COMMON VULNERABILITIES IN CRITICAL INFRASTRUCTURE CONTROL SYSTEMS

Jason Stamp, John Dillinger, and William Young
Networked Systems Survivability and Assurance Department

Jennifer DePoy
Information Operations Red Team & Assessments Department

Sandia National Laboratories
Albuquerque, NM 87185-0785
22 May 2003
(2nd edition, revised 11 November 2003)

Sandia National Laboratories report SAND2003-1772C.

Sandia is a multiprogram laboratory operated by Sandia Corporation, a Lockheed Martin Company, for the United States Department of Energy's National Nuclear Security Administration under contract DE-AC04-94AL85000.

ABSTRACT

Sandia National Laboratories, as part of its mission to ensure national security, has engaged in vulnerability assessments for IT systems with the main focus on control and automation systems used in United States critical infrastructures. Over the last few years, diverse customers from the electric power, petroleum, natural gas, and water infrastructure have partnered with us to gain insight into their critical vulnerabilities and learn mitigation strategies. This report describes the generalized trends in vulnerabilities observed from the assessments, as well as typical reasons for these security issues and an introduction to an effective mitigation strategy. Overall, most security vulnerabilities in infrastructure include failures to adequately define security sensitivity for automation system data, identify and protect a security perimeter, build comprehensive security through defense-in-depth, and restrict access to data and services to authenticated users based on operational requirements. Many of these vulnerabilities result from deficient or nonexistent security governance and administration, as well as budgetary pressure and employee attrition in system automation. Also, the industry is largely unaware of the threat environment and adversary capabilities. Finally, automation administrators themselves cause many security deficiencies, through the widespread deployment of complex modern information technology equipment in control systems without adequate security education and training. Comprehensive mitigation includes improved security awareness, development of strong and effective security governance, and amelioration of security vulnerabilities through the careful configuration and integration of technology.

TABLE OF CONTENTS

1 INTRODUCTION TO PROCESS CONTROL SYSTEM SECURITY 1

1.1 SYSTEM DATA 1
1.2 SECURITY ADMINISTRATION 1
1.3 ARCHITECTURE 2
1.4 NETWORKS 3
1.5 PLATFORMS 3

2 THE NEED FOR SECURITY IN PROCESS CONTROL SYSTEMS 4

2.1 CRITICAL INFRASTRUCTURE 4
2.2 MANUFACTURING AND INDUSTRY 5
2.3 CONSEQUENCES 5
2.4 HISTORICAL EXAMPLES OF PCS TAMPERING 6

3 OBSERVED VULNERABILITIES AND THEIR CAUSES 7

3.1 PCS DATA 7
3.2 SECURITY ADMINISTRATION 7
3.3 ARCHITECTURE 8
3.4 NETWORKS 9
3.5 PLATFORMS 11

4 CONCLUSION 13

5 ACRONYMS 14

6 REFERENCES 14

1 INTRODUCTION TO PROCESS CONTROL SYSTEM SECURITY

An automation system, often referred to as a process control system (PCS) or supervisory control and data acquisition (SCADA) system, is critical to the safe, reliable, and efficient operation of many physical processes. PCS is used extensively in infrastructure (including electric power, water, petroleum, and natural gas), as well as in various manufacturing operations. Electronic automation of control enables quicker and more coordinated system management compared to human operation, and in many cases there is no effective alternative to the use of PCS.

The Sandia interpretation of the terms PCS and SCADA includes the overall collection of control systems that measure and change the process. For example, in electric power this comprises traditional concepts like SCADA, automatic generation control, protection, and other autonomous systems. Essentially, any subsystem that electronically measures state, alters process control parameters, presents/stores/communicates data, or the management thereof is subsumed in this definition of PCS.

Many diverse elements compromise a functional PCS. The amalgamated PCS can be broken down into five heterogeneous categories to facilitate security analysis.

1.1 System data

Data is the fundamental element in any information architecture. Equipment is used to sample, communicate, present, output, and store data; system security is applied to preserve data attributes (availability, authenticity, integrity, and confidentiality) which ensures the reliable operation of the overall information system.

1.2 Security administration

The administration constituent of a PCS encompasses such non-automation functions as documentation and procedure. The cardinal element of PCS documentation is the system security policy, which prescribes the goals and responsibilities for PCS security. The security policy is the genesis for every other requisite administrative component, which subsequently prescribe procedures for system implementation, operation, and maintenance. Therefore, effective security policy is at the root of effective PCS security (Figure 1).

Components of system administration include security plans, equipment implementation guidance, configuration management, and security enforcement and auditing.

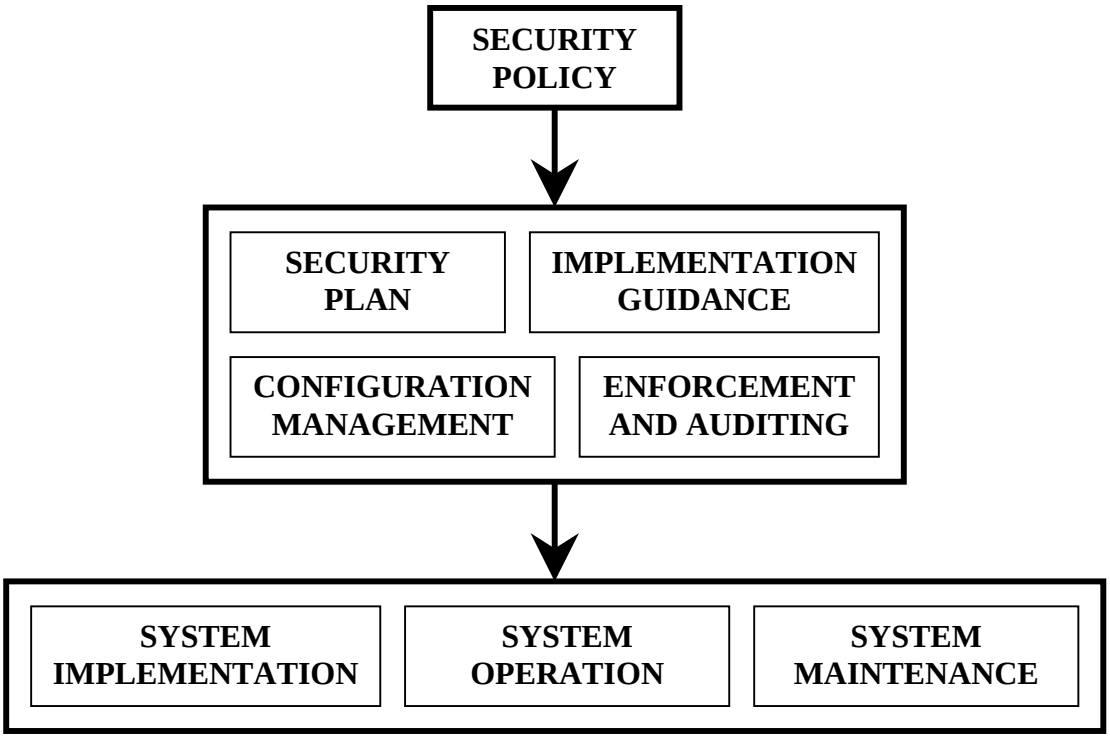

Figure 1. PCS administration.

A security plan documents the overall security architecture for a system or subsystem. Typical elements include policies and procedures for operational security, user and data authentication, backup policies, and system perimeter/security enclaves, among other things. Implementation guides are used to extract and apply relevant parts of the security policy and plan to individual and collected system equipment. Configuration management prescribes procedures and documentation to fully chronicle the state and configuration of each component in the system. Finally, enforcement and auditing encompass the functions of ensuring that the security policy, plan, implantation guidance, and configuration management are followed during implementation and maintenance, and to periodically check system security during operation.

1.3 Architecture

The architecture of the PCS refers to its control and data storage hierarchy. The architecture for the distribution of automation functionality is critical to reliability of the functional whole. At one extreme, totally centralized authority for automation means that remote stations function as little more than boundaries for analog and digital control and measurement signals; this is the decades-old traditional model. At the other extreme, completely decentralized authority resembles the agent model, where operations depend on the emergent behavior of smaller entities with limited capabilities and viewpoints.

Another important balance in the architecture concerns the amount of automated versus human control. Often, automated control is necessary for situations where human

intervention is temporally infeasible; however, in situations where human control is feasible yet automated control is desirable, equilibrium among security and efficiency must be obtained.

The current paradigm for data storage in automation systems includes local, transient storage for critical values required by the automation operation, and centralized storage of all relevant data records (usually sampled less often than most local storage). While local storage is driven by engineering requirements, the main data store is constrained by economic costs for implementation and management against requirements for usage of the data and data reliability.

1.4 Networks

PCS networks include all data transmission elements wholly owned and administered by the utility, in addition to data transport functionality of external networks traversed by PCS data. Networking devices can include lower-level end communications equipment (modems, etc.), advanced networking devices (routers, firewalls, etc.), and the link equipment itself (cables, rights-of-way, microwave dishes, etc.). Network functionality includes the capability of the network to deliver SCADA messages securely and reliably to support system operation.

1.5 Platforms

The term “platforms” refers to the computing hardware (inclusive of PCS-specific industrial platforms) and software (like applications and operating systems) in PCS. Platforms sample, store, process, and output PCS data.

2 THE NEED FOR SECURITY IN PROCESS CONTROL SYSTEMS

PCS is pervasive in manufacturing and infrastructure processes. Often, enormous potential safety impacts to the general populace are possible if PCS malfunctions; moderate to severe economic damage is also feasible. At a minimum, PCS unreliability will encourage public discontent and unease.

Security for PCS should be paramount given the potential consequences, and will only grow in importance as newer PCS (with more acute vulnerabilities) are installed. Unfortunately, budgetary restrictions for utilities are often manifest in PCS administration, where funding for personnel and equipment are many times clearly inadequate. Another problem is natural attrition through aging of key personnel in PCS administration and also in utility operations. Finally, corporate social pressures between PCS administrators and IT departments often lead to counterproductive suspicion and inefficient communication between fiefdoms.

Often, the arcane nature of PCS implementations is considered the primary defense mechanism through the "security through obscurity" argument. This chimerical theory unfortunately contributes to false confidence. Obscure systems are merely difficult to understand so that the malefactor must make a larger up-front investment to understand the system. Once the requisite knowledge is attained, attack paths are clear and consequences fated.

2.1 Critical infrastructure

Electric power is often credited with being the first infrastructure sector to deploy PCS extensively. Originally known as SCADA, the system was designed to allow irregular operation of remote devices, and often used tone control as a protocol. Water sourcing, treatment, and distribution utilities later added remote sensing and control, as did fossil fuel refining and distribution networks. Eventually, the original primitive technology was replaced with modern digital/analog hybrid networks based on contemporary communication protocols and microprocessors.

Currently, infrastructure utilities rely very heavily on their PCS systems in real-time, and they have been in use for so long that it is unclear how successful or efficient manual operations would actually be. Furthermore, there are considerations concerning the uncertain results of intrusion, as these scenarios have not been adequately enumerated.

Each utility should address their PCS as a hypercritical system by using very tight security safeguards. The PCS has enormous value by reducing costs and improving performance through automation, and this value must be reflected in the system's security.

2.2 Manufacturing and industry

PCS have also extensively penetrated the manufacturing industry. Some manufacturing processes are extraordinarily sensitive temporally, such that only computerized control is feasible (e.g. semiconductor manufacturing, extrusion processes, etc.). Others are of a gargantuan scale where the additional reliability of modern microprocessor control is desperately desired, because of the belief that PCS are more accurate and less prone to errors than human control. This assumption is invalid if the PCS is left insecure.

2.3 Consequences

Each organization must consider potential consequences from PCS intrusion. Adversaries identify and exploit vulnerabilities to execute attacks, and the effects of those attacks become one or more consequences. Well-defined policy and procedures lead to mitigation techniques designed to thwart attacks, managing the risk to eliminate or minimize the consequences.

The degradation of the physical plant, economic status, or national confidence could all justify mitigation. The fiscal justification for mitigation has to be derived by the cost-benefit compared to the effects of the consequence.

2.3.1 Physical impacts

Physical impacts encompass the set of direct consequences of PCS misoperation. The potential effects of paramount importance include personal injury or loss of life. Other effects include the loss of property (including data) or damage to the environment.

2.3.2 Economic impacts

Economic impacts are a second-order effect from physical impacts ensuing from cyber intrusion. Physical impacts could result in repercussions to system operations, which in turn inflict a greater economic loss on the facility or company. On a larger scale, these effects could negatively impact the local, regional, national, or possibly global economy.

2.3.3 Social impacts

Another second-order effect, the consequence from the loss of national or public confidence in an organization is many times overlooked. It is, however, a very real target and one that can be accomplished through cyber attack. Social impacts may possibly lead to heavily depressed public confidence or the rise of popular extremism.

2.4 Historical examples of PCS tampering

Few historical accounts of PCS attack exist. Some are apparently untrue, as was the case with the Salt River Project attack in Arizona [1, 2], or exaggerated like the Cal-ISO incident (detailed below). The question of feasibility for PCS hacking is contested [3], as is the potential extent of consequences [4].

2.4.1 Australian sewage release

One attack that verifiably did occur happened in April 2000 at Maroochy Shire, Queensland [5, 6]. Copious quantities of sewage were released into parks, rivers, and a hotel, severely fouling the environment. A former contractor for the PCS at the local water treatment facility was eventually convicted of the deeds and incarcerated.

The attacker had several advantages, in that he was familiar with the PCS and had the necessary software to interact with the system. However, several PCS vulnerabilities contributed to the consequence. First, the system used inadequately protected wireless communication, thereby granting the attacker a network beachhead for his misbehavior. Furthermore, a system with effective security administration should have quickly disabled the credentials of the contractor upon completion of the PCS installation, which would have prevented or complicated the attack.

The fact that the attack involved an insider should not be of any comfort to administrators. Insider knowledge may be reasonably assumed to be available for a determined adversary.

2.4.2 California system operator hack

Attackers, possibly from China, were able to gain access into one of the computer networks at the California Independent System Operator (Cal-ISO) [7, 8] in May 2001. The Cal-ISO has hierarchical control over a number of PCS networks operated by its constituent transmission owners. This hack was apparently unsuccessful at penetrating any PCS network, yet it uncomfortably extended a period of longer than two weeks.

3 OBSERVED VULNERABILITIES AND THEIR CAUSES

In this section are listed the vulnerabilities typically observed in Sandia's assessment experience. The order of these vulnerabilities does not necessarily reflect any priority in terms of likelihood of occurrence or severity of impact. The vulnerabilities are grouped in the categories of (1) Data, (2) Security Administration, (3) Architecture, (4) Network, and (5) Platforms to assist in determining optimal mitigation strategies. Any given PCS will usually exhibit a subset of these vulnerabilities, but may also have some unique additional problems.

3.1 PCS Data

Sensitivity levels for PCS data are usually not established; in fact, they have never been observed during an assessment. An essential characteristic of secure information systems is the identification and classification of data into categories of similar sensitivity. Absence of these fundamental distinctions makes it impractical and fruitless to identify where security precautions are appropriate (for example, which communication links to secure, databases requiring protection, etc). The lack of data classifications is a direct byproduct of the deficient administration in PCS security.

3.2 Security Administration

Few PCS are governed by security policies; fewer still include integrated, effective PCS-specific security administration. Systems without security policy and administration do not possess measurable, self-perpetuating security, and experience has shown that each ungoverned information network will eventually sprout vulnerabilities.

Policy is the genesis of secure system implementation, operation, and maintenance. Absent effective policy, security atrophies and is ruined in the fluid attack and vulnerability environment. Unfortunately, the attitudes of most PCS administrators are products of the security-free legacy environment, and the distaste for security administration self-perpetuates in each generation of PCS administrators. Consequently, the security condition of PCS is deplorable, and not improving.

Procedures that contribute to security must be predicated upon elements of the policy to be coherent and effective. Some important components of security procedures include security plans, implementation guides, and security enforcement including auditing controls.

Furthermore, security training is essential to an effectual staff but is neglected for cost or other reasons; the security posture of the PCS is adulterated by the omission. Finally, while configuration management is practiced somewhat regularly (but not universally) in critical infrastructure, its effectiveness is enfeebled by the use of informal procedures or irregular exercise.

In most cases, security administration is inadequate in PCS systems. Table 1 summarizes the typical situation.

Table 1. Common vulnerabilities for PCS administration.

Category	Vulnerability
Policy	The PCS has no specific documented security policy. This key vulnerability generates the proliferation of procedural and technical vulnerabilities.
Procedures	The PCS often has no specific or documented security plan.
	Implementation guides for equipment and systems are usually absent or deficient.
	There are no administrative mechanisms for security enforcement in the system lifecycle.
	Security audits are rarely performed, if at all.
Training	There is neither formal security training nor official documented security procedures.
Configuration Management	Usually, there is no formal configuration management and no officially documented procedures. Hence, there are neither formal requirements, nor a consistent approach for configuration management.

3.3 Architecture

Architecturally, many PCS include centralized data storage and control. Often, these are single points-of-failure, which in not necessarily a vulnerability confined to legacy or modern architectures, or even PCS for that matter.

Occasionally, physical damage to infrastructure assets may be possible through permissible operation of PCS control equipment. An effective control hierarchy would preclude this possibility.

Finally, many companies are leveraging their PCS communication links and networks for the conveyance of signals associated with emergency services at their facilities. Worse still, security, fire, and other systems are occasionally being integrated into the PCS as points of measurement and control. As examples, a door alarm may be wired as a PCS sensor, or the release of fire extinguishing material might be controlled through the PCS. As noted, the state of PCS security is generally abominable; cavalierly integrating these systems with PCS geometrically compounds the potential for intrusion and disruption.

3.4 Networks

Vulnerabilities in PCS networks depend on the type of system. Legacy PCS implementations rely on proprietary protocols and relatively primitive, low-bandwidth data channels. While there are fewer opportunities for disruptive behavior compared to newer networks, which closely resemble modern TCP/IP systems, great problems are inherent because of the technology's age.

Security in legacy PCS is lamentable. Designed, built, and implemented in a time ere network intrusion and trespass, only rudimentary integrity checking is available for data, and that usually only during data communication. Accounting and logging are largely nonexistent, rendering configuration management arduous and forensics preposterous.

Configuration passwords are often simple and may be limited in effectiveness by the device itself. Wireless links are ill-protected as they roam the rural countryside. Networking equipment in these systems, particularly when physical access is presumed, is acutely vulnerable to attack.

Systems with contemporary technologies like Ethernet, routers, and firewalls have vulnerabilities that are more publicized than the vulnerabilities in the older networks. Therefore, ill-managed systems carry tremendous risk in light of the massive accumulation of attacks and adversaries worldwide.

Besides the administrative deficiencies manifest in the insecure configuration and management of the PCS network, two additional factors contribute great vulnerability. The first is the blind trust in the capability of PCS links to faithfully transmit data. The geographically sparse PCS network generally forces links of considerable span. These needs are filled by either cabled or wireless connections, which may be exclusively used by the PCS or shared. Shared links are more economically sensible, but many times the PCS systems at either end of the link are not adequately shielded from other entities using it. Furthermore, unsecured information on wireless and shared links is susceptible to eavesdropping or manipulation, and even long or unprotected unshared cable links may be vulnerable to a significant degree.

The second factor is the connections between the PCS and external networks. An external network is any network that is not part of the PCS. Examples include interfaces to an administrative (non-automation) network or connections to other PCS systems for information transfer or mutual control. Often, interfaces to external systems assume that the outside network can be trusted, which leaves PCS security dependent on one or more organizations.

Table 2. Common vulnerabilities for PCS networks.

Category	Vulnerability
Administration	Minimal data flow control is employed (e.g. minimal use of access control lists, virtual private networks, or virtual LANs).
	Configurations are not stored or backed up for network devices.
	Passwords are not encrypted in transit.
	Passwords exist indefinitely on network devices.
	Passwords on devices are shared.
	Minimal administrative access controls are applied.
Hardware	There is inadequate physical protection of network equipment.
	Non-critical personnel have physical access to equipment.
Perimeter	No security perimeter has been defined for the system that defines access points which must be secured.
	Firewalls are nonexistent or poorly configured at interfaces to external (non-PCS) networks.
	PCS networks are used for non-PCS traffic.
Monitoring & Logging	Firewall and router logs are neither collected nor examined.
	There is no security monitoring on the PCS network.
Link Security	Critical monitoring and control paths are unidentified, complicating redundancy or contingency plans.
	PCS connections over vulnerable links are not protected with encryption.
Remote Access	Authentication for remote access is substandard or nonexistent.
	Remote access into the PCS network utilizes shared passwords and shared accounts.
Wireless Connections	Wireless LAN technology used in the PCS network without strong authentication and/or data protection between clients and access points.

3.5 Platforms

For convenience of analysis in assessments, computer platforms in PCS networks are partitioned into two groups: proprietary and non-proprietary. The PCS-specific and proprietary platforms, like remote telemetry units (RTUs), intelligent electronic devices (IEDs), and programmable logic controllers (PLCs), interface with the process control and measurement hardware (which can include solenoids, motors, transformers, etc.). These devices are often specialized hardware, with functionality restricted to the operational requirements of the target market.

Password control for these devices can often be defeated locally (for example, by various means through the console port) adding further onus to the physical protection, since password access to RTUs usually provide carte blanche to the device. Once access has been granted by the device, a perpetrator has the capability to immediately effect misoperation of the system, or more insidiously to alter the parameters of a device that monitors the system for unsafe conditions, thereby potentially allowing those conditions to exist. Older PCS will include platforms with systemic security deficiencies based on their age, similarly to networking equipment in legacy PCS.

A further issue is the pervasive remote access and configuration available to RTUs. In some companies, nearly every remote unit is attached to a network or a modem for management. Unfortunately, authentication is universally weak for RTUs (usually a single password), and is further weakened by passing identification tokens over networks.

PCS applications, databases, and interfaces are shifting from proprietary platforms to modern IT-style computers running Windows or UNIX-style operating systems. Vendors prefer these environments for development, but the deployment of PCS software on these devices mandates that particular attention is applied to securing the platform. Newer platforms are complex and include many capabilities, which could lead to plentiful vulnerabilities if misconfigured, but alternatively may be leveraged for enhanced security when implemented carefully. However, these platforms are usually set up with default configurations and rarely updated; as a result, much vulnerability exists at critical points in a PCS system.

Common vulnerabilities applying to either or both types of platforms in PCS networks are itemized in Table 3.

Table 3. Common vulnerabilities for PCS platforms.

Category	Vulnerability
Administration	OS security patches are not maintained.
	Configurations are not stored or backed up for important platforms, including IEDs.
	Default OS configurations are utilized, which enables insecure and unnecessary services.
	Passwords are often stored in plain sight near critical systems.
	Power-on and screen saver passwords are not utilized.
	Passwords are not encrypted in transit.
	Passwords exist indefinitely on platforms.
	Passwords on devices are shared.
	There are no time limit, character length, or character type requirements for the passwords.
	Minimal administrative access controls are applied.
	Users have administrator privileges.
Hardware	There is inadequate physical protection of critical platforms.
	Non-critical personnel have physical access to equipment.
	Dial-up access exists on individual workstations within the SCADA network.
Monitoring & Logging	System logs are neither collected nor examined.
Malware Protection	Virus checking software is uninstalled, unused, or not updated.

4 CONCLUSION

The vulnerability assessment experience of Sandia National Laboratories facilitates the aggregation and publication of common vulnerabilities in PCS for critical infrastructure. These vulnerabilities relate to data, administration, architecture, networks, and platforms. Problems with PCS security policy lead to poor administrative procedures and vulnerabilities in the system implementation. Differing PCS architectures and equipment include distinct security weaknesses. Each vulnerability is a significant problem considering the potential consequences of PCS misoperation.

5 ACRONYMS

AGC ..... Automatic generation control
ECC..... Energy control center
EMS ..... Energy management system
FACTS ..... Flexible AC transmission system
IED..... Intelligent electronic device
IT..... Information technology
LAN ..... Local area network
PCS ..... Process control system
PLC ..... Programmable logic controller
RTU..... Remote terminal unit
SCADA ..... Supervisory control and data acquisition
TCP/IP..... Transmission control protocol / Internet protocol

6 REFERENCES

[1] "Cyber-Attacks by Al Qaeda Feared," Barton Gellman, *Washington Post*, 27 June 2002: Page A01

[2] "eTerrorism: Assessing the infrastructure risk," Robert Lemos, *ZDNet Australia*, 27 August 2002: http://www.zdnet.com.au/newstech/security/story/0,2000048600,20267698,00.htm

[3] "Frontline: Cyber War!" *Public Broadcasting System*, 24 April 2003: http://www.pbs.org/wgbh/pages/frontline/shows/cyberwar/view/

[4] "US 'fears al-Qaeda hack attack,'" Kevin Anderson, *BBC News Online*, 27 June 2002: http://news.bbc.co.uk/1/hi/sci/tech/2070706.stm

[5] "Cyber terrorism a mouse-click away," Garry Barker, *The Age* (Melbourne), 8 July 2002, http://www.theage.com.au/articles/2002/07/07/1025667089019.html

[6] "Hacker jailed for revenge sewage attacks," Tony Smith, *The Register* (UK), 31 October 2001: http://www.theregister.co.uk/content/4/22579.html

[7] "California hack points to possible IT surveillance threat," Dan Verton, *Computerworld*, 12 June 2001: http://www.computerworld.com/industrytopics/energy/story/0,10801,61313,00.html

[8] "Cyberterrorists don't care about your PC," *ZDNet*, 11 July 2002: http://www. nc-india.com/news/stories/61744.html