Reflections on the 30th Anniversary of the IEEE Symposium on Security and Privacy

Peter G. Neumann
Computer Science Laboratory
SRI International
Menlo Park, California, USA
neumann@csl.sri.com

Matt Bishop, Sean Peisert
Computer Science
UC Davis
Davis, California, USA
{bishop, peisert}@cs.ucdavis.edu

Marv Schaefer
Woodbine, Maryland, USA
bwapast@verizon.net

I. SUMMARY

This article is a retrospective of concepts and people who have contributed significantly to the IEEE Symposium on Security and Privacy over the past 30 years.

• We identify many individuals who have contributed to SSP as program chairs, general chairs, and heads of the overseeing IEEE technical committee.

• We recognize SSP participants who have provided significant leadership in creating and funding opportunities for research and development in security and privacy. Some contributions to advances in security are also discussed in following articles by Carl Landwehr and Douglas Maughan, both of whom have been major instigators of R&D programs at multiple U.S. government agencies.

• We highlight some influential SSP papers from three decades, and also efforts that have had significant impact in providing or stimulating effective technology transfer, as well as authors and educators whose work provided major contributions to academic curricula, all helping instill trustworthiness into computer-communication security.

• We identify some of the anniversary event honorees.

II. NOTABLE SSP PEOPLE

The 66 individuals listed in Table I all had significant roles in SSPs, mostly as program chairs and/or general chairs. Those who were *also* officers of the IEEE Technical Committee on Security and Privacy (TC-SP, which oversees SSP) are noted with *plus signs*, while two others who were TC officers but neither program chairs nor general chairs are noted with *asterisks*. All these individuals enhanced the success of SSPs, as well as many unmentioned others who provided additional volunteer services.

Stan Ames and George Davida were SSP 1980's organizers, more or less by the seat of their pants. They were essentially our founding fathers, bringing together the

Table I
SSP ORGANIZERS

Martin Abadi	Ulf Lindqvist
Stan Ames	Steve Lipner +
Lee Badger	Teresa Lunt
David Bailey	Patrick McDaniel
David Bell	John McHugh +
Steve Bellovin	John McLean
Terry Benzel +	Catherine Meadows
Tom Berson +	Jon Millen +
Matt Bishop	Bob Morris
G.R. Blakley	Andrew Myers
Bob Blakley	Roger Needham
Deborah Cooper +	Peter Neumann
George Davida	Hilarie Orman +
Richard DeMillo	Vern Paxson
Dorothy Denning	Adrian Perrig
George Dinolt	Birgit Pfitzman
Deborah Downs	Chuck Pfleeger *
David Du	Mike Reiter +
David Evans	Avi Rubin
Stephanie Forrest	John Rushby
Cristi Garvey	Marv Schaefer
Virgil Gligor	Roger Schell
Li Gong	Dan Schnackenberg
Yong Guan	David Shambroom
Tom Hinke *	Deborah Shands
Heather Hinton +	Dawn Song
Cynthia Irvine +	Peter Tasker
Paul Karger	Steve Tate
Steve Kent	Rein Turn
Richard Kemmerer +	Giovanni Vigna
Dale Johnson	David Wagner
Carl Landwehr +	Michael Waidner
Wenke Lee	Clark Weissman

Table II
SSP 1980 ATTENDEES

Stan Ames	Aileen MacGahan
Karl Auerbach	Leonard McNeill
Peppe Barbarino	Ralph Merkle
G.R. Blakley	Serge Miranda
David A. Bonyun	Daryll Maravek
George I. Davida	Frank Myers
Richard DeMillo	Peter Neumann
Dorothy Denning	Steven P. Reiss
Whitfield Diffie	Larry Robinson
J.K. Everton	Walter L. Ruzzo
Rich Feiertag	Mark Sadler
Dennis W. Fife	Adi Shamir
Don Good	Gus Simmons
Michael A. Harrison	Marv Schaefer
Martin Hellman	C.P. Schnorr
Lance Hoffman	Jennings T. Smith
Ingemar Ingemarson	Allen Stoughton
John P. Jordan	Joseph J. Tardo
Paul Karger	Rein Turn
Gerald Kreissig	Tony Wasserman
Stanley Kurzban	Bruce J. Walker
Richard Lipton	P.T. Withington
Lishing Liu	Lawrence Yelowitz

46 participants listed in Table II. Paul Karger and Peter Neumann are the most recent SSP attendees who were also present in 1980. Others from the 1980 SSP who are still active in work more or less related to security and privacy include George Davida, Dorothy Denning, Whit Diffie, Rich Feiertag, Lance Hoffman, Adi Shamir, Joe Tardo and Larry Yelowitz. Marv Schaefer returned to probe his memory for this article, after his past decade as the proprietor of Books With a Past (which included some surprising rare classics on cryptography and security).

Ames, Davida, G.R. Blakley (Bob's father), Marv Schaefer and Rein Turn were instrumental in organizing 1981. 1982 saw pre-proceedings distributed beforehand, when Neumann was program chairman, with assistance from Bob Morris, and with Roger Schell as general chair. 1983 again had pre-proceedings, under G.R. Blakley and Dorothy Denning. Beginning in 1984, the IEEE Computer Society produced proceedings in time for the meeting, and SSP began to develop some of the organizational structure and refinements of the reviewing process that emerged subsequently.

III. SIGNIFICANT SSP PAPERS

This is clearly not a complete history or a detailed self-contained analysis. It reflects our personal opinions and some other inputs. We encourage younger readers to cull the cumulative SSP DVD for papers of interest.

The 1980s

The 1980s were a period of can-do optimism and significant principle-based experimentation with worked examples, followed by recognition of the complexity of the problems that were known at the time. We suspected the problem set would get worse, but had no clear vision as to how soon it would! This was the period of Data Secure Unix, KVM/370, SRI's Provably Secure Operating System (PSOS), Ford Aerospace's Kernelized Secure Operating System (KSOS), SDBMS and SeaView, the Strategic Air Command Defense Information Network (SACDIN), the entertainingly overhyped universal Secure Ada Target (SAT), Secure Xenix, and the Secure Communications Processor (SCOMP) and Blacker crypto controller both of which addressed least privilege and covert channels.

NSA's Hilda Faust expressed significant doubt about the reality of covert-channel threats. Specifically, she objected strongly that there were so many easier ways to subvert system confinement that going through the contortions of signaling protocols was overkill. Next came the discovery of really high-throughput channels, and then unbounded and undetectable hardware channels. Frustration mounted as the technology became classified by the worried agencies. Finally, the military and commercial computer security initiatives collapsed because of the NCSC's evaluation priorities may have killed off incentives to invest in harder alternatives.

1980 included harbingers of things to come. David Bonyun had a worked-example paper on the SDBMS Kernel that was prototyped for Roger Schell at the Air Force Electronic Systems Directorate (ESD) at Hanscom Field. Serge Miranda (Toulouse) had a survey of secure database management systems that was seminal. The papers by Gus Simmons and Davida-DeMillo-Lipton were valuable. This was also the first of two meetings where the cryptographers left during a system session for private discussions.

In 1981, David Bonyun's paper on auditing picked up on the desire for intrusion detection that had been suggested by Jim Anderson [1]. Query modification (Dorothy Denning), Shirley/Schell, and Jon Millen's Flow Analysis of Formal Specs were also important early papers. Miller-Resnick proved to be an important lead-in to MLS DBMS architectures, though it wasn't

too obvious at the time that the Military Message System (MMS) would lead to that. (Debbie Cooper and Marv Schaefer were inspired to try a subsequent NRL project based on ideas in that paper.)

In 1982, Kemmerer's storage/timing channel paper was very timely, as was an important contribution to correlation analysis in the Kernelized VM (KVM) by Jane Solomon. Morrie Gasser and Gary Grossman presented highly contrasting semi-worked models for establishing secure LANs. Steve Lipner's paper on how MLS could be used in commercial applications provoked considerable discussion. Joseph Goguen and José Meseguer's noninterference paper was the basis for subsequent research (including their 1984 unwinding paper). 1982 also had a panel in which cryppies and system folks were actually together in a single session!

By 1983, the Woods Hole workshop put on by the National Academies' Air Force Studies Board produced research ideas for secure database management systems, urged the development of misuse-detetion systems, and also launched the idea of crypto-seals into the limelight, even though the idea was shot down during the workshop! That was the beginning of several attempts to produce true MLS DBMS prototypes, even as interim solutions were being undertaken; it led to several SSP papers noted below. Randell and Rushby's Distributed Secure System paper predestined the field of MILS systems (Multiple Independent Levels of Security). Hinke, Althouse and Kemmerer introduced Clark Weissman's idea of a formally modeled and verified secure review/release workstation. Berson, Feiertag and Bauer did the Processor-per-Domain guard. Both of these two papers indirectly led to the compartmented-mode workstation (CMW) that followed, in which some semblance of multilevel security was attempted, albeit with relatively low assurance. Virgil Gligor's paper on denials of service raised concerns that for the most part had previously been ignored.

1984 was when papers on worked examples really began to show up. KVM (Barry Gold et al.), Landwehr's hardware requirement paper, Paul Karger's paper on capabilities and lattices, and Dorothy Denning's crypto-seal paper were there, but the big change was the heavy emphasis on Formal Methodism. Euclid, Gypsy and Ada as *verifiable programming languages* were primarily there because it was believed that object code would end up being the hard problem, and that source code verification would be under control *soon.* With the help of misguided verifiable Ada initiatives, those hopes were subsequently crushed. McLean, Landwehr and Heitmeyer produced a sweet paper on the MMS

model, and Millen's paper on The Interrogator was around for a good while, revisited in 1995.

1985 continued the Formal Methodists' quest for supremacy. Terry Benzel's paper on the Secure Communications Processor (SCOMP) A1 evaluation was highly relevant, as was Gligor's Hardware analysis of the SCOMP. Gus Simmons' paper of broadcasting a secret stood out. Dorothy Denning presented a landmark paper on commutative filters, and Rich Graubart's new religion (crypto seals) started to take hits from the gathered audience. Boebert et al., gave a lovely paper on the Secure Ada Target (SAT). Papers by Terry Vickers Benzel and D.A. Tavilla, John McHugh and Don Good, and Norm Proctor on the Restricted Access (RAP) Guard also deserve mention.

Butler Lampson credits Jim Morris for saying "Capabilities are the way of the future, and always will be." In 1986 KeyKos came to the fore. It is still being reincarnated. Secure Xenix split up root privileges, and was the only Unix-class NSA/TCSEC B2 system. Leslie Chalmers gave an important paper that differentiated between security practices in the military and elsewhere—one that became important only after everyone had their own inconsistently maintained PC/OSs. Covert channels were a downer at this point. Dobson and Randell had a paper on building a secure system out of unreliable insecure components, which now appears to be the only way anything can be built (albeit without adequate trustworthiness). Haigh and Young extended noninterference for the SAT. Birrell, Lampson, Needham and Schroeder introduced a global authentication service that did not require global trust— which pioneered trust establishment in large-scale, long-lived distributed systems and networks.

1987 seemed to overendow the CMW. The Clark-Wilson paper became the other most-cited paper at the time, and it is still important. (See Section V.) There was a masterful paper by Paul Karger on Discretionary Trojan Horses, and Millen's covert channel capacity paper became a landmark despite the CMW stuff. John McLean's reasoning about security models began the Dueling-Formal-Modelist paradigm that still resurfaces. SeaView provided an off-the-shelf Oracle database system that was untrusted for multilevel security and yet became a multilevel-secure DMBS via its underlying MLS kernel (*balanced assurance*). Darrell McCullough introduced the series of Hook-Up property papers, ensuring that the formal Methodists would continue being funded. Young and McHugh considered mappings between implementation and specifications.

1988 brought Round 2 of the Duelling-Formal-

Modelists in McLean's and David Elliott Bell's papers; break-time debates diminished the audience for Jeremy Jacob's subsequent lovely paper on Tony Hoare's CSP and security specifications. Clark Weissman's talk on Blacker deservedly won acclaim at the symposium, although the paper could not yet be published. Ted Lee had a paper on a Biba-like model as a means of enforcing commercial security. Paul Karger produced a sensible data integrity paper using *secure capabilities.* While noninterference and composability of security properties continued to be addressed, the Crocker/Cohen/Landauer (née Rho)/Orman paper on the State-Delta reverification of FM8501 microprocessor was an impressive advance in applied formal methods! Viruses and intrusion detection were also treated at the symposium, and SeaView's polyinstantiation (different content for the same file name at different security levels) continued, along with a triad of tried-and-true analyses of Cristi Garvey and Amu Wu's ASD-Views project. People still cared about covert channels. McCullough extended his work on noninterference and the composability of security properties. John Markoff was introduced to Bob Morris (Robert Tappan Morris's father), who became a widely quoted source.

1989 was the Year of the Virus. The most news-related paper of the SSPs up until then was the Eichin-Rochlis analysis of the Internet Worm (With Microscope and Tweezers). This may well have been the beginning of the end for Formal Methodism's dominance of the symposia, though, as there were four papers and a panel on intrusion detection and virus-related flaws. Dave Brewer and Mike Nash presented their Chinese Wall Security Model and, while it didn't have as much expected impact as the Clark-Wilson model, in sooth it provided a basis for the popularity of hardware-based isolation kernels (proposed earlier by Randell and Rushby) in the form of IBM's PRSM, Amdahl's MDF and Hitachi's domain separation hardware. The SAT continued to be discussed by Sami Saydjari, et al., in their Logical Coprocessor Kernel (LoCK) Trek paper. Karger's immediate revocation paper still stands out, as does Li Gong's Identity-Based Capability System. The 10th SSP opened with three Fundamentals Revisited papers by Steve Walker (Network Security), Ted Lee (TCBs vs People), and Marv Schaefer (Symbol Security Condition Considered Harmful). These papers, the virus papers, and the newer results on aggregation and inference that came in from the SeaView Saga ushered in the new decade of pragmatic attempts to address the coming loss of control, but not yet of hope. A new thread of decreased-expectation Trusted Mockery papers was introduced by Branstad, Tajalli, Mayer and Dalva.

The 1990s

The 1990s were a time of growth, when ideas that had been discussed in the 1980s began to be realized, and when the application of methods developed in the 1980s bore fruit, and suggested new directions. Throughout, the topics of verification, assurance, covert channels, intrusion detection, and cryptography were examined and refined.

In 1990, the Heberlein et al. paper on a network-based intrusion detection system laid the foundation for distributed and wide-area misuse detection systems, and discussed a tool still in use today. Other papers discussed security aspects of the kernel and audit for the VAX Virtual Machine Monitor system, and challenged the use of MAC and DAC controls by presenting realistic situations in which these controls do not provide the necessary security. Cathy Meadows combined the Chinese Wall model with a multilevel policy to limit user access to aggregated data. Gong, Needham and Yahalom also extended reasoning about cryptographic protocols to include beliefs, so the logic could take into account information *implied* by the message as well as the explicit message content.

The 1991 symposium saw a flurry of work in covert channels; Wray's paper analyzed timing channels, Karger and Wray's paper a storage channel, and Porras and Kemmerer provided a general theory of analysis using covert flow trees. Other papers analyzed cryptographic protocols again; for example, Meadows discussed a system for studying key management protocols, and Tardo and Alagappan analyzed SPX, a distributed authentication service using public key certificates. Attendees also presented other work, especially on verification and on intrusion detection systems.

1992's program was quite diverse. Stubblebine and Gligor examined message integrity in cryptographic protocols, with interesting results. Bellovin and Merritt presented their EKE protocol paper this year, and Millen compared a base for protecting against denial of service attacks to a TCB. In addition to other papers on security models, covert channels, database security, and a paper on a trusted B3 window system, the proceedings contained the famous Blacker paper (noted above in 1988, but not cleared for publication until 1992).

In 1993, the theme of assurance recurred. Stubblebine and Gligor revisited integrity with a paper on how to design protocols for protecting message integrity. Another paper discussed assurance in distributed trusted Mach, and work on modeling computer viruses was

presented. Several other topics, such as work on cryptographic protocols and modeling covert timing channels, explored other topics.

Theory and practice of system engineering returned with a vengeance in 1994, with Abadi and Needham's paper on engineering practice for cryptographic protocols. McLean's delightful paper on composition for *possibilistic* security properties, and Gong and Qian's work examined the interoperation of secure systems, presenting results on its complexity and composability, extended the theory of composition of security properties. Reiter's paper presented a secure group-membership protocol. Another interesting paper by Forrest, Perelson, Allen and Cherukuri applied to computer systems the idea of *foreign* data and processes taken from the biological notion of infection, to distinguish legitimate data and processes from altered data and unauthorized processes. The application of biology to computer security would grow from this.

The 1995 symposium saw Sibert, Porras and Lindell raise a number of questions about hardware features, and existing flaws, that might produce security problems. A paper describing a domain type enforcement language, DTEL, applied the notion of type checking to UNIX systems. Commerce was a hot topic, with two papers on the application of cryptographic protocols to it, and a panel that examined e-commerce. Staniford(-Chen) and Heberlein presented their work on using statistical parameters of network connections to trace attacks. Kang, Moscowitz and Lee extended the NRL Data Pump to a network to handle covert channels and denier of service attacks. Millen analyzed the security of protocols with great success using a model and a tool called the Interrogator.

1996 brought extensions to the application of biological ideas with Forrest, Hofmayer, Somayaji and Longstaff's paper on anomaly-based intrusion detection using system-call data and Dhaeseleer, Forrest and Halman's paper on detecting change. Anderson applied security concepts to the medical arena with a paper on a policy model for Clinical Information System Security. Java security came under scrutiny with a paper by Dean, Felten and Wallach describing security flaws that arguably arose from weaknesses in design methodology. Finally, panelists from industry, academia, and government discussed education in computer security.

Testing widely accepted ideas seemed to be the hallmark of the 1997 symposium, which started with a debate on the value of the TCB concept (with Bob Blakely and Darrell Kienzle arguing it was fundamentally flawed, and Shockley and Downey arguing

that it has merit), followed by Arbaugh, Farber and Smith's work on AEGIS, an architecture for secure bootstrapping and Syverson's, Goldschlag's and Reed's analysis of the degree of anonymity provided by an implementation of onion routing. Intrusion detection work abounded, with Ko, Levitt and Ruschitzka's paper on specification-based intrusion detection, and Lindqvist and Jonsson's work systematically classifying intrusions to provide a taxonomy useful for incident reporting, intrusion detection systems, and so forth. Nor was theory neglected; Zakinthinos and Lee developed a general theory of security properties. John Mitchell, M. Mitchell and Stern used Murϕ, a general purpose state enumeration tool, to analyze cryptographic and other security-related protocols.

Reporting on Java security continued during the 1998 symposium. Wallach and Felten studied the internals of Java with their paper on Java stack inspection, while Malkhi, Reiter and Rubin routed applets to a *playground machine* on which they could run without damage to the user's system, yet route all input and output from and to the user's machine. Ghosh, O'Connor, and McGraw used software fault injection to dynamically find flaws in software. Key distribution for slow devices that has great relevance in the world of wireless systems. Bradley et al. looked for malicious routers that withheld or dropped packets by examining conservation of flow. Hinton introduced a way to represent, and then evaluate, assumptions about the desired behavior of the *environment* in which a system was used, thereby illuminating the strength (or weakness) of the basis for security assertions.

The penultimate year of the decade ended with papers on firewall management and software wrappers. Millen looked at reconfigurable systems that lost services due to failing components, and viewed the failure as a *flow* analogous to information flow; he was able to use Meadow's results in that arena to determine how to reconfigure the system using replacement components to restore services. Lindqvist and Porras used an expert system toolset, P-BEST, to detect misuse by analyzing several types of datasets and rule sets for attacks against which there was little defense; they showed that this scheme was suitable for realtime misuse detection. User acceptability was at the center of the the design of Adage, an authorization service for distributed applications.

1999 included 12 pages of short papers that surveyed changes in security research over the first 20 SSPs: G.R. Blakely (cryptography), Gligor (operating system security), Lipner (evaluation criteria and commercial

technology), Millen (covert channels), McLean (formal methods), and Stephen Kent (network security). Other papers looked at what changes might occur in the next 20 years: Weiser (use of computers), Needham (hardware environment), Shrobe (software technology), Orman (networking), and Snow (assurance, and the lack of it). Although but 10 years have passed, the reader is invited to revisit those papers and see how far along the path we have come—and how much farther we still have to go.

The 2000s

The dot-com boom had begun its bust just about two months prior to the 2000 SSP (after SSP submissions). Nonetheless, open source technologies such as Linux, Apache, and BSD were in full bloom, in competition with Sun's Solaris, Microsoft's Windows and its IIS Web server. Neumann, Lipner, Schneider and McGraw presented four short papers for an open-source panel session, with Brian Witten also on the panel.

In 2000, "the network was the computer" (also the motto of Sun Microsystems said) and analyses of networks received a surge of attention with key discussions of conservation of flow in network protocols by Hughes, Aura and Bishop; model checking of network vulnerabilities by Ritchey and Ammann; and automated analyses of firewalls by Mayer, Wool and Ziskind. During the dot-com boom, the rate of generation and storage of information increased as never before—and this included health care and medical records, creating obvious concerns. Irvine and Levin moderated a panel on health care and privacy.

With the startups and stock markets in full downward slide from the dot-com bust, 2001 also represented a return to tradition. Wagner and Dean considered performing intrusion detection via static analysis. Several papers on intrusion detection were presented, including a method for detecting anomalous program behaviors by Sekar, Bendre, Dhurjati and Bollineni. Old friends such as cryptography, information control, and access control dominated SSP, with papers exploring applications of traditional methods to modern concepts—such as applications of cryptography to voice recognition and mobile code.

The 1996 work by Forrest, Hofmeyr, Somayaji and Longstaff spawned a resurgence of interest in advanced machine-learning techniques, forensics, and other research described in many papers. In 2002, it also brought a key question: "why 6?", which led Tan and Maxion to apply the scientific method to the forefront to find out why sequences of length 6 provided the

best results for an intrusion-detection system. They recreated the scenario used by the original researchers, downloaded their software and data, and re-ran the experiments on both the original data and new data. Tan and Maxion's work not only supported the original research by explaining an observed phenomenon, but also emphasized the need for and value of the scientific method, and how well the original researchers had documented their work. Distributed intrusion detection and attack graphs also took the stage, with Sheyner et al. focusing on automated generation of attack graphs, Kruegel, Valeur, Vigna and Kemmerer focusing on IDS for high-speed networks, Cuppens and Miège also focusing on correlating alerts on networks, and Ko and Redmond applying noninterference to intrusion detection.

As in 2001, SSP 2003 saw a return to many old topics such as formal methods and crypto embedding, with discussion of hardware security for the first time in several years. The paper by Govindavajhala and Appel was particularly noteworthy, using bit flips to attack a virtual machine.

SSP has often focused on the technologies or algorithms themselves. 2004 added voting integrity, a topic that previously had existed primarily in magazines such as *IEEE Security & Privacy Magazine,* and later in workshops and conferences (the Electronic Voting Technology (EVT) workshop — organized by ACCURATE, A Center for Correct, Usable, Reliable, Auditable and Transparent Elections, supported by USENIX, and now combined with the Workshop on Trustworthy Elections (WOTE)). On the heels of government-sponsored investigations of the integrity of e-voting, and public concern about U.S. election meltdowns, Kohno, Stubblefield, Rubin and Wallach evaluated the technical elements of the Diebold (now Premier Election Systems) AccuVote-TS 4.3.1 electronic voting machine. They were also joined by a rare element of physical, rather than purely digital security, as Asonov and Agrawal explored *acoustic emanations* from keyboards. Yaar, Perrig and Sing re-incarnated capabilities in a network-level disguise, with a stateless mechanism for protection against large-scale DDOS attacks in the Internet.

Computer worms experienced a resurgence in the early to mid 2000's, with, among others, *Code Red* in 2002, *Sapphire* and *Blaster* in 2003, and *Witty* and *Sasser*. Researchers dove into analyzing worms and developing means to discover, quarantine, and prevent them from disrupting networks. As time passed, the worms became more sophisticated — for example, by exploiting polymorphism, and so became harder to

detect, analyze, and counter. In 2005, Newsome, Karp and Song focused on signature generation of just such worms.

Virtual machines had been around for decades, but in the mid-2000s, they gained considerable mainstream popularity. VMs were used as security tools, but were also occasionally liabilities. In 2006, King et al. extended the threat of kernel-based rootkits to rootkits that played the role of virtual machine monitors. Molnar, Kohno, Sastry and Wagner also continued their work in electronic voting machine security with their paper, Tamper-Evident History-Independent, Subliminal -Free Data Structures on PROM Storage.

2007 saw a large variety in approaches to security. For example Cui, Peinado, Wang and Locasto presented a key advance in the worm and botnet threat with their work on ShieldGen, which enabled automatic data patch generation of zero-day attacks, and was the first of numerous other SSP papers in the area. Huffmire et al. also developed new and important primitives for reconfigurable hardware. On the opposite end of the spectrum, Schechter, Dhamija, Ozment and Fischer performed usability studies on website authentication.

In 2008, something important changed: *data* anonymization and security rather than simply security of computers and networks took the stage. In particular, Cretu et al. presented their work in sanitizing training data for anomaly sensors; and Narayanan and Shmatikov, discussed de-anonymization of large datasets, as they mined the Netflix Prize datasets and Internet Movie Database in an effort to reverse engineer as much of the identity of reviewers as possible.

In SSP 2009, the best paper, Native Client: A Sandbox for Portable, Untrusted x86 Code, by Bennet Yee et al. combined various long-time research threads into a practical system. Narayanan and Shmatikov extended their earlier work by applying their techniques to even richer datasets from Twitter, Flickr, and LiveJournal. Yu et al. examined recommendation system security for the first time at SSP.

As we write this, SSP 2010 is not yet *history*. We expect it will be revisited in the 40th anniversary SSP.

IV. TECHNOLOGY TRANSFER

Several SSP attendees have inspired transfers of technology via start-ups and corporate acquisitions, in some cases with extensive real-world applicability. Examples include the following.

- Bill Arbaugh: Komoku Inc. (increasing the trustworthy of bootloads)—acquired by Microsoft, and now in the current product line
- Tom Berson: Anagram Laboratories, Sytek (secure local networks)—sold to Hughes Aircraft Corporation in 1988, becoming part of Hughes Network Systems
- Earl Boebert: Secure Computing Corporation (type-based security in LoCK, SAT, SideWinder, etc.)
- Steve Crocker: CyberCash Inc., Shinkuro Inc., Longitude Systems
- Tom Haigh: SCC. Adventium Labs
- Roger Schell: Gemini (GEMSOS), Novell
- Bruce Schneier: Counterpane Systems
- Also, Bob Blakley (IBM), Whit Diffie (Bell Northern Research, Sun Microsystems), Li Gong (SRI, Sun, Microsoft, Google, Mozilla), Paul Karger (DEC, IBM), Butler Lampson (PARC, DEC-SRC, Microsoft), Steve Lipner (Microsoft), Roger Needham (MSR), Mike Schroeder (PARC, DEC-SRC, MSR), and Steve Walker (Trusted Information Systems) have made important corporate contributions.

V. EDUCATION

Some of the most important early contributions predate SSP. These include Willis Ware's 1970 RAND report [9] and Jim Anderson's 1972 report [1]. The Anderson report was hugely influential in establishing computer security as a field and in the early years of SSP, at which Jim was a regular attendee for at least the first 20 years. (Jim is in the front row of the 1999 group photo, next to Tom Berson and Dick Kemmerer!)

In addition, Rein Turn's three Artech House volumes of collected papers on security, Matt Bishop's computer security books [2], [3], and Matt's NSA-sponsored collections of seminal papers (http://csrc.nist.gov/publications/history/) (including the Anderson Report) are valuable. The original Saltzer-Schroeder paper [8] and the succeeding Saltzer-Kaashoek book [7] are noteworthy, as well as earlier books by Morrie Gasser [4], and Chuck Pfleeger [6].

Many academic SSP participants have had major impacts on the teaching of security and privacy, such as Steve Bellovin, Matt Bishop, Matt Blaze, Virgil Gligor, Dick Kemmerer, Adrian Perrig, Mike Reiter, Avi Rubin, Dawn Song, Giovanni Vigna, David Wagner, and Dan Wallach, to name just a few.

Various SSP papers have become widely used in academic curricula. For example, Clark and Wilson's 1987 paper, A Comparison of Commercial and Military Computer Security Policies, significantly advanced the understanding of application integrity. Papers on composition of policy, such as McCullough's 1987 paper, Specifications for Multi-Level Security and a Hook-Up

Property, led to an exploration of the conditions under which different secure systems could be composed to produce a secure system. Dorothy Denning's 1986 paper, An Intrusion-Detection Model, fostered much work in analyzing systems and networks for compromises, and developing techniques to extract useful information from logs. Self-Nonself Discrimination in a Computer, 1994, by Forrest et al. led to the application of biological paradigms to protection and intrusion detection. Other papers such as Eichin and Rochlis' 1989 paper, With Microscope and Tweezers: An Analysis of the Internet Virus (actually a Worm) of November 1988, and Schuba et al.'s 1997 paper, Analysis of a Denial of Service Attack on TCP, described attacks in detail. Still others, such as Halperin et al.'s 2008 paper, Pacemakers and Implantable Cardiac Defibrillators: Software Radio Attacks and Zero-Power Defenses, presented security risks where they were least expected. The 2004 Kohno et al. paper, Analysis of an Electronic Voting System, reminded us that the application of security principles and practices is as important as discovering them.

VI. Research Incentivizers

Some SSP attendees have also played important roles in funding, incentivizing, stimulating, and directing R&D relevant to SSP from within the U.S. Government, particularly Lee Badger (DARPA), Drew Dean (DARPA), David Du (NSF), Carl Landwehr (NRL, NSF, IARPA, and NSF again), Karl Levitt (NSF), Teresa Lunt (DARPA), Hilda Faust Mathieu (NSA), Hilarie Orman (DARPA), Douglas Maughan (NSA, DARPA, DHS), Sami Saydjari (NSA, DARPA), Steve Walker (NSA, DARPA, OSD), and Jeanette Wing (NSF). Several other SSP attendees were influential in stimulating the intellectual conduct of such R&D, including Becky Bace, Dan Edwards, Ted Linden, Ann Marmor-Squires (all formerly at NSA), and Ken Shotting (still at NSA). In addition, Roger Schell served as Associate Director of the National Computer Security Center (NCSC, a relatively public arm of NSA); and Marv Schaefer and Bob Morris both served as the NCSC Chief Scientist.

Some pre-SSP history is also worth noting. ARPA contributed extensively to MIT supporting the design and development of Multics (which began in earnest in 1965). Roger Schell initiated significant efforts in computer security R&D when he was at AF-ESD. Roger and Paul Karger were involved in the MIT-Honeywell Multics AIM MLS retrofit in the early 1970s (along with Jerry Saltzer, Mike Schroeder and Rich Feiertag at MIT; Tom van Vleck at Honeywell; Steve Lipner, Jon Millen, Stan Ames, Ken Biba, David Bell, Len La

Padula, P.T. Withington, and Lee Schiller at MITRE; with Peter Neumann at SRI also participating). Roger's AF-ESD/MITRE group, the National Bureau of Standards (now NIST), H.O. Lubbes (NRL/SPAWAR), Doug Hogan and Hilda Faust (NSA) were aggressively sponsoring R&D, and were pretty much the only relevant funders of security research prior to 1980, along with the late JCR Licklider and Larry Roberts (ARPA)—who funded the ADEPT-50 security model and multilevel *secure* operating system in 1966-68. Other early funding included SRI's Provably Secure Operating System (NSA, 1973-80), SDC's contract with IBM to penetrate VM/370 in 1972-73, and its later work on KVM.

VII. Awards/Recognitions

The first two individuals below have played huge roles in funding research and stimulating advances in security and privacy. Other recognitions follow.

• Carl Landwehr, for many years in government organizations carrying out and incentivizing important research, and for his long-standing roles in the IEEE TC-SP, the IEEE *Security and Privacy Magazine,* and the Cipher Newsletter, as well as SSP. Carl receives an Outstanding Community Service Award from the Computer Society Technical Committee on Security and Privacy.

• Douglas Maughan, for his many years in government organizations carrying out and incentivizing important research, development, system evaluations, and technology transfer, for activities with the INFOSEC Security Council, and for producing an outstanding roadmap for future security research [5]. Doug receives an Outstanding Community Service Award from the Computer Society Technical Committee on Security and Privacy.

• John Markoff, for his superbly computer-literate and educationally valuable journalism, bringing the topics of SSP clearly into the public eye with his incisive and thoughtful writing throughout most of SSP's 30 years, with frequent newspaper articles, books, and occasional media appearances. John receives an Outstanding Community Service Award from the Computer Society Technical Committee on Security and Privacy.

• Jerry Saltzer, for his major contributions to the design and teaching of secure computer systems since the mid-1960s (culminating in [7]), and his major roles in Multics, Athena, Kerberos, and end-to-end security. His work has far-reaching importance. In addition, Jerry is the 2010 recipient of the National Computer Security,

Award given annually by NSA and NIST,[1] which is being presented to Jerry at SSP 2010 by Tim Grance.

We recognize several older SSP papers that subsequently appear to have had particularly significant impact, for the designated reasons relating to theoretical advances or practical utility in various areas.

- 1980s: Clark-Wilson (practical implications for application integrity); Goguen-Meseguer (theoretical formulation of noninterference and unwinding); Dobson-Randell (reality); Kemmerer (storage/timing channels); Denning (misuse detection); Weissman (Blacker)

- 1990s: Blaze-Feigenbaum-Lacy (decentralized trust management); Abadi-Needham (practical aspects of crypto); Dean-Felten-Wallach (Java security); Karger-Wray (storage channels)

- 2000s: Wagner-Dean (static analysis)

We anticipate that many other papers from the past and present decades will also be deserving of such recognition in the future, but we have not attempted to anticipate which ones might be so considered.

- We distinguish a few SSP papers that are frequently cited, listed alphabetically by first author.[2]

  ⋆ Blaze, Feigenbaum and Lacy, Decentralized trust management, 1996.

  ⋆ Cuppens and Miège, Alert correlation in a cooperative intrusion detection framework, 2002

  ⋆ Forrest, Hofmeyr, Somayaji and Longstaff, A sense of self for Unix processes, 1996.

  ⋆ Goguen and Meseguer, Unwinding and Inference Control, 1984, and Security Policies and Security Models, 1982.

  ⋆ Goldberg, Wagner, Thomas and Brewer, A secure environment for untrusted helper applications, 1996

  ⋆ Gong, A secure identity-based capability system, 1989

  ⋆ Song, Wagner, Perrig, Practical techniques for searches on encrypted data, 2000

Many other individuals also deserve recognition, as indicated.

- George Davida and Stan Ames, SSP's founding fathers.

- Jon Millen and Dick Kemmerer, for the most SSPs attended. (Each of them missed out in 1980 because of schedule conflicts.)

---

[1]Previous recipients of this award are Jim Anderson, Dennis Branstad, Steven Bellovin, David Clark, Robert Courtney, Dorothy Denning, Whit Diffie, Virgil Gligor, Marty Hellman, Butler Lampson, Peter Neumann, Donn Parker, Ron Rivest, Roger Schell, Mike Schroeder, Eugene Spafford, Walter Tuchman, Steve Walker, and Willis Ware—almost every one of whom has been an SSP attendee!

[2]Our efforts to be more comprehensive have not been satisfactory. For example, Citeseer and Google Scholar both provide incomplete coverage of SSP papers. Thus we eschew giving specific counts.

- Adrian Perrig, for the most accepted papers (17), followed by Dawn Song, and Mike Reiter, who overtook Millen, Gligor and Lunt.

- Clark Weissman, for the paper that took longest span between submission to publication in the proceedings (Blacker, four years, accepted and presented in 1988, published only in 1992)

- Terry Benzel, for long-standing organizing contributions to SSP and TC-SP

- Tom Berson, for long-standing contributions to SSP and TC-SP, especially for his role as chief negotiator of the Claremont contract for many years.

- Karl Levitt, for multiple roles as a researcher, educator, government program manager, and participant in the Infosec Research Council government consortium.

- Dorothy Denning, for her unique style of presentation—with successive years of intricate multiple-viewgraph overlays, including a black box with emergent dental-floss. Dorothy apparently found it difficult to recall the exact order of fold-overs in her most elaborate sequence, but graciously reconstructed and annotated a simpler example:

  http://www.csl.sri.com/neumann/denning.pdf.

- Peter Neumann, for his innumerable contributions to both SSP and the field, usually coupled with taking RISKS making good (and bad) puns, and for leading the work on this paper. [Disclaimer: Peter was not involved in this selection.]

- Matt Bishop, for his educational efforts, books, and collections of classic papers noted above. [Disclaimer: Matt was not involved in this selection.]

- Marv Schaefer, for his outstanding work, his seminal role as NCSC Chief Scientist, his incredible historical, literary, and linguistic knowledge, and for inspiring The Marv Schaefer Players, which are awarded the distinction of having had the Best Theatrical Presentation at SSP. See Marv Schaefer, Curt Barker and Chuck Pfleeger, The Tea and I: An Allergy, 1989.
(Alle-gory details are online: http://ieeexplore.ieee.org/stamp/stamp.jsp?tp=&arnumber=36292
Debbie Cooper played the Dark Lady. In gown and pointy-hat, Ellen McDermott was the Reclusive Priestess (holding an oversized Cliff Notes for the Trusted Network Interpretation, TNI). Debbie Estrin did a realistic portrayal of the Maiden Scorned, much paean to the pain of Debbie Cooper and Tom Berson. When the people whose personages were obliquely depicted recognized themselves, the cast was briefly visited by a few security officers! [Disclaimer: Marv was not involved in this selection.]

- Finally, we owe hearty thanks to Hilarie Orman,

who played a vital role in producing the 30th anniversary banquet event (which was conceived jointly by her, Cynthia Irvine and Terry Benzel). Hilarie's long-standing involvement with SSP and the IEEE Computer Society Technical Committee on Security and Privacy (recently, Cipher Newsletter Editor, and as of 2010 the TC-SP Chair) has been very productive. Hilarie is also recognized for the idea and execution of combined all-years DVD for SSP and the Computer Security Foundations workshop. (Jonathan Herzog is the co-editor on the CSF side.) This was a project she lobbied for with both conferences over a period of years, and which has been invaluable to researchers whether or not they were present in past meetings.

All in all, the past 30 years of SSP have been extraordinarily filled with interesting ideas and interesting people, and we are very happy to have been able to revisit some of our memories. Although we sought to be objective throughout, we have undoubtedly failed to identify other important contributions because our selections inherently reflect our own opinions.

VIII. SSP Dinosaurs

Along the lines of the SSP troglodytes[3] named in Table II and other early SSP attendees, a few specific dinosaurs are worth noting:

⋆ *Steg(an)osaurs* (possibly implying constructive or other uses of information hiding and covert channels): Jon Millen, Virgil Gligor, and Marv Schaefer.

⋆ *Brontësaurs:* Debbie Cooper, Dorothy Denning, Debbie Downs, Teresa Lunt, Cathy Meadows, Grace Nebaldi, Hilarie Orman, Dawn Song, and other long-time SSP Janes (albeit not Austentatiously).

⋆ *Archosaurs:* Those who have long stressed low-vulnerability system architectures (as in crocodilians) that minimize what must be trustworthy (and trusted)—e.g., Boebert, Gligor, Lampson, Needham, Neumann, Saltzer, Schaefer, Schell, Schroeder, and many others.

In addition, a few other dinosaur types seem worth noting more generally:

⋆ *Veloci(w)raptors:* Past authors have dealt with security-preserving speed-ups and other optimizations, or with security-enhancing wrappers. Few have dealt with both. Small and agile predators continue to harass large systems.

---

[3]Here, *troglodyte* is a polymorphic term. On one hand, it often refers to primitive people—cavemen and cavewomen (and security is still primitive in many regards). On the other hand, its Greek derivation is *one who creeps into holes,* which has the nicely ambiguous connotation of finding security vulnerabilities and research lacunae.

⋆ *Ankylosaurs:* Those who still believe that COTS systems are well-armored (ignoring even their ankyl-biters!).

⋆ *Archaeopteryxes:* Those who have transitioned security from land to air.

⋆ *Spinosaurs:* Those who insist on claiming 100% security.

⋆ *Wannanosauruses:* Even if you really don't wanna know them, these were very small and pesky, like microraptors—and stealthy malware.

⋆ *P(e)terodactyl:* Despite PGN's heavy-footed poetic license (as in *dactylic petameter*?), he's one of the still-active dinosaurs. (Is this his Glorious Swansong?)

IX. In Memoriam

Several of our long-time contributors and participants can unfortunately no longer be with us for the celebration, notably including Jim Anderson, Joseph Goguen, Ted Linden, Roger Needham, Dan Schnackenberg, and Rein Turn. We miss them all, and deeply regret if we have omitted others.

X. Conclusions

This article has focused primarily on the extended SSP family, which we believe has had significant impact on security and privacy. The advances in research and development noted here are considerable. However, although the body of SSP works and other contributions such as the Saltzer-Schroeder paper [8] and the recent Saltzer-Kaashoek book [7] have provided some important directions for the future, the collected wisdom still needs to be more widely deployed in practice. For example, the pervasive nature of malware (from the Internet Worm to viruses and Conficker) and continuing exploits (such as iPhone and Predator Drone so-called *hacks*) suggest that some of the lessons of the past and outstanding research are frequently ignored in practice.

A prevailing myth is that if something is not now on the Web, it never existed. Less facetiously, if something meaningful happened in computer-related security and privacy, it is likely to have been a topic presented and discussed at SSP, and its progenitors were here at one time or another.

Note: We are grateful to David Evans and Virgil Gligor for their very helpful comments, and Ulf Lindqvist and Jenny McNeill for their assistance way beyond their roles in SSP.

REFERENCES

[1] J.P. Anderson. Computer Security Technology Planning Study. Technical Report ESD-TR-73-51, U.S. Air Force Electronic Systems Division, October 1972. (Two volumes).

[2] M. Bishop. *Computer Security: Art and Science*. Addison-Wesley Professional, Boston, MA, 2003.

[3] M. Bishop. *Introduction to Computer Security*. Addison-Wesley, Reading, Massachusetts, 2004.

[4] M. Gasser. *Building a Secure Computer System*. Van Nostrand Reinhold Company, New York, 1988.

[5] D. Maughan. A Roadmap for Cybersecurity Research. Technical report, Department of Homeland Security, November 2009.

[6] C.P. Pfleeger. *Security in Computing*. Prentice-Hall, Englewood Cliffs, New Jersey, 1996. Second edition.

[7] J.H. Saltzer and F. Kaashoek. *Principles of Computer System Design*. Morgan Kaufmann, 2009. Chapters 1-6 only. Chapters 7-11 are online: http://ocw.mit.edu/Saltzer-Kaashoek.

[8] J.H. Saltzer and M.D. Schroeder. The Protection of Information in Computer Systems. *Proceedings of the IEEE*, 63(9):1278–1308, September 1975.

[9] W.H. Ware. Security Controls for Computer Systems. Technical report, RAND report for the Defense Science Board, 1970. http://cryptome.org/sccs.htm.