Composing a High-Assurance Infrastructure out of TCB Components

Mark R. Heckman <mark.heckman@aesec.com>

Roger R. Schell <roger.schell@aesec.com>

Edwards E. Reed <ed.reed@aesec.com>

5th Annual Layered Assurance Workshop, December 2011

Infrastructure is Critical!

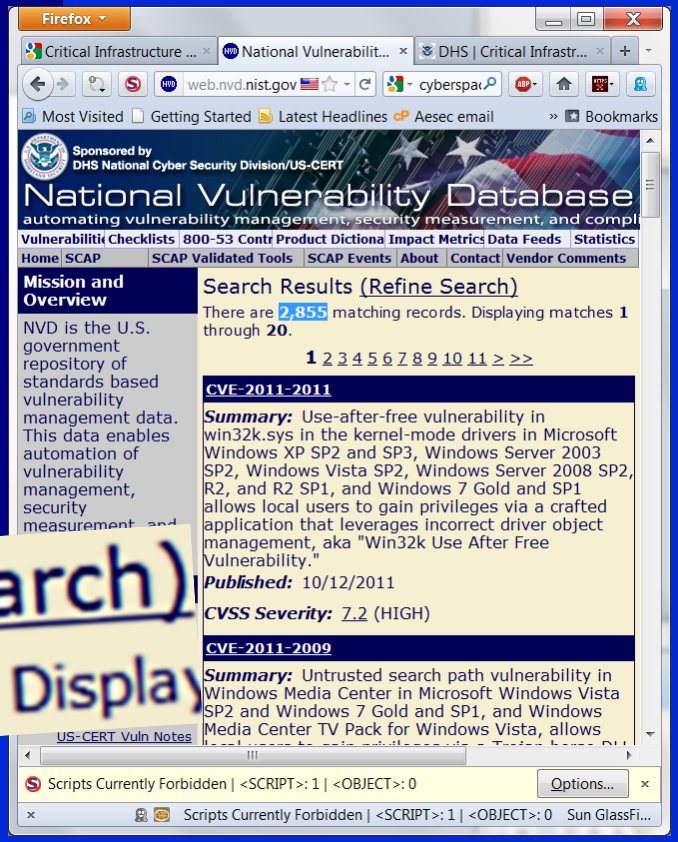
"...incapacitation or destruction would have a debilitating effect on security, national economic security, public health or safety, or any combination thereof."
--Department of Homeland Security

"...great risks threaten nations, private enterprises, and individual rights."
--President's Cyberspace Policy Review

Reality Check

```
A problem has been detected and windows has been shut down to prevent damage
to your computer.

MEMORY_MANAGEMENT

If this is the first time you've seen this Stop error screen,
restart your computer. If this screen appears again, follow
these steps:

Check to make sure any new hardware or software is properly installed.
If this is a new installation, ask your hardware or software manufacturer
for any Windows updates you might need.

If problems continue, disable or remove any newly installed hardware
or software. Disable BIOS memory options such as caching or shadowing.
If you need to use Safe Mode to remove or disable components, restart
your computer, press F8 to select Advanced Startup Options, and then
select Safe Mode.

Technical information:

*** STOP: 0x0000001A (0x00041287,0x035D8000,0x00000000,0x00000000)



Collecting data for crash dump ...
Initializing disk for crash dump ...
Beginning dump of physical memory.
Dumping physical memory to disk:  95
```

You're using Windows!



Search Results (Refine Search)

There are 2,855 matching records. Displa

Same applies to Linux

Compensating Controls

- Government programs for dealing with insecure infrastructure networks:
  - *Build Security In* (DHS) – Practices, tools, guidelines, rules, principles for building security into ***application software***
  - OPSAID (DOE) - "Interoperable security architecture for common process control system ***add-on security devices***"
  - Lemnos (DOE) – Configuration profiles and testing procedures for devices defined in OPSAID
    - First commercial result is VPN/Firewall Gateway
  - Defense in Depth (DHS) - Recommended practices for improving industrial control systems security

Defense in Depth

- Firewalls
- Logs
- IDS
- User Education
- Secure Application Development
- **Operating System**

Subversion

- Stealthy system sabotage
- Disables protection mechanisms
- Becomes part of the system and hard to find
- Can occur at any time during system lifecycle:
  - Design, Implementation, Distribution, Maintenance, Support, or Operation
- "Supply chain risk" (per DHS's Joe Jarzombek)
  - Exploitable flaws (accidental)
  - Backdoors (intentional)

Something is Missing

- Those programs ignore securing the OS. Why?
  - Expense?
  - Perceived lack of alternatives?
- Overlooks proven technology
  - Techniques based on years of research
  - For the most-sensitive Government systems
- High-assurance, evaluable systems criteria
  - Trusted Computer System Evaluation Criteria (TCSEC) and Trusted Network Interpretation (TNI)
  - Common Criteria
- Why doesn't this technology get more attention?

Science, not Politics

- Argument is for using good technology
  - Not one criteria over another
- But TCSEC/TNI is better suited for developing secure infrastructure networks
  - TCSEC is systems (not component) criteria
  - TNI explains how to apply TCSEC to network
  - How to compose network out of evaluated components
- Based on unified TCSEC security policy
- CC is aimed at components, not systems
  - No equivalent CC protection profile
  - No equivalent, vetted CC composition method

More Useful TCSEC Features

- Composition steps
  - Define decomposable Network TCB (NTCB) policy
  - Evaluate components separately
  - Composition can be shown to satisfy NTCB policy
- NTCB policy must include trusted comm. channel
- TCSEC Class A1 aimed at preventing subversion
  - E.g., secure distribution is built-in
- Can compose more restrictive policies
  - "TCB subsets" (in TDI)
- Good science to solve today's problems

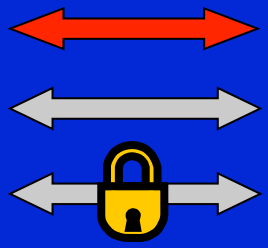
Example Applications

- Apply TCSEC/TNI to secure infrastructure:
  - Secure communications channel prototype
  - Secure partitioned controller
- Together have evaluable Class A1 network
- Use GEMSOS Class A1 TCB as base system

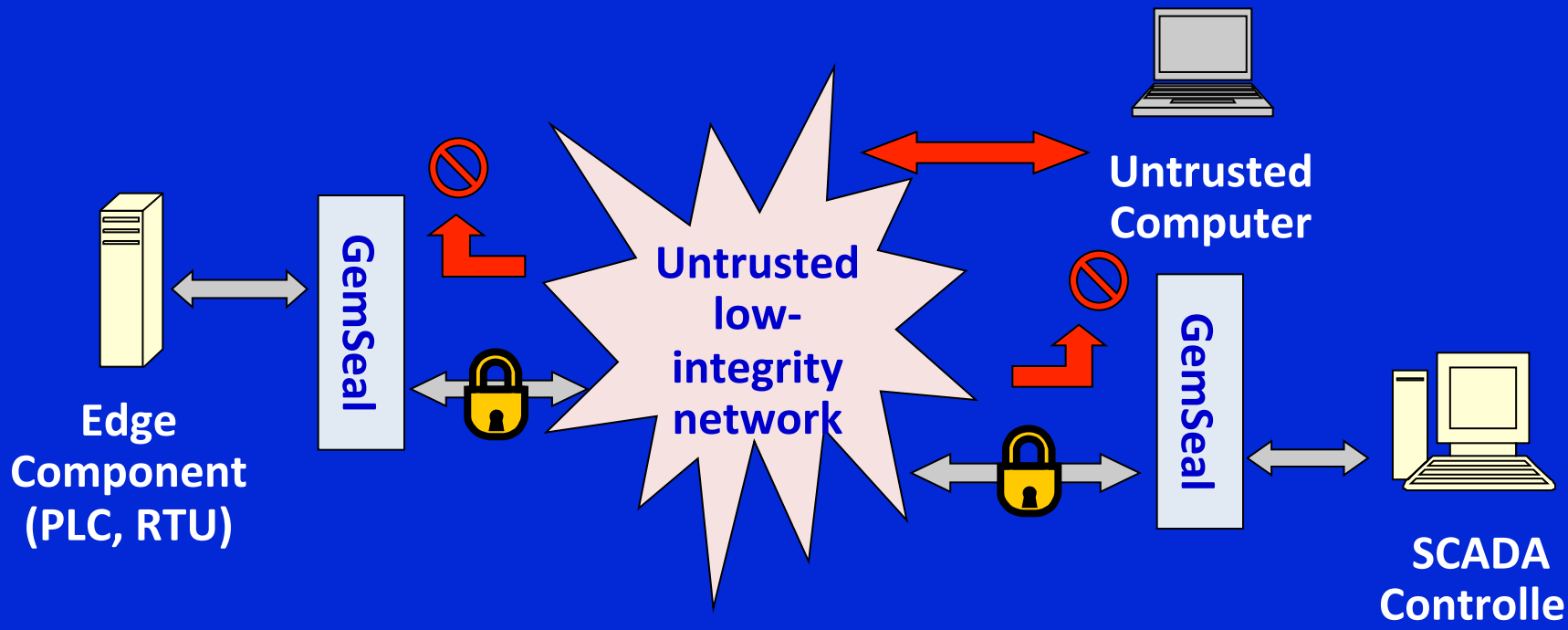
GEMSOS Services for Trusted Applications

- Core security kernel already has in it
  - Crypto services
  - Data seal device
  - Used in support of trusted distribution & recovery
- Trusted Application Support
  - True protection Rings (8) to protect trusted apps
- Result
  - Dramatically simplifies building & accreditation
    - Of security services like crypto seal guards
    - Other applications

Secure Communications Channel



- Unsealed low-integrity packets
- Unsealed high-integrity packets
- Sealed high-integrity packets



GemSeal guards built on GEMSOS

GemSeal Guard

- Each guard has both high and low interfaces
- Sealing packets – forwarding from high to low
  - Associate source interface label with each packet
  - Generate cryptographic seal of packet data + label
  - "High-Sealed" packets include packet data + seal
  - Send "High-Sealed" packets via low network interface
- Releasing packets – delivering from low to high
  - Guards only release packets with valid seals
  - Only released to interfaces matching their sealed labels
  - Can have multiple levels, not just high/low

GEMSOS + Crypto Seals

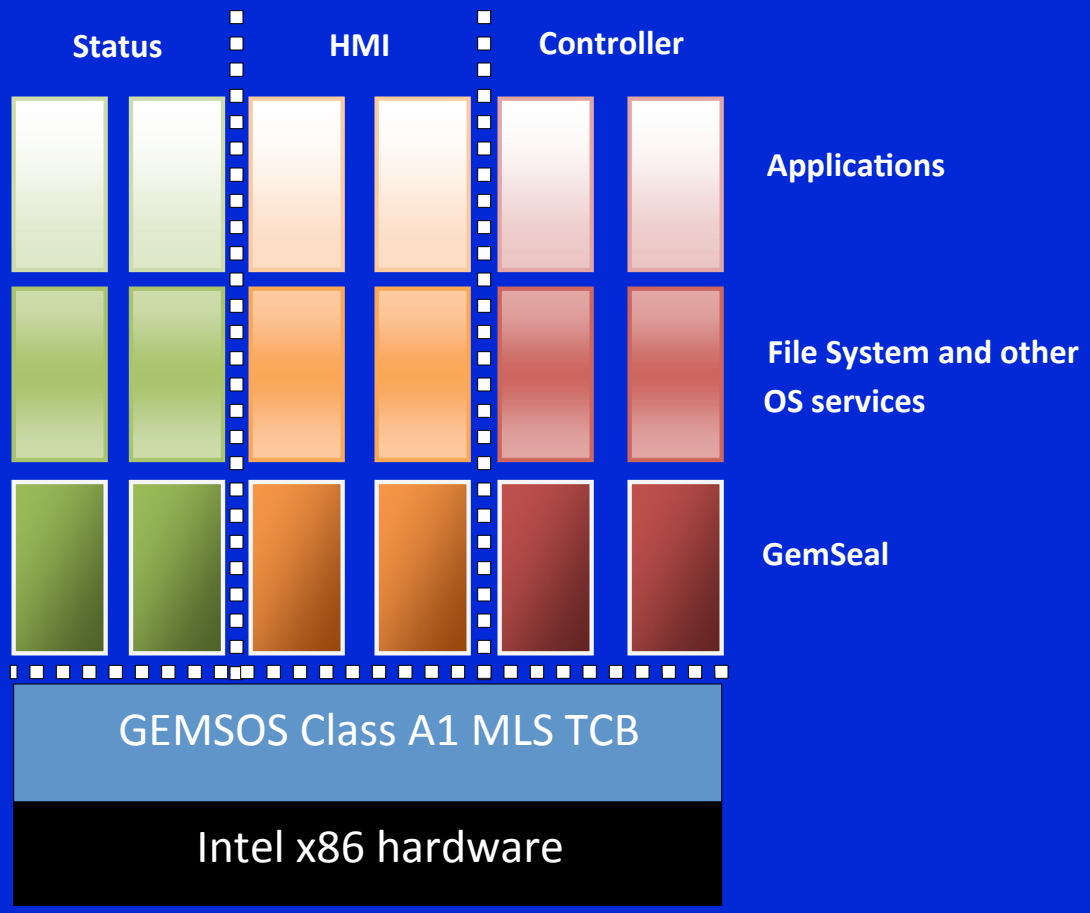
- GEMSOS used crypto seals in Class A1 Evaluation
  - To meet Class A1 Label Integrity requirements
  - Integral to Trusted Recovery & Trusted Distribution
- GEMSOS publishes security services via APIs:
  - Data Sealing Device (and Cryptographic Services)
  - Key Management
  - Trusted Recovery & Distribution
- GemSeal uses GEMSOS APIs for crypto seals
  - Previously evaluated, stable, public interfaces
  - Minimal new trusted code
    - Generate seal
    - Validate integrity/authenticity of sealed packet & label
    - Release validated packet to equivalently labeled destination

Build Secure Applications

- Build infrastructure applications on a TCB
  - Use POSIX-like API that runs on GEMSOS
- Leverage Mandatory Access Control
- Partition applications for “least privilege”
- Use MAC to protect high-integrity parts

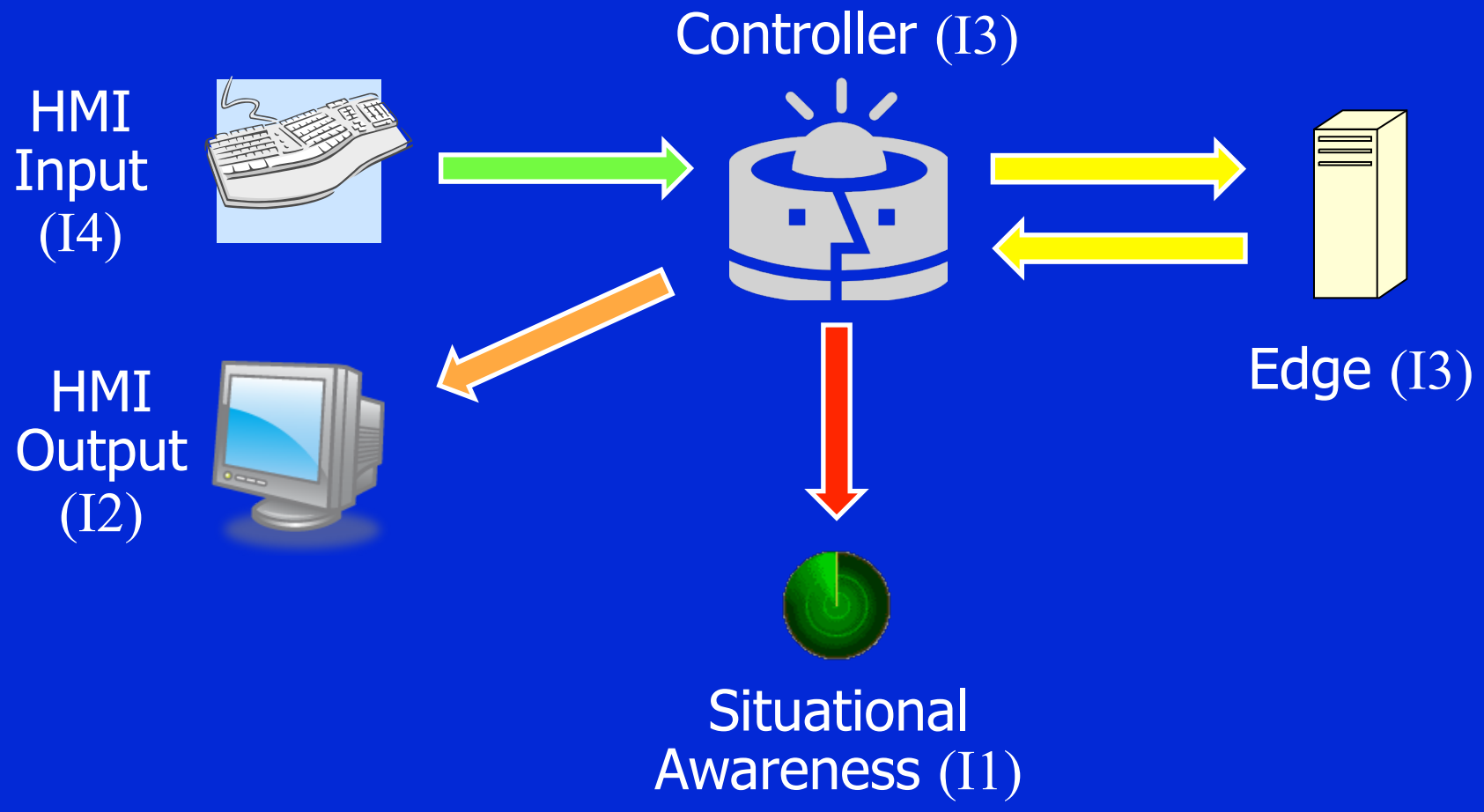
Controller on a TCB Concept

- "Controller" manages critical system functions
- "HMI" manages human-machine interface
- "Status" collects and distributes situational awareness information



Sensitivity Labels

- Integrity labels: I4 > I3 > I2 > I1



Conclusion

- Add security to insecure systems?
  - Doesn't work!
- Use proven techniques for building security
  - Any sound criteria equivalent to Class A1 will do
  - Verifiable protection
  - Mitigates the risk of subversion and unknown flaws
- Can apply to critical infrastructure security

Questions?

Composing a High-Assurance Infrastructure out of TCB Components

Mark R. Heckman <mark.heckman@aesec.com>

Roger R. Schell <roger.schell@aesec.com>

Edwards E. Reed <ed.reed@aesec.com>

5th Annual Layered Assurance Workshop, December 2011

GEMSOS Class A1 Evaluation

- BIOS: “Kernel in PROM”
  - Execution begins in kernel
- Chipset + CPU
  - Vendor must supply evidence (schematics)
  - Government-Intel-Gemini NDA
  - Any unpublished instructions/features disclosed
  - Show necessary and required functions for policy
- HW threat assessment:
  - Much harder to subvert than SW
  - HW analysis “beyond Class A1” (no good techniques)
  - Some analysis of origin, design, etc. (“NSA foundry”)

TCSEC/TNI Not Just DoD

- Originally designed to meet needs of DoD
- Includes both secrecy and integrity policies
- MAC Lattice of access classes isomorphic to any boolean policy
- A mature, proven trusted systems technology
  - Subversion-resistance built in
  - Not necessary to use TCSEC as organizational policy
- Six completed Class A1 evals demonstrate successful process