

# Security-Hardened Attack-Resistant Platform (SHARP)

Presented by Clifford Glantz, PNNL

*on behalf of*

R. Eric Robinson (*[eric.robinson@pnl.gov](mailto:eric.robinson@pnl.gov)*; 509.375.4464)

Brad Woodworth (*[bradley.woodworth@pnl.gov](mailto:bradley.woodworth@pnl.gov)*; 509.375.3917)

Ron Pawlowski (*[ron.pawlowski@pnl.gov](mailto:ron.pawlowski@pnl.gov)*; 509.372.4116)

***Pacific Northwest National Laboratory I3P Security Tools Team***

This work was supported under Award number 2003-TK-TX-0003 from the U.S. Department of Homeland Security, Science and Technology Directorate. Points of view in this document are those of the authors and do not necessarily represent the official position of the U.S. Department of Homeland Security or the Science and Technology Directorate. The I3P is managed by Dartmouth College.

Approved for Public Release; Distribution Unlimited. MITRE No. 06-0760. Copyright © 2006 by the Trustees of Dartmouth College. The I3P Logo is a trademark of Dartmouth College. All information contained in this document may not be reproduced without permission by the I3P.

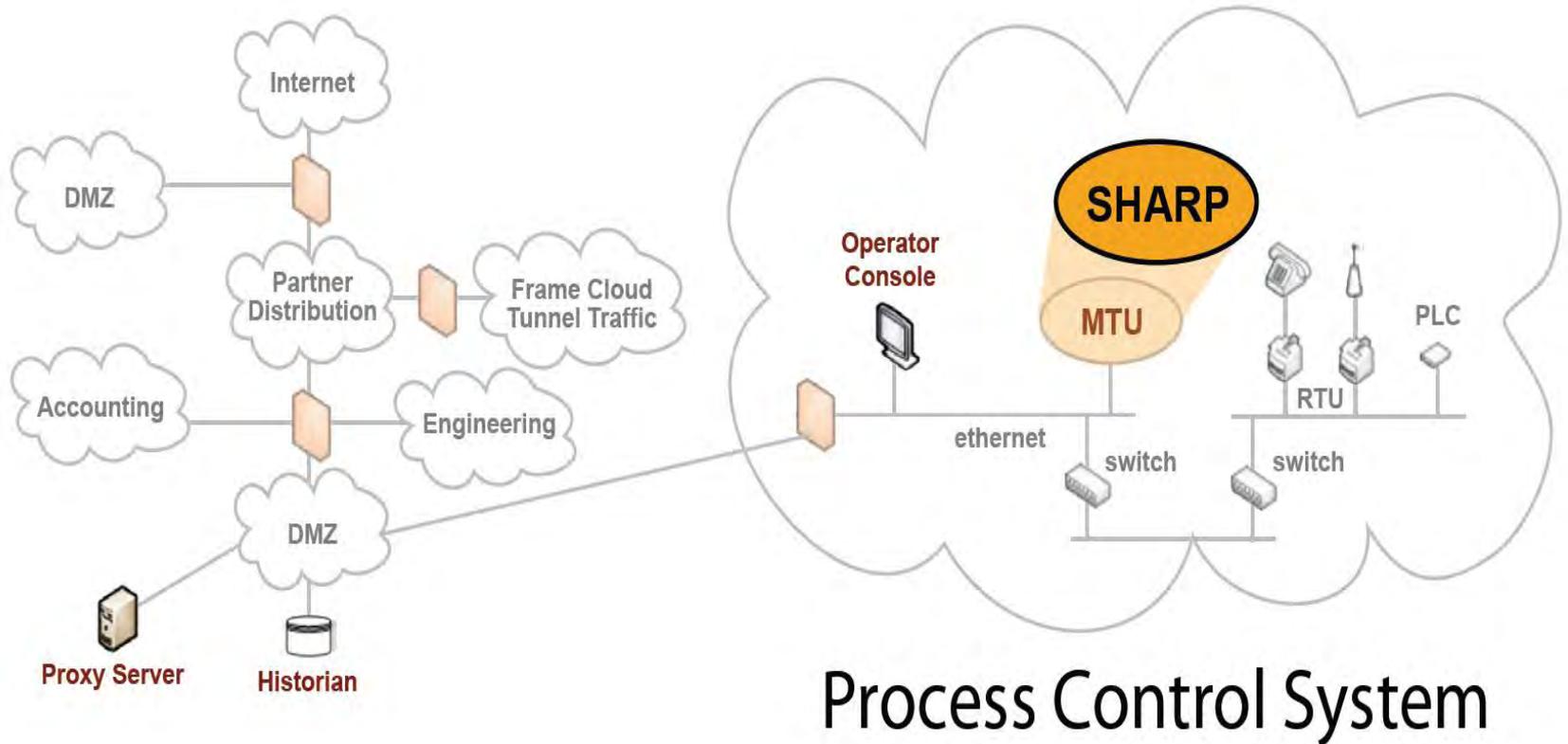
# The Problem...

- ◆ **Valuable and productive legacy systems can be hard to protect.**
- ◆ **For example, some may:**
  - Run operating systems that have a sordid security history.
  - They may expose themselves unduly by offering web or database services.
  - Be configured to maximize functionality at the expense of security.

# SHARP to the Rescue...

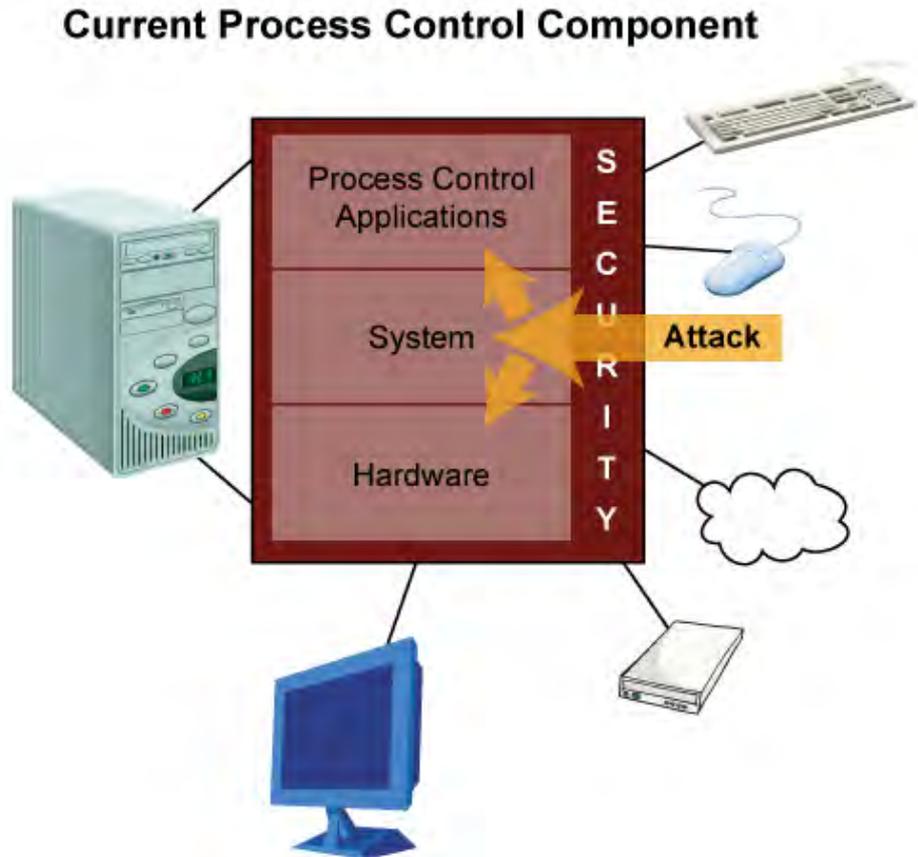
- ◆ **The Security-Hardened Attack Resistant Platform (SHARP) provides a vendor with an infrastructure-independent, high-security environment for networked process control systems.**
- ◆ **SHARP is designed to be a drop-in component on an existing PCS, thus allowing users to increase security while keeping their current process control investments.**
- ◆ **SHARP's architecture is designed to **limit access to sensitive data and software**, **increase the difficulty of a successful attack**, and **reduce interruption to operations in the event of a successful attack**.**

# SHARP : Where Does it Go?



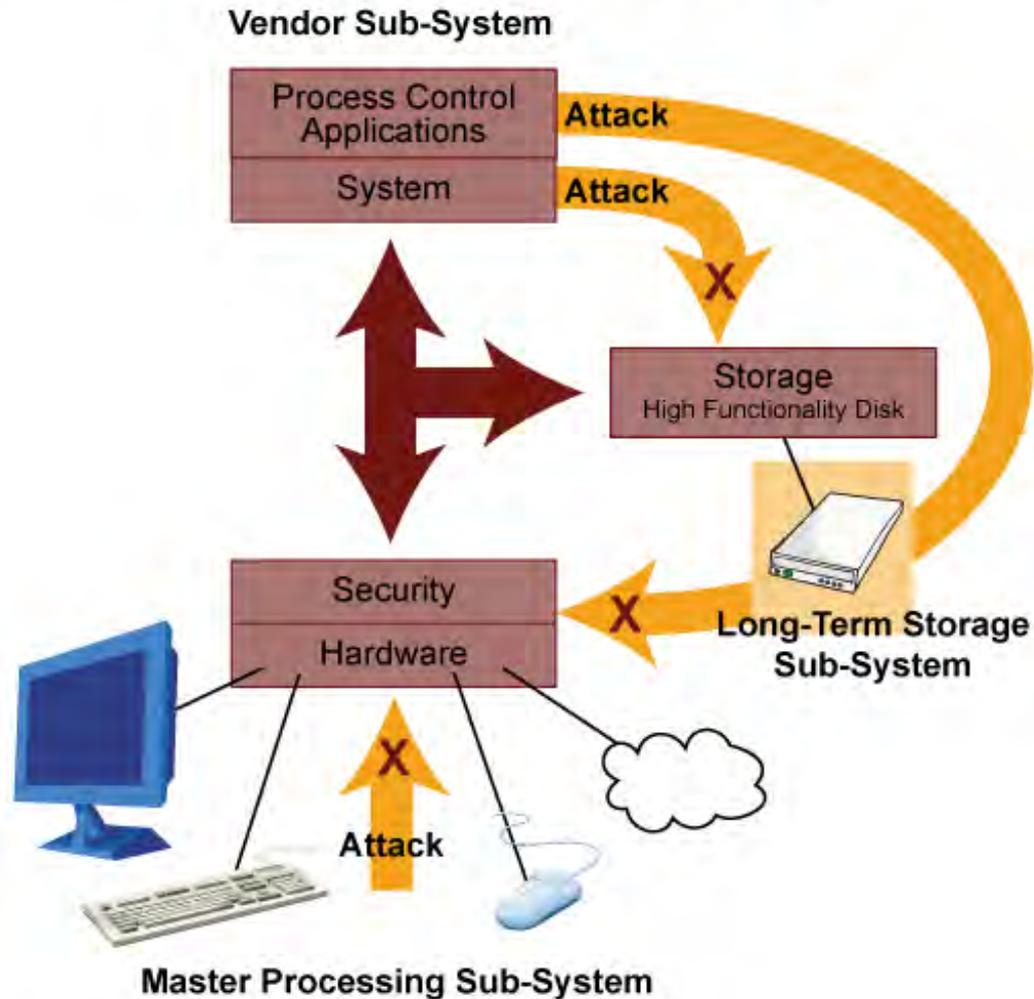
- ◆ The *master terminal unit* (MTU) is the current focus, but SHARP can be applied elsewhere as a *front-end processor* (FEP)

# A Typical MTU or FEP Configuration

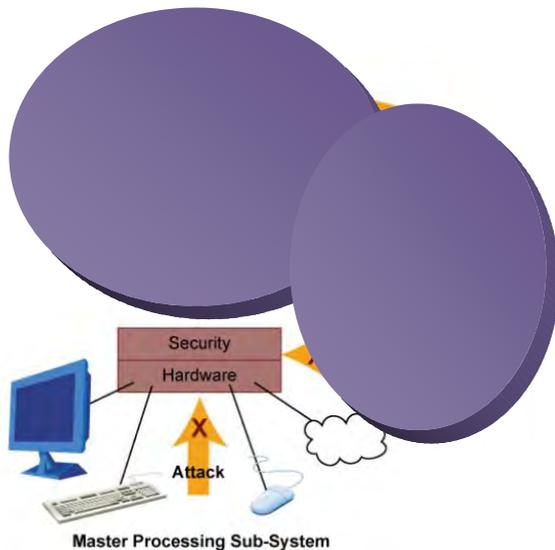


# SHARP – The Difference...

## Security-Hardened Attack Resistant Platform

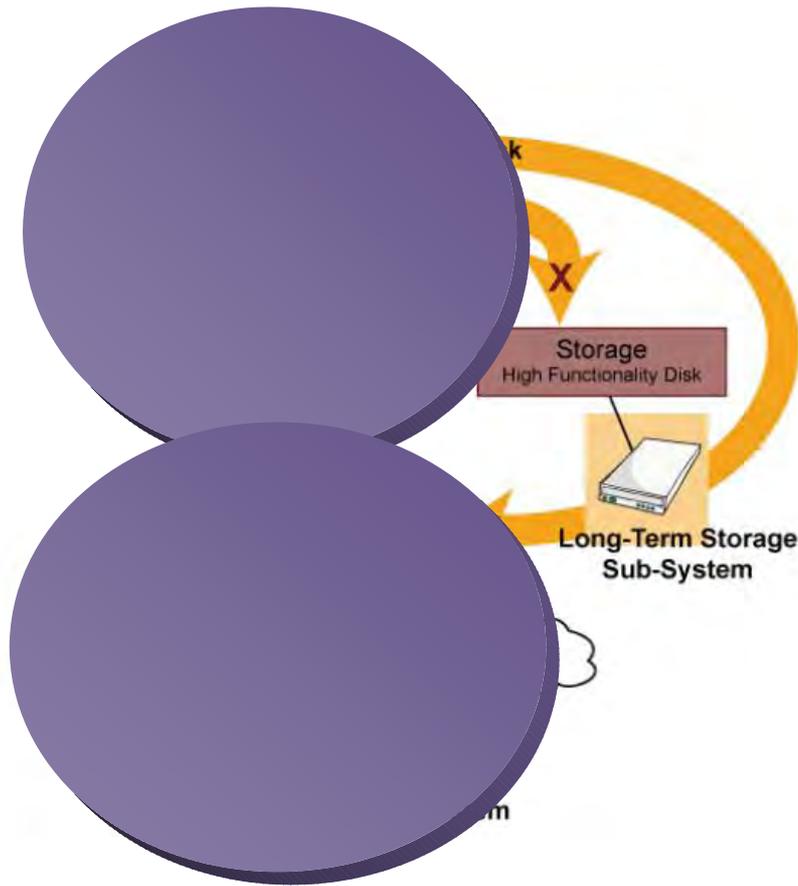


# SHARP: The MPS



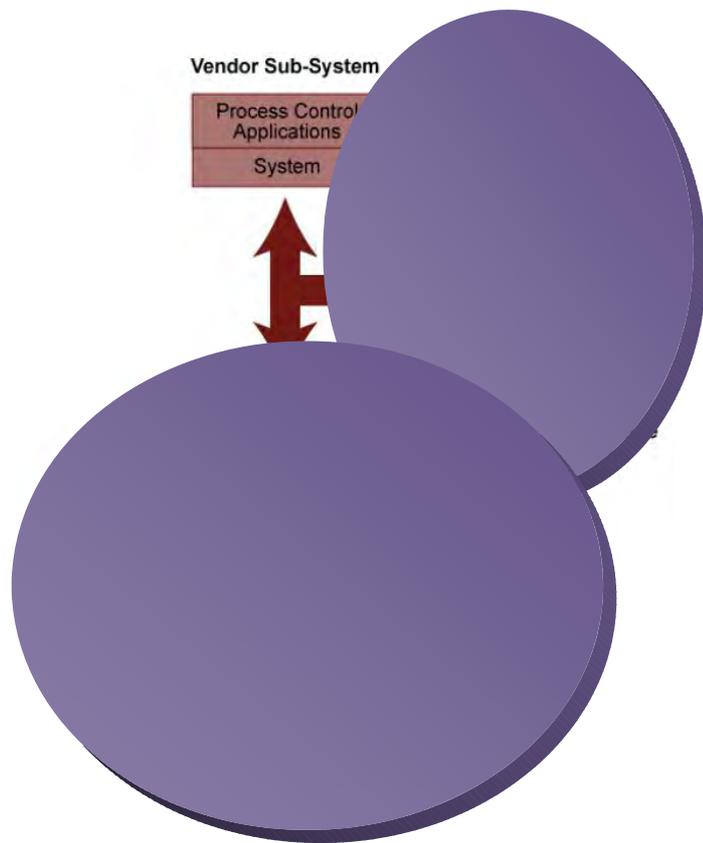
- The Master Processor Sub-System (MPS) separates the external network from the active Vendor Sub-System (VS).
- It runs without user interaction to mitigate vulnerabilities and protect against external and internal threats.
- Provides validation of itself (i.e., detects successful attacks)
- Boots from read-only media, any detected coercion is remedied by a restart from the known good state
- Uses a minimized operating system
- Validates the other system components
- Provides cryptographic encryption to reduce insider and outsider threats

# SHARP: The LSS



- ◆ The Long Term Storage Sub-System (LSS) provides storage for the SHARP.
- ◆ Runs separately from the other system components
- ◆ Secured by limited access using only required protocols
- ◆ Can provide encrypted storage to reduce insider threat
- ◆ Uses a minimized operating system to reduce the number of potential attack vectors.

# SHARP: The VS



- ◆ The Vendor Sub-System (VS) is the high value, legacy control system.
- ◆ The VS runs as usual with the added protection of the MPS, and the high reliability and security of the LSS.
- ◆ The VS continues to provide its legacy services and capabilities
- ◆ Access is restricted to authorized personnel and services via the MPS, protecting it from subversion



# SHARP Monitors

- ◆ **SHARP employs a File Monitor, Network Monitor, and Memory Monitor.**
- ◆ **The File Monitor looks for policy violations in VS-LSS communications and responds accordingly (e.g., by interrupting or reversing the activity, alerting operations).**
- ◆ **The Network Monitor looks at ingress and egress sides of the MPS network stack and uses a policy-based decision engine to adaptively respond to network based denial of service attacks.**
- ◆ **The Memory Monitor looks for unexpected changes in MPS memory process images. The system can respond by restarting the process from an image stored on CDROM.**

# SHARP: Key Themes

- ◆ **Use minimized operating systems to reduce complexity thus reducing the number of attack vectors.**
- ◆ **Partition – place high value, harder to secure systems behind high performance (low latency) systems to enhance security and monitoring.**
- ◆ **Harden the environment of each system.**
- ◆ **Separate the access privileges of each system. *For example, the system administrator for the low-security partition can be a different person than the administrator of the high security partition***

# No Man is an Island...



- ◆ **SHARP can work in concert with other tools.**
- ◆ **For example, we can:**
  - use DEADBOLT to check our source code
  - use the APT policy tool to check the correctness of our policy constraints
  - be integrated with Jason Stamp's (SNL) "SLAP"

# Next Steps

- ◆ **Transitioning from “working proof” to “bench tested”**
- ◆ **Work starting soon to “componentize” SHARP**
- ◆ **SHARP developers are seeking partnerships with industry and process control system vendors to participate in the testing and fine-tuning of SHARP.**

# Summary

- **Complex systems are hard to secure, especially when application services are integrated with security related and other system services.**
- **SHARP is a platform that can be used as part of a layered approach to better secure the insecure.**
- **SHARP uses a “trusted computing metaphor” to insulate high value legacy systems from attack.**
- **SHARP attempts to provide continued operations during an active attack.**
- **Detailed information is available at the I3P web site at <http://www.thei3p.org>**

# SHARP Contacts

- ◆ R. Eric Robinson

[eric.robinson@pnl.gov](mailto:eric.robinson@pnl.gov)

**509.375.4464**

- ◆ Brad Woodworth

[bradley.woodworth@pnl.gov](mailto:bradley.woodworth@pnl.gov)

**509.375.3917**

