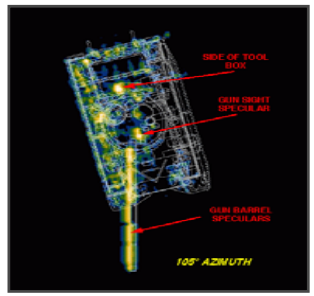
DoD Software Protection Initiative - HPEC 23 Sep 2003

Jeff Hughes
AT-SPI Technology Office
AFRL/SN
2241 Avionics Circle
WPAFB, OH 45433-7320
(937) 477-3089
AT-SPI_outreach@wpafb.af.mil

Software Protection Initiative

- **Direction**
  - Dec 13, 2001: USD(AT&L) memo formally kick-starts the DoD Software Protection Initiative
- **Mission**
  - Prevent the unauthorized distribution and exploitation of application software critical to national security
- **Vision**
  - Establish the Software Protection Initiative as an integral layer of the defense-in-depth concept for information assurance
  - Complement existing information assurance efforts in network security and operating systems access controls with an application-centric approach to protecting critical DoD intellectual property



Science & Engineering/ Modeling & Simulation Software

Mission Support Software running on COTS

Enterprise Software

What's at Stake?

- **Comprehensive collection efforts are underway to steal critical technologies**
  - **Application software is a high-value target**
    - **The examples below illustrate the difficulties in protecting critical technology**


USAF F-111 (1964)


Russian Su-24 (1964)


USAF AWACS (1977)


Russian A-50 (1980)


NASA Space Shuttle (1981)


Russian Space Shuttle (1983)

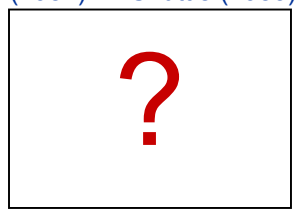
AF B-1 (1984)


Russian Tu-160 (1987)


NASA/USAF X-29 (1989)


Russian Su-37 Berkut (1997)


USAF F/A-22 (200?)



Stealth Fighter (200?)

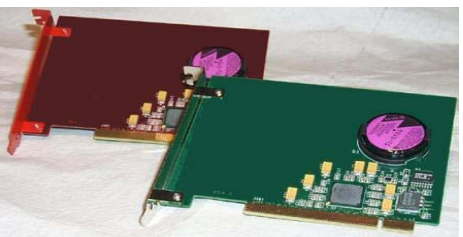
(Sources: Michael Schwartz, The role of espionage in the Soviet atomic bomb project; AFOSI Detachment 709 open source analysis)

- **Use of SPI technology will allow us to :**
  - **Maintain operational superiority**
  - **Ensure our ability to dominate the battlespace**
  - **Provide defense-in-depth for U.S. forces**

Software Protection Initiative Protection Technologies

- **Current commercial practices focus on revenue protection and have minimal shelf life**

- **Military grade protection must provide robust protection, reliability, and scalability**
  - **Current, most robust protection measures involve hardware and software**
  - **Hardware is embedded with trust which forms the foundation of the protection technology**
  - **Software application talks to the hardware to ensure protected execution**



PCI Card

USB Device

Network Device