

**STEVE H. WEINGART**  
572 Wagon Wheel  
Spring Branch, TX 78070  
(830) 885 6065  
shw@gulf-stream.net

## **SUMMARY:**

Senior electronics/hardware design engineer and manager/team leader with skills in architecture, design, and implementation of analog, digital, CPLD/FPGA, and microprocessor/embedded systems. Extensive background in cryptographic and physical security systems design and penetration. Experience with networking and development of web-based information processing and retrieval systems. Management and project leadership experience, as well as vendor, manufacturing, and test interface experience. RoHS conversion/compliance experience.

## **EMPLOYMENT:**

**Engineering/Networking Consultant & Owner**, Gulfstream Technologies, Inc.; Boca Raton, FL. and Spring Branch, TX. Intervals: 1995 – Present.

Projects for Secure Systems and Smart Cards, IBM Thomas J. Watson Research Center:

- IBM 4758 Secure Processor (hardware architecture and prototype implementation, physical security design, FIPS 140-1 level 4 validation documentation and coordination).
- IBM Citadel II Secure Processor Research Project.
- IBM 4755 ISA gate array reconstruction (debug of faulty Verilog design in field).
- Power Analysis (SPA/DPA) Attacks on Smart Cards.
- Penetration Analysis for Physical Security Systems.

Other projects:

- SSP7100 Security Coprocessor Development for Futurex
- File/Web server installation, Networking/computer support.
- Computer Services

Duties: Architecture, design, implementation, and technology transfer of embedded electronic systems for computer security. Team leader for several phases of several of these projects. Technology transfer and technology training supplied for U.S. and European development and manufacturing groups. Professional association papers authored and patents filed in conjunction with the development of new technologies. Also worked with group at IBM Charlotte, NC, to debug and correct mistakes in a product critical ASIC (IBM 4755 gate array). CPLD/FPGA design – mixed ABEL and schematic -- simulation in Synario, card schematics and layout in Orcad, PADS and Schema, some test code in REXX and C. Most recent project: Security coprocessor development using an IBM 405GP PPC. Web, file, VPN and discussion group server installation and networking support under Linux and Windows 95, 98, 2000 & XP). General computer services.

**Chief Scientist**, Futurex; Bulverde, TX. 2004 to 2006.

Projects:

- Redesign of 1U Product Line (KMS7000, EBS7000) to improved manufacturability and lowered cost. Moving to a common platform has lead to the rapid development of additional products (SKI3000 & 4000). Included design of Ethernet HW for new network based products.
- Development of improved processes and procedures to improve efficiency and performance in engineering, manufacturing and operations.

- FIPS 140-2 level 3 validation process for Futurex cryptographic products

Duties: Management and hardware development, oversight of outsourced manufacturing operation. Development of engineering and manufacturing process and procedure. Representation of company at technical venues (conferences, standards organizations). Responsible for setting the technical direction of the company. Design and implementation of new cryptographic, networking and support hardware. Manufacturing conversion for RoHS compliance.

**Senior Hardware Engineer**, Cryptographic Appliances, Inc., Roseville, CA.  
2001 – 2002 (Telecommuted from Boca Raton, FL)

Project: Trillian Cardbus/PCI Secure processor

Duties: Architecture, design, implementation of embedded electronic systems for computer security and cryptography. Research and development into low cost/high manufacturability physical security sensor technology (FPGA design in Quartus II, mixed VHDL and schematic, simulation in ModelSim, card schematics and printed circuit layout in Orcad).

**Research Staff Member**, IBM, Thomas J. Watson Research Center, Yorktown Heights/Hawthorne, NY, 1999 – 2001. (Telecommuted from Boca Raton, FL)

Projects for Secure Systems and Smart Cards, IBM Thomas J. Watson Research Center:

- IBM 4758 Secure Processor and follow-on devices (hardware architecture and prototype implementation, physical security design, FIPS 140-1 level 4 validation documentation and coordination). This work resulted in the first FIPS 140-1 level 4 validated device.
- Power Analysis (SPA/DPA) Attacks on Smart Cards.
- Penetration Analysis for Physical Security Systems.

Duties: Architecture, design, implementation, and technology transfer of embedded electronic systems for computer security. Team leader for several phases of several of these projects. Technology transfer and technology training supplied for U.S. and European development and manufacturing groups. Professional association papers authored and patents filed in conjunction with the development of new technologies. (CPLD/FPGA design -- mixed ABEL and schematic -- and simulation in Synario, card schematics and layout in Orcad, some test code in REXX and C)

**Partner & Manager of Computer Operations**, Professional Review Network, Inc., Boca Raton FL/Somers, NY. 1996 – 1999

Duties: Development of a web-based automated insurance utilization review system that algorithmically reviewed patient input data for clinical necessity of care. Management of development, I/S, and user support. Design and implementation of all software for initial production (HTML, JavaScript, CGI scripts in REXX, some Perl), developed care algorithm methodology, and implemented CGI-forms based SSL secured web site.

**Advisory Engineer**, SDI, Sunrise, FL. assigned to: IBM Manufacturing Technology Center, Boca Raton, FL. 1993 - 1995.

Project: Development of a Hard Disk Media Flatness Test Tool; Lead Hardware Engineer.

Duties: Design, implementation and integration of system electronics including; A DSP controlled 20 MHz. CCD line-scan camera interface/data processor, signal capture/conversion electronics, digitally

controlled servo/motion control devices, machine control I/O, system power distribution and grounding. (CPLD/FPGA design, -- mixed ABEL and schematic -- simulation in Synario, card schematics in Schema and layout in Pads).

**Advisory Engineer**, IBM, Boca Raton, FL. 1991 - 1993

Projects:

- IBM PDS Speech Recognition System; Lead Hardware Engineer.
- IBM ThinkPad 700T; Lead Planar Engineer.

Duties: Leader/member of development team. Debug and redesign based on test and manufacturing findings. Coordination of test process for thermal, environmental and EMC/EMI testing. Interfaced with and coordinated physical design and manufacturing groups during development. (schematics in ViewLogic, PLD design in ABEL).

**Advisory Engineer** (highest position attained), IBM Thomas J. Watson Research Center, Yorktown Heights, NY, 1983 - 1991.

Projects:

- Citadel security co-processor; Architect, Lead Hardware Engineer.
- ABYSS security co-processor; Hardware Design Engineer.
- Experimental electron microscope video; Hardware Design Engineer.

Duties: Architecture, design and implementation of secure co-processors including microcomputers (80386SX, Z80, 8051), cryptographic hardware (high speed DES), physically secure packaging (including prototype package tooling) and physical security electronics (analog, micro-power). On NIST panel that assisted in the writing of FIPS 140-1. Experimentation in the area of electron beam testing and lithography, and optical testing and lithography. Design and implementation of analog and digital hardware for scanning electron microscopes. Also responsible for upgrading SEM video systems, and repair and maintenance of SEMs. Design and implementation of servo and control electronics used for positioning in optical testing. (schematics in Schema and CBDS, layout in PADS and CBDS, PLD design in ABEL).

Duties also included: Design tool selection and maintenance, system and LAN software installation and support (DOS, OS/2), interface circuitry (PC bus and Microchannel), test software in assembler and REXX, and materials selection for packaging.

**Senior Electronics Design Engineer**, L.J. Gonzer Associates, assigned to IBM, Thomas J. Watson Research Center, Yorktown Heights, NY, 1982 - 1983.

Project: ESP, XY to octopole SEM scanning conversion system.

Duties: Design and implementation of analog and digital hardware for scanning electron microscopes, including an 8 pole electrostatic deflection system which included an opto-isolated computer interface, a high speed digital deflection calculator, raster generator, digital to analog converters, and deflection amplifiers.

## EDUCATION:

University of Miami, Coral Gables, FL. Bachelor of Science:  
Electrical Engineering, August 1978.

## HONORS AND ASSOCIATIONS:

- Eta Kappa Nu, Electrical Engineering Honors Society.
- IBM Outstanding Innovation Award.
- IBM First, Second and Third Patent Plateau Awards
- Eagle Scout, Boy Scouts of America.
- IBM Boeblingen Lab Innovation Contest **IDEal 1998** Winning Team Member. The main assessment criteria for the Innovation contest are: Relevance for the IDE (IBM Deutschland Entwicklung, IBM Germany Development), actually achieved results, visible evidence, improvement of IBM's competitive position and individual creativity.
- Divisional award, IBM Microelectronics Division, 9/2000, for manufacturing emergency recovery work in 1999.

## PROFESSIONAL ACTIVITIES:

- Invited member of NIST FIPS 140-1 (Computer Security) standard panel.
- Invited attendee of NIST FIPS 140-3 Physical Security Workshop
- Invited Talks
  - **Physical Security Devices for Computer Subsystems: A Survey of Attacks and Defenses**. Presented to JASON (DARPA study group), summer, 1998.
  - **Physical Security Devices for Computer Subsystems: A Survey of Attacks and Defenses** and **Physical Security and Hardware Architecture for the IBM 4758 PCI Cryptographic Coprocessor**. Presented at the Cambridge University Computer Science Department, Cambridge England.
  - **Physical Security Devices for Computer Subsystems: Design, Pitfalls, and a Few Hacks**. Presented to the S. FL Embedded Developer's Group. Nov 2001.
  - **Decrypting Cryptography** Presented to the ACE conference; San Diego, CA; 2003, and the EBUG Conference; Barcelona Spain 2004
- Papers and publications (authored or co-authored).
  - **Physical Security for the uAbyss System**. IEEE Security and Privacy, 1987.
  - **An Evaluation System for the Physical Security of Computing Systems**. IEEE Sixth Annual Computer Security Applications Conference, 1990. (co-authored)
  - **Physical Security Devices for Computer Subsystems: A Survey of Attacks and Defenses**. IBM Security ITL, 1991.
  - **Gray Market Computer Chips**. IBM Confidential industry white paper, Feb., 1998. (co-authored)

- **Building a High Performance, Programmable Secure Coprocessor** . Computer Networks and ISDN Systems, Special Issue on Network Security (to appear) (co-authored).
- **Using a High Performance, Programmable Secure Coprocessor**. 2nd International Conference on Financial Cryptography. 1998. (co-authored)
- **Validating a High-Performance, Programmable Secure Coprocessor**. IBM Research Report (co-authored).
- **Physical Security for Computing Systems: A survey of Attacks and Defenses**. Cryptographic and Embedded Systems Workshop, 2000
- **Building the IBM 4758 Secure Coprocessor**. IEEE Computer, 10/2001, pp 57 – 66 (co-authored)
- **Mind the Gap: Updating FIPS 140**. NIST FIPS 140 Physical Security Workshop, 2005. (co-authored)
- Patents, issued:
  - **Tamper-responding encapsulated enclosure having flexible protective mesh structure I**
  - **Tamper-responding encapsulated enclosure having flexible protective mesh structure II**
  - **Externally controlled DSP with input/output FIFOs operating asynchronously and independently of a system environment**.
  - **Data protection by detection of intrusion into electronic assemblies I**.
  - **Data protection by detection of intrusion into electronic assemblies II**.
  - **Tamper-resistant packaging for protection of information stored in electronic circuitry**.
  - **Apparatus for Detecting Cable Attachment**
  - **Hardware Access Control Locking**.
  - **Establishing and Employing the Provable Untampered State of a Device**
  - **Securely Downloading and Executing Code from Mutually Suspicious Authorities**.
- Patents, applied for:

- **Method and Device for Securely Handling Information in a Cryptographic Information Processing System.**
  - **Additional patents applied for, or in process, still confidential**
- 
- Two published inventions.

**REFERENCES:** Available on Request.