6

New Security Paradigms: Orthodoxy and Heresy

Hilary H. Hosmer, President
Data Security, Inc.
58 Wilson Road, Bedford. MA 01730 U.S.A.
Phone and FAX: (617) 275-8231
Email: Hosmer@dockmaster.ncsc.mil

1 INTRODUCTION

Our computer technology has outpaced our security paradigms. The more we interconnect via common graphical interfaces, the more vulnerable we are to hackers, viruses and Trojan horses. Because incremental improvements in security technology will never permit us to catch up, this paper explores radical new ways to meet the security needs of today and tomorrow.

2 OVERVIEW

I first define what a security paradigm is and review why the information security community needs new ones. I describe selected paradigms, some from the New Security Paradigms Workshop and some from other sources. Finally, I describe how we can go further.

I hope to challenge orthodox ideas about information security and stimulate you to come up with something better. I apologize for not being able to include many other worthwhile ideas in this talk, and for focusing on the work that I know the best. Hopefully, our fifty-minutes together today will be profound, challenging, and fun.

3 DEFINITIONS

A *paradigm* is a model or template used as a standard. For example, a carpenter, blacksmith, or quilt-maker would use a paradigm to make a standard set of dowels, horseshoes, or quilt squares. Today's builders of secure systems use the Orange Book (NCSC, 1975) or the *Common Criteria* (CC, 1996) as a guide.

Harvard Professor Thomas Kuhn in his 1940's work on scientific revolutions (Kuhn, 1970) redefined a *paradigm* as a fundamental model of reality, such as the geocentric view of the universe or the feudal social order. Kuhn defined a *paradigm shift* as a movement from one fundamental model of reality to another. Normally, science progresses in incremental steps, but paradigm shifts sometimes permit great leaps forward.

Kuhn observed a repeated pattern in the history of science. Discrepancies between an existing paradigm and its ability to explain observable reality accumulate over many years. Eventually, someone of insight, a Kepler or Einstein, analyzes the problem afresh and synthesizes a radical new solution which is very controversial and denounced as heresy if it

S. K. Katsikas et al. (eds.), *Information Systems Security*

threatens the status quo. If worthwhile, the new idea attracts adherents and defenders. As the defenders of the old paradigm die off, the new paradigm becomes the new orthodoxy. The pattern then repeats itself.

Paradigm shifts are not limited to scientific revolutions. Social revolutions, like feminism, communism, human rights, and civil rights, get much of their momentum from a society-wide shift in perspective or "consciousness-raising." Every religion represents a paradigm shift from what went before.

Paradigms can be communicated both mathematically (e.g., Einstein's E = mc2) and metaphorically (e.g., Newton's universe as a giant clock or Jesus' parables of tolerance). Metaphors speed the absorption of new paradigms.

4 THE INFORMATION SECURITY PROBLEM

The Internet is an information highway for hackers and information warriors as well as law-abiding citizens. A small proportion of actual security breaches make daily headlines. Yet sales of trusted systems are quite low, due perhaps to inconvenience, loss of functionality, and obsolescence.

The TCSEC or Orange Book, our eleven-year old security paradigm for representing and reasoning about computer security, has been overtaken by the rapid development and the widespread success of information technology (Hosmer, 1992a). It doesn't handle large communications networks, address integrity, or protect privacy.

The security community has addressed these shortcomings piecemeal. Each book in the "Rainbow Series", for example, represents an attempt to enlarge the Orange Book to meet specific needs. The Canadian (CSE, 1993) and the European (CEC, 1991) Criteria, built on the Orange Book, incorporate many improvements that are now being harmonized into a *Common Criteria* (Cugini, 1995). However, extending our evaluation standards isn't enough to:

- Keep up with rapid technical change;
- Adapt to changes in underlying needs;
- Resolve inherent contradictions;
- Break out of the existing paradigm.
- Develop order-of-magnitude improvements.

It is clear that we need new security paradigms, but how do we get them?

5 HOW TO GET NEW PARADIGMS

Ask the Right Questions

A key element in generating new paradigms is to examine fundamental, often unspoken assumptions. What is trust? What is a computer? What are the dimensions of security? Why must we have just one system security policy? Where do we collide with reality? Do we provide what people really need?

Grant Permission

Sometimes simply being given permission for "out of the box" thinking is sufficient to inspire researchers to generate new paradigms.

> You are hereby granted permission to solve INFOSEC
> problems in deeper, more creative way

Figure 1: Permission to Go Outside Boundaries

Respect Nonconformity

Intellectual curiosity drives new paradigm research, which requires both intuitive and logical thinking. Typically, a researcher surveying the field will be dismayed at the state-of-the-art and decide to do something better. Innovators often pursue their own topics, oblivious to what is currently in fashion.

Organize Like-Minded People

New paradigms, like new products, require champions. I started the New Security Paradigms Workshop (NSPW) in 1992 to try another approach to solving some of the longstanding inherent INFOSEC problems. I wanted a creative, multidisciplinary, freewheeling, and nurturing community which would encourage researchers to look at computer security in fundamentally different ways.

ACM SIGSAC offered to sponsor the workshop, and 13 remarkable people came. We presented papers to each other, then worked as teams to figure out what the new paradigms being proposed had in common. Common themes included cooperation rather than control, and decentralization to manage complexity.

The National Computer Security Conference invited us to present the best papers at two half-day sessions at the 1992 Baltimore Conference. The sessions sparked a lot of controversy, and "new security paradigms" quickly became a buzzword.

The NSPW has met annually ever since with about twenty participants, about twelve presenters, and two or three group exercises. Admission is by submitting a paper or working on one of the committees. Please come! Proceedings from the previous NSPW workshops are available from IEEE Computer Society Press.

Provide Financial Support

Sponsors have the funds to organize cross-disciplinary problem-solving workshops and Institutes, like the COMPASS and "guru" workshops, or the Santa Fe Institute (Waldrop, 1992). They also can support those capable of radical new ideas for extended periods of time. Sir Isaac Newton and Charles Babbage, the father of computing, were given (in different decades) the same university chair.

Sponsors can charter high-powered committees to develop new paradigms, as with the Joint Security Commission which produced *Redefining Security* (JSC, 1994), the DISA group that created the *DGSA* (DoD, 1993), and the multinational team which produced the *Common Criteria* (LaFountain, 1995).

Sponsors can stay on the look-out for promising ideas and people and provide support. For example, after the first year, the U.S. Department of Defense provided scholarship funds for the New Security Paradigms Workshop.

Distribute the New Ideas

Publish papers, present the ideas in as many different fora as possible, and talk to influential people.

6 EXAMPLE NEW SECURITY PARADIGMS

I describe here just a few of the more interesting unofficial security paradigms developed recently.

Trust Redefined

Dorothy Denning argued that "trust" is not a property of a system, i.e. something that can be designed in, modelled, etc. Trust is an assessment (Denning, 1993). She maintains that the market is a good measure of trust, and that clients buy products which have proved to be "trustworthy".

Computers Redesigned

Cryptographer Yvo Desmedt (Desmedt, 1993) starts from scratch to build a more secure computer. Because multiple users greatly complicate the access problem, he eliminates multi-user computers altogether, arguing that the low cost and rapidly increasing functionality of today's processors makes it unnecessary to share them.

Molecular biologists such as RSA's Leonard Adelman are using DNA genetic material to solve decryption, image-processing, NP, and other problems where massive parallel processing is appropriate (Robinson, 1996).

Crossing Disciplines

Most criteria for evaluating secure systems are based upon how the system is developed, rather than any objective measure of security, points out Catherine Meadows of the Naval Research Laboratory (Meadows, 1995). She shows that the current security paradigm is generally restricted to a subset of approaches used in dependability (Laprie, 1992), largely focusing on fault prevention and removal, while neglecting fault tolerance and forecast. She argues that the current security paradigm is fast becoming obsolete, and she presents a new fault-based model for INFOSEC. Bret Michaels of Berkeley CA did similar cross-disciplinary work with safety and security policies for his Ph.D.

Fuzzy Logic for Security

Lofti Zadeh's fuzzy logic (Zadeh, 1987) is like going from black and white to color. Instead of bivalent alternatives like [**Yes**/No] or [**On**/Off] or [**True**/False], a full spectrum of possibilities is available, e.g.,

True, **mostly true**, **somewhat true**, **almost true**, almost false , somewhat false, mostly false, False

Figure 2: Mulivalent Responses

Fuzzy logic is a superset of all current logic, so it enlarges all forms of logic. Fuzzy logic, because it handles vagueness and continuous data, has many potential application in security. It's a promising way to represent non-traditional policies, like privacy, integrity and availability (Hosmer, 1995). It can be used for risk analysis (Schmucker, 1984), password authentication biometrics (deRu, 1995), user interfaces, and formal methods.

The Local Control Paradigm

Autonomy or local control isn't new. For example, adults have control over most of their own lives, as long as they live within natural and legal constraints.

"Artificial life" researcher Craig Reynolds (McLean, 1993) simulated the behavior of a flock of "boids" with three simple rules[1] governing local boid-to-boid interaction. His boids flocked like real birds, avoiding obstacles, and regrouping. Local control permitted his artifacts to adapt organically to changing conditions.

> "A single set of top-level rules would be impossibly cumbersome and complicated, "requiring rules for the boids in every possible situation.... Since it is effectively impossible to cover *every* conceivable situation, top-down systems are forever running into combinations of events they don't know how to handle. They tend to be touchy and fragile..." (McLean,1993)

Figure 3: The Case for Local Control

The runaway success of the Internet illustrates the success of a functional and "organic" framework. Centralized network security policies, like those advocated in the Red Book (Trusted Network Interpretation), can't work in such rapidly-growing and changing environments. We need local control to secure our networks, and systems built from the bottom up, despite the eloquent arguments of formal modelers (Eckert, 1995).

[1] Local Boid Rules: 1. Maintain a minimum distance from other objects;
2. Try to match velocities with neighboring boids;
3. Move toward the perceived center of mass.

Ruth Nelson of Information Systems Security advocates local control for networks in her work on "Mutual Suspicion" (Nelson, 1990) and "Security for Infinite Networks." (Nelson, 1995) In her paradigm, each computer system is ultimately responsible for enforcing its own security. It must be suspicious in its interactions with other systems, even where protected by firewalls. This is the only way that it is possible to get secure and scalable networks.

Aspects of this paradigm are being implemented in products, such as Windows NT, that provide security for networked personal computers, and in standards, such as the *DGSA* in which each Local Subscriber Environment (LSE) is responsible for enforcing its own security policies, including basic rules for controlling the import and export of data between information domains (Hilborn, 1995).

The MultiPolicy Paradigm

Although a single system security policy is traditional, multiple policies may be necessary if there are:

1. Multiple security goals, such as privacy, confidentiality and integrity;
2. Diverse constituents with individual goals and plans, such as the United Nations (U.N.), European Community (EC), and other federations;
3. Separately evaluated pieces, e.g. a Trusted DBMS and Trusted OS;
4. Changing circumstances, like moving from peace to war.

In a series of papers (Hosmer, 1990; 1991a; 1992b; 1991b; 1991c; 1993a; 1992c; 1993b) Data Security Inc. proposed a new security paradigm that permits multiple, perhaps contradictory security policies in a system or a network. The MultiPolicy Paradigm permits multiple distinct security policy domains, administered by different organizational entities each with complete policy autonomy in its domain, to be modelled in a computer system or a network. Metapolicies control the interactions of the multiple policies. Multiple labels indicate which policies apply to each object. We implemented this paradigm in 1993-1995 as the MultiPolicy Machine (MPM) and are licensing the technology under the trademark *ANTILOPER*.

Although several researchers and two standards organizations, the ISO and the *DGSA,* have adopted several of the MultiPolicy Paradigm's concepts (e.g. policy domains which cross computers) and terms (e.g. metapolicy and multipolicy), the DGSA differs in several significant respects. Because the DGSA is the USA's target security architecture for the Department of Defense for the next 30 years, these differences merit discussion. I use Gene Hilborn's formal model (Hilborn, 1995) of the DGSA information domain concept, presented in 1995, to illustrate.

The DGSA's information domain concept (a set of members, one security policy, and a set of objects) seems identical at first glance to the MPM policy domain concept (everything that comes under one policy administrator), but there are subtle differences with major impact.

1. In the DGSA model, every information domain is always separate, while in the MPM model, the degree of domain separation may be explicitly specified.
2. In the DGSA, objects in each information domain must share the same "security attributes." Unless "same security attributes" means "same classification levels and categories," relatively unimportant security attributes (e.g., the earliest date something can be released to

the public) could fragment DGSA implementations into an unsupportable number of information domains;

3. An object in the DGSA comes under only one security policy. An object in the MPM may come under any number of security policies, indicated by the contents of its security label and mediated by the relevant metapolicies.
4. The DGSA's comprehensive metapolicy will interfere with possibly desirable local domain security policies. For example, the DGSA metapolicy "Only members of an information domain can have access to objects in that domain" might preclude unknown individuals (non-members) from accessing World-Wide Web home pages.
5. The MPM permits the use of fuzzy as well as traditional logic. For example, fuzzy degrees of domain membership may be used.
6. DGSA policy decision results in Hilborn's paper appear to be always ANDed, while MPM conflict-resolution permits policy results to be combined in ways that are appropriate to the application.

   In health care, for example, a safety policy should have precedence over confidentiality, rather than being vetoed by it. The MPM policy manager's decision table below illustrates how easy it is to specify how policy conflicts can be resolved.

Vote from Safety Policy1	Vote From Confidentiality Policy2	Resulting Vote from MPM Conflict Resolution Metapolicy
Yes	Yes	Yes
Yes	No	Yes
No	Yes	No
No	No	No

Figure 4: Resolving Policy Conflicts

7. The MPM uses metapolicies in several ways, while Hilborn's DGSA model uses the term only in the sentence of "higher overall policy."
8. The MPM includes a Policy Manager to enter, modify, and delete security policies;
9. While the DGSA model focuses on {subject, object} access control pairs, the MPM permits and encourages Clark and Wilson {user, program, object} access control triples, important because unapproved programs operating on behalf of a user are a major security risk.

Overall, the DGSA's information domain multipolicy system is less flexible than the MultiPolicy Machine (MPM). This rigidity conflicts with the flexibility of the proposed Common Criteria evaluation standard described in the next section.

7 OFFICIALLY-SPONSORED PARADIGMS

Several new government initiatives are responding to the changing security environment and the problems with the current paradigms raised. Among these are the *DGSA (*which we have already discussed), the *Common Criteria*, Information Warfare, and Security as Risk

Management. Because these initiatives are both radical and careful to protect everyone's investment in existing systems, they sometimes seem like "paradigm straddles."

Common Criteria

The *Common Criteria* (CC, 1996) harmonize the criteria of several nations into a single international standard. A central feature of the new multinational *Common Criteria* is the ability to specify (or select) a Protection Profile that summarizes threats and requirements, providing more flexibility. It allows separate functional and assurance requirements, which are called components because they can be combined in many ways. Assurance can be measured in seven hierarchical levels from low assurance to high assurance. Functions are packaged with threats and dependencies to aid the user in selecting a desirable set of security features.

I believe the Common Criteria framework will permit substantial technical evolution.

Information Warfare

The Persian Gulf War has been described as the first "Information War." (Campen, 1992) President Hussein's communications and command and control systems were targeted early, causing troops to be cut off from their leaders. U.S. satellite-based communications were out of reach of Iraq's missiles, so one side could see and hear everything on the battlefield, while the other was dumb and blind. Access and denial to information were critical, and the war was over quickly.

> An information security expert was given the assignment of selecting targets that would bring down Saddam Hussein's communications system. For the first time in his life he was confronted with the ethical dilemmas inherent in making life and death decisions. He had crossed from defense to offense, and it wasn't comfortable. He retired shortly thereafter. [2]

Figure 5: Going on the Offensive

Security has traditionally been a defensive exercise. Information Warfare turns this around so that computer security expertise can be used as an *offensive* weapon to break into competitor's data banks and/or bring down enemy information systems(Schwartau, 1994). A terrorist, for example, could bring down a computerized stock exchange via an electromagnetic pulse.

Information warfare strategies apply to civilian enterprise as well as the military. Although espionage has been around for millennia, computer networks provide an "information highway" to data of interest. If a teenager with no money and just a few years experience can hack his

[2] Personal conversation.

way undetected into major systems, imagine what a well-funded professional operating under government sponsorship without fear of legal reprisal can do (Power, 1995).

Information warfare strategies, tactics, and techniques are highly classified. However, much of the defense against such techniques is what the security community has been doing all along.

Security as Risk Management

Risk management, based upon cost/benefit analysis, provides a rational way to spend limited funds available for security. It's a very useful paradigm.

Redefining Security, by the DOD/CIA Joint Security Commission (JSC, 1994), argues that military and intelligence "security policies, practices, and procedures developed during the Cold War must be changed." It proposes to "reduce current levels of security in accordance with risk management principles" and to simplify the cumbersome DOD classification/clearance system [with its four levels and 4000-5000 different compartments].

Commercial businesses are also taking a risk management approach. Aetna Insurance, for example, recognizes that it would be bankrupt if the information systems (IS) didn't function properly, and has combined IS with corporate risk management (Tate, 1989).

Although risk management has been widely adopted, researchers maintain that risk management paradigms must improve (Fletcher, 1994).

Don Howe (Howe, 1992) and Booysen and Eloff (Booysen , 1995) advocate expanding Boehm's (Boehm, 1988) spiral system development model with its built-in risk analysis activities to accommodate secure system engineering and the development of secure application systems.

Sharon Fletcher and her co-authors (Fletcher, 1994) describe two generations of risk management paradigms and propose a third:

- First generation:
  - Mainframe-based;
  - Protected classified information.
  - Assumed a predefined set of risks to apply to all systems;
  - Oriented toward compliance.
- Second generation (where we are now):
  - Passive and active threats;
  - Threats impact assets through vulnerabilities;
  - System-specific risk assessment;
  - Range of mitigation strategies.
- Third generation (where we are going):
  - Managing risk throughout the life of the software system;
  - System risk models that accommodate interactions and dependencies among risk-related elements (system dynamics);
  - New tools, e.g.
    - Risk identification matrix;
    - Risk mitigators matrix;
  - Total risk management.

Risk management will make a major difference in how one looks at the security of information systems. Rather than all or nothing, one gets the best security one can for the cost and the need. However, risk management can't solve the biggest research problem identified earlier, developing order-of-magnitude improvements to keep up with new technology.

8 WHERE TO NOW?

Clearly, we are still in the process of developing new paradigms. What do we do now?

Solving real problems rather than formal ones provides insight and inspires innovation. Emphasize paradigms that solve pragmatic problems, such as better expression of software surety requirements, and application-focused security. Require our security scientists to monitor advances in other computer technology, since there is a new generation about every seven years. Emphasize real system design, function, and use.

Provide support for innovation. Recognize that it may come from unexpected sources.

Put diverse people with different perspectives together to solve problems. Encourage people from other disciplines to join the search for information security solutions. Thomas Kuhn found that most developers of new paradigms had extensive experience in other disciplines and made their significant contributions after being in a new discipline for only about four years! Newcomers often don't see things in a conventional manner, while experienced scientists have the know-how to challenge conventional wisdom.

Exploit the broad vision of the "Graybeards" and "Founding Mothers", who see the underlying patterns and needs clearly, and use them as mentors to young innovators to solve "impossible" problems.

Pay special attention to loners who have been working quietly on their own, and to long-time heretics who have been complaining while orthodoxy prevailed. Each has a piece of the truth.

Look for common themes and vision. Most importantly, ask fundamental questions!

9 CONCLUSIONS

Only a few years ago, the computer security paradigm could be summarized as the contents of the Rainbow Series: the Orange Book, the Red Book, the Yellow Book, etc. These managed to identify and prioritize security features, and establish fairly clear guidelines for secure systems. Now we need more. Just to keep up, we need new ways of thinking and order-of-magnitude changes.

In this paper I have reviewed a few of the evolving paradigms, both official and unofficial, emerging in INFOSEC research. I hope you will consider contributing some of your own ideas, arising from deep experience, to the search for new paradigms. I hope you will address others' fledgling attempts constructively and supportively. If you are in a position to encourage others, I hope you will suggest that new security paradigms be a workshop or seminar topic.

10 ACKNOWLEDGEMENTS

Thank you to the Conference Chair, Dr. Dimitris Gritzalis, and to the Programme Committee chaired by Prof. Katsikas for inviting me to speak here on the beautiful island of Samos. Thank you to Ruth Nelson who commented on each draft, and to Alan MacRobert for sharing his professional editing expertise. I would especially like to acknowledge program committee member Dr. Willis Ware, the father of computer security, who has been calling for new security paradigms for several years.

11 REFERENCES

National Computer Security Center (NCSC), *Trusted Computer System Evaluation Criteria,* DOD-STD-025, 1975.

Common Criteria Editorial Board representing USA, Canada, France, UK, and Germany (CC), *Common Criteria for Information Technology Security Evaluation (CC),* to be published in quarter 1 1996.

Kuhn, Thomas, *The Structure of Scientific Revolutions*, 2nd Edition, University of Chicago Press, Chicago, 1970.

Hosmer, Hilary, "The Multipolicy Paradigm", *Proceedings of the 15th National Computer Security Conference*, Baltimore, MD, 1992.

Communications Security Establishment (CSE), *The Canadian Trusted Computer Product Evaluation Criteria,* Version 3.0e, Jan 1993.

Commission of the European Community (CEC), *Information Technology Security Evaluation Criteria,* Version 1.2, June 1991.

Cugini, Janet, "The Common Criteria: On the Road to International Harmonization, *Computer Standards and Interfaces, 17, 1995.*

Waldrop, Mitchell, *Complexity, The Emerging Science at the Edge of Order and Chaos,* Simon and Schuster, 1992.

Joint Security Commission (JSC), *Redefining Security,* Washington, D.C., February 1994.

Department of Defense (DoD), Defense Information System Security Program, *Department of Defense (DOD) Goal Security Architecture (DGSA),* Version 1.0, August, 1993.

LaFountain, Steve, and Lynne Ambuel, "Protection Profiles and the Common Criteria", Tutorial, Annual Computer Security Applications Conference, December 12, 1995.

Denning, Dorothy, "A New Paradigm For Trusted Systems", *Proceedings of the ACM SIGSAC New Security Paradigms Workshop,* Little Compton, R.I. Sept. 22-24, 1992, IEEE Press, 1993.

Desmedt, Yvo, "Computer Security By Redefining What A Computer Is," *Proceedings of the ACM SIGSAC New Security Paradigms Workshop*, Little Compton, R.I. Aug. 2-5, 1993, IEEE Press 1993.

Robinson, Clarence, "Molecular Biology Computation Captures International Research", *Signal, AFCEA's International Journal,* February 1996.

Meadows, Catherine, "Applying the Dependability Paradigm to Computer Security", *Proceedings of the ACM SIGSAC New Security Paradigms Workshop*, La Jolla, CA, August 22-25, 1995, IEEE Press 1995.

Laprie, J-C. "Dependability: A Unifying Concept for Reliable, Safe, Secure Computing," LAAS-CNRS, Toulouse, Esprit Basic Research Project 6362, PDCS Technical Report Series, April 1992.

Zadeh, Lofti, *Fuzzy Sets and Applications: Selected Papers by L.A. Zadeh,* ed. by Yager, Ovchinnikov, Tong, and Nguyen, published by John Wiley and Sons, 1987.

Hosmer, Hilary H. "Security is Fuzzy! Applying Fuzzy Logic to the Multipolicy Paradigm", *Proceedings of the ACM SIGSAC New Security Paradigms Workshop*, Little Compton, R.I., 1993, reprinted in *Computer Security Journal,* Volume XI, Number 2, Fall 1995.

Schmucker, Kurt, *Fuzzy Sets, Natural Language Computation, and Risk Analysis,* Computer Security Press, 1984.

W.G. deRu and JHP Eloff, "Reinforcing Password Authentication with Typing Biometrics", *Information Security - the Next Decade, Proceedings of IFIP SEC '95 Conference, Capetown, South Africa,* edited by H.P. Eloff and Sebastiaan H. Von Solms, published by Chapman and Hall, 1995.

McLean, John, "New Paradigms For High Assurance Software", *Proceedings of the ACM SIGSAC New Security Paradigms Workshop,* Little Compton, R.I. 1992, IEEE Press 1993.

Eckert, Claudia, "Matching Security Policies to Application Needs", *Information Security - the Next Decade, Proceedings of IFIP SEC '95 Conference, Capetown, South Africa,* edited by H.P. Eloff and Sebastiaan H. Von Solms, published by Chapman and Hall, 1995.

Nelson, Ruth, D. Becker, J. Brunell and J. Heimann,"Mutual Suspicion for Network Security," *Proceedings of the 13th National Computer Security Conference*, Baltimore, MD, September 1990.

Nelson, Ruth, and Hilary Hosmer, "Security for Infinite Networks", *Proceedings of the ACM SIGSAC New Security Paradigms Workshop*, La Jolla, CA. Aug. 22-25, 1995, IEEE Press 1995.

Hilborn, Gene, "Information Domains Metapolicy", *Proceedings of the 18th National Information Systems Security Conference,* Baltimore, October 1995.

Hosmer, Hilary, "Integrating Security Policies", *Proceedings of the Third RADC MLS DBMS Workshop,* Castile, NY. June 1990, MITRE Technical Paper MTP 385.

Hosmer, Hilary H. "The Multipolicy Model, A Working Paper", *Proceedings of the Fourth RADC Workshop on Multilevel Secure Database Systems*, Little Compton, Rhode Island, June 1991.

Hosmer, Hilary H., "Metapolicies I", ACM SIGSAC Data Management Workshop, San Antonio, TX, December 1991, *ACM SIGSAC Review 1992.*

Hosmer, Hilary H., "Shared Sensitivity Labels", *Database Security, Status and Prospects,* North-Holland, 1991.

Hosmer, Hilary, "The Multipolicy Machine: A New Paradigm For Multilevel Secure Systems," *Proceedings of Standard Security Label for GOSIP, an Invitational Workshop,* April 1991, *NISTIR 4614,* June 1991.

Hosmer, Hilary, "The Multipolicy Paradigm for Trusted Systems", *Proceedings of the 1992 New Security Paradigms Workshop,* Little Compton, R.I. Sept. 22-24, 1992. IEEE Press, 1993.

Hosmer, Hilary, "Metapolicies II", *Proceedings of the 15th National Computer Security Conference*, Baltimore, MD, 1992.

Hosmer, Hilary, "Multipolicy System Composition," *Proceedings of the 16th National Computer Security Conference*, Baltimore, MD, 1993.

Campen, Alan, editor, *The First Information War, AFCEA International Press, 1992.*

Schwartau, Winn, *Information Warfare,* Thunder's Mouth Press, *1994.*

Power, Richard, *Current and Future Danger: A CSI Primer on Computer Crime and Information Warfare,* Computer Security Institute, 1995.

Tate, Paul, "Risk! The Third Factor", *Datamation*, April 15, 1988, reprinted in Barry Boehm's *Software Risk Management*, IEEE Computer Society Press, 1989.

Fletcher, Sharon, "The Risk-Based Information Security Design Paradigm", *Proceedings of the IFIP SEC '94 Conference*, May 23-27, 1994, Curacao, NA.

Howe, Donald, "Information System Security Engineering: A Spiral Approach to Revolution", *Proceedings of the ACM SIGSAC New Security Paradigms Workshop*, Little Compton, R.I. 1992.

Booysen, H.A.S. and J.H.P. Eloff, "A Methodology for the Development of Secure Application Systems", *Information Security - the Next Decade, Proceedings of IFIP SEC '95 Conference, Capetown, South Africa*, edited by H.P. Eloff and Sebastiaan H. Von Solms, published by Chapman and Hall, 1995.

Boehm, B.W. "A Spiral Model of Software Development and Enhancement", *IEEE Computer*, May 1988.

Fletcher, S. K., R. Halbgewachs, R.M. Jansma, M.D. Murphy, J.J. Lim, and G.D. Wyss, "Software Risk Management and Assurance", *Proceedings of the ACM SIGSAC New Security Paradigms Workshop*, Little Compton, R.I. 1994.

12 BIOGRAPHY

Hilary Hosmer founded Data Security, Inc., an INFOSEC research and consulting firm (Bedford, MA, USA) in 1990. Ms. Hosmer has twenty years experience in the computer industry, working with such firms as Honeywell, DEC, Blue Cross, and MITRE Corp. She also taught computer information systems at Bentley College for five years. She graduated from Bryn Mawr College (PA), the University of Massachusetts, and the Honeywell School of Information Sciences. Her list of research publications is three pages long. She founded the New Security Paradigms Workshop and The Security Consortium. Her honors include nominations to: *Who's Who Among American Women*, *Who's Who Among Emerging Leaders*, and *Who's Who in the World*.