Quis Custodiet ipsos Custodes? A New Paradigm for Analyzing Security Paradigms

With appreciation to the Roman poet Juvenal.

Panel Chair/Editor: Sean Peisert

Sean Peisert
UC Davis and LBNL
peisert@cs.ucdavis.edu

Matt Bishop
UC Davis
bishop@cs.ucdavis.edu

Laura Corriss
Barry University
mcorriss@mail.barry.edu

Steven J. Greenwald
Independent Consultant
sjg6@gate.net

ABSTRACT

We believe in the existence of more than one single security paradigm. We also believe that until we find a way to identify and understand these multi-paradigms, we will never have the ability to identify and thus confront and protect ourselves from the risks and threats from the outside and the inside. We believe that a majority of people working in the security community work within one paradigm without recognizing that constraint. The paradigm in which they work may shift or even expand based on new data and experiences, but it still limits their approaches and analyses.

Therefore, at NSPW 2009, we presented, as a mechanism for the workshop processes, a computer security problem caused by the composition of multiple paradigms and that can only get resolved by a shift in focus or mindset to reflect those paradigm compositions. This panel was designed to take full advantage of the unique NSPW workshop process by studying and "workshopping" our multi-paradigm composition analysis paradigm. Our hypothesis was that this type of radical panel approach at NSPW would work as the best way to further elucidate the issues, refine the approach, create awareness of the problem, and potentially solve this problem (or at least ensure we take the right approach).

Therefore, we decided to present a situation that demonstrates the restricting universe of discourse of each security paradigm and what happens with the resulting inadvertent and invisible multi-paradigm composition. Our panel investigated, through a live exploration, how individuals in the security community work in different paradigms without any awareness of that. Our panel delved into this issue more deeply by presenting a scenario followed by the usual NSPW interactive process. Initially our hope, and ultimately, our conclusion, is that this resulted in a method for elucidating the new, composed, paradigm by illustrating, among other things, the misunderstanding and non-comprehension of people due to the inadvertent composition of differing universes of discourse.

1. INTRODUCTION AND PROBLEM STATEMENT

We believe that no single security paradigm exists.

We also believe that until we find a way to identify and understand these multi-paradigms, we will never have the ability to identify and thus confront and protect ourselves from the risks and threats from the outside and the inside.

Our panel investigated, through a live exploration, that individuals in the security community work in different paradigms without any awareness of that. We showed how individuals' mindsets affect more than just communications. The security community's biggest problem is that we cannot identify the proper risks because we cannot even *conceive* of the possibilities. They reside outside out world view. For now.

1.1 Concept

We all recognize that new paradigms form the basis for NSPW. We have lately realized that we all might profit greatly by questioning the role and nature of security paradigms themselves and especially the way in which multiple security paradigms *compose*. We also think that we have come up with a new security paradigm and analysis method that attendees will find not only highly intriguing, but also very surprising and that they will certainly wish to explore. We will challenge not only the *status quo ante* but the entire idea of a *status quo ante* in security paradigms. We believe this because we question nothing less than *the role and nature of security paradigms themselves*. Combined with the usual spirited discussion that occurs at NSPW, we have no doubt at all that this will result in a very productive and very interesting panel for all concerned.

1.2 The New Paradigm for Analyzing Multi-Paradigm Composition

Hypothesis: Even within the same organization different and conflicting security paradigms cause different mindsets that cause different interpretations and foci resulting in a situation where the res-

olution of security problems can be extremely difficult if not impossible.

Simply put, the composition of multiple security paradigms causes the above problems. Worse yet, most organizations do not even realize that they compose different security paradigms.

We believe in the existences of more than one security paradigm but we also believe that the majority of people working in the security community only ever work within one paradigm. The paradigm in which they work may shift or even expand based on new data and experiences but it still limits them.

We therefore presented, as a mechanism for the workshop processes, a computer security problem caused by the composition of multiple paradigms and that can only get resolved by a shift in focus or mindset to reflect those paradigm compositions or that gets resolved by somebody outside of the computer security community (or thinking that way) because it required a paradigm shift to reflect multi-paradigm compositions or a *shift in focus or mindset*. We demonstrated that in the security community, despite all our talk of changing paradigms or introducing new paradigms, we really have only one current paradigm (per person) with which most security people work, even if that paradigm may shift a bit. We believe that a lot of our current threats come from outside the security community and therefore outside our current paradigms and that this means that our mindsets cannot even consider the risks and possibilities they introduce. We will not solve these problems until we understand the other paradigms in which other people work. We therefore need to find a way to understand them and to change our mindset.

Because of this, we decided to present a situation that demonstrates the restricting universe of discourse of each security paradigm and what happens with the resulting *inadvertent* and *invisible* multi-paradigm composition.

We assert that we need to study these things, and we also assert that we need a new paradigm in which to do it. Our paradigm has its roots in multi-paradigm commissions, such as the work done by the Rogers Commission [5] that investigated the Space Shuttle *Challenger* Accident in 1985–1987. The commission was chaired by a former secretary of state and attorney general, and consisted also of a former astronaut, multiple engineers, an astronomer, a publisher of a space-related magazine, a test pilot and, of course, Nobel Prize winning physicist Richard P. Feynman, among others. One could argue that it succeeded due to only Feynman himself, who famously demonstrated the cause of the accident before Congress with a piece of rubber and a glass of ice water [6], and whose own (highly regarded) recommendations were denied a place in the report, but allowed (under duress) as an appendix [7]. We feel this argument has a lot of merit, but we also argue that Feynman's role was a sufficient condition for success, but not a necessary one. We argue that the real strength of the panel was its composition of people with such hugely different *paradigms* of thinking and behaving. Thus, we demonstrated that a panel similarly constructed with different *paradigms*—itself a new, or rarely used paradigm—can be similarly successful when used to investigate/solve security problems. Further, this method has had success in other contexts, too.

For example, Marv Schaefer (who worked with us on this panel), worked at a commissioner for NORAD (North American Aerospace Defense command). One of NORAD's systems was supposed to send status messages to every Air Force base in the country. The system caused too many false alarms, resulting in the procedural error of operators at the various bases turning off their local alarm after they found that the system still seemed to work without the alarms. A commission was put together to study the problem with the false alarms. After several false starts with only "impossible" situations remaining, one engineer, acting in frustration, slammed his hand down on one of the black boxes in question and caused the error by accident. The commission eventually determined that multiple factors from different paradigms caused the false alarms, including bad hardware, a mathematically weak checksum algorithm, and weak protocols (specifically, only $1/8^{th}$ of the valid packets would get through without an alarm). Further, weak procedures (e.g., turning off the alarms) exacerbated the problem. A null hypothesis failed twice using a multi-paradigm group of statisticians, mathematicians, computer security experts, electrical engineers, communications security people and protocol people, radar engineers, military folks in command and control, etc.

We could cite other examples, of course.

Thus, this method has worked successfully, but not one has ever explicitly articulated it before, nor has it been proposed as a general technique for analyzing security problems. *Thus, we tested this theory live, in person, at NSPW.*

In this paper, we discuss background work in this area, present a scenario that we role-played at NSPW, and discuss what we learned about the multi-paradigm analysis process. In the original panel proposal, we did not present the application of the panelists' paradigms to the scenarios in this proposal, as we believed that the application and discussion should happen live and at the workshop rather than having the workshop merely be a rehash of this proposal; in fact, we believed presenting the material prematurely would work as counter-productive. In this paper, we reveal the paradigms and scenario.

2. BACKGROUND

There are too many security problems causes by multi-paradigm composition to list in this paper. However, even within the last several month at the time of writing this, someone opened a manhole in San Jose, California, cut three cables, and took out Internet and telephone access for much of the southern Bay Area [1]. Earlier in the week, reports surfaced that much of the power infrastructure has been "owned" by computers originating in China, Russia, and North Korea [8] A few weeks ago, it was reported that a U.S. Circuit judge and election officials have been manipulating the votes cast on electronic voting machines for years [3]. The Conficker worm has morphed yet again [10].

Managers, politicians, academics, and the public look to computer security professionals to solve these problems. But the problems continue to re-occur. In light of this, how can we continue to trust trust [15]?

Perhaps a new model is necessary for preventing, understanding, identifying, and correcting security problems. In this paper, we propose one. The model is not simply that we need more "secure programming" (though we agree that we do), but a notion of how systems (insecure or not) are understood, used, woven together, maintained, and ultimately made more secure.

Computer scientists spend large amounts of time understanding how computers function in the real world. With the additional multidisciplinary expertise, such as psychology, computer scientists have extended their studies to understanding how how end users operate computers, as well as how computer programmers function via empirical studies [14] of N-version programming [11], "extreme" programming [2], and the *Mythical Man Month* [4]. Specifically with regard to computer security, computer scientists have also studied the efficacy of security software [12]. One question that computer scientists have barely touched on is: how do computer security professionals work? More specifically, how do they work together to solve problems? For example, consider "red teams" of penetration testers: when are more people in a team (or more

teams) effective at finding new things, and when are they finding different things? One of the last links in the chain that has received almost no attention is the security professional. More broadly, when do they succeed, when do they fail, and what assumptions do they make? How could they be made more successful?

Why is this important? Virtually all computer security relies on a human component somewhere in the chain. Whether an end-user, a corporate security administrator, a programmer at an anti-virus software vendor, or the security administrator at an ISP, all have some responsibility for and impact of security of the network and the hosts on it.

This has become particularly true with electronic voting in the United States, so we choose this as an easy-to-understand example. The Election Assistance Commission (EAC) has recently put out a set of Voluntary Voting System Guidelines (VVSG) [13] which now also consists of a National Voluntary Lab Accreditation Program (NVLAP) to verify adherence.[1] The latest VVSG also now includes a section on open-ended vulnerability testing (OEVT). But what should that section contain? How useful is open-ended penetration testing in comparison to static/dynamic system analysis? How many independent labs are necessary? What should the standards be? If there are truly useful standards, is it still open-ended?

We pose the following questions.

1. How do security professionals work?
2. When do separate red teams start finding different vulnerabilities?
3. How often do sysadmins make the same errors?
4. How often do auditors find the same things?
5. How often do forensic analysts find the same things?
6. How do failures happen, can they be fixed, and how can they be prevented?

2.1 The Specific Multi-Paradigm Composition Problem

- We have multiple security paradigms in our field.
- We have multiple risks because of these different paradigms
- Someone working in a different field cannot even conceive of another problem where someone may take advantage of a security hole because they have no awareness of the *notion* a security hole.

3. STRUCTURE OF PANEL

Our panel consists of five people with highly heterogeneous paradigms and agendas. Again, these are not just backgrounds but also interests, viewpoints, roles, and manners of thinking. For example: business-IT, academia, military/IC, and banking. These qualities combine to be different *paradigms*. Thus, our panel focused on the results coming out of applying these paradigms to an in-depth scenario and evaluating the threat issues based on their paradigms, rather than simply attempting to or seeking to take different positions on a particular topic. Our goal was to have the panelists evaluate these things based on their paradigm, and *not* to actually have the panelists solve the threat. The panel then iterated due to the cross-fertilization of multi-paradigms using a consistent set of scenarios/bases (using "bases" in the inductive sense of the term). For example, consider a scenario involving audits. How might applying a paradigm versed in *management* (both technical and processes) interact with a paradigm versed in *academia*? On the surface the two might appear to simply conflict, but how might the case be different if the parties are not major stakeholders in the outcome? Or if moderating (or interpreting) parties were also involved?

Going into this panel, the panelists all agreed that we had *no* idea what result, if any, would happen, but we all felt very strongly that NSPW would provide the perfect means to apply this approach and run what we think will turn out as a fine experiment for all in attendance. For example, by us not invoking a traditional single paradigm method, we caught the participants off-guard, and of course, anything to do with true (and new) paradigm investigation works as the "meat" of NSPW. We received questions like, "How would one use penetration testers in each person's paradigm?"

In order to explicate our thesis that we need a new security paradigm for the analysis of multi-paradigm compositions, we decided to create a fictitious, yet realistic, scenario consisting of a fictitious country named "Ministata" that has experienced a grave failure of its e-voting system. (Please see the fictitious news article and press releases in Appendix A and B that we handed out before the panel and during the panel, respectively, to provide historical background for the NSPW attendees. Please also see Appendix C for a detailed discussion on how the scenario played out.)

Finally, as a note, we believed that the effectiveness of this demonstration was based in part on the element of surprise to the audience as this allows them to come to independent conclusions even in the presence of deliberate false-leads and red-herrings that we will use for emphasis. We debated this somewhat "dramatic" approach among ourselves, and we all believed that this would work as the most effective way to get the most "bang for the buck" out of the NSPW method. Thus, the original panel proposal for this demonstration was not listed in the pre-proceedings along with the other NSPW 2009 papers.

4. WHAT WE LEARNED

Our panel delved into this issue more deeply via presentation of a scenario followed by the usual NSPW interactive process. Initially our hope, and ultimately, our conclusion, is that this resulted in a method for elucidating the new, composed, paradigm by illustrating, among other things, the misunderstanding and non-comprehension of people due to the inadvertent composition of differing universes of discourse.

The panelists, consisting of a statistician, a forensic analyst, a troubleshooter, and a management expert, all have not only very different jobs, but different paradigms. Thus, the way in which the panelists interacted was also very different.

The purpose of the panel was to evaluate, via simulation, "a new paradigm for analyzing security paradigms." We did this using scenario centered around problems with electronic voting in the made- up, but based-on-real-events "Ministata" election. Obviously a simulation is not real life. Thus, it is not possible to say "yes—this is successful!" based on our simulation. A commission or panel format is merely a demonstration of the multi-paradigm paradigm. Other such formats using the multi-paradigm approach could suffice as well. Further, we note that the *paradigm* of individuals is not the only element to study, even though it encompasses a number of important characteristics. On the other hand, there were a number of things that came out during the simulation, and the fact that there were a number of things that we learned made the panel meaningful.

[1] http://www.eac.gov/program-areas/voting-systems/test-lab-accreditation

Limits. The panel analyzed the issues, and came to interesting conclusions, but the panel can't (couldn't) answer everything.

Impact of Paradigms. Different panelists had different paradigms (obviously). There are several implications of this:

- that they have different agendas and therefore seek to reach an outcome that they personally want to see. *Personal agenda* differed highly between panelists. Malice was not be required, simply different methods, conclusions, or personal goals.
- also, because they have different goals, they focus on different to talk about what they are credible in. Though it may be tempting to talk about areas outside a given panelist's area of expertise, this is risky, and can cause them to lose credibility.
- both due to credibility issues as well as simply different interests panelists can end up talking past each other, again, either due to interest/focus or as a diversionary tactic.
- Credibility is an interesting factor: panelists may seek to maintain their own credibility and reduce the credibility of others.

5. CONCLUSION

We selected a scenario that most of us are familiar with: a close election with some shenanigans involved. This means that we did not need to orient people on the process involved in the scenario; simply on the results, and on the data that indicates questionable behavior. It was a perfect environment to bring out the differing paradigms of management (non-technical people run elections, at least in the United States), forensics (analyzing what happened both with respect to the election and to the computers), mathematics and statistics (to determine whether anything untoward is probable), and assurance (ranging from low to high). Each of these disciplines views problems very differently, and the topic allowed us to bring out these differences.

Though we genuinely did do not know what will result, we looked forward to the panel with great anticipation. Ultimately, the process helped us demonstrate and fine tune our new security paradigm for analyzing multi-paradigm compositions and we feel that we achieved positive results from the workshopping process.

Acknowledgements

All authors gratefully and wholeheartedly wish to thank a number of people who made this panel and paper possible: Marvin Schaefer, who worked with us early on to develop the ideas behind this panel; Brian Snow, who participated in the simulation; Anil Somayaji, our pre-workshop shepherd, and Christian Probst, our post-workshop shepherd, for their excellent guidance; and all of the attendees of NSPW 2009 whose participation in this experiment made it possible.

Matt Bishop was supported in part by the National Science Foundation under Grant Number CNS-0716827 to the University of California at Davis.

Sean Peisert was supported in part by the National Science Foundation under Grant Number CNS-0831002 to the University of California at Davis.

The opinions, findings, and conclusions contained in this document are those of the authors and should not be ascribed to and do not necessarily reflect the views of the funding sources of any author.

6. REFERENCES

[1] N. Asimov, R. Kim, and K. Fagan. Sabotage attacks knock out phone service. *San Francisco Chronicle*, April 10 2009.

[2] K. Beck. *Extreme Programming Explained: Embrace Change*. Addison-Wesley, 1999.

[3] M. Blaze. Is the E-Voting Honeymoon Over? `http://www.crypto.com/blog/vote_fraud_in_kentucky/`, March 23, 2009.

[4] F. P. Brooks. *The Mythical Man-Month*. Addison-Wesley Reading, MA;, 1995.

[5] R. Commission. Report of the Presidential Commission on the Space Shuttle *Challenger* Accident. `http://history.nasa.gov/rogersrep/genindex.htm`, 1986–1987.

[6] R. P. Feynman. *Why Do* You *Care What Other People Think? Further Adventures of a Curious Character*. W. W. Norton, 1988.

[7] R. P. Feynman. The Presidential Commission on the Space Shuttle Challenger Accident Report, Volume 1, Appendix F: "Personal Observations on the Reliability of the Shuttle", June 6, 1986.

[8] S. Gorman. Electricity Grid in U.S. Penetrated By Spies. *Wall Street Journal*, page A1, April 8, 2009.

[9] S. J. Greenwald and M. Schaefer. Assurance in life/nation critical endeavors: a panel. In *Proceedings of the 2002 New Security Paradigms Workshop*, pages 91–96, New York, NY, USA, September 2002. ACM.

[10] G. Keizer. Conficker cashes in, installs spam bots and scareware. *Computerworld*, 2009.

[11] J. C. Knight and N. G. Leveson. An Experimental Evaluation of The Assumption of Independence in MultiVersion Programming. *IEEE Transactions on Software Engineering*, 12(1):96–109, January 1986.

[12] J. McHugh. Testing Intrusion Detection Systems: A Critique of the 1998 and 1999 DARPA Intrusion Detection System Evaluations as Performed by the Lincoln Laboratory. *ACM Transactions on Information and System Security (TISSEC)*, 3(4):262–294, November 2000.

[13] National Institute of Standards and Technology (NIST). Voluntary Voting System Guidelines (VVSG). `http://vote.nist.gov/vvsg-report.htm`.

[14] S. Peisert and M. Bishop. How to Design Computer Security Experiments. In *Proceedings of the Fifth World Conference on Information Security Education (WISE)*, pages 141–148, West Point, NY, June 2007.

[15] K. Thompson. Reflections on Trusting Trust. *Communications of the ACM*, 27(8):761–763, August 1984.

APPENDIX A: INFORMATION HANDOUT FOR ATTENDEES

The New Ministata Times

September 8, 2009

Governor of Ministata Appoints Commission on E-Voting Disaster

By Arthur C. Lynn and Ginger Clarke, New Ministata Times staff reporters

A day after Governor Devo pledged to appoint a commission to investigate the Ministata e-voting disaster, he announced the names of the commissioners and stated that they will convene within the week.

"I have every indication that this panel of experts will get to the bottom of the situation," said Governor Devo, adding, "They have my vote of confidence."

In a shocking result, reports from the recent election for the Minstata Senate race indicate that the write-in candidate, the Flying Spaghetti Monster won with 53% of the vote. The unofficial results gave 12% of the remaining votes to Hank the Angry Drunken Dwarf, 8% for Jack Johnson, the Demopublican candidate, 8% to John Jackson, the Republicrat candidate, 8% to Free Waterfall, Jr., the Progressive Party candidate, and 8% to J.W. Booth, the Regressive Party candidate.

A spokesperson for the Ministata chapter of the Church of Flying Spaghetti Monster (http://www.venganza.org/), the reverend Sauce E. Linguini, said, "Clearly this miracle shows that Ministata has been touched by His noodly appendage. We welcome the benign guidance of the Flying Spaghetti Monster in the Ministata Senate."

Still, there were signs that showed that the citizens of Ministata continued to feel very upset and angry over the still uncertified outcome of the e-voting race, where the Flying Spaghetti Monster, a write-in candidate, seemingly won the election for senator. At a protest rally, the head of "Humans Against Dimwitted Electronic Superiority" (HADES), Spetzle Matzaball, said, "Voting forms the foundation of any democracy. If we have no faith in our voting system then we might as well not bother voting, select a good dictator, and get our money back from that stupid voting machine company."

Experts widely agree that the fact that a write-in candidate named "The Flying Spaghetti Monster" won by a landslide shows clear evidence of either vote tampering, or some other failure of Minstata's new electronic voting system.

Gil Bates, the head of Votes-R-Us, the maker of the voting system, stated, "Obviously the right and left wing forces of this country have gotten together to make a mockery of the election process. This has nothing to do with our fine voting machines."

When asked for comments, Jack Johnson, the Demopublican Party Senate candidate said, "I hail governor Devo's appointment of this commission." John Jackson, the Republicrat Party Senate candidate responded, saying, "I salute governor Devo's appointment of this commission."

Arthur C. Lynn reported from the Port of Townsville, Ministata. Ginger Clarke contributed reporting from Capitalville, Ministata.

Press Release: Biographies of the Commissioners of the Ministata Special Commission on E-Voting

Media Contact:
Ministata Office of the Governor
The Honorable Wee R. Devo

September 8, 2009

For immediate release

Governor Devo today announced his creation of the Ministata Special Commission on E-Voting, along with his appointment of the following special commissioners.

Commissioner Sean Peisert, Ph.D.

Dr. Peisert currently works as head Forensic Analyst for the Ministata Attorney General's office. He worked on the recent widely publicized debacle involving the election machines for the United Aerospace Workers union, a notorious incident where he helped prove fraud in the election of their new president. Ministata Governor Devo (then Attorney General) worked closely with him during the investigation. Dr. Peisert then briefly retired from public service while he pursued his Ph.D. on a special scholars grant from the Ministata Ministry of Education & Warfare Systems (MEWS), receiving his Ph.D. in Forensic Sciences in a record six months, and winning the Ministata Best Dissertation Award (the first recipient of the award, created by Governor Devo to encourage scholarship). His winning dissertation, "Digital Forensics: What's In It For You?" led to Governor Devo appointing him to his current position.

Dr. Peisert's bestselling novel (22 weeks on the New York Times bestseller list), "Resolving the Unexpected in Elections: Election Officials' Options," has just gotten made into a movie by Steven Spielburg, starring William Shatner, Tom Cruise, and Pamela Anderson, with a release date scheduled for early 2010.

Commissioner Matt Bishop, Ph.D.

Prof. Bishop works as a mathematician at the University of Ministata at Nyvus. During a fact-finding trip, Lieutenant-Governor Devo first met Prof. Bishop in a private high-stakes poker game at the Monte Carlo Casino in Monaco, where Prof. Bishop impressed him with his command of game theory, statistics, and his ability to draw to an inside straight.

Many experts in the field of statistics and probability widely regard Prof. Bishop as an expert in the area of the study of the mathematical modeling of voting machines and of the application of statistics and game theory to games of chance. Dr. Bishop also famously donated to charity the royalties he earned for his invention of the statistical algorithms behind the success of the AE-35, a deep space communications device.

Commissioner Steven J. Greenwald, Ph.D.

Dr. Greenwald works as CEO of Metaphysically Secure Systems Incorporated which specializes in computer security and particularly the field of Lofty Assurance (LA), which Dr. Greenwald invented during his Ph.D. work. He has worked as a security consultant to governor Devo's former Wall Street investment firm ("Soldman Gaks, LLC.").

After Colonel Greenwald retired from the Ministata Self-Defense Forces, where he commanded a special forces unit in the Ministata Lesser Icebeast Self-Defense Brigade, he founded Metaphysically Secure Systems Incorporated after inventing the field of Binary Security for multinational corporations which currently protects 87.65% of all multinational corporations. A popular media commentator, Dr. Greenwald has summed up Binary Security as, "Hey, it either works or it don't!" which has become a popular catchphrase among the public during the recent e-voting issues.

Dr. Greenwald, who, after his formation of the New Wave band Oved and high-profile whirlwind fling with Icelandic Supermodel Njørd, disclaimed any overt ties to the military industrial complex and the Ministata intelligence community during the "Don't Spit on a Fish" scandal, and announced his intention to retire from public life after a traumatic attack by an octopus, stating, "I just wish to lead a quiet life of the mind; my modesty is my best quality after all."

A mere two weeks after his retirement, Governor Devo called him out of his meditative work at his Las Vegas High Roller's Nunnery and Casino, so that he could lead the Ministata Special Forces during the Great Icebeast Stampede. During the crisis, Colonel Greenwald famously stated, in answer to a reporter's question asking if the icebeasts merely followed their usual migratory route: "Not one inch! Not one centimeter! No, not even a millimeter will we give to these smelly beasts! Let them build their own oil refineries instead of walking through ours! Have you seen the tar and goo they track around? Disgusting! We should kill them all, feed them to the ravenous octopuses, and make their hides into yerts and sell them to the Mongolians so that we can recoup the expenses of this disaster." He steadfastly maintains that he had nothing to do with the Great Icebeast Massacre (where, despite the name, only two icebeasts suffered minor injury) and that the two icebeasts got bruised while he made a special emergency investigatory trip to Monaco, stating, "Governor Devo can attest to my presence at the Monte Carlo Casino in Monaco at the time of the massacre while I performed an in-depth study of the well-known Monte Carlo statistical method by using probabilistic approaches with the goal of attempting to determine if we could possibly peacefully resolve the Great Icebeast Stampede crisis by using random techniques involving rotating wheels with tiny white spheres thrown in them. I theorized that such a system would invoke neuroanatomical anomalies and terrify the horrid beasts and scare them away. Unfortunately, the crisis ended peacefully so I could not prove my theory."

–30–

APPENDIX B: ADDITIONAL HANDOUT FOR ATTENDEES

Press Release: Additional Biography of the Commission Chair of the Ministata Special Commission on E-Voting

September 9, 2009

For immediate release

Governor Devo's office today announced a revision to the Special Commissioners that he appointed to the Ministata Special Commission on E-Voting, along with his appointment of the following special commissioners.

Commission Chairperson Laura Corriss, M.S.

Ms. Corriss, an expert business manager, currently works as Senior Vice President for Electronic Systems Audit for the firm of Pricey-Icehouse (which has no role or responsibility for the auditing of state elections). Her long record of past service to the state includes her working as the State Supervisor of Elections.

Governor Devo has praised Ms. Corriss for her knowledge of business as well as her effectiveness as a manager. During the recent Great Icebeast Stampede, many credit Ms. Corriss' crisis management as leading to a good and peaceful outcome that ultimately saved many oil refineries built on the migratory routes of the great icebeasts. Environmental groups applauded her due to her saving the lives of many of the Great Icebeasts who otherwise would have gotten killed by the Ministata Self-Defense Forces.

Ms Corriss has experience in the identification, research, and resolution of problems related to enterprise database management systems with her division providing enterprise database management system support. She has particular expertise in finance and crisis management.

Her selfless volunteer work for the Save the Icebeasts Foundation led to Governor Devo appointing Ms. Corriss as a crisis manager during the Great Icebeast Stampede, where many have credited her with restraining the Ministata Self-Defense Forces from taking too aggressive a role. However, she has received criticism from the Ministata Oil Refinery Group, a trade association, for costing the oil industry "a small fortune having to clean up after those filthy creatures tramped through our nice clean oil refineries." At the time, Ms. Corriss made a fact-finding trip to Monaco, in order to study the paleontological evidence in the Monaco Oceanographic Museum. "Many have criticized my trip, but the museum has some evidence of an extinct sea-going relative to the great icebeast which I thought had bearing on the situation."

She holds an M.S. in Computer Science and Information Systems and a B.A. in Urban Affairs. She currently works on her M.B.A., studying the role of management on the migratory patterns of icebeasts.

APPENDIX C: SCENARIO AGENDA

Scenario: Ministata Commission on E-Voting Disaster

Session 1 (Introduction)

1. We explained NSPW attendees that we have, for the purpose of the panel, a simulation in order to elucidate a new paradigm. Not everything is as it seems. Everyone can read it within the context of e-voting *or* other things. We did not reveal the multi-paradigm method up-front.
2. We introduced each of the panelists and then will explain that we present a simulation in which the governor of "Ministata" convened a special commission to look at an e-voting disaster.
3. We pointed to the pre-proceedings handout (Appendix A).

Session 2 (In Character)

1. Sean convened the commission and described the scenario.
2. We described that the election for the Minstata Senate race indicate that the write-in candidate, the Flying Spaghetti Monster won with 53% of the vote. The unofficial results gave 12% of the remaining votes to Hank the Angry Drunken Dwarf, 8% for Jack Johnson, the Demopublican candidate, 8% to John Jackson, the Republicrat candidate, 8% to Free Waterfall, Jr., the Progressive Party candidate, and 8% to J.W. Booth, the Regressive Party candidate.

3. We described that in the recent Ministata election for Senate, "The Flying Spaghetti Monster" putatively won as the write-in candidate on the DRE (electronic voting) system, demonstrating a clear technological problem. Because of this, the governor of Ministata appointed a commission to investigate this incident with goals of determining the causes, identifying who or what had responsibility, and how to prevent such things happening again.
4. We announced that the governor has appointed a commission tasked with identifying the exact problem.
5. We then announced that following an uproar about academics and techies running the commission, the governor has appointed Laura, an expert in business management, to chair the commission.
6. Laura handed out the revised handout (Appendix B).
7. Laura re-convened the commission and describes the reasons for its convention and tasks.
8. Laura state the reasons why each commissioner got selected. She mentioned that in consultation with the governor she did not include the person who selected these voting machines because of conflict of issues concerns. We provided more details in the Panelist Roles/Bios section, but in brief:
   (a) Laura represents the security management point of view and actually chairs the meeting. Laura worked as the former supervisor of elections for the state and currently works as the Senior Vice President for Electronic Systems Audit for the firm of Pricey-Icehouse.
   (b) Sean represents the digital forensic analyst point of view from the Ministata Attorney General's office.
   (c) Matt represents the academic mathematician/statistician point of view.
   (d) Steve represents the the general problem-solving point of view (assurance).
9. Laura stated the presently known facts.
   (a) The notion of a "protest vote" makes it possible (but not probable) that the write-in candidate has won.
   (b) The two major parties (the Demopubicans and the Republicrats) have challenged the results because neither has won.
   (c) The Flying Spaghetti Monster has no legal fund and therefore cannot easily stand up to a challenge.
   (d) The ballot also has one other major issue that appears unaffected (the election for the ceremonial office of Crocodile Catcher).
   (e) Most voters believe that The Flying Spaghetti Monster won by chicanery or error.
   (f) The major parties stress that they do not believe any claims that The Flying Spaghetti Monster won like Ralph Nader (e.g., as a legitimate protest vote).
   (g) Cast votes presumably get stored on flash memory cards by design.
   (h) If a voting machine crashes, some procedure must get followed. What, exactly?

Session 3 (In Character)

1. Laura called a committee meeting.
2. Things progressed in their multi-paradigm way.
3. Sean received a phone call that the FBP (Federal Bureau of Persecution, part of the Department of Fatherland Security) has discovered from one of their routine scourings of public library lending records as part of the War on Orgone, that according to their intelligence analysts, the attack almost-certainly might have possibly originated on a public-access Internet workstation at the *Wilhelm Reich Memorial Public Library* in Townsville, Ministata. Steve smiles.
4. Things continue.
5. Sean gets another phone call from the FBP that they have discovered that the *Wilhelm Reich Memorial Public Library* in Townsville, Ministata has surveillance cameras and they now examine the recordings. Steve smiles a lot, comments on the elegance of the attack, etc.
6. Things continue.
7. Sean gets a final phone call from the FBP notifying us that they have discovered *all* surveillance cameras in the *Wilhelm Reich Memorial Public Library* in Townsville, Ministata cleverly disabled—except for one, a system put in only recently as a little-known test. Steve blanches.
8. Things continue.
9. The vendor found a bug in the software used on both DREs and DRE+VVPATs. They got the fix certified, put the patch out on an unannounced web site (protected from crawlers and robots), and told the election officials to download the patch from that site, run it on the original software, and use that and use that. This was done just before the DREs were tested but after the original software was loaded (so the new software had to be reloaded).
10. A bug in the cryptography: the memory cards containing the ballots are digitally signed. First, a SHA-1 hash of the contents of the memory is computed. The resulting 160 bits are padded on the left with 0 bits to obtain 2048 bits. This is then signed using RSA. To validate, the signature is deciphered using the corresponding RSA public key, and the hash of the memory is computed. The 160 bits of the recomputed hash is compared to the low-order 160 bits of the deciphered signature; a match validates the digital signature. The error, of course, is that the high-order 1888 ($= 2048 - 160$) bits are not checked.
11. An FBP agent arrives on the scene to arrest the insider on the panel: Laura, as it turns out.
12. Things continue.
13. The DREs are compromised by Steve finding the patch on the web server and enhancing it to include the FSM. This doesn't show up on tests because the software can tell when the machine is in "test" mode. It also can compromise fleeing voter VVPAT entries. The ability of the EMS to receive data over the phone is exploited to upload a new version of the patch that changes the EMS software to report Hank the Angry Drunken Dwarf as getting 4% more votes than the Democratic candidate.
14. A second insider manipulating the election for Hank the Angry, Drunken Dwarf is identified.

Background Information

1. Each Ministata county is in charge of its own election, but all counties follow general rules laid out by the Ministata Secretary of Elections and Contributions. Each county has

a set of electronic voting machines. Some of these print paper representations of votes that a voter can visually check before casting them; others do not have paper, but display the recorded votes on the screen before the voter casts them. A paper record of the votes is called a "Voter-Verified Paper Audit Trail" (VVPAT for short). Machines with them are called "DRE+VVPAT", and machines without them are called "DRE" (for Direct Recording Electronic). Each county seat (called, in this context, "Election Central") has a Windows-based Election Management System ("EMS"), this housed at Election Central. The Secretary of State has a Master Election System used to report state totals.

2. Before each election, the DREs are updated with the latest software release. Each is then tested using a preselected ballot (the Logic and Acquisition test, or "L&A test"). Once they pass, they are sealed with tamperproof tape, and sent home with poll workers for *at most* one night. Early in the morning, the poll workers take the machines to the polling station, and set them up. The machines are not networked or connected to phone lines.
3. To vote, a voter is given a "smart card" activated by a poll worker. The voter inserts the card into the DRE. Once he voter votes, the DRE voids the card, which is returned to the poll workers. When a vote is cast, the DRE writes it to three different memories, one of which is externally removable and the other two of which are internal. The externally removable memory card is in a locked bay, and sealed with tamperproof tape. The bay is also sealed with tamperproof tape.
4. Some counties use Voter-Verified Paper Audit Trails (VVPATs).
5. At the end of the day, the poll workers shut down each DRE. The external memory with the votes is removed. One DRE is brought up in administrative mode and connected to a telephone line. The DRE then telephones the Election Management System at Election Central and reports *unofficial* results that it totaled from the cards, plus the reporting system.
6. The cards contain the official records, and are then driven to Election Central, where over the next 3 days their contents are vetted and any corrections made (for example, voiding provisional ballots or accepting them). Then final tallies are produced and reported as the official results.
7. 30% of the machines were DRE + VVPATs. All Crocodile Catcher votes on the cards matched those on the VVPAT, for those sites where audits were done. Only 5% of those races were undervotes. On those systems, the FSM was listed as a write-in on 10% of the ballots. Also, on most systems, the votes on all 3 memory cards agree; on some, the two external ones differ from the internal ones.
8. 70% of the machines were DREs without VVPATs. The Crocodile Catcher undervotes were rampant on these, and the FSM was listed on enough ballots on these to win. The memory cards show no errors.
9. In all precincts throughout Ministata, the poll workers reported crashes and having to restart the voting systems.
10. The other irregularity noted was in the race for the prestigious position of Crocodile Catcher, a hotly-contested race. Approximately 18,000 ballots were undervoted in this race.
11. We finished up. Sean summed things up, and will then revealed the multi-paradigm composition paradigm and give a brief intro to that (about 5 minutes) and that we as a group also had no idea what would result from the ensuing discussion.
12. Open-ended conclusion.

Some Mulitparadigm Ideas that the Commission Discussed

- Insider threat(s).
- Parity errors during transmissions due to a bad/naive error checking algorithm.
- Transaction problems: there is right way to do this, but inconsistency between flash cards with two cards makes it difficulty to detect which is right. Majority voting with three cards is a possible solution. For example, if there is a crash while voting, and the inconsistency is with one card, then in reality, all ballots are inconsistent if the reason is due to memory problems, etc. There can be expectations about what two cards agreeing means even if all are inconsistent. For example: what if two cards agree on one race, but not all races? (Obviously one of those cards is still suspect.) What if the cards come from the same lot numbers at the factory? What if they're different? What if the failure rates are different (they are in Florida: the primary must be 99.99% reliable and the secondary must be 99.95% reliable)? How does this affect majority voting for reading the votes? In many cases, the inconsistency may simply not be resolvable by established procedures. For example, if arbitrary test cases are used on election day during the voting process, how can it be ensured that a Trojan horse in the system does not recognize the tests as tests and therefore seemingly behave properly in order to pass (fool) the tests? Inconsistency also assumes an initial state—how can you know you're starting in the initial state? Was any of it brought up in the correct initial state? How does this impact the Basic Security Theorem (BST) of BLP?
- Need to run a known test case *in situ* to determine if everything works properly—but if we have a Trojan horse? The we cannot trust what's in the machine.
- The term"majority voting" means different things to different people. For example, assumptions by non-technical people can be quite different.
- Independent contributing causes that allowed exploitation of a security hole or leak.
- Quite possible to do it right and still get it wrong!
- The need for a strong null hypothesis $\rightarrow$ proof/disproof from people in the other disciplines.

Panelist Background (Fictitious)

The following has pertinence for the commission scenario of the panel. For actual biographical information on each of the panel participants please refer to Appendix D.

Laura Corris, M.S.. Senior Vice President for Electronic Systems Audit for the firm of Pricey-Icehouse. Laura worked as the former supervisor of elections for the state. The Governor of Ministata and others view her as an astute businesswoman and dispassionate manager. Adept at handing extreme crisis situations and with a record of effecting good outcome. Pricey-Icehouse had no responsibility for the auditing of the state elections. **Role:** Commission Chairperson. **Paradigm Represented:** Business management.

Sean Peisert, Ph.D.. Forensic Analyst for the Ministata Attorney General's office. A relatively new Ph.D. concentrating in the new field of digital forensics. He worked on the recent debacle involving the election machines for the United Aerospace Workers

union, a notorious incident where he (among others) successfully proved fraud in the election of their new president. **Role:** Digital forensicist/analyst. **Paradigm Represented:** Law enforcement and justice system.

Matt Bishop, Ph.D.. Mathematician. University of Ministata at Nyvus. Expert in game theory and statistics. Hand picked by Ms. Corriss; they attended college together. **Role:** expert mathematician with experience in studying the mathematical modeling of voting machines. **Paradigm Represented:** Mathematical community.

Steven J. Greenwald, Ph.D.. CEO of Metaphysically Secure Systems Incorporated. World renowned playboy, reformed hacker, founder and CEO of Metaphysically Secure Systems Incorporated and a self-professed leader in the field of binary security for multinational corporations with not-well-known but desirable links to the military industrial complex and intelligence community. Has an honorable reputation as a "hired-gun" in the field. Regarded by some as an encyclopedic synthesist able to integrate disparate mindsets and data. Ph.D. in computer security and security consultant to governor Devo's former Wall Street investment firm ("Soldman Gaks, LLC."). **Role:** computer security, particularly assurance. Reputation as a general trouble shooter in the field. **Paradigm Represented:** Computer security (CIA+N: confidentiality, integrity, availability, plus non-repudiation).

APPENDIX D: PANELIST REAL BIOS

Sean Peisert

Sean Peisert is jointly appointed as a research scientist at the University of California, Davis and Lawrence Berkeley National Laboratory, where he does research in computer security. He is particularly interested in computer forensic analysis, intrusion detection, vulnerability analysis, security policy modeling, electronic voting, the insider threat, and empirical studies of security. Previously, he was an I3P Fellow and postdoc at UC Davis, was a postdoc and lecturer at the University of California, San Diego (UCSD), was a computer security researcher at the San Diego Supercomputer Center (SDSC), and co-founded a software company. He received his Ph.D., Masters and Bachelors degrees in Computer Science from UCSD, where his dissertation focused on a developing a systematic approach to forensic logging.

Matt Bishop

Matt Bishop received his Ph.D. in computer science from Purdue University, where he specialized in computer security, in 1984. He was a research scientist at the Research Institute of Advanced Computer Science and was on the faculty at Dartmouth College before joining the Department of Computer Science at the University of California at Davis.

His main research area is the analysis of vulnerabilities in computer systems, including modeling them, building tools to detect vulnerabilities, and ameliorating or eliminating them. This includes detecting and handling all types of malicious logic. He is active in the areas of network security, the study of denial of service attacks and defenses, policy modeling, software assurance testing, and formal modeling of access control. He also studies the issue of trust as an underpinning for security policies, procedures, and mechanisms.

He is active in information assurance education, is a charter member of the Colloquium on Information Systems Security Education, and led a project to gather and make available many unpublished seminal works in computer security. His textbook, *Computer Security: Art and Science*, was published in December 2002 by Addison-Wesley Professional.

He also teaches software engineering, machine architecture, operating systems, programming, and (of course) computer security.

Laura Corriss

Laura Corriss works as Director of System Services for the Administrative Information Systems department at Barry University. Among her duties, she identifies, researches and resolves problems related to enterprise database management systems, supervises and mentors the programming staff, and provides database analysis and support, particularly for the Financial Aid and Finance departments.

Prior to working for Barry University Laura worked as the MIS Manager for CFX/LaFleurette, a cut-flower importer and a manufacturer of bouquets & arrangements. Prior to that she managed the computer department at Mayor's Jewelers where she first got exposed to management of computer security.

She received her M.S. degree in Computer Science and Information Systems from Barry University in 1988. She earned a B.A. in Urban Affairs from Duquesne University. She is currently working on her M.B.A.

Steven J. Greenwald

Steve Greenwald first programmed a computer in 1974 (a UNIVAC Specta 70) and within weeks entered the security community and hacker culture at a time when "hacker" did not mean "cracker." In his early days he did some things for intellectual exploration that he now regrets, even though he broke no laws.

After earning his bachelor's in Chemistry from Emory University in 1978, he worked in the business world as a programmer analyst, systems analyst, and software engineer. This exposed him to a very wide variety of projects. He also taught (after earning his M.S. in Computer Science and Information Systems) as an adjunct in the School of Computer Science at Barry University. During this period (in the Miami area and coincident with the era of the "cocaine cowboys") he got exposed to a huge amount of real-world security issues and concerns.

In 1994 he earned his Ph.D. in Computer and Information Sciences from the University of Florida with a dissertation in the field of distributed information security. He worked as a Visiting Assistant Professor at the University of Florida and then went to work as a computer scientist in the Formal Methods section (code 5543) of the Center for High Assurance Computer Systems (CHACS) at the U.S. Naval Research Laboratory in Washington, D.C. working under Cathy Meadows.

Since 1996 he works as an independent consultant in the field of Information Security specializing in distributed security, formal methods, security policy modeling, covert channels, resource based security, multi-level security, and related areas. He also works with organizational/enterprise security policy consulting, evaluation, training, and auditing. He keeps his client list confidential, but his clients run the gamut from the very large to the very small.

A Senior Fellow of Applied Computer Security Associates (ACSA), he also does the usual professional service within the community (including over a decade's work with NSPW including serving as general chair and program chair).

His website contains more information about him, including some of his publications:
`http://SteveGreenwald.com`