Title

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

Authors
Peisert, Sean
Bishop, Matt
Corris, Laura
et al.

Publication Date
2009-09-01

DOI
10.1145/1719030.1719041

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
California, U.S.A.
peisert@cs.ucdavis.edu

Matt Bishop
UC Davis
Davis, CA, U.S.A.
bishop@cs.ucdavis.edu

Laura Corriss
Barry University
Miami Shores, FL, U.S.A.
mcorriss@mail.barry.edu

Steven J. Greenwald
Independent Consultant
North Miami, FL, U.S.A.
sjg6@gate.net

ABSTRACT

Do you believe that more than one single security paradigm exists? We do.

We also believe that we have a major problem because of all these security paradigms: until we find a way to identify and understand how these paradigms restrict our analyses we will never have the ability to do a good job identifying risks and threats, let alone protect ourselves from them.

We also believe that the majority of people working in the security community use only one paradigm without recognizing that self-imposed constraint. The paradigm they use may change or even expand based on new data and experiences, but it still continues to limit their approaches and analyses, and therefore limit their effectiveness.

At NSPW 2009 we presented a panel simulation using four analysts in order to demonstrate how security paradigms constrain perceptions and points of view, and how the combination of the different paradigms confuses the analysts' conclusions. Our panel used real-time, interactive exploration to investigate how individuals in the security community work together within their different paradigms and how they often lack awareness of their particular paradigms while working in the same way that a fish does not notice the water in which it swims.

We presented a provocative, live scenario followed by an intensive analysis with NSPW audience participation. We hoped that this would illustrate the misunderstandings and erroneous conclusions that can emerge from the inadvertent and often faulty composition of differing universes of discourse.

Ultimately this led to a new paradigm for dealing with the compositions of the paradigms held by various individuals that we call "Multi-Paradigm Composition Analysis."

NSPW'09, September 8–11, 2009, Oxford, United Kingdom
Copyright 2010 ACM 978-1-60558-845-2/09/09 ...$10.00.

Categories and Subject Descriptors

H.1.2 [**Models and Principles**]: User/Machine Systems—*Software psychology*; K.6.1 [**Management of Computing And Information Systems**]: Project and People Management; K.6.5 [**Computers and Society**]: Management Of Computing And Information Systems—*Security and Protection*

General Terms

Experimentation, Human Factors, Management, Security

Keywords

collective paradigms, consulting, computer security, cybersecurity, digital forensics, e-voting, forensics, information security, Kuhn, management, multi-paradigm composition analysis, New Security Paradigms Workshop, NSPW, paradigm, reality tunnels, statistical analysis, voting

1. INTRODUCTION

We believe that no single security paradigm exists. Rather, many different and at times conflicting security paradigms exist. We also believe that until we find a way to identify and understand how these paradigms restrict our analyses, we will no have the ability to adequately identify risks and threats, let alone protect ourselves from them.

1.1 Concept

We presented a computer security problem caused by the composition of multiple incompatible paradigms. We designed things such that an analyst could only resolve the problem by shifting focus and mindset to reflect parts of each of those different paradigms.

We constructed our panel to study our paradigm in a fashion appropriate for NSPW—an explanation of the problem and the rôles of the members of the panel followed by intensive discussion. We also "layered" the presentation, so that as the panel session progressed, the panelists revealed more information that helped shape each paradigm, and also so that the discussion among the panelists as well as with the audience influenced the interpretation of events under each paradigm.

This approach, we felt, would work as the best way to further elucidate the issues, refine the approaches, create awareness of the problem, and potentially solve this problem (or at least ensure the panelists took the right approach investigating the problem).

New paradigms form the basis for papers and panels presented at NSPW. We investigate the "paradigm of paradigms" by questioning the rôle and nature of security paradigms themselves, and especially the ways in which multiple security paradigms *compose*.

Specifically, we challenge the idea that one investigator, working with one particular security paradigm, can ever sufficiently explore all facets of a security problem.

Our panel employed an exercise, described later, to investigate how the different paradigms that individuals in the security community use influence their thoughts and without them, or others, having awareness of it. We showed how individuals' mindsets affect more than just communications. We think that one of the security community's biggest problem lies in the fact that we cannot identify the proper risks because we cannot even *conceive* of the possibilities. These extra-paradigm issues reside outside our world view. For now.

1.2 The New Paradigm for Multi-Paradigm Composition Analysis

We used the hypothesis that, even within the same organization, different and conflicting security paradigms cause different and conflicting mindsets. These in turn cause different interpretations. This creates situations in which a heterogeneous group (in the multi-paradigm sense) that attempts to resolve a security problem may encounter extreme difficulties and may even find it impossible to resolve the problem.

Simply put, the composition of multiple security paradigms will cause the above problems. Worse yet, most organizations do not even have *awareness* that security investigations involve composing different security paradigms.

Even though we believe in the existence of more than one security paradigm, we also believe that the majority of people working in the security community only work within a single paradigm. The paradigm in which they work may change or expand based on new data and experiences, but it still limits them. Sometimes severely.

We therefore presented a computer security problem whose resolution required a shift in mindset that created a new paradigm from the composition of several different security paradigms. Either the computer security experts needed to make this shift, or someone from a different discipline had to suggest the alternate paradigm. The panel demonstrated that the computer security community tends to have a single mindset driven by a single paradigm.[1] As threats generally come from loci other than computer security experts, they often lie outside our current paradigm(s). This means that we might find it difficult, if not downright impossible, to arrive at the "right" answer, in which we properly evaluate and compensate for these threats. We therefore need to understand the paradigms used by computer security non-experts. Only then can we change our paradigms, and our mindset, appropriately.

1.3 The Construction of Our Experiment

Studying these paradigms requires a new paradigm, or "metaparadigm," from which to proceed. Our new paradigm has its roots in formal commissions that brought together investigators from many fields, and hence involved multiple paradigms. We used as iconic the Rogers Commission [20] that investigated the Space Shuttle *Challenger* accident in 1985–1987.

The Rogers Commission had very diverse membership. A former Secretary of State and Attorney General chaired it, and it included a former astronaut, several engineers, an astronomer, a publisher of a space-related magazine, a test pilot, and Nobel Prize-winning physicist Richard P. Feynman. Famously, Feynman demonstrated the cause of the accident before Congress with a piece of rubber and a glass of ice water [8]. The commission denied his (highly regarded) recommendations a place in the report, but allowed them (under duress) as an appendix [9]. Feynman's rôle worked as a sufficient condition for success, but not a necessary one. The real strength of the panel resided in its composition of people with wildly different *paradigms* causing diverse ways of thinking and acting. We argued that a panel with members who used different *paradigms*—itself a new, or rarely used paradigm—can have equal success when used to investigate/solve security problems. Further, this method has had success in other contexts.

As one example of other success, Marv Schaefer related to us[2] that he once worked at a commissioner for NORAD (the North American Aerospace Defense command). One of NORAD's systems had the design function of sending status messages to every Air Force base in the country, but the system caused too many false alarms. The operators at the various bases discovered that the system still seemed to work without their local alarms, so they committed the simple procedural error of turning off the alarms. The commission studied the problem with the false alarms and after several false starts only "impossible" situations remained. However, at one point, one engineer, acting in frustration, slammed his hand down on one of the exonerated black boxes involved and thereby accidentally and serendipitously caused a false alarm! The commission eventually determined that multiple factors caused the false alarms, including bad hardware, a mathematically weak checksum algorithm, and weak protocols (specifically, only one eighth of the valid packets would get through without an alarm). Further, weak procedures (such as turning off the alarms) exacerbated the problem. A null hypothesis, examined twice by a group of statisticians, mathematicians, computer security experts, electrical engineers, communications security people, protocol people, radar engineers, and military experts in command and control, did not get rejected—erroneously.

Thus, others have successfully used methods similar to what we suggest. But we could not find the method articulated explicitly in the domain of computer security; we have never seen it proposed as a general technique for analyzing security problems. So, we decided to test this theory at NSPW.

One note concerning methodology: in our original panel proposal to the NSPW program committee we did not present the application of the panelists' paradigms to the scenario, because we did not want to bias the discussion at the workshop. In fact, we believed presenting the panel as an examination of paradigms would prevent the panel session from achieving its goal. In this paper, we present both the paradigms and the scenario (as well as the usual background and conclusions).

[1] Or, equivalently, a single mindset created by several equivalent or fairly insignificantly differing paradigms (for example, "confidentiality, integrity, availability" vs. "confidentiality, availability, integrity, non-repudiation."

[2] Private communication.

2. BACKGROUND

So many security problems get caused by multi-paradigm composition that we consider it infeasible to list them, but we give a few recent examples.

- In mid-2009 someone opened a manhole in San Jose, California and cut three cables, terminating Internet and telephone access for much of the southern San Francisco Bay Area [1].
- Around the same time, reports surfaced that much of the power infrastructure had gotten "owned" by computers originating in China, Russia, and North Korea [10].
- Election officials in Clay County, Kentucky, got accused of manipulating the votes cast on electronic voting machines for years [3].
- The Conficker worm morphed yet again [12].

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" [22]?

We view a new model as necessary for preventing, understanding, identifying, and correcting security problems. The model we present combines our notions of how systems (non-secure or not) get understood, used, woven together, maintained, and ultimately (we hope) made more secure.

Computer scientists spend much time understanding how computers function in the real world. With additional multidisciplinary expertise in other areas such as psychology, computer scientists have extended their studies to understand how end users operate computers, and used empirical studies [19] to examine how computer programmers work, such as by using N-version programming [13], "extreme" programming [2], and the classic *Mythical Man Month* [4]. With respect to computer security, computer scientists have also studied the efficacy of security software [16].

But computer scientists have barely studied the question: *how do computer security professionals work?* More specifically, how do they work together to solve problems? As an example, consider "red teams."[3] When two teams examine the same system, can we measure their effectiveness at finding the same things as well as finding different things? As another example, when do security professionals succeed, when do they fail, and what assumptions do they make? How could we make them more successful?

This has importance because virtually all computer security relies on a human component. An end-user, a corporate security administrator, a programmer at an anti-virus software vendor, or a security administrator at an ISP, all have some responsibility for, and impact on, the security of a network and the hosts on it.

2.1 The Human Component: Electronic Voting Example

Electronic voting (e-voting) in the United States works as one component of an election process that relies on many people—voters, poll workers, vote counters, system administrators, and vendors, among others—with a broad range of computer expertise. Due to its wide practice, most people have familiarity with voting and that makes it easy to understand; therefore, we used it as a basis for our scenario. Current events in the e-voting community added to the attractiveness of this choice and worked as a bonus.

At the request of the Election Assistance Commission (EAC), the National Institute of Standards and Technology (NIST) developed a proposed set of Voluntary Voting System Guidelines (VVSG) [18]. These guidelines describe a National Voluntary Lab Accreditation Program (NVLAP) to verify adherence to the standards.[4] If we give the same system to two different test labs, what procedures and methodologies will ensure that both labs will arrive at the same result? The guidelines also include a section on open-ended vulnerability testing (OEVT), their name for penetration testing. This raises the question of standardizing those tests. Specifically how can one ensure that two teams reach the same assessment of the system that they test?

2.2 Questions Involving Security Professionals

As both labs and "red teams" involve many people, how those people approach the problem, analyze the system, and conduct their tests and experiments appears critical to obtaining meaningful and useful results, as well as replicability.

This leads to 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 we fix them, and how can we prevent them?

We can now start to make some meaningful observations.

2.3 The Multi-Paradigm Composition Problem

- We have multiple security paradigms in our field.
- We have multiple risks because of these different paradigms
- Someone unaware of the *notion* of a security hole due to the constraints of his paradigm cannot *even think* that someone may take advantage of such a security hole.

3. STRUCTURE OF THE PANEL

We constructed our four-person panel to have highly heterogeneous paradigms and agendas. More than just backgrounds, this also included interests, viewpoints, rôles, and manners of thinking. The panelists came from business-IT, academia, the military/ intelligence community, and banking, with each area using different *paradigms*. Thus, our panel focused on the results coming out of applying these paradigms to a detailed scenario. We had the goal of having our panelists evaluate threats, information, and actions based on their paradigm, and *not* to have the panelists actually determine what happened. To that end, the panel began with a consistent set of scenarios and bases (using "bases" in the inductive sense of the term). It then iterated to allow the paradigms to cross-fertilize. For example, consider a scenario involving audits. How might applying a paradigm versed in *management* (both technical

[3] Also called "teams of penetration testers."

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

and processes) interact with a paradigm versed in *academia*? On the surface the two might appear simply to conflict, but how would things change if the parties had no major stake in the outcome? Or if information got passed/leaked through moderating (or interpreting) parties?

Before the panel began, the panelists had *no* idea what result, if any, would ensue. All felt strongly that NSPW would provide the ideal venue to test this approach.[5] After all, anything to do with true (and new) paradigm investigation speaks to the *raison d'être* of NSPW. By not invoking a traditional single paradigm method, the panel caught the participants off-guard, causing questions like "How would one use penetration testers in each person's paradigm?"

In order to test our thesis that we need a new security paradigm for the analysis of multi-paradigm compositions, the panel used a fictitious yet realistic scenario in which a fictitious country named "Ministata" experienced a serious 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 and during the panel, respectively, to provide the historical background for the NSPW attendees; Appendix C for a detailed discussion of how the scenario played out,and see see Appendix E for an arrest warrant used in the scenario.)

Finally, we partly based the effectiveness of this demonstration on the element of surprise to the audience. It allowed them to come to independent conclusions even in the presence of deliberate false leads and misdirections. We panelists debated this somewhat "dramatic" approach among ourselves, and we all believed that this would work as the most effective way to use the heavily interactive NSPW method. Thus, we omitted the original panel proposal from the pre-proceedings.

4. WHAT WE LEARNED

The panelists consisted of a statistician, a forensic analyst, a troubleshooter, and a management expert. All had not only very different jobs, but viewed the problem through different paradigms. The panelists all interacted in very different ways, which we viewed as quite important.

We gave the panel the purpose of evaluating "a paradigm for analyzing security paradigms." The panel used a scenario centered around problems with electronic voting in the imaginary "Ministata" election.[6] Obviously a simulation does not work the same as "reality," and therefore we do not view the panel results as conclusive. A commission or panel format merely works as a demonstration of the "multi-paradigm composition analysis" paradigm. Further, we should study elements other than the *paradigm* of the individuals, even though it encompasses a number of important characteristics. Yet the emergence of many ideas based on the paradigms, and the lessons learned from them, meant that we viewed the panel as a success.

4.1 The Impact of Multiple Paradigms

Different panelists had different paradigms. This had the following implications.

- The panelists had different agendas and therefore sought to reach an outcome that they personally desired. *Personal agendas* differed greatly among the panelists. The cause did not necessarily involve malice, but more likely simply different methods, conclusions, or personal goals.
- Because they had different goals, the panelists talked about areas in which they appeared credible. Though they felt tempted to talk about areas outside a panelist's area of expertise, such talk could cause them to lose credibility.
- Both due to credibility issues and different interests, panelists could end up talking past each other, either unintentionally or quite deliberately as a diversionary tactic.
- Panelists might seek to maintain their own credibility and reduce the credibility of others.
- The mis-match of paradigms lead to diversions, intentional or otherwise.

As an example of these impacts, consider the situation in which Sean asked Steve a question that Steve, as a commissioner on the voting panel, did not want to answer and also wished to deflect. To create a distraction, Steve responded by asking Matt, in his statistician rôle, about what he viewed as the "null hypothesis" for the statistical experiments that Matt proposed. Indeed, Matt had proposed only the outline of the experiment, and so had not developed a precise null hypothesis. Hence he stumbled through the answer (as Steve anticipated, because he knew that coming up with a good null hypothesis works as very tricky and time-consuming). Thus, Steve's question to Matt both served as a distraction and misdirection [15] away from himself and a discrediting of Matt.[7]

A related situation occurs when one person knows another person's paradigm, but the reverse does not hold. The person who has more information, therefore, has an advantage. This concept seems akin to certain elements in warfare such as a false leak. *Operation Mincemeat* [17], from World War II, works as a good example of this. The British wanted to persuade the Axis powers that they intended Sardinia, not Sicily, as the target for troops moving from North Africa to Europe. So they put into the Atlantic near Spain a body dressed as a British officer complete with documentation designed to lead the Germans to conclude that the British would target Sardinia for the invasion—and also to lead them to believe that the British use Sicily as the cover story target! The people who devised the deception understood the German Intelligence paradigm, and therefore crafted the documentation and detritus with the body accordingly. Thus, for the British involved in the deception, a knowledge of the German paradigm worked as critical; and the Germans not knowing the British paradigm that led to the deception had equally critical (bad) results.

As another example, during World War II, the German counterespionage agency captured every British spy sent into the Netherlands as soon as the spies landed—unknown to the British. The Germans then had the spies send the information that they wanted the British to have. But the reverse also happened—the British captured every German spy in England, and had those spies send the information they wanted the Germans to have. The events happened almost concurrently. Neither side expected the other to do what each had done, even though both had done the same thing. This occurred as an effect of the difference between the paradigm of capturing or *turning* agents and the paradigm of *managing* agents.

A similar incident involved Norway running a heavy water facility for the Germans. The Norwegian underground destroyed it with the help of the Allies. However, the Norwegian underground

[5] All also felt that the NSPW attendees would benefit from the panel and that worked as one of our considerations.

[6] However, we used (mostly) real problems that occurred in different elections.

[7] Steve wishes to emphasize that he does not routinely engage in legerdemain during his work as a consultant.

did not want the Germans to take retribution on Norwiegan civilians. So the underground left a Thompson submachine gun (a type used used by the Americans) to divert attention from the Norwegian underground and toward the Americans as the culprits for the destruction of the heavy water facility.

We realized, as a complicating factor during the panel, that the audience had its own collective paradigm as well. This affected how the audience reacted both during and at the conclusion of the panel. Part of the reaction happened undoubtedly due to our performing part of the panel, and the scenario, on a moving bus/coach. But we had additional factors. For example, the audience never asked about the conclusion to the scenario, which the panelists intentionally left hanging. One might ask what that says about the way the panel worked: did the audience get so fixated on the "paradigm" of expecting an answer that they never even wondered why they didn't get one? Perhaps the authority (the "federal agent" who arrested Sean) provided the answer/closure that they expected—despite strong hints that others on the panel might have had criminal involvement. Yet we got no questions about anything more regarding this. We found that quite surprising, given the usual curiosity of the group and the probing questions it asks.

We posit that at some point we lulled the audience into a particular reality tunnel.[8] At what point did they experience so much information and authority that what simply *appeared* as the truth actually *turned* into their reality? Perhaps Philip K. Dick said this best: "Reality is that which, when you stop believing in it, doesn't go away." [7]

Reality tunnels constrain one's view of reality and to a certain extent also constrain one's sensory input. They form a matrix and filter for how we interpret and perceive the world and thus they can facilitate the creation of illusion. For example, when police interrogate witnesses, they may interview twenty people and obtain twenty different points of view (or "facts"). On the other hand, when one changes one's point of view, facts that have appeared completely inexplicable may suddenly seem obvious. Because of this, and more, we must emphasize that the word "Paradigm" does not work as simple another buzzword, at least in the Kuhnian sense in which we use it. People use paradigms whether they know it or not, and they cannot easily change their paradigms. Most people find it impossible to maintain more than a single paradigm simultaneously. People lock themselves into a universe of discourse and simply cannot view the world differently unless they shift to a different paradigm.

Such paradigm shifts have proven successful in other areas, such as psychology. For instance, an example of this comes from the psychoanalyst Robert Lindner, in the true story, "The Jet Propelled Couch; the story of Kirk" in his book, *The Fifty-Minute Hour* [14, pp. 221–293], where he so nearly bonded in therapy with an anonymized patient (widely regard as Paul Linebarger also known by his science-fiction writer alias Cordwainer Smith) that he suffered the same psychotic delusions until the cured patient snapped him out of it.

As far back as 1893, even Sir Arthur Conan Doyle's Sherlock Holmes referred to the importance of paradigm shifts to understanding his subject:

> "You'll get results, Inspector, by always putting yourself in the other fellow's place, and thinking what you would do yourself. It takes some imagination, but it pays." [5]

> "You know my methods in such cases, Watson. I put myself in the man's place and, having first gauged his intelligence, I try to imagine how I should myself have proceeded under the same circumstances." [6]

Thus, due to the negative effects that reality tunnels can have, we believe that the following works as one of the key lessons learned from this exercise:

Always have awareness of multiple paradigms.

Indeed, although this simulation focused on a single paradigm for each member, increasing the awareness of this focus in our lives makes us able to see that other paradigms exist and have utility. In fact, except for Laura, we found the security management paradigm as the most difficult paradigm to accept and of which we should have awareness. Many noted that without management buying into security, one will have problems developing things like good security policies.

One final unexpected paradigm entered the area of the illusion of control. This arose as follows: the simulation experiment had Sean as the "panel chair," and he duly followed the plan the rest of us gave him. While doing that, at the properly agreed-on time he announced to Laura that he thought he detected a threatening insider on the panel. Completely unbeknownst to Sean, he walked into the secretly pre-arranged trap of Steve and Matt, who had previously conspired to have Sean "arrested." The illusion of control caused Sean's blindness and complete obliviousness to this unexpected change in "plans," whereas had he not acted as the panel chair he might have sensed something odd happening beforehand.

This meant that two members of the "commission" got totally blindsided due to their unawareness of other paradigms: Matt when Steve hit him with the null-hypothesis question, and Sean when he got metaphorically clapped in irons by Brian Snow (acting as the Federal Bureau of Persecution agent).

5. CONCLUSIONS

The panel used a scenario with which most people have great familiarity: a very close election with some shenanigans involved. This meant that the audience needed no orientation on the process involved in the scenario; simply on the results, and on the data that indicated questionable behavior. We felt it a perfect scenario 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 the reported results had statistic significance), and troubleshooting and consulting in assurance (ranging from low to high assurance). Each of these disciplines views problems very differently, and the topic allowed the panelists to bring out these differences.

Ultimately, the process helped demonstrate and refine the new security paradigm for analyzing multi-paradigm compositions. The multi-paradigm concept seems much more common than the panelists thought, and works quite profoundly. Additionally, everyone working in collaborative environments could benefit from understanding that multi-paradigms exist, understanding the different paradigms that their colleagues use, and shifting to alternative paradigms.

5.1 Recommendations

We close with some recommendations, not only for the field in general, but for NSPW.

[8] For more information on the notion of reality maps and tunnels, see [24]

1. We feel it of great importance to include, indeed *invite*, people who use different paradigms. For example, several people who attend NSPW also work as managers, but when at NSPW none of them actually use or espouse the management paradigm and, indeed, seem to avoid it and instead use scientific and academic paradigms. One of the panelist-participants, Laura Corriss, *did* explicitly represent the security management paradigm, and she used that paradigm throughout the workshop. Her observations, comments, and reactions appeared very different from the managers who lapsed into the scientific and academic paradigms. This perfectly illustrates how job title and background differ from a paradigm, because paradigms can change depending on the environment in which people work/reside. Thus, we believe that NSPW would profit from having even only one person who uses a paradigm other than a computer scientist or academic paradigm.

2. In the past, including those who represent the life sciences [21] and military science [23], paradigms have contributed greatly to the discussions. The participants in both these cases had doctorates in computer science, but had expertise and experience in other disciplines, and had the capability of representing paradigms from those disciplines.

3. One problem with the panel occurred due to its location, specifically most of it happening on a bus/coach. The audience could not see the panelists' body language. Though we could not avoid this location for this particular workshop, we would have found it interesting to see how body language would have altered the audience's perception of the panelists' paradigms. As an example of the information contained in body language, consider the first panel session, which introduced the scenario. That session did not take place on the bus. We noticed that the audience could get lulled into mirroring the body posture of the panel almost exactly (see Figure 1). Thus, if a panel of this nature ever again gets presented, we suggest that the presentation work such that it does not lose the opportunity to cause body language interactions with the audience and panel.

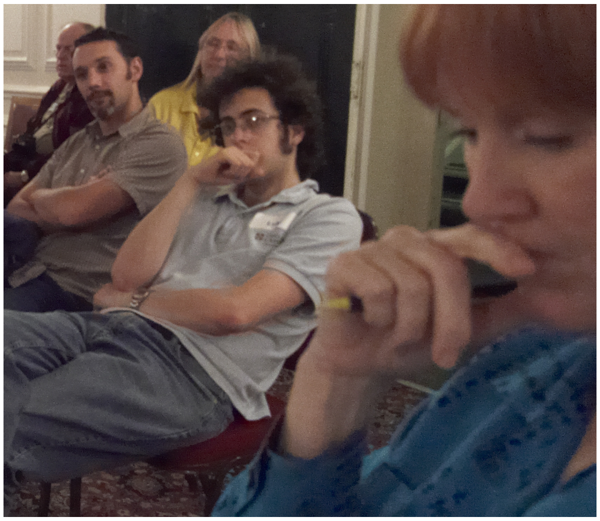

Figure 1. Body posture (foreground; from right to left): Panelist Laura Corriss and attendees Luke Church and Matt Williamson.

4. Finally, suppose we asked the attendees which paradigm (or group of paradigms) they represent when attending. We would find it interesting to determine if the one that they claim to represent actually works as the one they use. Further, given their different backgrounds, we would find it equally interesting to see when (or if) the attendees actually *can* represent paradigms other than their primary paradigm. Then we could ask attendees to evaluate and comment on papers using the different paradigms in which they have expertise. Thus, the session chairs could learn to monitor the discussion in order to prevent spurious paradigms from derailing the discussion, and also could deliberatly evoke paradigms that contribute to the discussion.

Acknowledgments

All authors gratefully and wholeheartedly thank several people who made this panel and paper possible: Marvin Schaefer worked with us early on to develop the ideas behind this panel; Brian Snow participated in the simulation and played the wonderful rôle of the Ministata Federal Bureau of Prosecution officer; Anil Somayaji acted as our pre-workshop shepherd, and Christian Probst acted as our post-workshop shepherd. All of them gave wonderful and excellent guidance. We thank all of the attendees of NSPW 2009 whose participation in this experiment made it possible.

Matt Bishop received support in part from the National Science Foundation under Grant Number CNS-0716827 to the University of California at Davis.

Sean Peisert received support in part from 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 belong to the authors and no one should ascribe them to the funding sources of any author; they do not necessarily reflect the views of the funding sources of any author.

We give appreciation to the cartoon *Futurama* for some of the names of the characters in our fictitious almost *roman á clef* voting scandal scenario.

We wrote this paper in E-Prime for Security (but left the appendices in the original regular English) [11].

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] A. Conan Doyle. The Adventure of the Musgrave Ritual. *Strand Magazine*, 1893.

[6] A. Conan Doyle. The Adventure of the the Retired Colourman. *Strand Magazine*, 1927.

[7] P. K. Dick. How To Build A Universe That Doesn't Fall Apart Two Days Later. In *I Hope I Shall Arrive Soon*. Doubleday, 1978.

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

[9] 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.

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

[11] S. J. Greenwald. E-Prime for security: A new security paradigm. In *Proceedings of the 2006 New Security Paradigms Workshop*, pages 87–95, Schloss Dagstuhl, Germany, September 2006. ACM.

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

[13] 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.

[14] R. Lindner. *The Fifty Minute Hour; a collection of true psychoanalytic tales*. Rinehart, New York, 1955.

[15] S. L. Macknik, M. King, J. Randi, A. Robbins, Teller, J. Thompson, and S. Martinez-Conde. Attention and awareness in stage magic: turning tricks into research. *Nature Reviews Neuroscience*, 9(11):871–879, July 30, 2008.

[16] 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.

[17] E. Montagu. *The Man Who Never Was*. Lippincott, Philadelphia, 1954.

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

[19] 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.

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

[21] A. Somayaji, M. Locasto, and J. Feyereisl. The future of biologically-inspired security: is there anything left to learn? In *Proceedings of the 2007 New Security Paradigms Workshop (NSPW)*, pages 49–54, 2007.

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

[23] D. J. Welch, N. Buchheit, and A. Ruocco. Discussion: strike back: offensive actions in information warfare. In *Proceedings of the 1999 New Security Paradigms Workshop (NSPW)*, pages 47–52, 2000.

[24] R. Wilson. *Quantum Psychology: How Brain Software Programs You and Your World, Second Edition*. New Falcon Publications, June 1990. ISBN-10: 1561840718, ISBN-13: 978-1561840717.

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 rôle 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 rôle. 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 rôle 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 rôles/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[9] arrives on the scene to arrest the insider on the panel: Laura, as it turns out[10].
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.

[9] played by Brian Snow

[10] Actually, we had Sean "arrested" but left this intact as deception

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? Then 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 → proof/disproof from people in the other disciplines.

Panelist Backgrounds (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 Corriss, 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. **Rôle:** 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. **Rôle:** 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. **Rôle:** 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."). **Rôle:** 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 an assistant adjunct professor at the University of California, Davis, and a research scientist Lawrence Berkeley National Laboratory. He performs research in computer security and is particularly interested in computer forensic analysis, intrusion detection, 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.

In late 2008, prior to the U.S. presidential election, he co-authored a document on "Resolving the Unexpected in Elections: Election Officials' Options," a guide to help election officials understanding how computer forensic techniques can be applied to issues with electronic voting machines and related systems. The document is distributed via the American Bar Association and the Center for Election Excellence.

He has been an NSPW PC member, local chair, and looks forward to being NSPW vice chair (2010) and general chair (2011).

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 Spectra 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. Concurrently with consulting, and from 2000-2009 he taught and conducted research as an adjunct professor with graduate research status at James Madison University's graduate INFOSEC program.

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`

APPENDIX E: WARRANT FOR ARREST OF COMMISSIONER PEISERT

WARRANT FOR ARREST

IN THE GENERAL COURT OF JUSTICE
DISTRICT COURT DIVISION

THE STATE OF MINISTATA vs.
Sean Peisert

To any officer with authority and jurisdiction to execute a warrant for arrest for the offense(s) charge below:

I, the undersigned, find that there is probable cause to believe that on or about that date of offense shown the defendant named above unlawfully, willfully, and feloniously did

1) Mopery in the First Degree

2) Loitering in a public library in the First Degree

3) Exploiting cryptographic system bugs in the Zeroth Degree

This act(s) was in violation of the law(s) referred to in this Warrant. This warrant is issued upon information furnished under oath by the complainant listed. You are DIRECTED to arrest the defendant and bring the defendant before a judicial official without unnecessary delay to answer for the charge(s) above.

Signature:

Location of Court: Orwellville, Ministata

Date: September 10, 2009