Authentication of a Computer-based System

Possible Authentication Methods Using the Computational Block as an Example

James L. Fuller
Pacific Northwest National Laboratory
Purpose of Authentication

- To assure the monitors that the “host-supplied” equipment is making credible measurements:
  - assure that the system is assembled as designed,
  - assure that the system functions as designed,
  - assure the monitors that the host-supplied equipment does not contain a “hidden-switch” that allows the host to pass out-of-spec materials.
The Hidden-Switch Issue

- The term “hidden-switch” is used to denote any method, device, or feature in the measurement system which could be used by the host to fool the monitor.
- A “hidden-switch” could enable the host to covertly and erroneously pass selected canisters.
- A “hidden-switch” could reside in either hardware, software, or a combination of both.
Methods of Authentication

- Use of trusted, unclassified calibration sources
  - Demonstrated in the course of operating the system and subject of another presentation
- Random selection of equipment
  - Possible application for both hardware and software
- Use of Documentation
  - An especially useful confidence building tool, if random detailed examinations are allowed

Ideas on how to use random selection and documentation will be described in detail for the case of the Computational Block.
Designing for Authentication

- Select elements that support transparency:
  - availability of extensive documentation;
  - minimal or no extraneous functionality;
  - software utilizing inexpensive or publicly available source code.

- Design and engineer the system to be easily inspectable:
  - design for ease of disassembly & reassembly;
  - use printed circuits rather than wirewrap, or hand-wired circuit;
  - use two-layer printed circuits rather than multiple layers;
  - spread out elements with labels accessible;
  - use a single layer of circuit boards;
  - removable and/or transparent lids;
  - provide easy-to-use test points.

- Using identical elements reduces authentication effort.
Computational Block—Location In System

NMC NEUTRON SENSOR

PU300/PU600 HPGe SENSOR

PU900 HPGe SENSOR

NMC CPU
AMPRO 386SX

SYMMETRY CPU
EMAC 486DX

PU300 / PU600 CPU
EMAC 486DX

PU900 CPU
EMAC 486DX

COMPUTATIONAL BLOCK CPU
AMPRO 386SX

HARDWARE-ONLY DATA BARRIER

Fiber Optic Data Link

OUTPUT DISPLAY
RED/GREEN LIGHTS
Attribute Measurement System
Computational Block

Push-Button
On/Off Switch
Computational Block Elements

Hardware
- Ampro CoreModule 3SXi – 80386 25-MHz processor card
- Ampro MiniModule SVG-II – Video controller card
- Diamond Systems: Emerald-MM-DIO – I/O card
  - Four COM ports and 48 bits of digital I/O
- Computer case with connectors
- Power Supply (AC to 5 VDC)

Software
- DataLight: ROM-DOS version 6.22 – Operating System
- WCSC: COMM-DRV/LIB version 17.0 – COM Port Driver Software
- LANL: DATA_ATT – Computational Block Software
- Microsoft: MS Visual C version 1.52 – Compiler
Computational Block—Inside-View

- Push-Button On/Off Switch
- Condor GSC20-5 5V 3.8A switching power supply
- Corcom6EC1 Line Filter & AC connector
- Fuse
- PC/104 Stack
  - Ampro: 3SXSi processor card
  - Ampro: SVG-II video card
  - Diamond Systems: Emerald-MM-DIO card
- Data Output
- Control Input
- Video Output
- NMC Pu600/300 Serial Inputs
- Pu900 Symmetry Inputs
AMPRO 3SXi Specifications

- 25 MHz 386SX processor
- 2 Mbytes DRAM memory (main memory)
- Shadow RAM support for BIOS
- 14 interrupt channels
- 7 DMA channels
- Three 8254-equivalent programmable timers
- Standard PC/AT keyboard port
- Standard PC speaker port
- Battery-backed real-time clock
- CMOS RAM (support for battery-free operation)
- Award ROM BIOS with Ampro embedded-system extensions
- Two serial ports (COM1 & COM2)(unused)
- One multimode parallel port (LPT)
- Floppy Disk Controller (unused)
- IDE Disk controller (unused)
- 32-pin byte wide memory socket (1.0 Mbyte PROM)
- 2-kbit configuration EEPROM (battery-free boot support)
- Watchdog Timer (trigger hardware reset or NMI)
Random Selection of Equipment

• The concept is that of the host providing the monitor multiple copies of key hardware or software to select for use and for private examination.

• If the measurement system is a relatively inexpensive, portable unit, then random selection by a monitor of complete systems provided by the host is a very powerful method of authentication:
  – allows for detailed private examination of equipment by host at a later time;
  – maximizes confidence of host in system.
Random Selection of Equipment, Continued

• Multiple copies of large, expensive versions of installed systems for random selection is not considered practical.

• For large systems, random selection of key hardware and software elements would also provide the monitor with significant confidence in the fidelity of a host-supplied system.
Random Selection Examples as Applied to the Computational Block

- It should be feasible to have multiple copies of the entire computational block subsystem.

- It should also be feasible to offer key elements of the computational block for random selection:
  - Ampro 3SXi motherboard example
  - Ampro 3SXi source-code-loaded PROM example.
Authentication Using Documentation

- The usefulness of documentation to authenticate complex hardware and software is limited by the complexity of the equipment.
  - This is one reason it is very important to utilize systems that are only as complex as they need to be, systems that have had extraneous functionality removed.
  - The right of the monitor to randomly select any subsystem of a complex system for focused inspection using detailed documentation can be an effective authentication tool.
Authentication Using Documentation, Continued

• The usefulness of detailed documentation for authentication is maximized if the integrated measurement system has been jointly developed.

• The usefulness of hardcopy source code documentation of software for authentication is limited, especially for complex code:
  — machine-readable source code expedites authentication measures;
  — methods and procedures to validate source code and compiled code would be a very good subject for joint development.
Using Documentation to Authenticate the System Configuration

- Hardware
  - Elements
  - Interconnections
  - Switch & jumper settings
  - Hardware settings made by software

- Software within the CPU
  - All executable code (in PROM)
  - BIOS code (in system ROM)
  - CPU setup parameters (in configuration memory)
  - Interrupt vectors (in RAM)
Detailed Computation Block Documentation

Chapter 1  Computational Block Overview
Chapter 2  CPU Card
Chapter 3  Video Card
Chapter 4  Quad COM Port and Digital-I/O Card
Chapter 5  Additional Hardware Support Documentation
Chapter 6  Commercial System Software
Chapter 7  Computational Block Applications Software
Chapter 8  PROM ICs
AMPRO 3SXí Schematics

- Five sheets of Ampro 3SXí schematics are available.
- Possession of schematics requires a nondisclosure agreement with Ampro, Inc.
- Schematics useful for:
  - determining 3SXí parts list,
  - discovering extraneous functionality,
  - jumper functional details,
  - selecting test points.
AMPRO 3SXi
Bottom View

- Quad NOR
- RS-486 Line Driver
- RS-232 Line Driver
- RAM Controller
- Clock
- Setup EEPROM
- 8-Bit Register
- 12V Flash Memory Programmer
- 8-Bit Register
# AMPRO 3SXi Parts List (ICs Only)

<table>
<thead>
<tr>
<th>Socket</th>
<th>Part: Vendor Part Number</th>
</tr>
</thead>
<tbody>
<tr>
<td>SO</td>
<td>32-pin Socket for 1Mx8 (1-Mbyte) PROM memory — Atmel, AT27C080</td>
</tr>
<tr>
<td>U5</td>
<td>1Mx16 (2-Mbyte) RAM Memory — Toshiba, TC5118160CFT-60</td>
</tr>
<tr>
<td>U6</td>
<td>1Mx8 (1-Mbyte) Flash Memory — Intel, 28F008SA</td>
</tr>
<tr>
<td>U8</td>
<td>Real-Time Clock w/ Setup CMOS Memory — Benchnmarq, BQ3285S</td>
</tr>
<tr>
<td>U9</td>
<td>Programmable Electrically Erasable Logic (PEEL) Chip — 16V8</td>
</tr>
<tr>
<td>U10</td>
<td>Embedded Microcontroller (386SX) — Acer Labs, ALi M6117C</td>
</tr>
<tr>
<td>U11</td>
<td>Power-on-Reset Chip — MAXIM, MAX809</td>
</tr>
<tr>
<td>U12</td>
<td>I/O Controller — SMSC, FDC37C666GT</td>
</tr>
<tr>
<td>U13-14</td>
<td>RS-232 Line Driver — SIPEX, SP211CA</td>
</tr>
<tr>
<td>U15</td>
<td>Quad 2-input NOR Gate — Fairchild, 74ACT02</td>
</tr>
<tr>
<td>U16</td>
<td>Non-Volatile RAM Controller — MAXIM, MXD1210</td>
</tr>
<tr>
<td>U17</td>
<td>Hex D-type Flip-Flop — Harris, 74HCT174</td>
</tr>
<tr>
<td>U18</td>
<td>Flash Memory Programming Supply — Linear Technologies, LTC1262</td>
</tr>
<tr>
<td>U19</td>
<td>2-kbit Setup EEPROM — Motorola, 93LC56X</td>
</tr>
<tr>
<td>U20</td>
<td>Clock Chip — ICS, AV9154-16</td>
</tr>
<tr>
<td>U21-23</td>
<td>8-bit Register — Fairchild, 74HCT245</td>
</tr>
<tr>
<td>U24</td>
<td>8-bit Register — Motorola, 74HCT244A</td>
</tr>
<tr>
<td>U25</td>
<td>RS486 Line Driver — Linear Technologies, LTC485</td>
</tr>
<tr>
<td>U35</td>
<td>8-bit Register — Fairchild, 74HCT245</td>
</tr>
</tbody>
</table>
AMPRO 3SXi Mechanical Dimensions

Figure 1–1. Mechanical Dimensions
AMPRO 3SXii Jumper and Connector Locations

Figure 2–1. Connector and Jumper Locations
## AMPRO 3SXi
### Hardware Jumpers

<table>
<thead>
<tr>
<th>FUNCTION</th>
<th>Default</th>
<th>Used</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>W1</td>
<td>RS-232C/RS-485 Select</td>
<td>1=2</td>
<td>1=2 COM2 uses RS-232C 2=3 COM2 uses RS-485</td>
</tr>
<tr>
<td>W2</td>
<td>BIOS/OEM Flash programming power enable</td>
<td>Off</td>
<td>On = connects V&lt;sub&gt;pp&lt;/sub&gt; for Flash EPROM programming</td>
</tr>
<tr>
<td>W3</td>
<td>Byte-Wide Socket Configuration</td>
<td>3=4 6=7 8=13 9=14 10=15</td>
<td>15-pins see page 2-23 for EPROM programming 27C080 = 1-Mbyte EPROM used</td>
</tr>
<tr>
<td>W4</td>
<td>Watchdog Timer Output Selection [if enabled in SETUP]</td>
<td>Off</td>
<td>1=2 = Hardware Reset 2=3 = I/O Channel Check (NMI) open = IRQ8 turns off interrupt</td>
</tr>
<tr>
<td>W5</td>
<td>DMA ACK1/ACK3 For Parallel Port = LPT</td>
<td>Off</td>
<td>1=2 selects DMA channel 1 2=3 selects DMA channel 3</td>
</tr>
<tr>
<td>W6</td>
<td>DMA REQ1/REQ3 For Parallel Port = LPT</td>
<td>Off</td>
<td>1=2 selects DMA channel 1 2=3 selects DMA channel 3</td>
</tr>
<tr>
<td>W7</td>
<td>Byte-Wide Backup Power Select</td>
<td>1=2 2=3</td>
<td>1=2 enable external battery for SO 2=3 connects device directly to V&lt;sub&gt;cc&lt;/sub&gt;</td>
</tr>
<tr>
<td>W8</td>
<td>Byte-Wide Battery Backup Power</td>
<td>Off</td>
<td>On = enables battery backup for memory in SO</td>
</tr>
<tr>
<td>W9</td>
<td>BIOS/Byte-Wide Swap</td>
<td>On</td>
<td>Off = enables access of a system BIOS from SO</td>
</tr>
<tr>
<td>W10</td>
<td>RS-485 Termination</td>
<td>Off</td>
<td>On = 100 ohm terminator</td>
</tr>
</tbody>
</table>
AMPRO 3SXi SETUP.COM

Parameters

- 1st Floppy: None
- 2nd Floppy: None
- ATA/IDE Disk 1: None
- ATA/IDE Disk 2: None
- Video: EGA/VGA
- Base Memory: 640
- Extended Memory: 1024
- Error Halt: No Halt
- Video Shadow RAM: Enabled
- System Power on Self Test (POST): Normal
- SCSI BIOS: Disabled
- Extended Serial Config: Disabled
- Extended BIOS: Enabled
- Adv Power Mgmt BIOS: Enabled
- Serial Port 1: Disabled
- Serial Port 2: Disabled
- Parallel Port: Enabled Mode: SPP
- Floppy Interface: Enabled
- IDE Interface: Enabled
- Mono/Color Jumper: Color
- Socket SO: 64K @D0000 hex
- OEM Flash: 64K @DE0000 hex
- Default Socket: SO
- Video State: Enabled
- Blank POST: Enabled
- Serial Boot Loader: Disabled
- Watchdog Timer: Disabled
- Hot Key Setup: Disabled
# AMPRO 3SXi I/O Parameters

## Interrupts, DMAs & Ports

<table>
<thead>
<tr>
<th>IRQ</th>
<th>DMA</th>
<th>PORT hex</th>
<th>CARD</th>
<th>FUNCTION</th>
</tr>
</thead>
<tbody>
<tr>
<td>0</td>
<td></td>
<td>040 – 043</td>
<td>3SX</td>
<td>ROM BIOS clock tick function from programmable timer 3</td>
</tr>
<tr>
<td>1</td>
<td></td>
<td>060 – 064</td>
<td>3SX</td>
<td>Keyboard interrupt</td>
</tr>
<tr>
<td>2</td>
<td></td>
<td>3</td>
<td>3SX</td>
<td>Cascade for IRQ8-15</td>
</tr>
<tr>
<td>3</td>
<td></td>
<td>108 – 10F</td>
<td>DIO</td>
<td>COM2 = PU300/PU600 [3SX Serial Port 2 IRQ disabled]</td>
</tr>
<tr>
<td>4</td>
<td></td>
<td>100 – 107</td>
<td>DIO</td>
<td>COM1 = NMC [3SX Serial Port 1 IRQ disabled]</td>
</tr>
<tr>
<td>5</td>
<td></td>
<td>278 – 27F</td>
<td>2nd LPT</td>
<td></td>
</tr>
<tr>
<td>6</td>
<td>2</td>
<td>3F0 – 3F7</td>
<td>3SX</td>
<td>Floppy controller 8-bit transfers</td>
</tr>
<tr>
<td>7</td>
<td></td>
<td>378 – 37F</td>
<td>3SX</td>
<td>LPT1 = Parallel Port (DMA 1 or 3 possible)</td>
</tr>
<tr>
<td>8</td>
<td></td>
<td>5</td>
<td>3SX</td>
<td>Reserved for battery-backed clock alarm</td>
</tr>
<tr>
<td>9</td>
<td></td>
<td>SVG-2</td>
<td>Video Controller if Jumper W1 On</td>
<td></td>
</tr>
<tr>
<td>10</td>
<td></td>
<td>118 – 11F</td>
<td>DIO</td>
<td>COM4 = Symmetry</td>
</tr>
<tr>
<td>11</td>
<td></td>
<td>110 – 117</td>
<td>DIO</td>
<td>COM3 = PU900</td>
</tr>
<tr>
<td>12</td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>13</td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>14</td>
<td></td>
<td>1F0 – 1F7</td>
<td>3SX</td>
<td>IDE hard disk controller</td>
</tr>
<tr>
<td>15</td>
<td></td>
<td>300 h</td>
<td>DIO</td>
<td>DIO Port 0 – Input bits from Input switches</td>
</tr>
<tr>
<td></td>
<td></td>
<td>304 h</td>
<td>DIO</td>
<td>DIO Port 4 – Output bits to Display lights</td>
</tr>
<tr>
<td></td>
<td></td>
<td>3052 h</td>
<td>DIO</td>
<td>DIO Port 5 – Output bits to Display lights</td>
</tr>
<tr>
<td></td>
<td></td>
<td>3B4 - 3DA &amp; 46E8</td>
<td>SVG-2</td>
<td>Standard VGA port addresses</td>
</tr>
<tr>
<td></td>
<td></td>
<td>0,1&amp;3</td>
<td>Available for 8-bit transfers</td>
<td></td>
</tr>
<tr>
<td></td>
<td></td>
<td>4</td>
<td>Cascade for DMA channel 0-3</td>
<td></td>
</tr>
<tr>
<td></td>
<td></td>
<td>5,6&amp;7</td>
<td>Available for 16-bit transfers</td>
<td></td>
</tr>
</tbody>
</table>
## AMPRO 3SXi Memory Map

<table>
<thead>
<tr>
<th>ADDRESS RANGE hex</th>
<th>SIZE bytes</th>
<th>FUNCTION</th>
</tr>
</thead>
<tbody>
<tr>
<td>DRAM 100000 – 1FFFFFF</td>
<td>1Mx16 1024k</td>
<td>2 Mbyte main memory = Toshiba, TC5118160CFT-60</td>
</tr>
<tr>
<td>0F0000 – 0FFFFFF</td>
<td>64k</td>
<td>Extended memory - 1 Mbyte of DRAM</td>
</tr>
<tr>
<td>0E0000 – 0FFFFFF</td>
<td>64k</td>
<td>Ampro ROM-BIOS – possible shadow copy in RAM</td>
</tr>
<tr>
<td>0D0000 – 0DFFFF</td>
<td>64k</td>
<td>Possible memory window into extended memory</td>
</tr>
<tr>
<td>0C0000 – 0CFFFF</td>
<td>64k</td>
<td>Flash or Socket memory window into 1 Mbyte of memory</td>
</tr>
<tr>
<td>0A0000 – 0BFFFF</td>
<td>128k</td>
<td>Video BIOS – possible shadow copy in RAM for speed</td>
</tr>
<tr>
<td>000000 – 09FFFF</td>
<td>640k</td>
<td>Video Screen RAM window into 512k bytes of video DRAM</td>
</tr>
</tbody>
</table>

Note: MEM /C memory map required for DRAM details

<table>
<thead>
<tr>
<th>ADDRESS RANGE hex</th>
<th>SIZE bytes</th>
<th>FUNCTION</th>
</tr>
</thead>
<tbody>
<tr>
<td>FLASH 010000 – 0FFFFF</td>
<td>1Mx8 960k</td>
<td>1 Mbyte BIOS &amp; OEM flash memory = Intel, 28F008SA</td>
</tr>
<tr>
<td>000000 – 00FFFFF</td>
<td>64k</td>
<td>Ampro BIOS</td>
</tr>
<tr>
<td>PROM – A 000000 – 07FFFF</td>
<td>512k</td>
<td>Byte-Wide Socket = 512 kbyte memory = 27F040</td>
</tr>
<tr>
<td>PROM – B 000000 – 0FFFFF</td>
<td>64k</td>
<td>User files</td>
</tr>
<tr>
<td>SETUP EEPROM 000000 – 0FFFFF</td>
<td>256</td>
<td>2-kbit EEPROM = Motorola, 93LC56X</td>
</tr>
<tr>
<td>SETUP NVSRAM 00E – 07F</td>
<td>114</td>
<td>Documentation is unclear</td>
</tr>
<tr>
<td>000 – 040</td>
<td>64</td>
<td>Setup info</td>
</tr>
<tr>
<td>000 – 00D</td>
<td>14</td>
<td>Real-time clock w/ 114x8 NVSRAM = Benchmarq BQ3285S</td>
</tr>
</tbody>
</table>

Note: MEM /C memory map required for DRAM details
Authenticating PROM Software

- The use of reference radiation sources is the most effective way to check system functionality.

- Random selection of PROMs is probably the most effective way to maximize monitor confidence in the system software.
  - Random selection of PROMs may not be feasible or allowed.

- Other methods to confirm the configuration of installed software exist.
  - All require the generation of a PROM image.
  - Bit-for-bit or hash function comparisons using monitor-supplied laptop computer.
  - “Private” comparisons: host provides the image to the monitor to take home and do with whatever he chooses, (including nothing).