Assurance in Life/Nation Critical Endeavors A Panel

Steven J. Greenwald
Independent Consultant
2521 NE 135th Street
North Miami, Florida 33181
USA
sjg6@gate.net

Marv Schaefer
Books With a Past, LLC
2465 Washington Road (MD 97), Suites 3, 5, 5
Glenwood, Maryland 21738
USA
bwapast@erols.com

ABSTRACT

Our thesis is that biometric and other intertwined technologies will be used to supplement the work of people in the security field. When these technologies are used, we fear that a high degree of misinterpretation and error is likely. Because of this, we need to identify the technical measures required for these systems. This thesis, along with a justification, and proof sketch, was given to the panelists.

Five areas of the technology life-cycle were investigated: modeling, implementation, interpretation of results, database protection, and social issues.

The format was simple. After the introduction, each panelist gave a brief presentation. Afterwards the workshop participated in a highly interactive and collegial way, with the panel chair keeping things orderly.

A lively discussion resulted, with many good comments and questions from the NSPW attendees, some of which we report.

1. INTRODUCTION

Your fantasies, Sir Quixote, it is true. That crazy brain of yours have been quite upset. - Miquel de Cervantes, *Don Quixote*

This panel emerged via a lot of crazy and upset brains!

When the NSPW Program Chairs, Carla Marceau and Simon Foley, put out a call for panel proposals, Mike Williams (our modern day Don Quixote) proposed a panel that would examine and ultimately fight against the biometric snake oil that seems to be particularly prevalent at this time.

New Security Paradigms Workshop '02, September 23-26, 2002, Virginia Beach, Virginia.

One minor problem with Mike's proposal was that probably everyone in attendance at the workshop would be in violent agreement with his windmill tilting. Noble as Mike's cause is, a consensus arose that his would make for a somewhat less controversial panel than is traditional for NSPW.

Steve Greenwald, in his role as Sancho Panza, submitted a counter proposal that was too political in nature to be acceptable. Carla and Simon wisely suggested that any panel proposal should be *primarily* a technical one, to which Steve agreed. They also suggested that there was the additional danger of being US-centric, and again Steve agreed with their wisdom.

Steve then contacted Marv Schaefer (somewhat like the shoddy Rocinante). Marv was recuperating from surgery on his foot, and was also scheduled for additional surgery that precluded him from attending NSPW 2002,[1] but even so was eager to help with the panel. Working together, we came up with our thesis.

2. THE THESIS

An interesting iteration of ideas ensued. We eventually came up with a thesis that we thought would be acceptable to the program chairs and would also ensure a lively and interesting panel.

We now present our thesis, along with a justification, and a proof sketch.

Thesis

Given that biometrics and other intertwined technologies will be used to supplement the work of people, and

Given that misinterpretation and error are highly likely to result in the deprivation of life, liberty, and happiness (in other words, these systems are "criticality one," or "man rated"),

Then we need to identify the technical measures that are needed to justify placing confidence in the implementation, installation, and use of such fundamental systems.

[1]Marv's feet have since made a complete recovery and have made him more of a modern-day reshoddy Rocinante.

Justification of the Relevance of the Thesis: Such things as the following, to name but a few.

- The proposed national ID card in the US, Ireland, and Great Britain.
- The proposed US Frequent Traveler smart card
- The US Federal Aviation Administration biometric smart card ID for law enforcement personnel and pilots (so they can board aircraft while possessing firearms).
- Watermarking systems for cash, passports and other interesting things.
- The proposed US national standard for driver's licenses.
- Credit card company biometrics on smart cards.
- Ear geometry biometrics.
- Knuckle crease biometrics.
- Face-recognition systems deployed in several US cities (an example of a known failure of technology).

Proof Sketch: We considered the issues, and realized that while there are many ways to view the problem, one natural way is to consider the technology lifecycle stages. These stages each have interesting implications (and examples). There are five stages of interest to us.

1. **Model.** Here are some examples to consider regarding the *soundness* of the model being used.
   (a) The strength of Cryptographic algorithms and protocols.
   (b) Watermarking systems.
   (c) Immutability of individual human characteristics.
   (d) Uniqueness of certain individual human characteristics.
   (e) Statements of security *desiderata.*
   (f) Security policies.
2. **Implementation.** Here are some examples concerning the *strength* and *correctness* of the implementation.
   (f) Claims of use.
   (g) Various forms of testing.
   (h) Software Engineering methodologies and processes.
   (i) Assurance arguments.
   (j) What *was* that security policy again?
3. **Interpretation.** Here are some examples concerning the *interpretation of results.*
   (k) Training of personnel in appropriate disciplines.
   - Statistics and probability, particularly Type I and Type II errors.
   - Education. For example, why the Johnny Cochran DNA argument was wrong.
   - Fingerprints! Can they be trusted?

   (l) Properties of contraband (*e.g.*, how to safely check if a firearm is unloaded).
4. **Database Protection..** Here are some examples of *protection* of the *integrity* of critical or biometric databases.
   (m) ID of characteristics.
   (n) "Dirty word" and association lists.
   (o) Incoming missile detection.
   (p) Fratricide, AKA "Friendly Fire."
   (q) Substitution of ID data to cause confusion (*e.g.*, someone stealing US Attorney General Ashcroft's fingerprint data and using it to spoof him).
   (r) Legal aspects, credibility, and "courtproofing."
   (s) Smart card tampering *àla* the recent work of Ross Anderson and his students. [2]
5. **Social Issues.** Here are some examples of *balancing* the *economic* and *social* justification versus correct use.
   (t) Disney's fuzzy biometric system.
   (u) The failure of Tampa's implementation of facial recognition systems in Ybor City.
   (v) The social implications of wrongful imprisonment or detainment, *etc.*
   (w) The appropriate remedies for injustices committed due to these issues.

Once we had our thesis and proof sketch, we started thinking about some knight-panelists willing to tilt at some windmills.

3. DRAMATIS PERSONNÆ

We wanted panelists who had strong positions on the above areas and we believe we were successful in our choices. While Marv was temporarily defeated by surgery,[3] we found panelists that each held carefully thought out views and had significant ideas.

The panel chair introduced the panel charge and the panelists. Then the panelists presented their positions, each taking about 10 minutes. When they were finished, the interaction with the rest of the New Security Paradigms Workshop started. The debate, comments, and questions were insightful, perceptive, informative, and as always at NSPW, collegial.

The names and qualifications of the panel follow in the order of their presentation.

- Steven J. Greenwald chaired the panel. He has been involved with NSPW starting in 1996 as an author,

[2] "Security Engineering: a Guide to Building Dependable Distributed Systems," John Wylie and Sons, 2001.
[3] But wouldn't want to be thought of as a toedy [sic].

was past program chair, past vice chair, and past general chair. He is an independent consultant in Information Security and an adjunct professor in Information Systems Security at James Madison University's graduate INFOSEC program. He is also a Research Fellow at Virginia's Commonwealth Information Security Center. His experience covers the spectrum from COBOL programming to NP-complete proofs. His interests include formal methods in INFOSEC, Role-Based Access Control (RBAC) and access control in general, decentralized security, user-centered security, resource based security, formal security policy modeling, NP-completeness and the decidability of various security mechanisms and properties, and covert channels. He earned his bachelor's degree in Chemistry from Emory University, an M.S. in Computer Science and Information Systems from Barry University, and the Ph.D. in Computer and Information Sciences with a dissertation in computer security from the University of Florida.

- John Michael (Mike) Williams entered the IT business 46 years ago, with Remington Rand Univac, when the first commercial computer was of that name and only 5 years old. He took to programming mechanical, electromechanical and electronic devices, taught himself the programming of a large-scale scientific computer and a small-scale business (punched-card/plugboard) computer, then became a programmer-analyst, systems programmer/project manager, system software product manager (publishing his first peer-reviewed paper 36 years ago), then a senior computer scientist/consultant engineer in commercial, civilian government and national defense applications. He became involved in computer security 29 years ago, and a specialist in it 25 years ago. He was a secure systems implementer, then an R&D manager for the largest such program then in industry, and has remained involved in such R&D since. His scope includes secure operating system architecture on several types of computers and networks (including parallel, and advanced avionics), advanced classified cryptographic systems, defense and international security evaluation and networking standards, clearance and labeling security policy for military and intelligence information, and perhaps the earliest "homeland defense" effort: NSTAC (the President's National Security Telecommunications Advisory Committee, founded during World War II). He was with what is now Unisys for more than 24 years, Computer Sciences Corporation for more than 8, a variety of start-ups, and co-founded a wireless-telecomm consulting partnership. His work has taken him to four NATO countries and to four others. He is a cleared consultant to the Institute for Defense Analyses, and semi-retired. He can be reached at John.Michael.Williams@Computer.org.

- Carla Marceau is the NSPW 2002 Senior Program Chair, and a Senior Principal Scientist at ATC-NY (formerly Odyssey Research Associates). Previously, Carla has worked at Cornell University, the University of Berne, the Swiss Federal Technical Institute (Lausanne), and MIT in several areas of computer science, including security, operating systems, programming environments, and program semantics. For the past five years she has been working on research projects in computer security. Carla has an A.B. from Harvard and an M.S. from MIT.

- Bob Blakley is the Chief Scientist for Security and Privacy at IBM Tivoli Software. He is the General Chair of the 2003 IEEE Symposium on Security and Privacy (AKA "Oakland"). He is a past general chair of NSPW. Bob serves on the "Authentication Technologies and Their Privacy Implications" panel of the National Academy of Science's Computer Science and Telecommunications Board (and is a contributor to "IDs: Not That Easy" which examines national identity systems issues). He is on the editorial board of Springer-Verlag's International Journal of Information Security. He was editor of the OMG CORBAsecurity specification and wrote a book on that topic. At the 2001 Annual Computer Security Applications Conference (ACSAC) he was honored as a "Distinguished Practitioner." He has an A.B. in Classics from Princeton University, and his M.S. and Ph.D. in Computer and Communications Science from the University of Michigan at Ann-Arbor.

While the next person could not be on the panel, he influenced it so much and his spirit pervaded the panel to such a degree that he deserves special mention as a sort of "panelist *in absentia.*"

- Marv Schaefer was present at the second NSPW, was very active in the organization as publications chair, was an NSPW author, and is a long-time participant. He has been very many things in life, educated as an algebraic number theorist and having been an active researcher in a wide range of computer and network security topics between 1968 and his retirement in 2000; currently he is an antiquarian bookseller and is on the editorial board of the Mathematical Association of America. His contributions are in areas such as the need for integrity over confidentiality, defending against the abuse of authority rather than of break-ins (*i.e.*, the misuses of existing mechanisms in authorized ways goes much farther than trying to break them). While serving as Chief Scientist at the NSA's National Computer Security Center (1982-6), Marv came to the conclusion that the formal methodists were too often off-base and their results often lacked relevance to proving the relevant security conditions and theorems. His NSPW research also focused on how analysis and defenses would better be focused on the problems that need to be solved (*i.e.*, the attacks that work) rather than the toy ones that formal methods found useful (*e.g.*, detecting violations of the *-property in abstract from specifications that are, at best, only coincidentally implemented in code). Marv is strongly concerned over the need for strict adherence to the scientific method and to the peer review process as necessary conditions to the acceptance and use of new technologies. He recommends strongly that readers of these *Proceedings* consult Imre Lakatos *Proofs and Refutations: The Logic of Mathematical Discovery* and

R.A. Demillo, R.J. Lipton, and A.J. Perlis "Social Processes and Proofs of Theorems and Programs", *Communications of the ACM* 22(5), 1979.

4. THE PANEL

The panelist's statements are included in the NSPW 2002 proceedings, so it would be redundant here to repeat their positions. Instead, we hope to give a fair recording of some of the issues that arose during the panel.[4]

Abe Singer mentioned tongue-in-cheek that we should have an "Evildoer Card" or a "National Intent Card" and then in a more serious vein said that we need mature technology instead of "obsolete stuff."

Holly Hosmer said that since all the technologies were so weak, shouldn't we use all of them?

John McHugh said that the fault tolerant community is doing what Carla suggests[5] and that we should pray for diversity sometimes.

Richard Newman (Nemo) asked Mike whether a true scientific proof of the validity of fingerprints exists. Or has it been done and we don't know it?

Bob Blakley noted that DNA source attribution is an issue in the DNA forensics community, and the community has resisted that.

Ira Moskowitz noted that if biometrics entered common use right now then it would drive us all crazy (*e.g.,* hotel doors with iris scanners). He thought this would be a good thing to demonstrate the technology's failures and to spur development. Bob suggested toilet locks would be a good candidate for biometrics.

Angela Sasse said that Germany is going biometric because they have no alternative. She said that in empirical tests with trained security guards they let 30% to 60% of the subjects get through (false negatives or "False Acceptance Rate" as the term used by the biometrics community). She said that we scientists must offer good alternatives to biometrics.

Abe Singer mentioned the US Immigration and Naturalization Service (INS) pass for frequent border crossers. It is a transponder system. Michael Franz, who is not a US national commented that every time he arrives in the US it says to him "Welcome home Michael."

Abe Singer noted that in San Diego the company that makes the photo radar systems to detect speeding automobiles is biased toward getting more lawbreakers since they get a commission for every citation.

Mike Williams noted that there are about 40,000 Closed Circuit TV (CCTV) systems in England and Wales. The average person has their face captured 300 times per day. Bob Blakley noted that in the UK people watch CCTV recreationally. He noted that we need smart people to interpret the data, like El Al uses, and that people are better at judging people than machines.

Kay Connelly noted that the use of modern DNA technology is repudiating old court convictions. She wondered if it were only of use for the defense.

Paul Dourish gave some common platitudes. "Technology will save us." "The right one will come along." These are all examples of erroneous beliefs. He said that guards should actually look at ID badges and cited an example on a bus where a guard checked all the passengers' IDs by having them hold them up for a few seconds while he quickly glanced at them.

Carla Marceau noted that one current problem is that people want cheap solutions.

Rebecca Grinter said that the best system would not remove the US Internal Revenue Service's old clunky computers. She said that engineering systems are used in an organic fashion and that "Nobody ever killed a bad policy. New things arrive on these sediments."

Nemo mentioned that retinal scans are now capable of detecting pregnancy, so there is another privacy issue to worry about. He said that we only want to raise the bar, not get perfect security. "We don't have great alternatives anyway, so why not use them to raise the bar?" Michael Franz compared this to home security saying, "My home security only has to be better than my neighbor's."

Srdjan Capkun said that he needed 6 separate Croatian documents to get a visa to leave for NSPW, each from a different authority. He commented that this is a mess, and not a deliberate policy and was not easy even if a person had all the right documents. He said, "Go to an easier country if you want to forge an ID." Holly commented that forging is easier and cheaper in a situation like that. Srdjan replied that in a system like Croatia's, one is always accumulating more and more documents.

5. WHITHER BIOMETRICS?

It was no surprise that among the NSPW participants there was universal disdain for the state-of-the-art in biometric systems.

What was a surprise was the consensus that biometrics were going to be adopted no matter how bad their performance. This explains a lot of the comments which we believe reflect a mindset of being resigned to living with inferior technology.

We find it ironic that the lessons learned from the past, in particular fingerprint technology, are not being applied to present systems. This is also of grave concern when we see the amount of wrongly convicted people who are being freed from prison every day due to advances in DNA technology. If the majority of the public adopts the view that biometric technology is as reliable as DNA technology then we may be

[4]Steve Greenwald is responsible for any mistakes in transcription/interpretation.
[5]Refer to her Carla Marceau's Panel Statement for more details on what she suggests.

due for more interesting times!

This leads us to the following four essential question areas regarding any biometric system.

1. **Scientific Strength.** What is the scientific evidence supporting the claim that a given biometric phenomenon is statistically valid as a unique identifier of an individual or a small class of individuals? How was this claim vetted by the knowledgeable scientific community? What were the dissenting viewpoints and what was their credibility? Are there known probable error rates relative to positive identifications based on this biometric phenomenon?

2. **Model Validity.** What is the model on which the computer-based or automated system is based for recognizing this particular biometric phenomenon? Same questions relative to vetting and review of the model.

3. **Implementation Assurance.** How was the model implemented (*e.g.,* what are the hardware and software components of the implementation)? Has the translation of the model been vetted, and how is it established that the translation into an implementation was correct and mathematically faithful? Above questions also apply.

4. **Implementation Safety and Efficacy.** How was the implementation tested? What are the environmental conditions of use? What are the known and theoretical failure modes for the implementation? How are operators of the implementation trained? How are the consumers of the implementation's outputs trained to interpret the results?

We feel that without posing and giving reasonable answers to these questions no biometric system ought ever be adopted.

6. W[H]ITHER SCIENTIFIC ANALYSIS?

Had he been present, our second author, Marv, would have stressed concern over the need for strict adherence to the "scientific method." In any technology in which safety, security, or human life is involved, there needs to be careful and thorough analysis in a process that is based on

1. observation, positing a hypothesis,

2. establishment of criteria for justifying the hypothesis,

3. performing reproducible logical or physical experiments (including the possibility of proof by formal mathematical means),

4. performing critical assessment of the evidence through expert peer review of the justification results, and

5. reiteration of the above process until appropriate levels of confidence are achieved.

The critical assessment and reiteration steps are essential, and need to be carried out with near religious fervor. Too often, this is not done because of concerns over cost, opportunity, and intellectual property. Also, too often, the analysis is performed by a group of individuals who have already "bought into" the idea behind the product and who, because of lack of special training or of appropriate levels of healthy skeptical inquiry, may not pose the appropriate challenges to the product's justification claims.

An example from the digital watermarking field may be of interest. Digital watermarks may be used to establish authenticity and to add assurance that the watermarked entity has not been modified. In many applications, the number of bits allocated to a watermark may necessarily have to be limited in order to prevent the watermark's appearance from becoming objectionably visible. The underlying technology will, therefore, involve a combination of optics (to limit discovery) and cryptology (to limit the attack space). The second author, Marv, is aware of a product that was designed for authentication of small photographs in which high optical quality and authenticity/immutability were primary criteria. The implementers, all of whom possessed advanced degrees in physics, selected a watermarking formula from a collection of available cryptographic algorithms, but did not understand the need for key-lengths that would withstand attacks based on the pigeonhole principle (birthday attack). Hence, their assurance arguments and evidence were not complete and did not address an existent counterfeiting vulnerability.

It is a lamentable trend in recent releases of far too many commercial software and hardware products, that it is the alpha or beta version that becomes the first public product offering. Products, and even *books*, are automatically released with liability-limiting licenses and caveats such as the following.

> Limit of Liability/Disclaimer of Warranty: While the publisher and author have tried their best efforts in preparing this book, they make no representations or warranties with respect to the accuracy or completeness of the contents of this book and specifically disclaim any implied warranties of merchantability or fitness for a particular purpose. . . . Neither the publisher nor author shall be liable for any loss of profit or any other commercial damages, including but not limited to special, incidental, consequential, or other damages.[6]

This caveat was contained in a "drama on the high seas as the world holds its breath" concerning events during the Cuban Missile Crisis by a publisher of principally technical texts.

Or consider the following, from *Mathematica* 4.2, a product widely used for symbolic computation and mathematical modeling, design, and analysis.

[6] *October Fury*, P.A. Huchthausen, John Wylie and Sons, 2002.

> WRI warrants that the product shall be free from defects in the physical media for a period of ninety days following date of purchase when used under normal conditions. The foregoing warranty is in lieu of all other warranties, express or implied. WRI does not warrant that the software is free from all bugs and omissions; the product is sold as is. WRI makes no representations, express or implied, with respect to the product or the software contained in the product, including without limitations, any implied warranties of merchantability, interoperability, or fitness for a particular purpose, all of which is expressly disclaimed. WRI does not warrant that the functions contained in the program will meet your requirements or that the operation of the program will be uninterrupted or error free. . . . In addition to the foregoing, you should recognize that all complex software systems and their documentation contain errors and omissions. WRI, its distributors and dealers shall not be responsible under any circumstances for providing information on or corrections to errors and omissions discovered at any time in the product, whether or not they are aware of the errors or omissions. WRI does not recommend the use of the software for applications in which errors or omissions could threaten life, injury or significant loss.

Clearly, such caveats should be causes for concern. The Wylie caveat is the same wording as is used in their mathematics and technical books, and appears to have been automatically applied to a history book without thought. The marketing of scientific books and products such as Excel, *Mathematica*, Quick Books, *etc.* all make claims or suggestions that the products are accurate, useful, and can be relied upon, and people buy such products with the intent to apply them to real applications related to the marketing.[7]

We can only assume that similar marketing claims and liability caveats accompany contemporary biometrics-based products. As always, *caveat emptor!*

ACKNOWLEDGMENTS

This panel evolved in an interesting way, and involved collaboration with a truly wonderful set of people. It was a pleasure to work with the panelists. The NSPW 2002 Program Chairs, Carla Marceau and Simon Foley, gave great guidance, and their wisdom was essential during the evolution of this panel. (Once the panel charge was straightened out and accepted, we surprised Carla by asking her to join us on the panel!) Dorothy Denning also gave valuable input but alas, despite her desire was unable to attend NSPW.

Extra-special thanks go to Mary Ellen Zurko who acted as scribe during a fast-paced panel. Her excellent notes were invaluable in our attempt to capture some of what went on during the panel.

We appreciate Laura Corriss' work and valuable comments in proofreading this paper as well as the slides used by the panel chair.

Finally, thanks are due to all the NSPW 2002 participants for making this such a vibrant panel. In the NSPW tradition of exceptional interactivity, all of them were *de facto* panelists.

[7] We refer the reader interested in this line of thought to B. Blakley, E. McDermott, and D. Geer. Information security is information risk management. In *Proceedings of the 2001 New Security Paradigms Workshop*, pages 97–104, Cloudcroft, New Mexico, September 10-13, 2001.