



# Trustworthy Information Systems – Myth or Enabler?

**Dr. Roger R. Schell**  
**roger.schell@aesc.com**

**AMCIS 2005**  
**August 13, 2005**

# Trustworthy IS – Myth or Enabler



- **The 3 levels of consciousness:**
  - 1 There is no Problem (Ignore Threat)
  - 2 There is no Solution (Ignore Science)
  - 3 There is no Free Lunch (Control Risk)
- **Key decision: how to allocate trust**

**RISK = THREAT x VULNERABILITY**

# Outline:

## Trustworthy IS – Myth or Enabler

---



- **Introduction**

- Problem – have professional threat NOW
- Potential – have proven technology NOW
- Where are we going – depends on us

# Business is About Trust

---



- **Trust, but verify**
- **Historically, trust was placed in humans**
  - Closed user groups, e.g., HR, sales, accounts payable
  - Authorized individuals within auditable processes
  - Individual accountability with well-defined recourse
- **Allocating this trust to IS is different**
  - You can't fire IS
  - You can't sue IS
  - Your enterprise application server won't sign an NDA
- **In past, there was less need to trust IS**
  - Attackers lacked either motive or opportunity
  - Growing trust in IS occurred "on Internet time"

# Where Trustworthy IS is Today

---



- **Rapidly growing threat of professional attack**
- **Rapidly growing dependence on IS**
  - On-demand computing is poster boy case
- **Have existence proof of high assurance solutions**
- **Sound technology languishes in future directions**
  - “Pixie dust” solutions rampant in evolving technology
  - Rapidly falling behind in ability to deliver security
- **Muddled response from scholars and practitioners**

Outline:

# Trustworthy IS – Myth or Enabler

---



- Introduction
- **Problem – have professional threat NOW**
- Potential – have proven technology NOW
- Where are we going – depends on us

# Problem is Professional Attacks



## Government

*I don't think most federal CIOs are as concerned about teenage hackers. What we're much more concerned about are governments who are putting teams in place to attack the information assets of the U.S.*

– Steven Cooper, CIO, Dept. Homeland Security, 2005

## Corporations

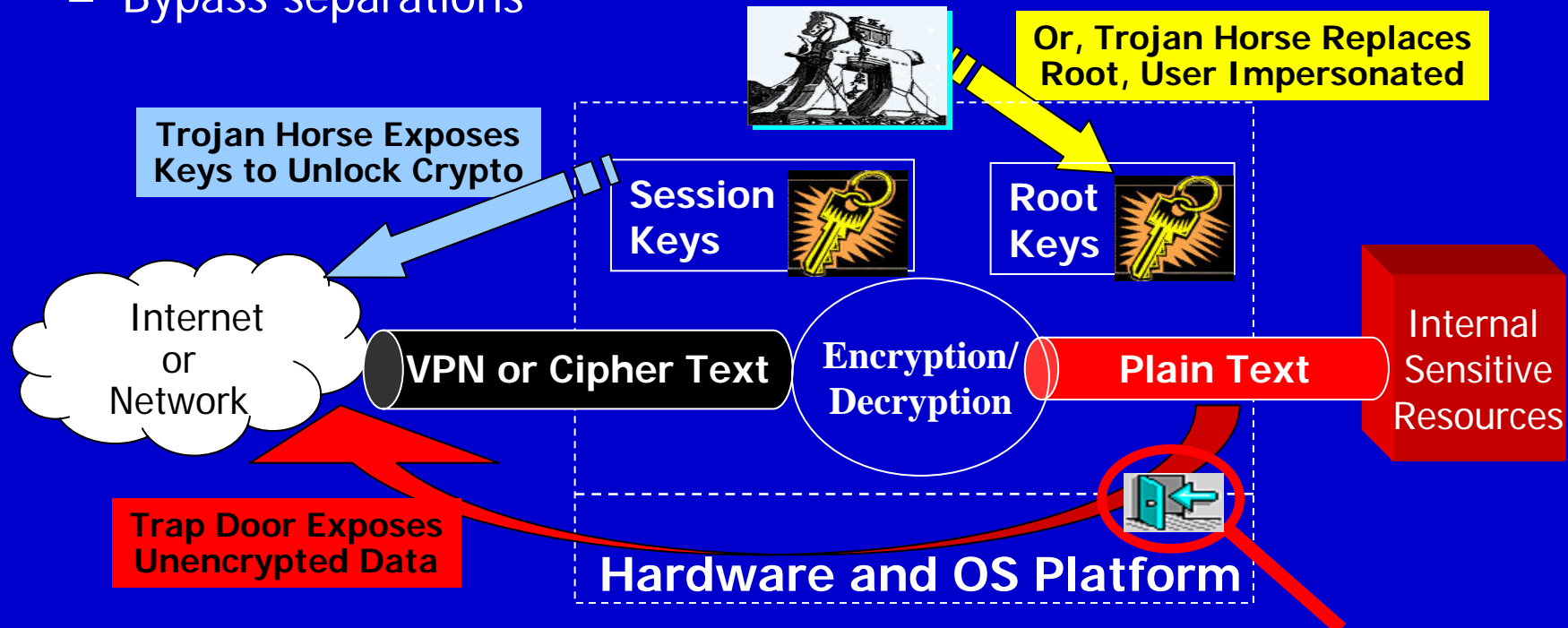
*Hackers who once set out to make names for themselves by creating the next fast-spreading virus are being replaced by organized criminals bent on stealing money, credit card numbers or extorting payments from wary companies.*

– Wall Street Journal, 2005

# The Professional Threat: Malicious Software



- **Professionals use trap doors, Trojan horses, worms, etc.**
  - Steal keys, forge certificates, or steal plain text
  - No need to crack cryptography
  - Bypass separations



- **Easy to subvert Trusted Solaris, SE Linux, Windows XP, IPSEC . . .**
  - Examples: Anderson, et. al. "Subversion as a Threat in Information Warfare," *JIW* (2004)

# Two Basic Steps for Attacker



- **Step #1 – Infrastructure subversion (trap door)**
  - Planned, deliberate insertion – like “Easter eggs”
  - Integral to other software at initial installation

**OR**

  - Added to software suite during lifecycle
  - Big personal priority: avoid being apprehended
- **Step #2 -- Effective execution of software**
  - Activated by unique “key” or trigger
    - Known only to attacker
  - Bootstrap for diverse attacks
  - Access and exfiltrate confidential information

# Decisions That Introduced Risk

---



- **Moving from closed network to open internet**
  - Use of VPNs to logically extend closed user groups
  - VPNs to create not-so-private networks
- **Building dependence on exposed machines**
  - Direct contact to potential planned, coordinated threat
  - Weak response is firewalls & intrusion detection
- **Internet integration removes natural barrier**
  - Hooking together all corporate business processes
  - Electrical continuity between Internet & sensitive data
  - Natural “compartments” for closed user groups are lost
  - On-demand computing is natural extension

# We Can't Plead Ignorance



*Nearly thirty years ago, Roger Schell accurately predicted the exact situation we find ourselves in: **systems not designed for the modern Internet threats**, poorly implemented, forcing the installation of nearly daily security patches, and many millions of systems being compromised on an ongoing basis.*

Dave Safford, Manager, IBM Global Security Analysis Lab  
“The Need for TCPA,” IBM Research, October, 2002  
[http://www.research.ibm.com/gsal/tcpa/why\\_tcpa.pdf](http://www.research.ibm.com/gsal/tcpa/why_tcpa.pdf)

- **“Tiger Teams” show subversion is tool of choice**
  - <http://www.airpower.maxwell.af.mil/airchronicles/aureview/1979/jan-feb/schell.html>
  - <http://www.acsac.org/2002/papers/classic-multics.pdf>
- **Practical experience -- 30+ years success**
  - The threat has not decreased
- **Can you buy IS solution from your mortal enemy?**
  - (Better figure out how, because likely you are)
  - Software of uncertain pedigree

# Outline:

## Trustworthy IS – Myth or Enabler

---



- Introduction
- Problem – have professional threat NOW
- **Potential – have proven technology NOW**
- Where are we going – depends on us

# Solutions Based in Science

---



- **Divide and conquer**
  - Not all problems are the same
  - The critical problem is fundamental ability to protect information
  
- **Distinguish between policies**
  - Some can be enforced with high assurance, some can't be
  - Some violations result in massive loss, others don't
  
- **Don't have to solve all hard problems at once**
  - Spend your money where it matters
  - Your enemies will

# Solutions Based in Science



- **Divide and conquer**
  - Not all problems are the same
  - The critical problem is fundamental ability to protect information
  - **Use TCB to isolate system protections**
- **Distinguish between policies**
  - Some can be enforced with high assurance, some can't be
  - Some violations result in massive loss, others don't
  - **Enforce MAC for closed user groups with crucial distinctions**
- **Don't have to solve all hard problems at once**
  - Spend your money where it matters
  - Your enemies will
  - **Leverage MAC TCB on selected components**

# Platform Subversion: Class A1/EAL7 is the Only Solution



Common Criteria	TCSEC (Orange Book)	Examples	Security Properties	Benefit to Customer
-----------------	---------------------	----------	---------------------	---------------------



EAL7

A1

Only one:  
GEMSOS



- No vulnerabilities
- No trap doors
- Immune to Trojans
- Verifiable

- Connect networks
- Trust separation

EAL6

B3

Digitalnet XTS

- Vulnerabilities
- Trap doors
- Resists Trojans
- Not verifiable

EAL5

B2

EAL4

B1

Trusted Solaris  
SE Linux

EAL3

C2

Windows

EAL2

C1

- Only “best commercial practice”

- Isolate networks
- No “crown jewels”

**Only Class A1 verifiably protects from flaws, trap doors, Trojan horses**

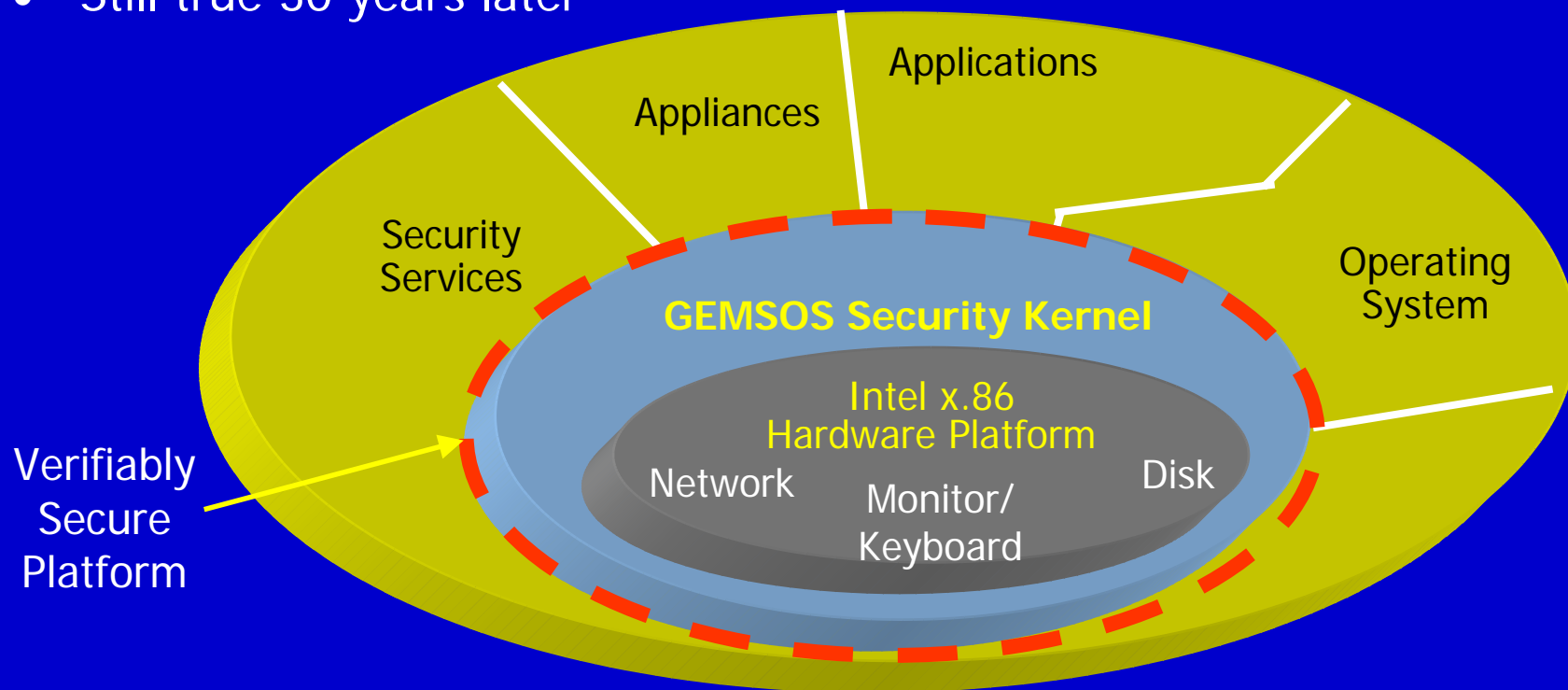
# Solution to Subversion: A "Security Kernel"



- *"The only way we know . . . to build highly secure software systems of any practical interest is the kernel approach."*

-- ARPA Review Group, 1970s (Butler Lampson, Draper Prize recipient)

- Still true 30 years later



**GEMSOS is the only general purpose kernel evaluated at Class A1**

# Verifiable Protection Technology



- **Only verify a subset of the system**
  - Security Kernel and key supporting services
  - Remaining OS and applications not verified
  - TNI (TCSEC) M-component minimizes for MAC
- **Formal methods for proven secure design**
- **Code correspondence**
  - Only way to prevent trap doors
- **Trusted distribution of Security Kernel**
- **Government evaluations**
  - Past objective & authoritative 3<sup>rd</sup> party – ITSEC & TCSEC Class A1
  - Future Common Criteria EAL7 of MAC policy enforcement
- **Example: GEMSOS kernel evaluation**
  - Blacker Class A1 for key distribution and access control platform
  - COTS security kernel evaluated as Class A1 TNI M-component
  - ITSEC evaluation in UK for MOD deployment
  - NSA validated Class A1 Rating Maintenance Program (RAMP)

# Outline:

## Trustworthy IS – Myth or Enabler

---



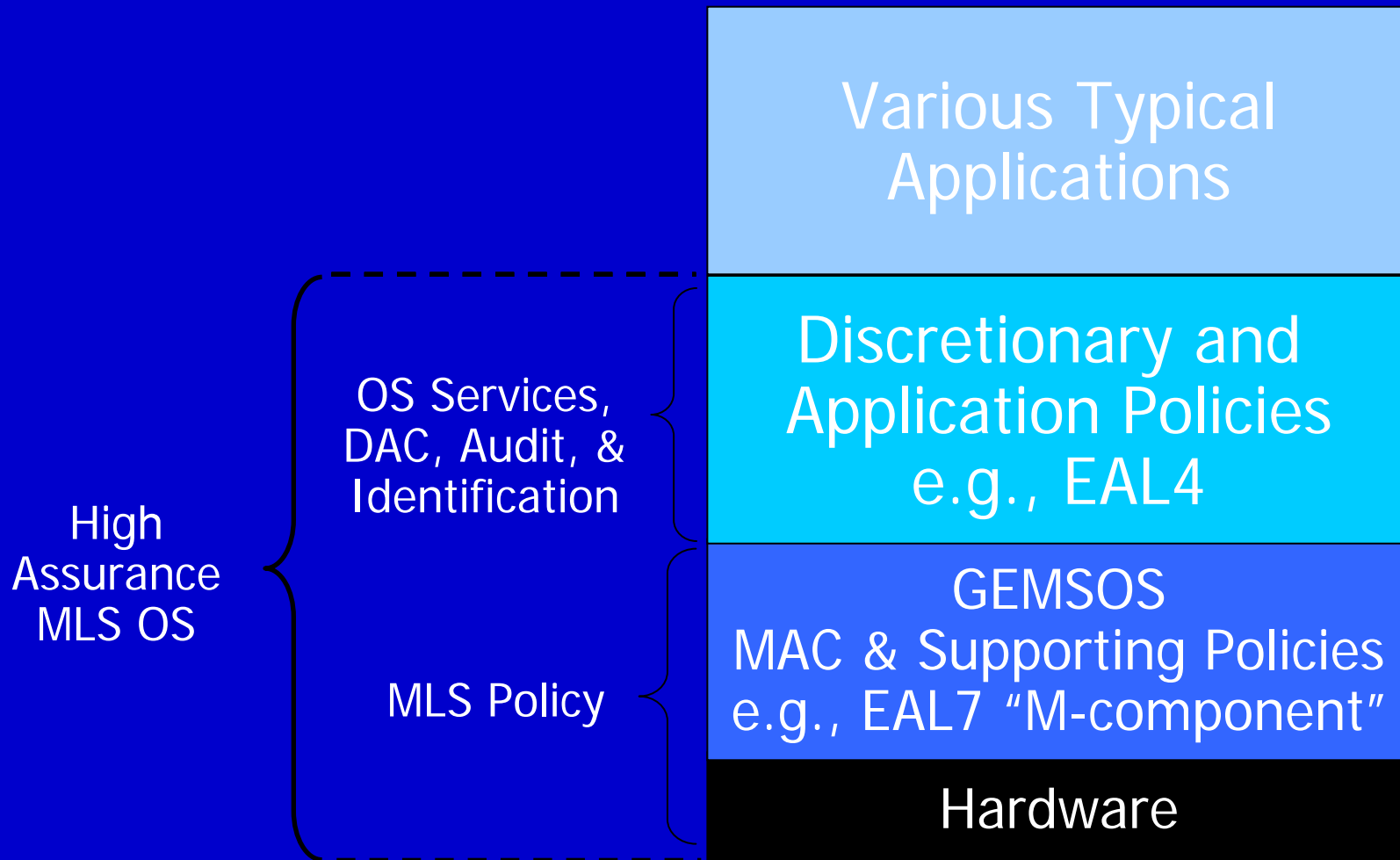
- Introduction
- Problem – have professional threat NOW
- Potential – have proven technology NOW
- **Where are we going – depends on us**

# “Pixie Dust” Doesn’t Work

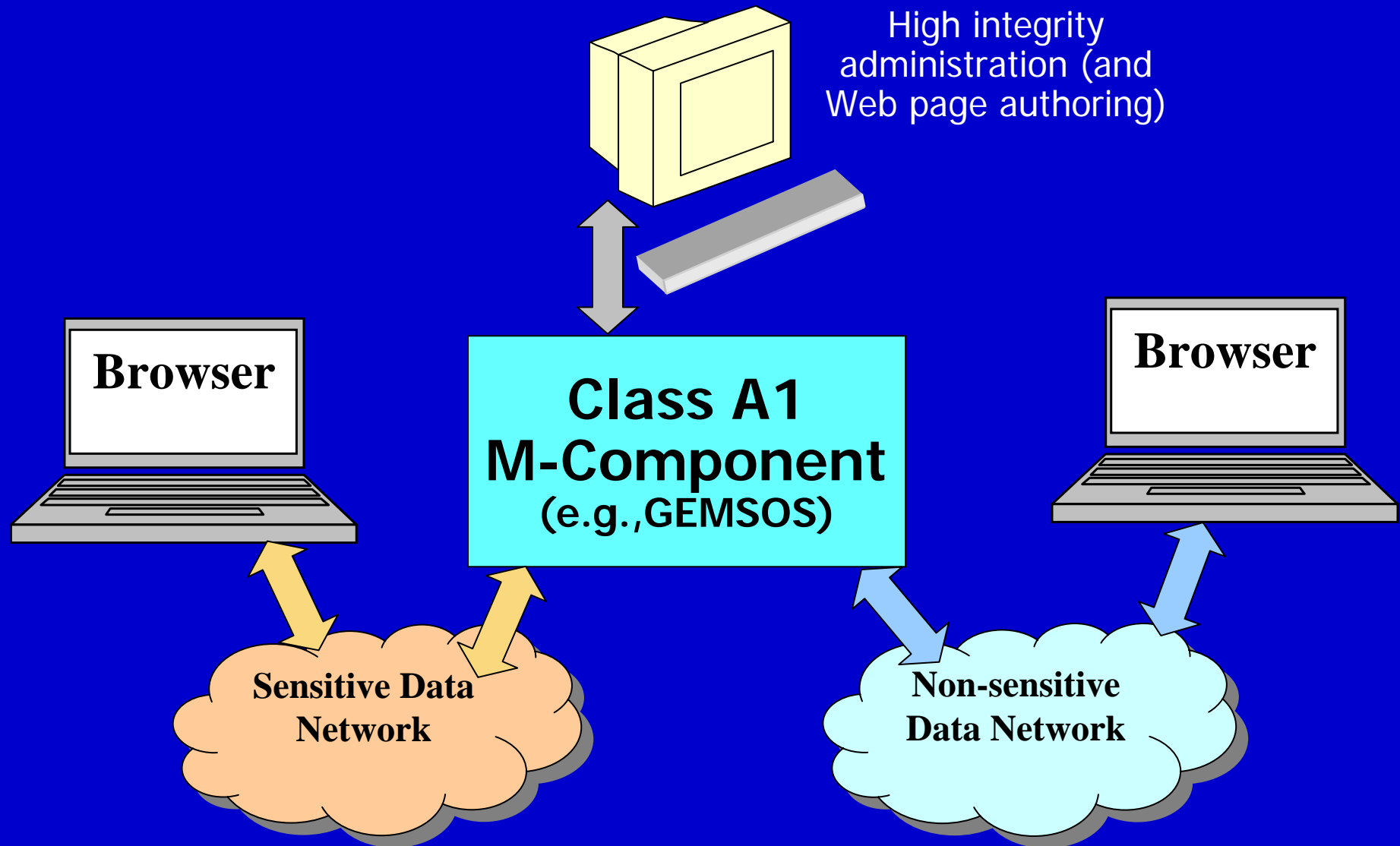


- **Penetrate and patch** – no basis for completeness
- **Linguistic controls** – lack computable basis
- **Process focus** – code inspection, “million eyes”
- **Cooperative developer view** – maturity models
- **Probabilistic threat model** – “defense in depth”
  - Design for amateurs (**ignore subversion**) – firewalls, IDS
- **Cryptography in weak context** – “opiate of the naive”
- **Hardware “protection” mechanism** – not related to security
  - Separation of policy and mechanism myth
  - E.g., “capabilities” for external controls, strong typing
  - Isolation & virtualization mechanisms **lacking tie to policy model**
- **“Secure” applications** – e.g. JAVA sandbox
- **Gratuitous formal methods** – code proofs
- **Fuzzy notion of assurance to deal with subversion**

# Sound Solutions – “DAC on MAC”



# Example – Web Server Demo



# Example Demo Properties



- **Controlled interface between multiple security domains**
  - Secrecy and integrity MAC policies of evaluated GEMSOS
  - Hierarchical and non-hierarchical relationships
- **High secrecy network can “read down”**
  - Straightforward extension to “transfer up”, e.g., FTP
- **Low integrity cannot modify high integrity web resources**
- **MAC enforcement independent of application behavior**
  - Web server applications are entirely untrusted
  - High level network interfaces are entirely untrusted
  - Web server application flaws can't violate MAC policy
- **Demo available Commercial Off The Shelf (COTS) today**

# Conclusion: Our Decisions are the Difference

---



- **Basic business issue:**  
**RISK = THREAT x VULNERABILITY**
- **We need to control RISK**
  - Valuable information, e.g., financial, privacy, audit
  - Liability for unauthorized access, e.g., regulatory
- **We don't control THREAT, i.e., professional attackers**
  - Reward for penetration provides motive
  - Internet access for e-business provides opportunity
- **But we can DECIDE to reduce VULNERABILITY**
  - Either appropriate assurance (Class A1 or equivalent in EAL7)
  - Or don't connect – e.g., forego on-demand computing

# Opportunity – Get Ahead of Professional Threat

---



- **Candidly communicate subversion threat to executives**
- **Evaluate new technologies**
  - Explicitly assess ability to meet professional threat
  - Recognize (high) assurance must be built in
- **Introduce and stimulate market**
  - Coordinated statements with other professionals
  - Explicitly state platform assurance significance
  - Emphasize assurance needs to hdw/sdw vendors
- **Trustworthy IS fundamentals in education**
  - Professional attacker and malicious subversion
  - Verifiable protection technology, with hands-on

# Trustworthy IS – Myth or Enabler

---



**IT 'S  
UP TO  
YOU**

*We have met the enemy and it is us. – Pogo*