worm. CERT/CC 2003.

[CER03c] CERT Advisory CA-2003-04 MS-SQL Server Worm. CERT/CC 2003.

[CHE93] Jeffrey O. Kephart, David M. Chess, and Steve R. White: *Computers and Epidemiology*. IEEE Spectrum 30(5):20-26

[COR00a] Anthony H. Cordesman: *Defending America: Redefining The Conceptual Borders of Homeland Defense*. Technical Report, Center for Strategic and International Studies. Washington, D.C., 2000.

[COR00b] Anthony H. Cordesman: *Asymmetric Warfare versus Counterterrorism: Rethinking CBRN and CIP Defense and Response*. Technical Report, Center for Strategic and International Studies. Washington, D.C., 2000.

[DAV03] Aaron Davis: *Computer Worm Snarls Web*. San Jose Mercury News, San Jose, CA, USA, January 26, 2003.

[GOU00] Vincent J. Goulding, jr.: *Back to the Future with Asymmetric Warfare*. Parameters: US Army War College Quarterly **XXX** (4): 21-30

[GRE98] Lawrence T. Greenberg, Seymour E. Goodman, and Kevin Soo Hoo: *Information Warfare and International Law.* National Defense University Press, Washington D.C., USA (1998).

[GRE01] Glenis Green: *Hacker Jailed for Sewage Sabotage*. The Brisbane Courier-Mail, Brisbane, Australia, November 1, 2001.

[JAC01] Ronald J. Jackson, Alistair J. Ramsay, Carina D. Christensen, Sandra Beaton, Diana F. Hall, and Ian A. Ramshaw: *Expression of Mouse Interleukin-4 by a Recombinant Ectromelia Virus Suppresses Cytolytic Lymphocyte Responses and Overcomes Genetic Resistance to Mousepox*. Journal of Virology **75**(3):1205-1210.

[KAH60] Herman Kahn: *On Thermonuclear War*. Princeton University Press, Princeton, NJ, USA, 1960.

[KEP91] Jeffrey O. Kephart and Steve R. White: *Directed-Graph Epidemiological Models of Computer Viruses*. In: Proceedings of the IEEE Symposium on Security & Privacy, Oakland, CA, USA, pp. 343-361, 1991.

[KER27] W. O. Kermack and A. G. McKendrick: *A Contribution to the Mathematical Theory of Epidemics*. Proceedings of the Royal Society of London A **115**:700-721

[LAQ87] Walter Laqueur: *The Age of Terrorism*. Little, Brown and Company, Boston, MA, USA, 1987

[McD89] J. C. McDonald (ed.): *Growing Vulnerability of the Public Switched Networks: Implications for National Security Emergency Preparedness*. National Academy Press, Washington, D.C., USA 1989.

[MOL96] Roger C. Molander, Andrew S. Riddile, and Peter A. Wilson: *Strategic Information Warfare: A New Face of War*. The RAND Corporation, Santa Monica, CA, USA. Report Number MR-964-OSD, prepared for the Office of the Secretary of Defense.

[NEI97] Robert E. Neilson: *Sun Tzu and Information Warfare*. National Defense University Press, Washington, D.C., USA 1997.

[NRC03] United States Nuclear Regulatory Commission Office of Nuclear Reactor Regulation: *NRC Information Notice 2003-14: Potential Vulnerability of*

Plant Computer Network to Worm Infection. Washington, D.C., USA, August 29, 2003.

[PET02] Ralph Peters: *Beyond Terror: Strategy in a Changing World*. Stackpole Books, Mechanicsburg, PA, USA, 2002.

[REE03] Martin Rees: *Our Final Century*. Heinemann, London, UK, 2003.

[THO01] Timothy L. Thomas: *Deciphering Asymmetry's Word Game*. Military Review **LXXXI** (4): 32-37

[WEB03] Cynthia L. Webb: *Worm Wars II*. The Washington Post, Washington, D.C., August 21, 2003.

[WIM02] Jeronimo Cello, Aniko V. Paul, and Eckhard Wimmer: *Chemical Synthesis of Poliovirus cDNA: Generation of Infectious Virus in the Absence of Natural Template*. Science **297**(5883):1016-1018.

[WOL01a] Stephen D. Wolthusen: *Layered Multipoint Network Defense and Security Policy Enforcement*. In: Proceedings from the Second Annual IEEE SMC Information Assurance Workshop. United States Military Academy, West Point, NY, USA, IEEE Press, pp. 100-108, June 2001.

[WOL01b] Stephen D. Wolthusen: *Security Policy Enforcement at the File System Level in the Windows NT Operating Systems Family*. In: Proceedings 17th Annual Computer Security Applications Conference, New Orleans, LA, USA, IEEE Computer Society Press, pp. 55-63, December 2001.

[WOL05] Stephen D. Wolthusen: *Information Assurance: An Operating Systems Perspective*. Cambridge University Press, Cambridge, UK, 2005. To appear.