Dr. Fred Cohen
572 Leona Drive - Livermore, CA 94550
http: //all.net/ - US+925-454-0171

This write-up details the contents of papers and other publications written by Fred Cohen in time sequence.

2011

F. Cohen, ”Digital Forensic Evidence Examination”, ASP Press, 3rd edition. 2011

Updates to include diplomatics and integrate definitions across fields. Enhancements and additional detailing of proofs and demonstrations for the physics of digital information.

F. Cohen, "A Case Study in Forensic Analysis of Control", Journal of Digital Forensics, Security, and Law., (pending publication in V5#4), 2011.

This paper extends the theoretical framework in the previous related publication to provide a case study in which claims of “Taking control” were evaluated for legal purposes.

F. Cohen, J. Lowrie, C. Preston, “The State of the Science of Digital Evidence Examination”, IFIP Seventh annual IFIP WG 11.9 International Conference on Digital Forensics, 2011/01/30, also published as a chapter in in “Advances in Digital Forensics VII”.

This paper suggests the state of the science and level of consensus in digital evidence examination. Elements of science and consensus are found lacking in some areas and present in others, but the studies involved are of only limited scientific value, and much further work is needed.

2011-02 - Why are we so concerned about governments getting our data?

This analyst report concludes: “Why do we worry about governments getting our private data? Because they have abused it in the past. But so have companies, including providing it to governments under legal mandates and in some cases even without such mandates. If we are going to trust someone other than ourselves, companies are far worse candidates than governments. But in truth, even the best of us are likely to depend on others in one way or another, and transitive trust has proven faulty again and again. In short, privacy is dead, and if you are forced to trust anyone or anything, governments are apparently the most trustworthy of the poor choices. “

2011-01b - The Bottom Ten List - Information Security Worst Practices - Getting Even Worse

This is the worst 10 security practices reflected in the previous year of experience.

2011-01 - Risk aggregation - again and again and again...

This analyst report concludes: “Why are we over-aggregating risks? There are lots of reasons. There is no way for competent professionals to wield leverage against management. There is no standard of care. There is no real legal mandate to deal with risk aggregation. Mitigation, regardless of how effective, is the ultimate excuse for sloppy architecture and design. Decision-makers can waive anything without apparent consequence. Nobody will stand up with the person who identifies a problem. We don't have a profession with properly defined standards of care. We don't have zoning boards or licensing or inspections according to database building codes. We don't even have assurance that auditors will find the problems, and if they do, there are no fines levied of requirements that the database not be used until fixed. And these are what we need.”

2011-00 - All.net has moved to the cloud!!!

This analyst report describes the decision-making process surrounding moving resources to external shared resources (the cloud) and why the all.net Web site was moved to the cloud.

2010

F. Cohen, ”Digital Forensic Evidence Examination”, ASP Press, 2nd edition 2010

Updates to add improved bibliography and more thorough coverage, fixes many minor errors in the original edition and adds improved definitions and consistent usage of terms.

F. Cohen, “Fundamentals of Digital Forensic Evidence”, (chapter in Handbook of Information and Communications Security, Springer, 2010, pp 789-808, Mark Stamp and Peter Stavroulakis, Ed.).

A summary article of the general way the field works.

F. Cohen, "A Method for Forensic Analysis of Control", IFIP TC11, Computers & Security, V29#8, pp 891-902, Nov., 2010, doi: 10.1016/j.cose.2010.05.003

This paper examines technical underpinnings for the notion of control as identified in laws and regulations in order to provide a technical basis for performing forensic analysis of digital forensic evidence in cases where taking control over systems or mechanisms is the issue.

F. Cohen, "Identifying and Attributing Similar Traces with Greatest Common Factor Analysis", (Submitted 2010)

This paper shows an efficient (less than n^2) algorithm for generating the set of all greatest common factors for a collection of structured content.

F. Cohen, "What Makes Critical Infrastructures Critical?", International Journal of Critical Infrastructure Protection(2010), doi: 10.1016/j.ijcip.2010.06.002.

This short piece describes the interdependencies that make infrastructures critical.

F. Cohen, "The Smarter Grid", IEEE Security and Privacy - On the Horizon, 2010, V8#1, January/February, 2010.

The visionaries of "smart grid" technology anticipate that over the next 10 years, the power grid will move from a relatively small number of carefully controlled devices into an Internet-like distributed computing environment performing "intelligent" distributed control of perhaps tens of billions of devices in the US alone. At a recent IEEE Spectrum meeting on the subject, in supporting the contention that the "smart grid" will be able to meet the security needs it will face, one of the presenters stated "We know how to secure the Internet". Not one person in the audience agreed when I asked for a show of hands in the Q&A period. The question is: "How do we get from here to there?"

F. Cohen, "Toward a Science of Digital Forensic Evidence Examination", IFIP TC11.8 International Conference on Digital Forensics", Hong Kong, China, Jan 4, 2010 (Keynote), Published in Advances in Digital Forensics VI, pp17-36, Springer, ISBN#3-642-15505-7, 2010.

This paper summarizes a keynote speech on moving toward a science of digital forensic evidence examination. The basic premise is that we are not a normal science today, and to get to normal science, we need to make progress in many areas. The question at hand, is where we should move as a community, and how we should get from here to there.

F. Cohen, “Digital Forensic Evidence Examination - The State of the Science - and Where to Go From Here”, NeFX Workshop, Sep 14, 2010.

This presentation and short paper takes the position that advancement of digital forensics requires advancement of the scientific basis through research.

F. Cohen, "Fonts for Forensics", IEEE SADFE (in conjunction with the IEEE Oakland Conference), 2010-05-19, Oakland, CA.

Like other latent evidence that cannot be directly perceived by people, bit sequences have to be presented through tools. Presentations of digital forensic evidence often involve the presentation of text versions of bit sequences representing traces of events that took place within digital systems. This paper is about creating fonts for the examination and presentation of particular classes of bit sequences presented in particular ways in legal situations. Unlike fonts used for other purposes, fonts for forensics are less about the beauty of the presentation and more about the tradeoff between readability and being definitive about what is present. In other words, what you see is what you get, rather than what you see is what looks nice.

F. Cohen, "The Bottom Ten List - Information Security Worst Practices”, EDPACS 41(1), January, 2010. (Reprinted from Analyst Newsletter)

F. Cohen, "Attribution of messages to sources in digital forensics cases", HICSS-43, Jan 7, 2010.

This paper presents advances in and limits on the attribution of messages to sources in digital forensics cases. It overviews current attribution technologies, the limits of those technologies, identifies ways in which attributions are made today and their limits, and discusses available methods for attribution within the legal system and the limits of digital forensic evidence for use in these purposes. It then presents a set of tools for message attribution now in use and identifies how they are being used and the limits of their applicability to forensics. The present and historical situation show a need for improved attribution, and clearly there is a long way to go before a sound scientific basis for attributions of messages to sources will be definitive.

F. Cohen, “Automated Control System Security”, On The Horizon - IEEE Security and Privacy, 2010-08.

Automated control systems (ACSs) lie at the heart of industrial and infrastructure systems, and as such, are one of the most critical parts of critical infrastructures. Yet the information security world has largely ignored these systems, and most of the information security folks I know seem to think that the same sorts of protective processes, measures, and mechanisms that apply to general purpose enterprise computers apply to ACSs. At the same time, most of the control systems engineers know almost nothing about information protection, and don't recognize even the potential for the sorts of things that information security professionals consider standard. This mismatch has to be addressed or we will be paying the price for it for at least one generation.

F. Cohen, “The Virtualization Solution”, On The Horizon - IEEE Security and Privacy, 2010-04.

Virtualization is increasingly being touted and used as the solution to the many ills we have in securing operating systems. But for many, it's just a case of “back to the future” with a twist. The twist could be good – or could be bad – for security – depending on how we use it. And if history has anything to teach us, it's that what can go wrong will go wrong – in the worst possible way. But there is always hope, if we can just figure out how to couch it.

2010-12b - Code book cryptography may be nearly dead
This analyst report describes how current search engines and digital libraries may be used to defeat code book cryptographic systems.

2010-12 - Changes to the Federal Rules of Evidence - Rule 26
This analyst report describes how changes to Rule 26 of the Federal Rules of Civil Procedure impact civil litigation for the better and move toward better forensics reports and reduce unnecessary cots.

2010-11 - How do we measure "security"?
This analyst report discusses the lack of an engineering and science discipline underlying information protection and identifies a possible path toward improving the situation/

2010-10 - Moving target defenses with and without cover deception
This analyst report is a detailed technical report identifying the fallacies associated with moving target defenses and how deception is essentially mandatory for such approaches to work well against serious attackers.

2010-09 - User Platform Selection Revisited
This analyst report examines the changes in user platforms over the last several years and identifies a methodology and evaluation of user platforms to support decisions for different situations.

2010-08 – The DMCA Still Restricts Forensics
This analyst report describes how updates to regulations now permit the disassembly and reverse engineering of systems and software for security research but not for forensics and the use in legal proceedings in the United States.

2010-07 - Mediated Investigative Electronic Discovery
This analyst report details how attempts to move toward “mediated electronic discovery” are flawed and the perils of moving this direction in terms of the legal process as it exists today.

2010-06 - The difference between responsibility and control
“... . A reasonable explanation for why protection fails to meet management goals is that the people who are responsible for protection, at all levels, don't have or exert adequate control to affect the desired outcomes. This difference between responsibility (R) and control (C) is at the core of how and why protection fails, and is one of the least understood and least measured quantities in protection today. ...”

2010-05 - The Virtualization Solution
This analyst report discusses the limitations of virtualization and the security implications of its use. It also assumes that this approach will be taken and identified approaches to improved protection in a heavily virtualized environment.

2010-04 - Attacks on information systems - a bedtime story
“Once upon a time, there were information systems that were not intentionally attacked,
because nobody knew how to attack them. Then the first practical information system was
implemented. ...”

2010-03 - The attacker only has to be right once - another information protection fallacy
This analyst report discusses the common fallacy that attackers only have to be right once while defenders have to be right all the time. It concludes: “The problem is not that attackers only have to be right once. The problem is that, after getting away with things again and again, after betting caught and released, after being fired but allowed to keep the money, after getting detected millions of times, they are still free to keep attacking. And eventually, they do succeed. That's the problem. It's not that they only have to be right once. It's that they get to be wrong so many times and get to keep on trying! “

2010-02b - Another ridiculous cyber warfare game to scare deciders into action
This analyst report describes the public relations surrounding war games and the announcement of their results to the public, typically right before funding decisions are made in the political system.

2010-02 - Developing the science of information protection
“At the dawn of the information age, like at the dawn of every other age, wild experimentation, rampant exploration, and many fits and starts have taken place, and are to be expected. But like any revolution, at some point, society settles down into normalcy. As the madness subsides, wild speculation yields to scientific exploration. Now is the time for the scientific approach to take its rightful position in bringing light were once there was only heat. ...”

2010-01 - The Bottom Ten List - Information Security Worst Practices

This analyst report provides the worst 10 security practices of the previous year.

2009

F. Cohen, ”Digital Forensic Evidence Examination”, ASP Press, 2009

The first attempt at a graduate science textbook in this area, it attempts to define the scientific basis for digital forensics evidence examination.

F. Cohen, "The past and future history of computer viruses", EICAR annual conference, Berlin, Germany, May 11-12, 2009.

This paper describes the history of computer viruses and identifies likely futures, which are not substantially different from the history.

F. Cohen, "Analysis of redundant traces for consistency", IEEE International Workshop on Computer Forensics in Software Engineering (CFSE 09), Seattle, Washington, USA, July 20-24, 2009

This paper is about the detection of inconsistencies and consistencies in redundant traces to detect forgeries, demonstrate forensic soundness, and lend weight to assertions made by forensic examiners performing analysis.

F. Cohen, "Two models of digital forensic examination", IEEE SADFE (in conjunction with the IEEE Oakland Conference), 2009-05-21, Oakland, CA

This paper examines an existing cost model of digital forensic evidence examination, identifies minor optimization improvements to that model, describes a new model, and uses the new model to show some fundamental theoretical limits of examination.

F. Cohen, "Issues and a case study in bulk email forensics", Fifth annual IFIP WG 11.9 International Conference on Digital Forensics, 2009/01/27, published as "Bulk Email Forensics" in the conference publication.

Recent legal matters involving unsolicited commercial email increasingly involve hundreds of thousands of email messages or more. As the volume of emails involved in these cases increases, manual methods for examination and interpretation of evidence become harder, more expensive, and more error prone. In addition, these cases increasingly show evidence of spoliation, and in some cases, of intentional evidence construction that is harder to detect as the actors become more sophisticated. The solution we propose and demonstrate comes in the form of improved automated techniques for analysis combined with more useful presentation to aid in interpretation.

F. Cohen and T. Johnson, "A Ph.D. Curriculum for Digital Forensics", HICSS-42, Jan 7, 2009.

This paper presents a curriculum for a doctorate in digital forensics and discusses the implementation of that curriculum in a graduate program. It includes overviews of all of the classes and in-depth coverage of specific areas that go beyond the Masters level. It also discusses how that program is being implemented at the California Sciences Institute, a Non-profit California Public Interest Educational Institution oriented toward graduate education in the areas of Advanced Investigation and National Security.

F. Cohen, "Information Assurance Architectural Models", HICSS-42 Product and Process Assurance Symposium Position Paper, Jan 5, 2009,

It is the position of this paper that the business models of information assurance have failed miserably when it comes to the issue of information protection, in large part because the assumptions made for most business models do not apply to information protection issues. We propose an alternative approach based on prior work in this field and directly address a position on the questions offered by the originators of the session.

F. Cohen, "Social tension and separation of duties”, EDPACS 38(5) (2009). (Reprinted from Analyst Newsletter).

People issues have always been key to information protection, and yet they are under-served because of the high level of technology involved in the emerging information age. The focus of this paper is on people issues, and in particular the intentional introduction of social tension into the workplace in order to have effective separation of duties.

2009-12-B - COFEE and the state of digital forensics

Computer Online Forensic Evidence Extractor (COFEE) is a software program developed by Microsoft for use by law enforcement. It was held closely by law enforcement for a period of time until it was revealed in the last year, and subsequently, several individuals released software intended to defeat the utility of COFEE. While a big deal has been made of the secrecy of this tool and other related matters, reasoned examination has been somewhat lacking in the open community, even though there have been validation studies undertaken of the tool. Thus this limited review of the situation is suited to this special end-of-year edition.

2009-12 - Using the right words

This article calls for the clear definition and use of common language for digital forensics (and information protection) as part of the movement toward a generally accepted scientific basis.

2009-11 - Passwords again - why we can't leave well enough alone

“I just tried to login to my bank account, and surprise surprise, US Bank now requires that, in order to access my bank account, I must provide them still more personal information, including answers to questions about my personal history, family, and world view. When I called them up, they told me "it's for your protection", but in fact, it doesn't protect me at all. At best, it protects them; and it probably doesn't even do that. I'm going to ask a simple question: If you can't protect my password, how can you protect even more private information? ...”

2009-10 - Partitioning and virtualization - a strategic approach

In summary: “The evolution and emerging systems and components are taking us forward to the past, and the architectures of the 1960s and 70s, reapplied to the new technologies and methods, will serve us well in building out a fast, flexible, reliable, lower cost, and more efficient information infrastructure for every size and type of enterprise. It's time to go back to the future.“

2009-09 - Forensics: The limits of my tools, my techniques, and myself

It ends: “I think it is important as a community that we recognize our limitations and our faults so we may best improve ourselves. At the same time, our scientific progress depends on our ability to find ways to reduce these faults and prevent the faults we know about from producing failures that are reasonably preventable. I hope, but don't expect, that everybody working in digital forensics will start to recognize their limitations and use more care and diligence in reporting their findings ...”

2009-08 - Virtualization and the cloud - Risks and Rewards

“The concept and realization of virtualization are compelling for certain situations, and the use of cloud computing concepts, as a form of distributed computing in a virtualized space, is just as compelling. But this should not be confused with the notion of the "public" vs. "private" vs. "outsourced" issue. “

2009-07 - The speed of light, it's easy to forge, email is always fast, and more

“People say all sorts of things, and in everyday conversations, this is no problem. But as IT professionals move increasingly into the space of digital forensics and the use of digital information in the context of the legal system, they must realize that exaggeration to make a point, or a lack of care and thought in sworn statements, may lead to disaster.”

2009-06 - Security Decisions: Deception - When and where to use it

This analyst report codifies decisions on when to use deception as a defense.

2009-05-B - Culture clash: Cloud computing and digital forensics

“Cloud computing is getting a great deal of attention these days, and there are a lot of good reasons to move into the clouds for a lot of people. Whether it's; .mac users who use Apple for their email, Web services, file sharing, and so forth; Google for gmail, advertisements, searches, and storage; or any of the other companies that provide services for free or fee, there is a lot to be said for the economy of scale when you don't really need integrity, availability, confidentiality, use control, or accountability. But what happens when you do?”

2009-05 - Protection testing: What protection testing should we do?

This analyst report discusses when to do what sorts of protection testing.

2009-04-B - Proposed Cyber-Security Law: What's the problem?

On or about March 31, 2009, Senators in the 111th Congress 1st Session initiated efforts to create a legal framework for "cybersecurity" for the United States. While this effort is laudable, there are several critical issues with this proposed legislation. This paper represents some of my initial thoughts. For each section of the proposed bill of interest to me, it includes "Basics" that describe the legislation, "Section by section analysis" that provides a third party analysis of the bill that I received via email, and my "Opinion" about issues with the section.

2009-04 - Risk management: There are no black swans

This analyst report dispels the excessive use of the term “black swans” when it comes to information protection and points out that essentially all of the things people call “black swans” are in fact things they should have known about if they did their work properly.

2009-03 - How spam vigilantes are wrecking email and encourage violations of law

This analyst report discusses the feedback mechanisms that are the result of antispam vigilantes and that are causing spammers to increasingly violate more laws and exploit more systems in order to send their already illegal spam. It suggests that enforcing laws would be a better alternative.

2009-02-B Digital forensics must come of age

“The digital forensics area is growing in magnitude and intensity, but it lacks in the underlying fundamentals needed to make it viable for legal matters at the volume and intensity they are likely to arise in the coming years. This breaking wave represents both a great challenge and a great opportunity. “

2009-02 - A structure for addressing digital forensics

This analyst report describes an overall structure used for understanding the issues of digital forensics.

2009-01 - Change management: How should I handle it?

This analyst report describes approaches to change management and what methods should be used in which situations based on risk levels and program maturity.

F. Cohen - Forensic Fonts, 2009 – A software product that implements a new presentation method for presenting symbol sequences for use in legal matters.

F. Cohen, “Depiction of Digital Data for Forensic Purposes”, (Patent pending – method and apparatus for presenting said data as exemplified by “Forensic Fonts”)

2008

F. Cohen, ”Enterprise Information Protection Architecture”, ASP Press, 2008

This book consolidates results from work in previous years including the CISO toolkit and various Burton Group publications. It was also republished under similar title by CRC press.

F. Cohen, “Challenges to Digital Forensic Evidence”, ASP Press, 2008

While many books have been written on digital forensics, this is the first book to look at it from a standpoint of an error model and to examine how digital forensic evidence may be challenged and how proper work can overcome and defeat most such challenges.

F. Cohen, “Control Requirements for Control Systems... Matching Surety to Risk”, EDPACS, 2008 (Reprinted from Analyst Newsletter)

Control systems are differentiated from other systems and issues to be addressed in identifying proper information controls are identified and discussed.

F. Cohen, “Making Compliance Simple – Not”, EDPACS, March 2008, V37#3. (Reprinted from Analyst Newsletter)

This article discusses the claims of “simple” approaches to compliance and, in essence, seeks to debunk the notion that compliance is simple by describing experiences with policy development for enterprises and discussing the decision processes involved.

F. Cohen and C. Preston, “A Method for Recovering Data From Failing Floppy Disks with a Practical Example”, Fourth annual IFIP WG 11.9 International Conference on Digital Forensics, 2008/01/27 to 30.

This paper is about a method for recovering data from floppy disks that are failing due to weak bits. It describes a repetitive read technique that has successfully recovered data from failing floppies in forensic cases and describes other related techniques. None of these techniques are new or particularly unique, however, they are not widely published to the best of the authors knowledge and some of the related analysis may be helpful in making more definitive determinations in some cases.

2008-12-B - Short Note: Twittering away your privacy

This analyst report shows examples of what privacy information is released when twitter is used to communicate.

2008-12 - Digital Forensic Evidence: A Wave Starting to Break

This article discusses the change in the legal system that is leading to a dramatic shift toward the use of digital forensic evidence. It concludes: “The digital forensics area is growing in magnitude and intensity, but it lacks in the underlying fundamentals needed to make it viable for legal matters at the volume and intensity they are likely to arise in the coming years. This breaking wave represents both a great challenge and a great opportunity.”

2008-11 - Security Decision: Zoning your network

This analyst report shows a part of a reference architecture oriented toward making decisions about how to structure network separation mechanisms.

2008-10 - Social tension and separation of duties

This analyst report starts: “People issues have always been key to information protection, and yet they are under-served because of the high level of technology involved in the emerging information age. This month, the focus is on people issues, and in particular the intentional introduction of social tension into the workplace in order to have effective separation of duties. “

2008-09 - Default deny is best practice? Not anymore!

“Default Deny - 1970s - 1990s - Died of not changing quickly enough to meet the needs of the world around it. Survived by its child - risk management.”

2008-08 - Control architecture: Access controls
This analyst report shows a part of a reference architecture oriented toward making decisions about access control models (as opposed to implementations).

2008-07 - Fault modeling, the scientific method, and thinking out of the box
"I have been identified by many folks as someone who "thinks outside the box". I personally reject this notion and sometimes reply that I just think in a different box. We all have limitations and these limitations form the box we think and act within. The box is formed by a combination of nature and nurture, and in my case, part of my graduate level nurturing was being educated in the ways of fault tolerant computing by folks that were there when the field was just developing. This is a key to understandings that I have of how to make progress on many of the seemingly unsolvable problems we face in the information protection arena. So I figured I would share the key and see if we can, together, unlock a lot of the boxes out there. ..."

2008-06 - Inventory Revisited - How to reduce security losses by 70%?
This analyst report discusses how inventory is fundamental to effective protection and identifies reasons that losses may drop substantially with better inventory.

2008-05 - Control Requirements for Control Systems... Matching Surety to Risk
This analyst report identifies control requirements specific to control systems and differentiates them from the control requirements from other systems.

2008-04 - The Botnets have come - The Botnets have come...
This article contrasts predictions from 1996 to 2008 figures on distributed coordinated attacks in general and botnets in particular.

2008-03 - Enterprise Information Protection - It's About the Business
This analyst report describes a top-level understanding of enterprise information protection.

2008-02 - The Digital Forensics World
This analyst report concludes: "The field of and market in digital forensics is in its earliest stages, with only rudimentary tools that serve only a limited part of the process. There is a long growth path ahead in this industry, and it will take a long time to make significant progress. As an industry, it is only being born, and it will be many years before it starts to mature in any meaningful way. It seems likely that, over time, this field will become a profession, with doctorate level experts at the top, certification processes mandates, professional standards applied, and regularly published refereed scientific journals forming the basis for analysis and presentation of materials in court. But for now, like the Wild West that was the Internet and is not yet well settled today, the area of digital forensics will continue to be a territory for innovation, exceptional individuals, major missteps by players here and there, and a lack of clear direction for the foreseeable future."

2008-02 - Get Smart About Security - Who Should Do Your Digital Forensics?
"While everyone with a systems administration account seems to think that they are forensics experts, the reality is quite different. Digital forensics is a specialty area fraught with special requirements and special pitfalls and should not be assumed to be covered by expertise in information security. ..."

2008-01 - Unintended Consequences
This short analyst report identifies challenges associated with dealing with unanticipated consequences.

2008-01 - Get Smart About Security - Accidental Security
"While most security education and training surrounds defeating intentional malicious attackers, many of the losses and much of the liability for those losses surrounds errors and omissions rather than malicious acts. Security against unintentional acts is quite different, and well worth considering. ..." Mistake of the month: "Over consolidation: should have known better!"

2007

F. Cohen, "A Framework for Deception", (chapter in National Security Issues in Science, Law, and Technology), Thomas A. Johnson, Ed. Taylor & Francis, 2007.
This chapter reviews the framework for deception used in more lengthy published papers.

F. Cohen, "Critical Infrastructure Protection: Issues and Answers", (one chapter in National Security Issues in Science, Law, and Technology), Thomas A. Johnson, Ed. Taylor & Francis, 2007. (in press).
This paper overviews key aspects of critical infrastructure protection covering largely areas covered in previous papers.

F. Cohen, "Information Warfare, Netwar, and Cyber Intelligence.", (chapter in National Security Issues in Science, Law, and Technology), Thomas A. Johnson, Ed. Taylor & Francis, 2007.
This summarizes issues in information warfare from a consolidated perspective.

2007-12 - Security, justice, and the future

This analyst report article is about ethics in the information protection profession.

2007-12 - Get Smart About Security - Security End-of-year

“Business has end of year processes such as closing out the books, spending unspent budget, deciding what to do over the next year, and so forth. While this tends to go with the fiscal year that is not always aligned with the calendar year, whenever you decide to do it, security has its own annual cycles. At the end of those cycles, there is, or should be, and end-of-year process.” Fraud of the month: “Reorganization or one-time charges”.

2007-11 - Security by Psychology

This analyst report ends: “Psychological issues have always been central to security, but they have not always been widely recognized for their role in the overall protection program. Security by psychology works and necessary in any protection program, but it must be well done to work well.”

2007-11 - Get Smart About Security - Covert Awareness

“Covert awareness must surely be an oxymoron if ever there was one. Any yet it is not. Covert awareness programs are awareness programs designed to create the social environment that supports sound and sensible security behaviors by creating social norms. They are covert because they seek to influence norms by presenting the proper behaviors as if they came from a friend and colleague and not from on high. ...” Fraud of the month: “We interpret based on how others interpret.”

2007-10 - Making compliance simple – not

This analyst report is about the inherently complex nature of compliance and how exaggerated claims of simplification should not be listened to.

2007-10 - Get Smart About Security - Measuring Compliance

“You will comply! Resistance is futile... For Star Trek fans, the compliance gurus sound like the Borg – an alien race that assimilates other races and cultures by force, turning them into drones doing the bidding of others. But in the real world, compliance is... something that an seemingly alien race forces all of us to do. Since we, more or less, have no choice about many compliance issues, once we resign ourselves to having to do it, how do we figure out how much we have done and how much is left to do? That's what measuring compliance is all about. ...” Fraud of the month: “Because.”

2007-09 - Identity Assurance and Risk Aggregation

This analyst report identifies the potential Achilles heel of identity assurance and management – the risk aggregation in the identity management systems and infrastructure.

2007-09 - Get Smart About Security - Identity Assurance

“Assuring that identified individuals and things are as they are portrayed is fundamental to most security processes. As a result, the conceptual need for identity assurance is indeed great. But the reality of assured identity is far more complex. ...” Fraud of the month: “Phantom employee”

2007-08 - The ethical challenge

“... Our analysis shows that unless and until the top executives and/or boards of directors learn enough to recognize that they need an independent security function, companies will continue to spend more and more for less and less in the security arena, will continue to take unnecessary and unjustified risks with their shareholders' money, and will fail to meet even the minimal standards of due diligence that thoughtful people could not deny.“

2007-08 - Get Smart About Security - Conflicts of Interest

“Eliminating conflicts of interest is, perhaps, the most basic fundamental of an effective security program, and yet few organizations today have even the most basic sort of requirement that the CISO be independent from the CIO. This basic problem has and will continue to cripple the ability to have an effective security program. ...” Fraud of the month: “Mechanisms of self-serving beliefs”

2007-07 - Security Decision Support

This is a market survey of available products for supporting making sound decisions about information security.

2007-07 - Get Smart About Security - Making Better Security Decisions

“It would sure be nice if we could make better strategic decisions about security. But how exactly do we do this? Despite efforts over several decades, decisions of today about security are much like those of long ago. They are highly dependent on the individuals making them and the specific circumstances. ...” Fraud of the month: “Help me get the money out”

2007-06 - User platform selection

This analyst report provides analysis of factors in user platform selection and identifies the situation as of that date with regard to decisions on user platform selection.

2007-06 - Get Smart About Security - Which User Platform

This article examines the tradeoffs between different user platforms. Fraud of the month: “People tend to reciprocate any gifts”

2007-05 - Risk Management

This is a basic article about risk management practices and methods.

2007-05 - Get Smart About Security - Managing Risks

This article is about people using their feelings and perspectives to manage risk. Fraud of the month: “Alter checks on their way to the printer”

2007-04 - Security Ethics and the Professional Societies

“At the RSA conference this year, there was an ethics panel made up of the heads of the 5 families of information security; ISACA, ISC2, ASIS, SANS, and ISSA – certifiers all. Based on what they said and the ethics standards they have in place for their members, as of 2007, the information security ethics situation as we see it is poor at best. ...”

2007-04 - Get Smart About Security - Information Content Inventory

This article concludes: “Hopefully I am preaching to the choir. You cannot effectively control what you don't know to exist, and for any substantial enterprise, this means the creation and proper maintenance of an inventory of information assets. (1) It is obvious and yet often forgotten. (2) You will have to create your own standards. (3) Get your assets in an inventory today. It's just common sense.” Fraud of the month: “Shorting”

2007-03 - Emerging Risk Management Space

This analyst report described products and methods in the emerging risk management product space.

2007-03 - Get Smart About Security - Sensible Security - You Wouldn't?

“... Sound security is sensible, but it only makes sense when you make sense of it...” Fraud of the month: “Paper firm”

2007-02 - Emerging Market Presence

This analyst report describes how the information security space looked at the time and how it was changing over time.

2007-02 - Get Smart About Security - Measuring Security

“Security metrics are among the most important and least well done things involved in managing security programs. What makes a good metric and how do we collect and present them? ...” This article seeks to answer this question. Fraud of the month: “Love shack”

2007-01 - Market Maturity and Adoption Analysis Summary

This analyst report was about the maturity of the information security market in terms of different areas of enterprise process and different business functions associated with security.

2007-01 - Get Smart About Security - Closing the Gap

This article discusses how you close the security gap once you do gap analysis. Fraud of the month: “Last year's money”

2007-00 - Analysis Framework

This article presented the analysis framework used for following articles analyzing the information security markets.

F. Cohen - Decider, 2007 – software program for aiding in decision-making and justification.

F. Cohen, “Method and/or System for Providing and/or Analyzing and/or Presenting Decision Strategies“, 60957455 (Patent pending method as exemplified by the Decider software products.)

2006

F. Cohen, "Challenges to Digital Forensic Evidence", (chapter in "Forensic Computer Crime Investigation", Thomas A. Johnson, Ed. Taylor & Francis, 2006

This outlines an error model for digital forensics and identifies how digital forensic evidence may be successfully challenged.

F. Cohen, “Security Decisions”, ASP Press, 2006

This is an attempt at defining a set of sound practices for making architectural and strategic decisions surrounding information protection for businesses and enterprises of all sizes.

F. Cohen, “IT Security Governance Guidebook with Security Program Metrics on CD-ROM.” , Taylor & Francis/CRC Press, 2006

This is a consolidated version of previous books for CRC Press.

F. Cohen, “The Use of Deception Techniques: Honeypots and Decoys”, (chapter in Handbook of Information Security), V3, p646. Wiley and Sons, 2006.

This article summarizes much of the research to date in the use of deception for information protection.

World War 3 ... Information Warfare Basics , ASP Press, 2006

This is an introductory book examining the issues in information warfare.

Information Security Awareness Basics , ASP Press, 2006

This is a small handbook for training workers to defeat most of the most common methods used against enterprises.

F. Cohen, "Outsourcing, Offshoring, and Security: What's the Difference?", Burton Group Report, 28 Jun 2006

Offshoring and outsourcing are increasingly a focus of public and enterprise attention and concern. In this overview, SRMS Principal Analyst Fred Cohen describes the issues associated with offshoring and outsourcing as they relate to information technology and suggests decisions criteria for when to do outsourcing and offshoring and how to handle the technology issues when they are done.

F. Cohen, "IT Risk Management and COSO", Burton Group Report, 24 May 2006

With the emergence of SOX section 404 and the increasing costs of IT audit for public companies, enterprises are increasingly asking themselves how to di IT risk management in the context of the COSO standard referred to in the SOX regulatory interpretation scheme. In this overview, principal analyst Fred Cohen will review COSO and SOX and discuss how risk management under COSO can be applied to the enterprise.

2006-12 - Get Smart About Security - The Security Schedule

This article discusses the things that are typically scheduled processes for security management. Fraud of the month: “Revenue smoothing”

2006-11 - Get Smart About Security - The Holidays Bring the Fraudsters

This is about building security awareness program that helps people by including information on the various fraud schemes currently underway. Fraud-of-the-month: “Need-help frauds”.

2006-10 - Get Smart About Security - Physical/Logical Convergence??

“Many have asserted that a convergence between physical and information security is underway, and clearly there is a case to be made for some level of convergence. But how closely will they converge and how closely should they converge? ...” Fraud of the month: “Phony job interviews (employer)”

2006-09 - Get Smart About Security - How can I Show I am Me in Email?

This article discusses authentication of authorship of email messages and how to deal with the underlying issues. Fraud of the month” “Phony job interviews (employee)”

2006-08 - Get Smart About Security - Service Oriented Architecture Security Elements

This article discusses the benefits and security limitations of service oriented architecture. Fraud of the month: “Vendor Kickbacks”

2006-07 - Get Smart About Security - The Life Expectancy of Defenses

This article discusses long-term investments in information protection versus the shorter-term investments commonly put in technical solutions to specific problems of the day. Fraud of the month: “Jamaican Switch – 419 Frauds”

2006-07 - Get Smart About Security - BONUS ISSUE: The End of the World as we Know it

This article details results of war gaming relating to terrorist threats. It details the work of a class at the University of New Haven in trying to identify how to attack, and alternatives for defense.

2006-06 - Get Smart About Security - Why the CISO should work for the CEO - Three Case Studies

“These three case studies show why we think Chief Information Security Officers (CISOs) should work for the Chief Executive Officers (CEOs). The situations are real and recent – the names are concealed to protect the shareholders. ...” Fraud of the month: “Resale or Theft of Company Inventory”

F. Cohen - JDM, 2006 – A software product for supporting judgement and decision-making processes using a set of decisions, alternatives for each decision, and associated selections, decision processes, standard bases, and defined basis for as-is, future, gap analysis, and transition planning.

F. Cohen - Security Decisions, 2006 – A software product to support making specific decisions about security based on elements of reference architecture.

F. Cohen - Surveyor, 2006 – A software product for doing surveys with custom instances supporting security-related surveys.

F. Cohen - Influence, 2006 – A software product for helping influence individuals or groups toward supporting desired objective.

F. Cohen, “Method and/or System for Providing and/or Analyzing Influence Strategies“, (Patent pending as exemplified by the Influence software product)

2005

Frauds, Spies, and Lies - and how to defeat them , ASP Press, 2005

> This book consolidates issues of frauds, intelligence operations, and other aspects of deception and provides specific methods for defeating these methods.

The CISO ToolKit: Security Checklists - Governance , ASP Press, 2005

> This is a collection of checklists to allow security governance to be tracked and verified.

The CISO ToolKit: Security Metrics , ASP Press, 2005

> This is a collection of security metrics covering the same set of issues as the governance guidebook but with measurements of performance relative to other organizations.

The CISO ToolKit: Governance Guidebook , ASP Press, 2005

> This is a book providing guidance regarding enterprise security governance.

F. Cohen, "Defending Against the Evil Insider", Burton Group Report, 16 Nov 2005

> Insiders are historically responsible for about 80% of the losses suffered from attacks involving information systems. But they are given less than 20% of the attention of outsider attacks. This overview discusses insider attacks and the methods used to limit them without completely eliminating the need for insiders.

F. Cohen, "Raising the Bar: Solving Medium-Risk Problems with Medium-Surety Solutions" 27 Sep 2005

> As risks associated with information systems, network, and content increase, the need to provide more sure systems to meet the challenges of mitigating those risks are also on the rise. In this report, Principal Analyst Fred Cohen discusses the limitations of low surety approaches and examines the current and future potentials for medium surety solutions to meet enterprise risk management needs.

P. Schacter and F. Cohen, "Enterprise Strategies for Defending Against Spyware", Burton Group Report, 23 Aug 2005

> The recent increase in the use of Trojan horses and similar techniques for extracting information from end user systems and exploiting the weaknesses in these systems is a serious problem for many enterprises. Spyware and adware are more than just a user inconvenience and can lead to identity theft and commercial fraud. This overview examines the problem and suggests strategies that enterprises can take to defend against spyware.

F. Cohen, "Security Metrics: Horses for Courses", Burton Group Report, 24 Jun 2005

> Although many measurements are currently taken in the information protection field, most of these measurements are not designed in a way that provides decision makers with meaningful feedback that allows them to track the information protection process for efficacy and make adaptations for improved performance. In this overview, Principal Analyst Fred Cohen discusses approaches to measuring security and the limitations of those approaches. This overview examines historical and current security metrics with an eye toward understanding what has to be measured, how it can be measured, and what to do with those measurements.

F. Cohen, "Security Governance for the Enterprise", Burton Group Report, 31 Mar 2005

> There are many approaches to building an effective enterprise-level information protection program, but only a few are in widespread use today and for the enterprise not already highly developed in this area or the new CISO, this guide to building and running an effective security governance program is key to success.

F. Cohen, "Business Continuity Planning for IT", Burton Group Report, 24 Mar 2005

> Business continuity planning is fundamental to effective operations for any enterprise. In this overview, SRMS Principal Analyst Fred Cohen describes systematic approaches to assuring that the proper level of availability is maintained across the spectrum of events that enterprises encounter.

D. Blum and F. Cohen, "A Systematic, Comprehensive Approach to Information Security", Burton Group Report, 24 Feb 2005

> This paper outlines the systematic comprehensive approach to information protection that is at the heart of the Burton Group information protection reference architecture and coverage.

F. Cohen, "Security Awareness, Training, and Education Programs for the Enterprise", Burton Group Report, 17 Jan 2005

> In this overview, Fred Cohen discusses security awareness programs used by enterprises to keep their users immunized against the many mishaps that create day-to-day, human-related vulnerabilities in their information protection posture.

F. Cohen, "Change Management for the Enterprise", Burton Group Report, 17 Jan 2005

> Burton Group principal analyst Fred Cohen discusses change management and the technologies

and management systems required in order for effective and appropriate change management to be applied at the enterprise level.

D. Blum and F. Cohen, "Concepts and Definitions", Burton Group Report, 17 Jan 2005

This is a write-up that defines central concepts and definitions used in the Burton Group coverage of security and risk management strategies.

2004

F. Cohen and D. Koike, “Misleading attackers with deception”, Information Assurance Workshop, 2004. Proceedings from the Fifth Annual IEEE SMC Publication Date: 10-11 June 2004 : pp. 30- 37

This paper discusses methods used to mislead attackers against computer systems and networks through the use of deception.

F. Cohen, "Computer Viruses", (one chapter in "The Computer Security Reference Book", Butterworth/Heinemann, Oxford, England, 2004.)

This was a summary paper of the computer virus issue at that time.

F. Cohen, "Database Security: Protecting the Critical Content of the Enterprise", Burton Group Report, 28 Oct 2004

In this overview, principal analyst Fred Cohen discusses critical protection issues associated with databases. The discussion covers issues ranging from the real impact of database security failures to the options for protecting those databases from those failures. This overview is critical for anyone securing an enterprise that has just-in-time supply chains, critical dependencies on databases, or high valued enterprise systems that use database technology as a core element of their implementation.

F. Cohen, "Building Secure Applications: How secure do you want to be today?", Burton Group Report, 09 Sep 2004

Burton Group principal analyst Fred Cohen discusses three different approaches to secure applications development and operation. Low-surety approaches to improving systems in widespread use are dramatically different from medium- and high-surety approaches required for systems that have to operate in medium- and high-risk environments. A wide range of techniques and strategies are reviewed and recommendations for changes in the way enterprises procure and think about applications security are provided.

F. Cohen, "Risk Aggregation: The Unintended Consequence", Burton Group Report, 27 Apr 2004

Are enterprises reducing risk when they centralized controls, or merely shifting it? This overview discusses risk aggregations associated with economies of scale the implications of this aggregation on the enterprise. It reviews risk management approaches to limiting and controlling risk aggregation and methods for mitigating aggregation in enterprise networks and information technology architectures.

F. Cohen, "Auditing and Audit Trails", Burton Group Report, 18 Mar 2004

Auditing and the generation, transmission, and long-term storage of audit related information has become increasingly critical as regulatory and business drivers have put pressure on enterprises and their IT staff to be able to demonstrate that they are in compliance with requirements, to debug system and network failures, and to provide legally viable evidence in support of a wide variety of processes. While IT audit has been a staple of enterprises for many years, the increased volume and variety of audit information has driven the audit analysis problem to new heights. This overview covers the different sources of audit-related information, the mechanisms used to generate, convey, store, and analyze that data, challenges associated with the audit process, and vendor products that support the IT audit process.

F. Cohen, “Cisco Security Features and Futures”, Burton Group Report, 2004.

Cisco has announced a number of new initiatives that should dramatically change the way security is done from the core of networks through office systems. This report overviews the full spectrum of Cisco products for their security capabilities and limitations and makes recommendations about how enterprises should use Cisco security capabilities today and what to expect of them in the future.

2003

F. Cohen, et. al. "Leading Attackers Through Attack Graphs with Deceptions", IFIP-TC11, `Computers and Security', V22#5, July 2003, pp. 402-411(10)

This paper describes a series of experiments in which specific deceptions were created in order to induce red teams attacking computer networks to attack network elements in sequence. It demonstrates the ability to control the path of an attacker through the use of deceptions and allows us to associate metrics with paths and their traversal.

F. Cohen, "Patch Management", Burton Group Report, 2003

Patch management is a critical component of timely security response. But automated patch management can cause major outages because of incompatibilities, lack of support, and many other limiting factors.This report considers patches and patch management, the limitations of current patch management systems, available technologies and product types, and enterprise strategies for handling patches and automated patch management.

F. Cohen, "The Evolving Role of Firewalls", Burton Group Report, 2003

In this document, Principal Analyst Fred Cohen discusses the evolving role of firewalls in enterprise networks. He describes the historical roots of the firewall technologies in use today, features and limitations associated with modern firewalls, how firewalls are managed, and how they integrate with other elements of enterprise network architecture. Decisions about firewalls and their future in enterprise protection are outlined and likely futures are discussed.

F. Cohen, "Linux Security Features", Burton Group Report, 2003 (unpublished due to Microsoft)

The increased effectiveness of Linux in secure server roles stems largely from special configurations, special software features, availability of more secure applications, and a well trained systems administration staff. This report focuses on tools and techniques used to secure Linux, and more generally, Unix-like servers in enterprise infrastructure applications. It identifies the wide range of security mechanisms available under Linux and discusses when and where to apply these mechanisms to provide enhanced protection.

F. Cohen, "Intrusion Detection and Response Systems", Burton Group Report, October, 2003

In this document, Principal Analyst Fred Cohen discusses both the utility and limitations of intrusion detection and response systems. This overview goes into detail on issues related to the use of these systems, placement of their components, reasonable expectations on their performance, and decision parameters surrounding technology selection.

F. Cohen, "Analysis of Information-Related Threats to Enterprises", Burton Group Report, 18 Sep 2003

In this document, Principal Analyst Fred Cohen discusses techniques and good practices for analyzing threats to information assets. This overview presents a set of techniques and methods for threat analysis that reviews and codifies the existing body of knowledge. It suggests an approach to threat assessment that applies an increasingly detailed analysis of threats as consequences increase, but also balances cost and time requirements to provide straightforward decision guidelines. A substantial number of examples illustrate cases where often ignored threats turned out to be important considerations.

F. Cohen, "Risk Management: Concepts and Frameworks", Burton Group Report, 18 July, 2003

In this document, Principal Analyst Fred Cohen discusses approaches to risk management for information technologies. This report reviews and codifies the existing body of knowledge and experience and presents an overview of tools and techniques available to support and document the decision-making process. It suggests an approach to risk management of increasing rigor when threats and consequences justify the effort, provides some straightforward decision guidelines, and identifies common pitfalls and how to avoid them.

F. Cohen, "Policy-Based Security and Enterprise Policy Management", Burton Group Report, 9 Dec 2003

In this report, Principal Analyst Fred Cohen discusses the emerging use of technical policy-description interfaces integrated into enterprise-wide decision and enforcement mechanisms and audit generation, collection, fusion, and analysis systems to form overall enterprise security controls. Policy-based controls are increasingly being explored for their utility in reducing costs while increasing effectiveness of controls across large enterprises. From the distributed security management space we have technical tools capable of setting protections, controlling users, and reporting on conditions; while from the policy management space we see an increased desire to apply policy languages to resolve the complexity that results from compliance and compliance-related changes across enterprises. This report sits at the intersection of these two areas and focuses on current enterprise-wide, policy-based control products and technologies.

F. Cohen, "Managing Network Security" Jul. 2003, Why?

This is the final article in the series and is about the who, what, where, when , how, and why of security.

F. Cohen, "Managing Network Security" Jun. 2003, Background Checks

This article is about background checks, their limitations, and notions underlying their validity.

F. Cohen, "Managing Network Security" May. 2003, Operations Security for the Rest of Us

This article is about how operations security can be applied in a reasonable and cost effective fashion to an event such as a company conference

F. Cohen, "Managing Network Security" Apr. 2003, Documenting Security

This article is about the (boring) criticality of doing good documentation in security.

F. Cohen, "Managing Network Security" Mar. 2003, Novelty Detection

This article is about an approach to network anomaly detection based on seeking novelty.

F. Cohen, "Managing Network Security" Feb. 2003, Switching Your Infrastructure

This article is about moving away from hub-based systems toi switched network infrastructure.

F. Cohen, "Managing Network Security" Jan. 2003, Security Programming

This article is about the difference between writing general sorts of programs and programs that meet security requirements.

F. Cohen, D Rodgers, V. Nagaeu, “Method and Apparatus for Providing Deception and/or Altered Execution of Logic in an Information System US Pat. 7,296,274.

Operating-system level deception mechanisms.

F. Cohen, D Koike, V. Nagaeu, “Method and Apparatus Providing Deception and/or Altered Operation in an Information System Operating System”, US Pat. 7,437,766 10/679,186

Operating-system level deception mechanisms.

F. Cohen, “Method and Apparatus for Specifying Communication Indication Matching and/or Responses” 20040153574 (pending)

A method and/or system providing and/or indicating configurable and selectable strategies for responding to data units.

F. Cohen, “Method and Apparatus for Invisible Network Responder” 20040148521 (pending)

A method and/or system providing and/or indicating configurable and selectable strategies for responding to data units.

F. Cohen, “Method and Apparatus for Configurable Communication Network Defenses” 20040162994 (pending)

A method and/or system providing and/or indicating configurable and selectable strategies for responding to data units.

2002

F. Cohen, "Managing Network Security" Dec. 2002, Back Up a Minute

This article discusses the problems with backups of various sorts and identifies that this problem still has not been adequately addressed even though it has been known since the beginning of the use of computers.

F. Cohen, "Managing Network Security" Nov. 2002, Breaking In... to test security?

This article takes the position that breaking in is a poor way to test security, not because it fails, but because you learn so little from it. Breaking in and claiming it was just a way to test security should be treated as a criminal act.

F. Cohen, "Managing Network Security" Oct., 2002 - Reworking Your Firewalls

This article identifies what firewalls are and are not good for, as opposed to the many claims made about them and why they are or are not worthwhile.

F. Cohen, "Managing Network Security" Sept, 2002 - Deception Rising

This article discusses the emergence of deception as a protection technology.

F. Cohen, "Managing Network Security" Aug, 2002 - You're in a Bind!

This article uses “The Devil Went Down to Georgia” as a theme for discussing DNS security issues.

F. Cohen, "Managing Network Security" July, 2002 - Smashed Again by Stupid Security (appears in Computer Frauds and Security Bulletin)

As I write this article, I am in the process of being smashed again, and I am getting a bit tired of simply taking it because I am too small and powerless to mean enough to the vendors who screw me for them to give a damn about providing me with the service I pay for. This article is about poor decision-making in the security space.

F. Cohen, "Managing Network Security" July, 2002 - Is Open Source More or Less Secure?

The answer is “No” and the article details the tradeoffs between open and closed source.

F. Cohen, "Managing Network Security" June, 2002 - Academia's Vital Role in Information Protection

This article seeks to destroy the errant viewpoint that academia is not relevant to real security as expressed by such statements as “That sounds like an 'academic' view” used to claim irrelevance.

F. Cohen, "Managing Network Security" May, 2002 - Terrorism and Cyberspace

This article describes what terrorists use “cyberspace” for, to wit: planning, finance, coordination of operations, political action, and propaganda.

F. Cohen, "Managing Network Security" April, 2002 - Misimpressions We Need to Extinguish

This article identified 12 widespread misimnpressions about security and seeks to dispel them.

F. Cohen, "Managing Network Security" March, 2002 - Embedded Security

This article discusses embedded security devices as a class and asserts that they are likely to increase in their utility and application.

F. Cohen, "Managing Network Security" February, 2002 - How to Get Around Your ISP

This article is about how to get around the so-called security measures provided by ISPs while In another sense, it is about how ISPs were starting to unnecessarily and, in my view, improperly, limit the use of the Internet by legitimate users for their commercial advantage. What was more recently called “net neutrality”.

F. Cohen, "Managing Network Security" January, 2002 - The End of the Internet as we Know it

This is about the transformation of the Internet from a lawless wasteland into a part of society that is worth investing in and protecting.

F. Cohen and Garrett Gee, 2002 - White Glove Bootable Linux CD

This was a bootable CD-ROM operating environment.

F. Cohen, 2002 - Responder - large-scale network deception system

This is a general purpose network deception device that is also the subject of several patents.

F. Cohen and Garrett Gee, 2002 - White Glove developer platform

This was a developers platform for making customized versions of the White Glove CD.

F. Cohen, Darrian Hale, et. al., 2002 - Resilience - Resilient network infrastructure

This was a resilient network infrastructure that would compensate for failures in components and portions of networks in near-real-time (within a few seconds) to counter denial of services and other sources of outages.

2001

F. Cohen, " 2001: Red Teaming Experiments with Deception Technologies"

This paper overviews a series of 30 experimental runs designed to measure the effects of deception defenses on attacks against computer systems and networks.

F. Cohen, " 2001: A Framework for Deception"

This paper overviews issues in the use of deception for information protection. Its objective is to create a framework for deception and an understanding of what is necessary for turning that framework into a practical capability for carrying out defensive deceptions for information protection.

F. Cohen, "Managing Network Security - The World Doesn't Want to be Fixed", Network Security, Dec., 2001.

This article describes why it is that the best technology, the best ideas, the best of anything, is almost certain to end up not being used or done - in security, making money from repeat business.

F. Cohen, "Managing Network Security: The Deception Defense", Network Security, Nov., 2001.

This article discusses the emergence of deception defenses and where, how, and why they work.

F. Cohen, "Managing Network Security: The DMCA ", Network Security, Oct., 2001.

This article discusses the Digital Millennium Copyright Act and how it impacted (until 2011) computer security research.

F. Cohen, "Managing Network Security: The Best Security Book Ever Written ", Network Security, Sep., 2001.

This article is about "Internet & Computer Ethics for Kids" by Winn Schwartau

F. Cohen, "Managing Network Security: Special Issue - The Balancing Act ", Network Security, Sep., 2001.

This article is about balance between security and freedom, privacy and power, and the Internet .

F. Cohen, "Managing Network Security: Bootable CDs", Network Security, Aug., 2001.

This article is about the utility of bootable CDs from security perspective.

F. Cohen, "Managing Network Security: A Matter of Power", Network Security, Jul., 2001.

This article is about power usage in computers and video displays and the need to adress energy issues as part of security in the broader sense.

F. Cohen, "Managing Network Security: The Wireless Revolution", Network Security, Jun., 2001.

The is about the emergence of wireless and related security issues.

F. Cohen, "Managing Network Security: The New Cyber Gang - A Real Threat Profile ", Network Security, May., 2001.

This article describes the activities of a cyber gang, how they operate (largely with impunity) and what to do about it.

F. Cohen, "Managing Network Security: To Prosecute or Not to Prosecute", Network Security, Apr., 2001.

This article is about what to do when you catch someone breaking the law and violating laws with regard to computer security issues.

F. Cohen, "Managing Network Security: Corporate Security Intelligence", Network Security, Mar., 2001.

This article is about having an effective intelligence process for corporate security.

F. Cohen, "Managing Network Security: Testing Your Security by Breaking In - NOT ", Network Security, Feb., 2001.

This article is about the notion that you can effectively test your defenses by trying to break into them. It favors testing, but identifies the limits, and suggests specific testing regimens that are likely to be effective.

F. Cohen, "Managing Network Security: Marketing Hyperbole at its Finest", Network Security, Jan., 2001.

This article is about breakthroughs in marketing technology – security technology in particular.

F. Cohen, Anthony Carathemus, et. al. 2001 - Secure DNS Server

This was the implementation os a secure authoritative-only DNS server.

F. Cohen, Anthony Carathemus, et. al. 2001 - Partition Dump

This is a program to extract partition information from disks even when the partitions fail to follow normal usage and standards.

F. Cohen, Eric Thomas, and Anthony Carathemus, 2001 - Invisible Router

This is a deception technology developed and tested at Sandia National Laboratories, and eventually deployed in military systems.

2000

F. Cohen, et. al. "A Mathematical Structure of Simple Defensive Network Deceptions", IFIP-TC11, `Computers and Security', Volume 19, Number 6, 1 October 2000, pp. 520-528(9)

In the last year, deception has emerged as one of the emerging techniques for effective information protection in networks. A natural side effect of the use of this technology is the desire to understand the mathematical properties underlying its utility. In the above cited paper, several informal notions were introduced - to wit: [Deception] increases the attacker's workload because they can't easily tell which of their attack attempts work and which fail... [Deception] allows defenders to track attacker attempts at entry and respond before attackers come across a vulnerability the defenders are susceptible to... [Deception exhausts attacker resources] [Deception increases the sophistication required for attack] [Deception increases attacker uncertainty] In this paper, we will examine these claims and provide a more mathematical foundation for this aspect of deception as a tool for network defense.

The Provisional Irish Republican Army, Special Cyber Terrorism Study – 2000

This study examined the issues of terrorism related to their use of information and information technology in the context of the specifics of the particular group and its history and motives.

The Animal Liberation Front (ALF), Special Cyber Terrorism Study – 2000

This study examined the issues of terrorism related to their use of information and information technology in the context of the specifics of the particular group and its history and motives.

Revolutionary Armed Forces of Colombia (FARC), Special Cyber Terrorism Study – 2000

This study examined the issues of terrorism related to their use of information and information technology in the context of the specifics of the particular group and its history and motives.

National Liberation Army (ELN)--Colombia, Special Cyber Terrorism Study – 2000

This study examined the issues of terrorism related to their use of information and information technology in the context of the specifics of the particular group and its history and motives.

Issues in Cyber-Terrorism, Special Cyber Terrorism Study – 2000

This study examined the underlying issues associated with terrorism and its use of information and information technology across the broad spectrum of group types.

F. Cohen, "Managing Network Security: The Millennium Article - Yet Again! - The Bots are Coming!!! The Bots are Coming!!!", Network Security, Dec., 2000.

Since this is the millennium article, I thought it would be a good time to look into the future and the past and to consider the big picture. In my view, the emerging 'bots' and the remainder of the automated intelligence function as it is developing represents the killer application of the Web that will transform the society and information technology once again

F. Cohen, "Managing Network Security: Why Everything Keeps Failing", Network Security, Nov., 2000.

Things we thought we could trust or that we once trusted are no longer trusted because they were never trustworthy and we have just now come to realize it. We live in a decaying world and we need to struggle eternally to keep it functioning with some level of assurance. This article addresses the use of diversity, redundancy, good intelligence, rapid detection, and appropriate response to deal with these issues.

F. Cohen, "Managing Network Security: The Threat", Network Security, Oct., 2000.

This article identifies and discusses the nature of the threats to information and systems.

F. Cohen, "Managing Network Security: Chipping ", Network Security, Sep., 2000.

Chipping is an old tradition in the spy game. Ever since computers became part of the landscape - and before that in telephony, hardware modification to allow remote access was part and parcel of the landscape. But historically, this has been a custom or semi-custom type of job, it has never been used in mass production like it is today... This article discusses chipping, its implications, and the nature of the situation at that time.

F. Cohen, "Managing Network Security: Understanding Viruses Bio-logically", Network Security, Aug., 2000.

This article discusses the "Pathogenesis of Computer Viruses" as opposed to non-computer viruses and identifies key factors that enable and support viruses to work toward an epidemic theory of computer viruses.

F. Cohen, "Managing Network Security: What does it do behind your back?", Network Security, Jul., 2000.

This article is about Trojan horses within commercial software designed to circumvent security through covert and not so covert channels so as to communicate back to their corporate sources and evade the protections of firewalls for their own purposes.

F. Cohen, "Managing Network Security: Why Can't We Do DNS Right?", Network Security, June, 2000.

“Call me a dreamer, but I imagine that some day in a galaxy far far away, somebody who runs one of the root servers will decide that instead of adding encryption and massive complexity and additional layers of untrsutworthy software to the already overburdened systems that form the improperly trusted core of the Internet, will decide to actually build the system with the minimum required software and verify it very carefully.”

F. Cohen, "Managing Network Security: Eliminating IP Address Forgery - 5 Years Old and Going Strong ", Network Security, May, 2000.

This article refreshes a 5-year old article identifying how to prevent IP address forgery and thus be able to attribute datagrams to IP addresses reliably. It urges the global community to redirect their activities in the direction of better attribution through simple and effective means.

F. Cohen, "Managing Network Security: Countering DCAs", Network Security, Apr., 2000.

This article describes how to defend against and track down the sources of distributed coordinated attacks (DCAs), which includes such things as what are now called botnets, distributed denial of service attacks, and a wide array of other similar methods.

F. Cohen, "Managing Network Security: Collaborative Defense", Network Security, Mar., 2000.

This article rallies in favor of cooperation between Internet participants toward the common defense.

F. Cohen, "Managing Network Security: Worker Monitoring ", Network Security, Feb., 2000.

This article identifies worker monitoring requirements, methods, applications, and limitations.

F. Cohen, "Managing Network Security: Digital Forensics ", Network Security, Jan., 2000.

This article identifies some basics of digital forensics, including some concepts that would ultimately become part of the physics of digital information, like the lack of unique history implied by incomplete traces, while discussing the notion of moving digital forensics toward a science.

F. Cohen, 2000 - D-Wall - Large-scale high fidelity deception system

This is a now-patented system and method that does large-scale high-fidelity network and system deceptions. It is the precursor of the Invisible Router and Responder.

F. Cohen, “Method and Apparatus for Network Deception/Emulation”, US Pat. 7,107,347.

1999

F. Cohen, "Simulating Cyber Attacks, Defenses, and Consequences", IFIP-TC11, `Computers and Security', 1999, vol. 18, no. 6, pp. 479-518(40)

This paper shows a method of simulating attacks and defenses on information systems using attack graphs and the classification system identified in earlier papers. IT demonstrates the complexity vs. accuracy tradeoffs, provides 1.2 million simulations that show how attacker and defender strength and time issues interact, and suggest the use of this method for design and relative comparison of defensive architectures.

F. Cohen, "30 Lies About Secure Electronic Commerce: The Truth Exposed", Institute for International Research Electronic Commerce Conference, Feb. 1999.

This article exposed many of the misimpressions about electronic commerce in the Internet age and is one of the “50 ways series” or articles.

F. Cohen, Cynthia Phillips, Laura Painton Swiler, Timothy Gaylor, Patricia Leary, Fran Rupley, Richard Isler, and Eli Dart "A Preliminary Classification Scheme for Information System Threats, Attacks, and Defenses; A

Cause and Effect Model; and Some Analysis Based on That Model", Encyclopedia of Computer Science, 1999.

This is a classification scheme for describing and modeling threats, attacks, and defenses for information, systems, and technologies, It forms the basis for a wide range of applications, ranging from analytical tools to simulation engines, many of which can be used on the all.net Web site.

F. Cohen, "Managing Network Security: Why it was done that way", Network Security, Dec., 1999.

This article discusses the requirement to document what was done and why it was done that was as part of change management in order to understand the reasons behind decisions made so that updates can take into account not only what is obvious, but why things are the way they are. It points out the perils of failing to do so.

F. Cohen, " So Much Evidence... So Little Time", Information Security Magazine, November. 1999. Special issue with articles by "The 20 Most Influential Figures in Information Security Today."

This article predict: (1) Digital forensics will adopt a marketing model to gather more in-depth criminal evidence, (2) Massive data collection and analysis capabilities will become available to law enforcement to combat cybercrime, (3) Massive data collection and forensic analysis will become commonplace on the corporate level, too, and (4) In the cyber-realm, individual privacy rights will whither and die on the vine. It also provides a limited basis for these predictions and other related information.

F. Cohen, "50 Ways to Defeat Your PKI and Other Cryptosystems", The 50 Ways Series at all.net. (/journal/50/index.html)

"Richard Power called me at 4:07 PM and told me he wanted 50 ways to defeat your PKI and Other Cryptosystems - 50 ways - 53 minutes - no problem. After taking 10 minutes to chat with Patrice about the coming CSI conference, I started out....[the 50 ways go here] ...It's 4:57 - no problem - I even responded to a few unrelated emails along the way. Time to email it off to Richard and take the kids to soccer."

F. Cohen, "50 Ways to Defeat Your Firewall", The 50 Ways Series at all.net. (/journal/50/index.html)

"My firewalls course covers this and a lot more, and has for many years, so I figured it was time for a 50-ways article. … [the 50 ways go here] ...Back to bed - another 20 minutes wasted."

F. Cohen, "Managing Network Security: The Limits of Cryptography", Network Security, Nov., 1999.

"This article is about cryptography and the excessive trust we are unnecessarily and unwisely placing in it. But, as such, it is also about risk management and the poor job we are doing of applying it to cryptography. So there are really only a few reasons that we make poor risk management decisions...."

F. Cohen, "Managing Network Security: Security Education in the Information Age", Network Security, Oct., 1999.

"... My assessment is that Internet-based security education today is rapidly approaching the level of effectiveness and interaction that televised two-way education achieved 20 years ago, and that it will likely not go far beyond this for quite some time to come....

F. Cohen, "Managing Network Security: In Your Face Information Warfare", Network Security, Sep., 1999.

"... there is a shooting war on in the cyber-world, and for the most part, those with the power to do something about it don't care enough to act decisively. There's nobody to call for help other than one of those high priced consultants who is already helping others to the point where they can likely only sell you their assistant at a hefty fee. You are on your own!"

F. Cohen, "Managing Network Security: What's Happening Out There", Network Security, Aug., 1999.

This article is about security metrics... "...Fight against the urge for steady statistical improvement relative to a meaningless statistic and start to use your access logs for something of value to your company and your program. Struggle to get a true understanding of the data at hand and to use it to the fullness of its capability...."

F. Cohen, "Managing Network Security: Attack and Defense Strategies", Network Security, July, 1999.

This article discusses attacker and defender strategies in the information arena. "A strategic analysis of network protection provides another tool in the risk manager's quiver. It allows the roll-up results of other risk management activities to be used in a meaningful way to make decisions about budget allocation and it provides an ability to continue to adapt your approach over time." It includes attacker strategies of speed, stealth, overwhelming force, indirection, randomness, least resistance, and easiest to find and defender strategies of dissuasion, deception, prevention, detection and reaction, repair, exploitation, capture and punishment, cover-up, and constant change. It provides a "game" matrix to allow analysis of attack and defense strategies.

F. Cohen, "Managing Network Security: The Limits of Awareness", Network Security, June, 1999.

This article talks about the use and misuse of security awareness, and what it is good for (i.e., preparing people to respond to identified things in desired ways).

F. Cohen, "Managing Network Security: Watching the World ", Network Security, May, 1999.

This discusses the issues associated with network traffic surveillance and its analysis.

F. Cohen, "Managing Network Security: Simulating Network Security ", Network Security, Apr., 1999.

This article discusses the different uses of simulation in the service of information protection, including detailing the operations of the security simulator, design aides, training games for attack and defense, network performance simulation, and strategic and tactical gaming.

F. Cohen, "Managing Network Security: The Millisecond Fantasy", Network Security, Mar., 1999.

This article challenges the notion that everything in computers is nearly instantaneous and describes the times associated with a wide range of activities related to computer security. This also describes the basis for timing used in the security simulator and some of the analytical and methods and experience associated with getting at those values.

F. Cohen, Eli Dart "DARE: Distributed Analysis and REsponse", SANS conference, San Diego, 1999.

This paper describes a system that uses interacting sensors and actuators in a network to scale defenses and services up and down based on detected activities in the rest of the network.

F. Cohen, "Managing Network Security: Returning Fire", Network Security, Feb., 1999.

It concludes... “Returning fire is not a job for the unskilled or meek, and definitely has its risks. On the other hand, it can be a very successful technique for defeating even the most serious of attacker. In the end, a strong offense is a good defense, assuming you can find the attackers. I do not advocate returning fire, but I can understand that the inability of the police to protect the average citizen leads to vigilante behavior. Perhaps an alternative would be a more effective police force, but then who wants to live in a police state?”

F. Cohen, "Managing Network Security: Anatomy of a Successful Sophisticated Attack", Network Security, Jan., 1999.

This article ends with... “The story you have just heard is true. The names and some of the details have been changed to protect the innocent. Jane and Jimmy continue to work for Mr. Phelps, and you might recognize them as highly successful members of your teams. They have not been caught, but some other like them have been. … Finding and catching this sort of perpetrator involves a combination of sound management practices in information protection and a solid investigation capability properly applied.”

F. Cohen, 1999 – ForensiX – Digital Forensics ToolKit for Linux and Unix

This tool was developed starting at an HTCIA conference as a Unix alternative to Windows-based tools and was eventually sold to a range of user communities before the DMCA made it more or less illegal to sell to anyone but law enforcement.

F. Cohen, 1999 - Network Security Simulator

This was one of the first simulators to simulate attack and defense of computer networks using a high enough complexity to produce meaningful results and low enough complexity for computation.

1998

Cohen F.; Phillips C.; Swiler L.P.; Gaylor T.; Leary P.; Rupley F.; Isler R., “A Cause and Effect Model of Attacks on Information Systems. Some Analysis Based on That Model, and The Application of that Model for CyberWarfare in CID”, IFIP-TC11 Computers and Security, V17#3, 1998 pp. 211-221 (11)

This paper examines a model of attack and defense at a level of granularity that permits useful analysis without excessive computational complexity.

F. Cohen, "A Note on the Role of Deception in Information Protection", IFIP-TC11, Computers and Security, 1998, vol. 17, no. 6, pp. 483-506(24)

This paper identifies the role and use of deception for information protection and gives examples of how deception may be effectively used for defenses by changing the computational and resource leverage for attacker and defender.

F. Cohen, "Managing Network Security: Balancing Risk", Network Security, Dec., 1998.

This article ends with: “We have discussed the notion of balance in a security program and given some examples of typical imbalances and methods for re-balancing. But I would be remiss if I didn't mention the fact that large systems tend to have large momentum. Re-balancing may take a long time, and if it does, this means that we will never be able to stay on the tight rope. The most important thing to do in order to get and keep your protection balance is to find ways to become nimble in your information protection program. But that discussion is for another day.”

F. Cohen, "Managing Network Security: The Real Y2K Issue?", Network Security, Nov., 1998.

This article ends with: “Summary: Computers don't have the brains of a piece of celery, and people who trust computers for critical functions without proper failsafes and verification are not much smarter. The Y2K problem is not a 2-digit year problem - it is a problem of people putting too much trust in technology and being in too much of a rush for local optima to do things right. If we keep going this direction - building a society on a house of cards - it will all fall down - and our society will go with it. Y2K is a symptom, not the disease. If we ignore the disease and simply treat the symptom, we will pay the price in our long term health - and eventually with our lives. The disease has been diagnosed and we have a viable - but not ultimate - cure. Let's start curing the disease with what we have today and use preventive measures to keep the disease from emerging again."

F. Cohen, "Managing Network Security: Time-Based Security?", Network Security, Oct., 1998.

This article starts with: "I just got a chance to read the draft version of Winn Schwartau's new book titled Time-Based Security and I thought it would be worthwhile reviewing the book and discussing some of the issues he covers." and ends with: "Time-based Security has been here since security was here and will likely be here for as long as security is a field. There is little here that we have not seen before, but as a collection taken in a new light, there is real value in this perspective." In between it goes into a wide range of related issues and points to earlier articles.

F. Cohen, "Managing Network Security: What Should I Report to Whom?", Network Security, Sep., 1998.

This article goes into some of the complexities associated with how people in security are squeezed from all sides because of competing duties and requirements. It is about the ethics of computer security and the challenges faced by those who are ethical.

F. Cohen, "Managing Network Security: Third Anniversary Article - The Seedy Side of Security", Network Security, Aug., 1998.

This article ends with: "There's a lot of money in the information security field today and much of it is being spent unwisely. The large dollar values are driving large numbers of poor quality people into the business and they are getting outrageous pay rates when they have little to really offer. At the same time, there are legitimate experts who are increasingly unable to differentiate themselves from the folks with good sales teams. The combination is a recipe for disaster to the unwary or uninitiated. I hope that some of the ideas I have provided here are of some use, but I fear that we have a long way to go in this industry." It is one of the article most commented on by readers.

F. Cohen, "Managing Network Security: How Does a Typical IT Audit Work?", Network Security, Jul., 1998.

This article examined how an IT audit (should/does) wotk from the standpoint of the person under audit.

F. Cohen, "Managing Network Security: Technical Protection for the Joint Venture", Network Security, Jun., 1998.

This is about approaches to technical security for joint ventures and similar situations when possible competitors are cooperating in limited ways. It identifies the "embassy", "enclave", and "enclosure" approaches and their limitations. It might have some useful applications for such areas as "cloud computing" or other similar collaboration environments.

F. Cohen, "Managing Network Security: Risk Staging", Network Security, May., 1998.

This article discusses risk management strategies that include the notion of choosing things not to protect in advance based on the tradeoffs associated with lost opportunities, lifecycle costs, and similar sorts of things. It may be considered by some to be counterintuitive, which makes it all the more interesting.

F. Cohen, "Managing Network Security: The Unpredictability Defense", Network Security, Apr., 1998.

According to Donn Parker, those who attack computers depend on their predictability in their attacks. This article discusses the use of deception to counter predictability as a defensive strategy, and discusses Deception ToolKit in this regard.

F. Cohen, "Managing Network Security: Red Teaming", Network Security, Mar., 1998.

This article discusses the benefits and limits of red teaming as an audit/evaluation approach.

F. Cohen, "Managing Network Security: The Management of Fear", Network Security, Feb., 1998.

This article discusses the way people manage perception so as to generate or remove fear and discuss things you can do to keep fear in its proper perspective.

F. Cohen, "Managing Network Security: Y2K - Alternative Solutions", Network Security, Jan., 1998.

This article includes... "It would be nice to have a technical solution to the year 2000 challenge, but for most organizations this is simply not going to happen. Instead, there will be failures. The trick is to keep the organization prospering even when the computer systems aren't prospering." and related approaches to looming large-scale information-related risks (Y2K in this case).

F. Cohen and E. Dart, 1998 - DARE - Distributed Analysis and Response

Software system for using deception to detect and automatically respond to detected intrusions in a cooperative manner across multiple machines in a network.

F. Cohen, 1998 - Deception Toolkit

A software product that provides user-level deceptions for services available via networks.

F. Cohen, 1998 - The Security Maze

A software product that trains users by crating a maze they pass through by correctly / incorrectly answering questions relating to computer security issues.

1997

F. Cohen, "Providing for Responsibility in a Global Information Infrastructure ", IFIP-TC11, `Computers and Security', 1997.

This article describes the need for attribution while retaining anonymity and suggests the use of identified anonymizer services which either allow legally mandated attribution of their users or take legal responsibility for the use of their services.

F. Cohen, et. al. "Intrusion Detection and Response", IFIP-TC11, `Computers and Security', V16,#6, 1997, pp. 516-516(1) (also appearing as a National Info-Sec Technical Baseline study from Dec, 1996)

This is the journal article resulting from a national technical baseline study of intrusion detection and response that identified many limitations of current intrusion detection systems and methods, most of which are still the case today.

F. Cohen, “Information System Defences: A Preliminary Classification Scheme”, IFIP TC-11, Computers and Security, V16,#2, 1997, pp. 94-114(21)

This paper classifies threats, attacks, and defenses, and forms the foundation for subsequent work that linked these together with a graph model for attack and defense simulation, analysis, and related methods.

F. Cohen, "Managing Network Security: 50 Ways to Defeat Your Intrusion Detection System", Network Security, Dec., 1997.

This article was done on an airline trip back, and was another in the 50-ways series. It's main purpose was to bring life to the work on the national technical baseline that was widely ignored in the research community. This article sparked far greater debate in that community.

F. Cohen, "Managing Network Security: To Outsource or Not to Outsource - That is the Question.", Network Security, Nov., 1997.

This article outlined the factors involved in outsourcing different aspects of information security.

F. Cohen, "Managing Network Security: The Network Security Game", Network Security, Oct., 1997.

This article is about the use of board games and similar tools in security awareness training.

F. Cohen, "Managing Network Security: Change Your Password - Doe See Doe", Network Security, Sep., 1997.

This article identifies flaws in the notions underlying regular password changes and identifies that the mindless application of such rules is detrimental to security. It identifies the reasons for password changes and the circumstances under which it is and is not a rational thing to do.

F. Cohen, "Managing Network Security: Penetration Testing?", Network Security, Aug., 1997.

This article ends: “Penetration testing is commonly used, but its overall effectiveness in improving protection is quite questionable. While it can be effective in raising awareness and in demonstrating select system weaknesses, it also has a number of negative side effects that should be considered before use. A more serious protection testing program should be considered as an alternative or as an enhancement of penetration testing efforts.”

F. Cohen, "Managing Network Security: Relativistic Risk Analysis", Network Security, Jun., 1997.

This article identifies that, while we cannot really do absolute risk analysis, we can in fact to reasonably sound risk analysis in comparing alternatives. To wuote: “Relativistic risk assessment works and it produces sensible results that can be easily explained, often without a high degree of dependency on uncertain numbers. It is one of the most convincing ways to show the benefits of one protective scheme over another and is particularly useful in cases where risks cannot be properly quantified with any degree of certainty.”

F. Cohen, "Managing Network Security: Prevent, Detect, and React", Network Security, May., 1997.

This article discusses the issues associated with prevention versus detection and reaction a strategies for defenders to use against attackers.

F. Cohen, "Managing Network Security: Would you like to play a game?", Network Security, Apr., 1997.

This article explores the use of different sorts of gaming for information protection, ranging from strategic gaming to devise strategies, to training games to improve human performance.

F. Cohen, "Protection Issues in ASCII Red Based on a Limited Unclassified Briefing" (C).

This classified paper identifies security issues in distributed computing environments and identifies specific issues associated with specific classified systems.

F. Cohen, "Managing Network Security: Risk Management or Risk Analysis?", Network Security, Mar., 1997.

This article differentiates risk management from risk assessment and discusses the methods used for each.

F. Cohen, "Managing Network Security: Network Security as a Control Issue?", Network Security, Feb., 1997.

This article discusses the virtual organization (vorg) associated with computer security in distributed computing environments.

F. Cohen, "Managing Network Security: Integrity First - Usually", Network Security, Jan., 1997.

This article discusses the historical focus of "CIA" (confidentiality, integrity, availability) and identifies that the ordering should be IAC because that is most often the real priority. The argument goes (approximately) If it gives wrong answers, it doesn't matter that it's available or secret, if it isn't working, it doesn't perform a useful purpose, and thus, for most purposes, secrecy is less important.

F. Cohen, 1997 - The Cracking Game

A software product that simulated methods used by attackers and allows users to learn about computer security issues by playing the game. Available for remote use on all.net

F. Cohen, 1997 - Automated Threat, Attack, and Defense Analysis Tool

A software product that analyzes and simulates attack and defense relating to information systems and networks. Available for remote use on all.net

1996

F. Cohen, "A Note on Distributed Coordinated Attacks", IFIP-TC11, `Computers and Security', Volume 15, Number 2, 1996, pp. 103-121(19), also appearing as an invited paper in 4th Computer Misuse and Anomaly Detection Workshop, Monterey, 1996 (referenced below).

In this paper, we describe a new class of highly distributed coordinated attacks and methods used for tracking down their sources. These are the generic class of attacks of which distributed denial of service attacks, botnets, and many other similar methods in use today fall.

F. Cohen, "A Secure World-Wide-Web daemon", IFIP-TC11, `Computers and Security', V15#8, 1996, pp. 707-724(18)

In this paper, we begin by discussing some of the protection-related history of world-wide-web servers and clients, some of their better-known vulnerabilities, and the need for a more secure server environment. We then discuss the protection goals we believe to be of import to a world-wide-web server, outline some of the principles we believe to be important to attaining such a server, and analyze the design of a server that we believe to be secure relative to our stated goals. Finally, we discuss some of the experience we have had with this server, the development of a secure gopher server using nearly the same code, and future work. This server was subsequently proven mathematically to meet the specifications and has withstood continuous attacks and acted as a Web server since that time without alteration. It was intended to show a different approach (using limited function, redundant storage, non-allocation after startup, minimal code, and input length and string limitation) to building a Web server.

F. Cohen, "A Note on Distributed Coordinated Attacks", 4th Computer Misuse and Anomaly Detection Workshop, Monterey, 1996 (also appearing above in Computers and Security, 1996).

This article identifies distributed coordinated attacks (DCAs) for the first time in a scientific publication, and discusses methods and limits on tracking DCAs to sources, identifies different modes in which they can be exploited, and discusses issues associated with defenses. Subsets of DCAs include modern "botnets" and distributed denial of service (DDoS) attacks.

F. Cohen, S. Cooper, et. al. "Intrusion Detection and Response", National InfoSec Technical Baseline, October, 1996. (Also appearing in SecureNet 97, March, 1997 and Computers and Security as cited above)

This is the first national technical baseline study performed by the National Infosec Technical Counsel.

F. Cohen, "Managing Network Security: Where Should We Concentrate Protection?", Network Security, Dec., 1996.

This article ends: "It is often hard to see the big picture in a big company, but in the case of information protection, only the big picture leads to cost effective results. Our brief overview of different sorts of networked systems demonstrated a wide range of possibilities, but the devil is in the details. Cost effective protection in today's networked environments requires a balance that can only be achieved through careful and detailed analysis of the systems as the operate within their environment."

F. Cohen, "Managing Network Security: How Good Do You Have to Be?", Network Security, Nov., 1996.

This article discusses the competitive nature of information protection and identifies the extent to which it is a competitive game.

F. Cohen, "Managing Network Security: Why Bother?", Network Security, Oct., 1996.

This is the first article in this series, and it argues that lax protection may be effective protection in some cases. In the end it is an article about balance.

F. Cohen, "Internet Holes - The SYN Flood", Network Security, Sep., 1996.

This is the last article in this series. It discusses the SYN flood attack on the TCP protocol and how it may be defeated with timeouts and other methods.

F. Cohen, "Internet Holes - Internet Incident Response", Network Security, Aug., 1996.

This article discusses incident response in the Internet environment and how collaboration is a requirement.

F. Cohen, "Internet Holes - Internet Lightning Rods", Network Security, July, 1996.

This article discusses how the all.net Internet domain acted as a lightning rod to attract attackers and the perils and benefits of having such systems.

F. Cohen, "Internet Holes - UDP Viruses", Network Security, June, 1996.

This article describes UDP viruses and identifies the effectiveness of single datagram viruses such as the “echo” port virus in taking down systems and infrastructures. It identifies the obvious need to not leave such services enabled or to limit their potential for exploitation with firewalls or other similar measures.

F. Cohen, "Internet Holes - Eliminating IP Address Forgery", Network Security, May, 1996.

This article discusses the issues of IP address forgery and identifies a specific set of protective settings for routers and gateways that essentially eliminated this problem. These settings were subsequently adopted by the CMU-CERT after this article was provided to them and became a widely accepted approach, even though it still isn't universally applied.

F. Cohen, "Internet Holes - Spam", Network Security,April , 1996.

This article discusses the challenges of spam in the Internet and identifies approaches to defeat it.

F. Cohen, "Internet Holes - The Human Element", Network Security, March, 1996.

This article includes such things as: “Perhaps the biggest Internet hole of all is the fact that when an incident is detected, there's no uniform or enforceable way to track down attackers and punish them.” and “There's an old saying about computer crime that goes something like this: The likelihood of getting detected is 1 in 100. If detected, the likelihood of getting caught is 1 in 50. If caught, the chances of being arrested are 1 in 10. If arrested, the chances of going to trial are 1 in 10. If you go to trial, the chances of being found guilty are 1 in 3. The average sentence is community service. If this is true, the risk is 1 in 1.5 million of being punished. We've done our part by cutting this down to 1 in 15,000. Now if we could only get everyone else to do their part, we could win this thing.”

F. Cohen, "Internet Holes - Automated Attack and Defense", Network Security, February, 1996.

This article ends (in part) “Automated attack tools appear to present a substantial threat to the Internet environment. If more than half of all Internet-based computers are vulnerable to attack by a few widely available automated tools, how can we help but be concerned about the existence of these tools? … Ultimately, the solution to automated attack tools is proper defenses. There are many effective defenses available today, but as a community, the people using the Internet have simply failed to use them. If we use the defenses available to us, we can be safe from all but the newest and most sophisticated threats, but as long as we refuse to take appropriate protective action, we will be vulnerable.”

F. Cohen, "Internet Holes - 50 Ways to Attack Your World Wide Web Systems", Network Security, December, 1995 - January, 1996.

This is the first article in the 50-ways series. It was written in response to a challenge that asserted it would pay $1,000 for each hole identified in Netscape. I am still awaiting my $50,000.

F. Cohen, 1996 - CID Database Analysis Tool

A software product that allows for automated analysis of attack and defense strategies relating to computer networks and systems. Available for remote execution on all.net

1995

Protection and Security on the Information Superhighway , John Wiley and Sons (1995)

This book overviews the issues of Internet attack and defense and provides the first widely published description of information protection posture assessments with examples.

F. Cohen, "The Internet, ..., and Information Security", Computer Society of South Africa, 7th Annual Conference, August, 1995, South Africa.

F. Cohen, "The Internet, Corporate Networks, and Firewalls", Computer Society of South Africa, 7th Annual Conference, August, 1995, South Africa.

F. Cohen, "Information Assurance", IFIP TC-11 World Congress, May, 1995, Cape Town, South Africa.

F. Cohen, "Internet Holes - Network News Transfer Protocol ", Network Security, November, 1995.

This article examines the network news transfer protocol and identifies various attack methods that can exploit that protocol.

F. Cohen, "Internet Holes – The Sendmail Maelstrom", Network Security, October, 1995.

This article discusses various attacks against sendmail in particular and the port 25 SMTP service in general.

F. Cohen, "Internet Holes - Packet Fragmentation Attacks", Network Security, September, 1995.

This article discusses packet fragmentation attacks, how they can be used to bypass protective mechanisms like firewalls, and what to do about it.

F. Cohen, "Internet Holes - Internet Control Message Protocol", Network Security, August, 1995.

This is the first article in this series. It discusses the Internet Control Message Protocol (ICMP), how it can be exploited, and what to do about it. It also introduces “Fred's First Law of Attacking Computers: Lie - chances are they'll believe you.”

F. Cohen, 1995 - Auditor - Internal Audit Tool

A software product to automate aspects of internal technical audits for computer security configuration.

F. Cohen, 1995 - Analyzer - Network Audit Tool

A software product to automate aspects of external technical audits for computer security configuration.

F. Cohen, 1995 - Trivial HTTP Daemon - provably secure web server

A software product that implements a secure Web server.

F. Cohen, 1995 - Secure Gopher Server - provably secure gopher server

A software product that implements a secure Gopher server.

1994

F. Cohen, “It's Alive!!!”, John Wiley and Sons (1994)

This book examines the view of computer viruses as life forms and discusses and exemplifies the benevolent use of reproductive programs.

F. Cohen, “A Short Course in Computer Viruses (2nd edition)”, John Wiley and Sons (1994)

This book is a Wiley update of the previous book on computer viruses.

F. Cohen, "Airbag Inflator Inspection System", LumenX Corporation, November, 1994.

This describes mechanisms used to control the manufacturing process of airbag inflators.

1993

F. Cohen, "Operating Systems Protection Through Program Evolution", IFIP-TC11 `Computers and Security' (1993) V12#6 (Oct. 1993) pp.565 – 584

In this paper, we introduce the use of program evolution as a technique for defending against automated attacks on operating systems. This paper identifies methods and a methodology for altering code and content so as to eliminate generic and automatic attacks against operating systems and other software bases. It was the first paper exploring code obfuscation for this purpose and includes many of the techniques currently being researched for similar protective effect.

J. Voas, J. Payne, F. Cohen "A Model for Detecting the Existence of Software Corruption in Real-Time", IFIP-TC11 "Computers and Security", V12#3 May, 1993 pp. 275-283.

This paper examines the mathematics underlying the detection of corruption by code inspection in real-time.

F. Cohen, "`Information Warfare Considerations", Norwegian Academy of Sciences, September, 1993.

This article discusses considerations surrounding the potential for information warfare and defenses.

F. Cohen, "Some Applications of Benevolent Viruses in Networked Computing Environments", `DPMA, IEEE, ACM Computer Virus and Security Conference', March 1993

This article discusses the potential to use computer viruses for benevolent purposes.

F. Cohen, R. Knecht, C. Preston, et. al., "Planning Considerations for Defensive Information Warfare - Information Assurance", Contract DCA 100-90-C-0058 T.O. 90-SAIC-019, November, 1993.

This study was a precursor to the President's Commission on Critical Infrastructure Protection. It also first defined the term “Information Assurance” as it is used today.

F. Cohen, "Threats and Defenses for WCCS", US Air Force, Wing Command and Control System, August, 1993.

This paper details potential threats and defenses for the Wing Command and Control System

(WCCS) used at that time for command and control of air operations.

F. Cohen, "Information Warfare Considerations", National Academy of Sciences - National Research Council, September, 1993.

This short paper is intended to be a brief examination of a topic which is not yet well defined or understood. Even the term Information Warfare is not widely understood or applied, and to a certain extent, this paper may help to define it.

F. Cohen, 1993 - Calendar Supplement

A software product that supplemented calendars for Microsoft operating systems to include holidays from around the World.

1992

F. Cohen, “A Short Course on Systems Administration and Security Under Unix”, ASP Press, (1992)

This short course provides understanding of information protection issues associated with the Unix timesharing system and identifies many issues that are still present today.

F. Cohen, “Payback - Automated Bill Collection System”, ASP Press (1992)

This is the manual for the “PayBack” software system.

F. Cohen, "A Formal Definition of Computer Worms and Some Related Results", IFIP-TC11 "Computers and Security" V11#7, November, 1992, pp. 641-652.

In this paper, we propose a formal definition of ‘Computer Worms’ and discuss some of their properties. We begin by reviewing the formal definition of ‘Computer Viruses’, and their properties. We then define ‘Computer Worms’ as a subclass of viruses, and show that many of the interesting properties derived for viruses hold for worms. Finally, we summarize results, draw conclusions, and propose further work.

F. Cohen, "Defense-In-Depth Against Computer Viruses", IFIP-TC11 "Computers and Security", V11#6, 1992 pp. 563-579.

In this paper, we discuss software based fault tolerant computing techniques used in defense against computer viruses and other integrity corruptions in modern computer systems. We begin with a summary of research on computer viruses, their potential for harm, and the extent to which this potential has been realized to date. We then examine major results on the application of fault tolerant software techniques for virus defense, including; the problems with conventional coding schemes in detecting intentional corruptions and the use of high performance cryptographic checksums for reliable detection; an optimal method for detecting viruses and preventing their further spread in untrusted computing environments; the use of redundancy and automated decision making for automatic and transparent repair of corruption and continuity of operation; and the use of fault avoidance techniques for limiting viral spread. Next we discuss the state-of-the-art in virus defense, its use of redundancy for defense-in-depth, the impact of this on the reliability of the mechanism, the implications of these results to other computing environments, and architectural issues in implementing hardware assisted virus defense based on the software fault tolerance techniques already in widespread use. Finally we summarize results, draw conclusions, and discuss further work.

F. Cohen and S. Mishra, "Some Initial Results From the QUT Virus Research Network", `The Virus Bulletin Conference', Edinburgh, Scotland, July, 1992 (keynote).

This describes some initial results from efforts at Queensland University of Technology in studying computer viruses and defenses.

F. Cohen, "Computer Viruses", (one chapter in "The Computer Security Reference Book" Butterworth/Heinemann (1992), Oxford, England

F. Cohen, "A Case for Benevolent Viruses" DPMA, IEEE, ACM Computer Virus and Security Conference, March 1992

In recent months, a controversy has arisen in the electronic and print media as to the viability of benevolent computer viruses and the morality of a contest to find useful applications of this technology. In this paper, we discuss the issues related to applying computer viruses for good instead of evil. We begin with some background on viruses and related topics in ‘life-like’ computational organisms. Next we examine some of the ma jor problems facing the current global computing environment and how viruses have the potential for helping to solve these problems. We then consider several widely stated arguments against the application of computer viruses for useful purposes and provide counterpoints.

F. Cohen, "Current Best Practice Against Computer Viruses with Examples from the DOS Operating System", DPMA, IEEE, ACM Computer Virus and Security Conference, March 1992

This describes the best available defenses against computer viruses of the day.

F. Cohen, 1992 - PayBack Automated Bill Collection Software

A software product to automate tracking and actions for the collection of bills for small companies.

1991

F. Cohen, "A Short Course in Computer Viruses", ASP Press (1991)

This book combines the various published works and lectures on computer viruses into a comprehensive short course.

F. Cohen, "A DOS Based POset Implementation", IFIP-TC11 "Computers and Security", V10#6, October 1991.

In this paper, we describe and discuss a DOS based POset (i.e. Partially Ordered Set) implementation. We begin with a short review of previous results on POset based protection. We then describe implementation details of POset based protection under DOS. Next we discuss management tools used to implement and control the protection system. Then we describe the problems encountered in integration into existing DOS environments and how automation is used to resolve these problems and keep management complexity low. Finally, we summarize results, draw conclusions, and describe further work.

F. Cohen, "A Note On High Integrity PC Bootstrapping", IFIP-TC11 "Computers and Security", V10#6, October 1991.

In this paper, we describe two techniques for assuring a high integrity startup in a PC based computing environment. We begin with background information on PC startup procedures and current integrity threats against normal PC startup. We then describe a sound technique for assuring a high integrity startup and the basis for its soundness. Next we show a second method which is not sound, but which works well against attacks not specifically directed against this defense.

F. Cohen, "A Cost Analysis of Typical Computer Viruses and Defenses", IFIP-TC11 "Computers and Security", V10#3, May, 1991 (also appearing in 4th DPMA, IEEE, ACM Computer Virus and Security Conference, 1991)

Various properties of computer viruses have been studied at length by many authors [1], but one of the areas where research results are relatively rare is evaluation of the costs of defenses. In this paper, we explore the costs of computer virus defenses in typical computing environments.

F. Cohen, "Fault Tolerant Software for Computer Virus Defense", November, 1991.

In this paper, we discuss the use of fault tolerant software techniques used in defense against computer viruses and other integrity corruptions in modern computer systems. We begin with a summary of research summaries on computer viruses, their potential for harm, and the extent to which this potential has been realized to date. We then examine major results on the application of fault tolerant software techniques for virus defense, including; the problems with conventional coding schemes in detecting intentional corruptions and the use of high performance cryptographic checksums for reliable detection; an optimal method for detecting viruses and preventing their further spread in untrusted computing environments; the use of redundancy and automated decision making for automatic and transparent repair of corruption and continuity of operation; and the use of fault avoidance techniques for limiting viral spread. Next we summarize several years of real-world results on the application of these techniques in DOS and UNIX computing environments, the implications of these results to other computing environments, and architectural issues in implementing hardware assisted virus defense based on the software fault tolerance techniques already in widespread use. (incomplete but published online)

F. Cohen, "Current Trends in Computer Viruses", Invited Paper, International Symposium on Information Security, Oct. 17-18, 1991, Tokyo, Japan

This paper summarized research results in computer virus defenses to that date.

F. Cohen, "Current Best Practice Against Computer Viruses", Invited Paper, 1991, 25th IEEE International Carnahan Conference on Security Technology, Oct. 1-3, 1991, Taiwan ROC.

This paper summarized research results in computer virus defenses to that date.

F. Cohen, "Exploiting Defense-In-Depth Against Computer Viruses", Invited Paper, The Oxbridge Sessions, Sept. 3-5, 1991, The Netherlands.

This paper described the potential for the use of increased redundancy for computer virus defense.

1990

F. Cohen, "The ASP Integrity Toolkit", ASP Press (1990)

This is the user manual for Integrity ToolKit – an early integrity-based product for protecting personal computers against corruptions of all sorts, including computer viruses.

F. Cohen, "Automated Integrity Maintenance for Viral Defense", IFIP-TC11 "Computers and Security", 1990

This paper discusses the use of automated mechanisms for integrity protection as a viral defense technique.

F. Cohen, "Computers Under Attack" (one paper), ACM/Addison Wesley (1990)

This book chapter summarized research results in computer viruses and defenses to that date.

F. Cohen, "A Summary of Results on Computer Viruses and Defenses", Invited Paper, 1990 NIST/DOD Conference on Computer Security.

This paper summarized research results in computer viruses and defenses to that date.

F. Cohen, "Integrity Maintenance in Untrusted Computing Environments", Invited Paper, IBC Computer Virus Conference, London, 1990.

This paper summarized research results in integrity maintenance for untrusted computer systems to that date.

F. Cohen, "Recent Advances in Integrity Maintenance in Untrusted Systems", Invited Paper, The Netherlands Computer Security Seminar, April 10-12, 1990.

This paper summarized research results in integrity maintenance for untrusted computer systems to that date.

F. Cohen, "A Note on the use of Pattern Matching in Computer Virus Detection", Invited Paper, Computer Security Conference, London, England, Oct 11-13, 1989, also appearing in DPMA, IEEE, ACM Computer Virus Clinic, 1990.

This paper described the limitations of pattern matching for detection of computer viruses.

1989

F. Cohen, "Computational Aspects of Computer Viruses", IFIP-TC11, "Computers and Security", V8 pp325-344, 1989.

This paper details the results from the 1986 dissertation on computational aspects of computer viruses and viral sets.

Y. J. Huang and F. Cohen, "Some Weak Points of One Fast Cryptographic Checksum Algorithm and its Improvement", IFIP-TC11 "Computers and Security", V8#1, February, 1989

In this paper, we examine a previous fast cryptographic checksum algorithm used for maintaining the integrity of files in an information system. We find two flaws in the previous analysis in that it is possible to append information to a file and generate a new valid cryptographic checksum for the modified file, and in that it is possible to forge changes to blocks whose value is less than the modulus used in the scheme under examination. We then show how this method can be improved to eliminate these problems while still maintaining its other beneficial properties.

B. Cohen and F. Cohen, "Error Prevention at a Radon Measurement Service Laboratory", Radiation Protection Management, V6#1, pp43-47, Jan. 1989

This paper describes the use of cryptographic methods and other protections for assuring integrity of results of scientific measurements.

F. Cohen, "Models of Practical Defenses Against Computer Viruses", IFIP-TC11, "Computers and Security", V8#2, April, 1989 pp149-160.

In this paper, we model complexity based virus detection mechanisms which detect modifications and thereby prevent computer viruses from causing secondary infections. We use these models to show how to protect information in both trusted and untrusted computing bases, show the optimality of these mechanisms, and discuss some of their features. The models indicate that we can cover changes at all levels of interpretation with a unified mechanism for describing interdependencies of information in a system, and we discuss the ramifications of this unification in some depth. This paper describes the interdependency relationships of integrity in information systems and details how trusted and untrusted systems can be operated so as to recursively detect and correct corruption. It identified integrity shells as an optimal solution for integrity protection in an untrusted system and provides the basis for the development of trusted computing group trusted platform modules that came more than 17 years later.

F. Cohen, "Computer Viruses - Attacks and Defensive Measures", London Corporate Computer Security Conference - Keynote Address, London, England, Feb. 14, 1989.

F. Cohen, 1989 - Integrity ToolKit - Integrity Shell and Access Control System

A software product for virus defense, integrity protection, access control, and related security measures on personal computers. This product included many / most of the technologies identified in related published papers.

F. Cohen, 1988 - Advanced Software Protection Scanner - Virus Scanner

This software product was a simple early virus detection system based on scanning technology.

1988

F. Cohen, "Two Secure Network File Servers", IFIP-TC11, "Computers and Security", V7#4, August, 1988.

In this paper, we describe the design and implementation of a two secure file servers which allow a trusted computer network to be built from untrusted computing bases. We begin with a brief review of recent results in the use of partial orderings for protection and administration of information networks, and introduce limited functionality TCB file servers as a means for allowing restricted information flow. We show the means by which such a server may be made provably secure, consider the practicality of implementation, and describe two prototype implementations for personal computers. We then summarize results and point out possible extensions of this work.

F. Cohen, "Designing Provably Correct Information Networks with Digital Diodes", IFIP-TC11, "Computers and Security", V7#3, June, 1988.

In this paper, we extend previous results in the design and administration of information networks under partial orderings [1] by introducing a 'digital diode' which can be used as a basic component in the control of information flow. We summarize previous results, and introduce the digital diode as the only necessary component in a general purpose flow control network. We show that with this component, we can build any desired POset network and show its information flow properties. We show a design for a digital diode, show it's correctness, show that any desired reliability of transmission can be attained, and show that no covert channels are present. We then show variations of this scheme with well defined and easily limited covert channels that allow end to end confirmation. We show means by which audit trails may be generated, cryptographic security may be provided, and automated administrative assistance may be made available for the administrator of the plugboard. We summarize results, make conclusions, and propose further work.

F. Cohen, "On the Implications of Computer Viruses and Methods of Defense", Invited Paper, IFIP-TC11, "Computers and Security", V7#2, April, 1988,

In this paper, we describe much of the previous and present work on computer viruses. We begin with a short history and bibliographic summary. We then describe some of the major issues that arise in the study of computer viruses and their protection ramifications. We describe most of the lines of research presently under way and some of their features and failings. We introduce a method by which certain classes of systems may be used in such a manner as to provide limited protection from computer viruses, and by which general purpose experiments in new protection mechanisms may be explored. Finally, we point out some of the social issues implied by viruses and the ramifications of our present social policies on the integrity of information residing in information systems.

F. Cohen, "Maintaining a Poor Person's Information Integrity", IFIP-TC11, "Computers and Security", V7#1, Feb 1988.

This describes a set of methods by which little or no resources may be applied while affording effective integrity protection for individuals using personal computers.

F. Cohen, "Current Trends in Computer Virus Research", 2nd Annual Invited Symp. on Computer Viruses - Keynote Address, Oct. 10, 1988. New York, NY

This paper summarized research results in computer viruses and defenses to that date.

F. Cohen, "Recovery Techniques in Computer Virus Attack", Invited Paper, Invitational Conference on Computer Viruses, 1988.

This paper discusses recovery methods for situations in which a virus has successfully penetrated a system and the limitations of recovery based on the potential for otherwise undetected corruption of systems and backups.

1987

F. Cohen, “Introductory Information Protection”, ASP Press (1987)

This book is an introduction to information protection as the issues existed at the time of publication. While many of these issues persist today, many things have changed since then.

F. Cohen, "A Cryptographic Checksum for Integrity Protection", IFIP-TC11 "Computers and Security", V6#6 (Dec. 1987), pp 505-810.

This paper describes a cryptographic checksum technique for verifying the integrity of information in computer systems with no built-in protection. The technique is based on the use of repeated encryption using an RSA cryptosystem as a pseudo-random number generator (PRNG), the use of a user specified key as a seed for the PRNG, and reduction in a pseudo-random modulus as a means for mixing user specified information with generated numbers.

F. Cohen, "Design and Protection of an Information Network Under a Partial Ordering: A Case Study", IFIP-

TC11, "Computers and Security", V6#4 (Aug. 1987) pp 332-338.

This is a case study using a POset structure for implementing trusted computing and limiting transitive information flow.

F. Cohen, "Design and Administration of Distributed and Hierarchical Information Networks Under Partial Orderings", IFIP-TC11, "Computers and Security", V6#3 (June 1987), pp 219-228.

In this paper, we extend previous results [1] in the protection and administration of information networks under partial orderings. We summarize previous results, and extend them to cover hierarchical networks. We consider distributed hierarchical administration, show a hierarchical network, and demonstrate a provably secure communications technique in which partial orderings are used to control flow, traffic analysis is minimized, local compromise does not cause global compromise, and distributed hierarchical administration works. We show means by which trusted and untrusted computing bases may be connected to form provably secure distributed information networks under partial orderings, and a risk analysis technique which takes advantage of the POset structure to reduce the complexity of analysis for these networks. We, summarize results and propose further extensions of this work.

F. Cohen, "Protection and Administration of Information Networks with Partial Orderings", IFIP-TC11, "Computers and Security", V6#2 (April 1987) pp 118-128.

In this paper, we examine the effect of combined security and integrity on information flow in a computer system or network. We trivially extend integrity levels to integrity lattices, and show that the combination of security and integrity lattices results in a partitioning of systems into closed subsets under transitivity. We generalize the integrity and security lattices to a simpler flow model, demonstrate some common pitfalls in administration of such systems, and show that the most general structure required for representing information flow in a general purpose transitive information system is a partial ordering. We show means for calculating information effects under this model, demonstrate sample calculations, and explore the effects of time on proper maintenance of controls. We then explain the design of an automated administrative assistant for protection administration in systems and networks under this model and introduce a provable rule based system for maintaining security, integrity, compartments, and other flow restrictions in administration of a flow control matrix.

F. Cohen, "Computer Viruses - Theory and Experiments", DOD/NBS 7th Conference on Computer Security, originally appearing in IFIP-sec 84, also appearing as invited paper in IFIP-TC11, "Computers and Security", V6#1 (Jan. 1987), pp 22-35 and other publications in several languages.

This is the first scientific paper written on computer viruses and defenses and their limits.

F. Cohen, M. Breuer, "A Roving Emulator", Conference on Modeling and Simulation, April, 1987.

This paper details the design of a new built-in test methodology for detecting and locating faults in digital systems. The technique is called roving emulation and consists of an off-line snap shot type emulation or simulation of operating components in a system. Its primary application is in testing systems in the field where real-time fault detection is not required. It is based on and is a relatively minor contribution to the work of M.A. Breuer, and A.A. Ismaeel in this area.

F. Cohen, 1987 - Advanced Software Protection - Crypto-Checksum Integrity Checker

This was an early automated tool for checking DOS-based systems for changes using cryptographic checksums.

F. Cohen, 1987 - TRP - Small business office software

This was small business office software.

1986

F. Cohen, "Information Protection", Curriculum Module for the graduate degree in Software Engineering, The Software Engineering Institute, June, 1986, also appearing in ACM SIGSAC in abbreviated form.

This was an early curriculum developed for information security.

F. Cohen, "A Complexity Based Integrity Maintenance Mechanism", Conference on Information Sciences and Systems, Princeton University, March 1986.

This paper addresses the problem of detecting integrity corruption in a system without "built-in" protection mechanisms. Since no built-in protection is provided, it is incumbent on the programs and data within the system to protect themselves. Any protection mechanism not based on making violations very complex may be trivially attacked, so a complexity based mechanism is desired.

F. Cohen, “Computer Viruses”,

Dissertation formally accepted.

F. Cohen, 1986 - VCE - Viral Computing Environment

This software implemented a viral computing environment in which computer viruses could safely execute next to non-viral software for automated maintenance purposes.

1985

F. Cohen, “Computer Viruses”, ASP Press, (1985)

This is the first serious book on computer viruses, the published version of Fred Cohen's Ph.D. dissertation on the subject.

F. Cohen, "A Secure Computer Network Design", IFIP-TC11, "Computers and Security", V4#3, (Sept. 1985), pp 189-205, also appearing in AFCEA Symp. and Expo. on Physical and Electronic Security, Aug. 1985.

This paper investigates fundamental issues in the design of computer networks capable of protecting information from illicit dissemination and modification. We examine networks with trusted and untrusted communications lines and develop a set of easily applied design rules for the connection of computers to form secure computer networks. Protocols that maintain security conditions are shown, covert channels and traffic analysis are examined, and a ‘good enough’ cryptosystem is shown to fulfill all of the network security and protocol requirements. Some attacks against these networks are analyzed for their effect, conclusions are presented, and future research is outlined.

F. Cohen, "Algorithmic Authentication of Identification", Information Age, V7#1 (Jan. 1985), pp 35-41.

This paper identifies a method os using something a person can do (as opposed to something they are, have, or know) as a method for authentication.

F. Cohen, "Recent Results in Computer Viruses", Conference on Information Sciences and Systems, Johns Hopkins University, March 1985.

This paper summarized research results in computer viruses and defenses to that date.

F. Cohen, 1985 - Legal Assistant - Law Office Software

This software automated many aspects of running a law office in the collection and general practice law areas.

1984

F. Cohen, "The HAD Cryptosystem", IACR Crypto84 rump session, Aug. 1984.

This short piece identifies the need for compression for all encryption systems and shows a trivial encryption system based on ideal compression.

F. Cohen, "Computer Security Methods and Systems", Conference on Information Sciences and Systems, Princeton University, March 1984.

This paper discusses methods and systems for computer security.

1983

F. Cohen, "Learning Networks for Database Access", Yale Conference on Adaptive Systems Theory, New Haven, CT, June, 1983.

This paper describes a method in which the computer automatically tries to complete database queries based on historical data from user behaviors.

M.A. Breuer, F. Cohen, and A.A. Ismaeel, "Roving Emulation", Built-In Self-Test Conference, March 1983.

This paper describes the technique of roving emulation.

F. Cohen, "The Delta-Net Model of Computation", Conference on Information Sciences and Systems, Johns Hopkins University, March 1983.

This paper describes a model of computation based on petri nets but with a differential approach.

1982

F. Cohen, "The U.S.C. Roving Emulator Engine", U.S.C. DISC Report #82-8, Dept of Electrical Engineering, University Park, LA, Ca. 90089-0781, Dec. 1982.

This was in internal report on the technical implementation of the USC roving emulator.

M.A. Breuer, F. Cohen, A.A. Ismaeel, "Roving Emulation as Applied to a (255,223) RS-encoder System", U.S.C. DISC Report #82-6, Dec. 1982.

This was in internal USC report on an application of roving emulation to a particular system.