A University Education
Cyber Security Paradigm Shift

For Engineers of Verifiably Secure Components and Systems

Dr. Roger R. Schell
schellr@ieee.org

- Distinguished Fellow, University of San Diego, Center for Cyber Security Engineering and Technology (CCSET)
- President, Aesec Corporation

National Initiative for Cybersecurity Education (NICE) , 2015
November 3 – 4, 2015
Paradise Point Conference Center
San Diego, CA 92109

The opinions expressed are solely those of the presenter and not necessarily those of any employer, sponsor, or associate.

Overview of Presentation

Science (or lack) underlying the mess we are in

- Past
- Present
- Future

Reference monitor a unifying scientific principle*

- Enables a paradigm shift for cyber security education
- Implementation called a "**security kernel**" [Anderson]

* Major credit: Cynthia E. Irvine, ***The reference monitor concept as a unifying principle in computer security education***. In Proceedings of the First World Conference on Information Systems Security Education, pp. 27–37, June 1999.

Perspective on Trusted Computing: Past, Present and Future

University of San Diego

The shortish version . . .

Often in the words of others

[paraphrase with emphasis added]

The Science of Trusted Systems: Past

University of San Diego

"Security kernel controls are effective against most internal **attacks**-including some that many **designers never consider**." [Ames et. al., IEEE Computer July 1983]

"security kernel distinguished by substantially dealing with the problems of **subversion** of security mechanism." [NCSC, circa 1984]

Legacy of Past Kernel Deployment: Withstood Nation State Adversary

"... isolating the security relevant code to a small protected kernel whose correctness can be certified." [**-- ARPA Review Group, 1970s (Butler Lampson)]**

- SACDIN Minuteman missile control (IBM)
- SCOMP for Multics comms (Honeywell)
- Secure Ethernet LAN (Boeing)
- GTNP/GEMSOS (Gemini Computers, Inc.)
  - Class A1 Blacker key distribution and access control
  - NSA evaluation of COTS Class A1 TNI M-component
  - MLS Pentagon enterprise "cloud" for OSD and USAF
  - ITSEC evaluation by UK CESG for MOD deployment
- Blacker "VPN" front-end (Unisys for NSA)

The Practice of Trusted Systems: Present

University of San Diego

"systems not designed for Internet threats, poorly implemented, nearly daily security patches, and millions of systems being compromised" [Safford, October, 2002]

The Practice of Trusted Systems: Present

"Nearly thirty years ago, Roger Schell accurately predicted the exact situation we find ourselves in: systems not designed for Internet threats, poorly implemented, nearly daily security patches, and millions of systems being compromised" [Safford, IBM, October, 2002]

No systematic data categorization (labeling)

- Only scientific basis to confine information flow

The Practice of Trusted Systems: Present

University of San Diego

Cyber security is much worse than recognized

- Growing threat of subversion by witted adversaries
  - Widely demonstrated “Easter egg” style artifices
- “Existential” threat – “a pre-9/11 moment”
- Sec Def Panetta: “could virtually paralyze the nation”

Bandaids and weak assurance can never work

- Current best practice is “Arms race we cannot win”
- Unsustainable penetrated and patch
- Ineffective monitoring and surveillance

Proven verifiable protection languishes

The Prospect for Trusted Systems: Future Depends on Choices

University of San Diego

"unthinkable that another thirty years will go by without one of two occurrences:

1. Either **horrific cyber disasters** will deprive society of much of the value of computers
2. Or available security kernel **technology will be delivered** in products that provide effective security" [Karger, IBM, ACSAC 2002]

- Cyber security education has major influence

Choice to Continue Present Path: To Future Horrific Cyber Disasters

University of San Diego

"Men's courses will foreshadow certain ends, to which, if persevered in, they must lead." – Dickens

- Disastrous 'certain ends' foreshadowed by:
  - More dependence on low assurance, e.g., cloud
  - Lack of purchase requirement for high assurance
  - Vested interests, e.g., "monopolist", new research
    - Competing govt "products", e.g., MISSI,NetTop,SELinux,MILS
    - Objection TCSEC interfered with research, products
  - Common "Best practice" misses subversion reality
  - Repeat failed practices, but expect different results

Choice to Depart Present Path: Deliver Future Skills and Products

"Men's courses will foreshadow certain ends, to which, if persevered in, they must lead. But if the courses be departed from, the ends will change." – Dickens

- "Ends will change' to reduce cyber risks by:
  - Leverage reference monitor, viz., security kernel
    - Pervasive data labeling, confidentiality and integrity
    - Kernel confines hosted applications and networks
  - Technology refresh can deploy in less than 2 years
    - Previously deployed kernels, e.g., COTS OEM RTOS
    - Aggressive phased, selective use, e.g., CDS and ICS
  - Commitment to **education**, evaluation and use
  - Align defense with threat, e.g., APT and subversion

Overview of Presentation

Science (or lack) underlying the mess we are in

- Past
- Present
- Future

Reference monitor a unifying scientific principle*

- Enables a paradigm shift for cyber security education
- Implementation called a "**security kernel**" [Anderson]

* Major credit: Cynthia E. Irvine, ***The reference monitor concept as a unifying principle in computer security education***. In Proceedings of the First World Conference on Information Systems Security Education, pp. 27–37, June 1999.

Paradigm Shift – Only Practical Way out of the Current Mess We're in

University of San Diego

The "facts" of the mess with current paradigm:

- Secure system on insecure platform is **impossibility**
- Traditional OS is untrustworthy – stream of patches
- Security kernel is "**only way** we know" for secure OS
- Half dozen kernels deployed – **no reported patches**
- Only existing kernel is practical to **deploy in 2 yrs**

Logical conclusion – change current paradigm

- Build **secure systems** on a existing security kernel

Cyber security engineering education is critical

- Current engineers not taught **how to build a kernel**
- Engineers not taught **to build systems** on kernel

Reference Monitor (RM) as Unifying Principle is a Paradigm Shift

University of San Diego

Supported by well-define body of knowledge

- Technology codified for **systems** in “Orange Book”
- Supporting guidelines in “Rainbow Series”

Approach: three strong “legs of the stool”

- Significantly mitigating software **subversion**
- Explicit mandatory access control (**MAC**) policy
- Systematically achieving **verifiable** protection

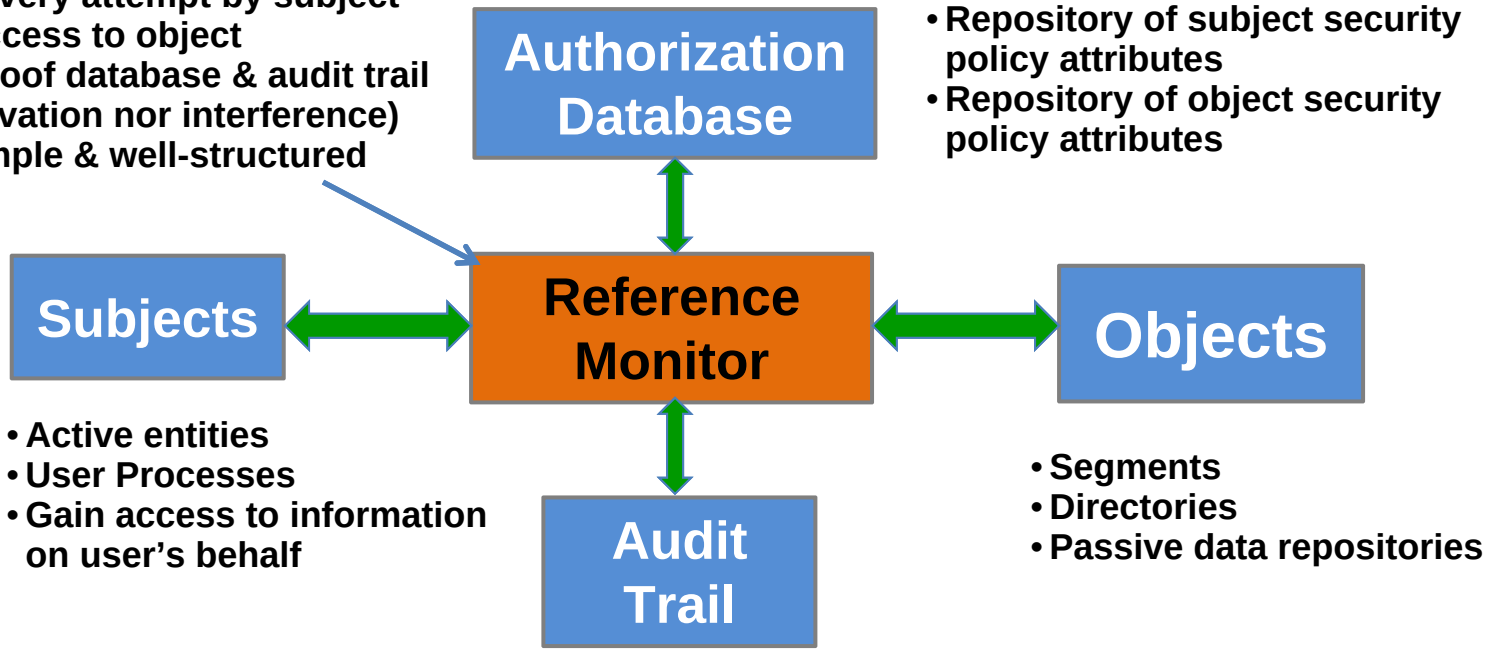
RM paradigm shift for cyber-security education

- Security must be built into education, not bolted on
- Same unifying principle for any education level

Example of MS degree organized around RM

Classic Reference Monitor Abstraction

- Enforces security policy
- Mediate every attempt by subject to gain access to object
- Tamperproof database & audit trail (no observation nor interference)
- Small, simple & well-structured



- Repository of subject security policy attributes
- Repository of object security policy attributes

- Active entities
- User Processes
- Gain access to information on user's behalf

- Segments
- Directories
- Passive data repositories

- Record of security-related events

Three Reference Monitor Principles

Tamper proof

- Isolation: protected unauthorized alteration
- Deals with subversion and malicious software

Always invoked

- Completeness: ALL subject to object references

Subject to analysis and test to assure correct

- Verifiability: perform its functions properly
- Can implement policy with high assurance

Hardware and software that implements RM

- Classic definition of security kernel [Anderson 72]

Illustrative University Education Cyber Security Engineering

University of San Diego

USD Considers Cyber Security Engineering MS

- Designed from outset based on reference monitor
- Leverage experience, e.g., Dr. Burnham UNO & USC

Three semester program

- Minimum of 27 units – **all** directed at cyber security
- Full on-line real-time distance education

Designed for heavy hands-on lab component

- Isolated **vulnerability validation** lab
- **Security kernel** application and administration lab

Lessons learned: hands-on labs are critical

- No substitute for lab exercises on real security kernel

RM is Scientific Basis for Three Semester Core Sequence

Security **policy** is RM foundation for assurance

- Maps to TNI (Red Book) "**MAID**" policy taxonomy
- Access control for both confidentiality and integrity
  - Mathematical partition into **M**andatory and **D**iscretionary
- **I**dentification for RM "subjects"
- Requirements for RM **A**udit file

Trusted systems design – build security kernel

- Linchpin is policy model "basic security theorem"

Secure **system engineering** – run on a kernel

- Composition methods – partitioned TCB and subsets
- Case studies of engineering verifiably secure system

RM Scientific Principles Pervasive in Illustrative Required Courses

University of San Diego

Foundations of Information Security

- Basic concept and terminology
- Students report assessment of cyber security press

Application and implementation of Cryptography

- Apply RM to protect keys, data and algorithms

Assurance in Cyberspace Security

- Techniques for analysis and test of RM

Distributed Systems and Network Security

- Network interpretation of RM
- Using Trusted Network Interpretation (TNI) concepts

RM Permeates Associated and Elective Courses

Software engineering for secure systems

Cyber security privacy consideration

Applied Cryptography

Secure Systems Administration

Computer and Network Forensics

Vulnerability discovery and validation

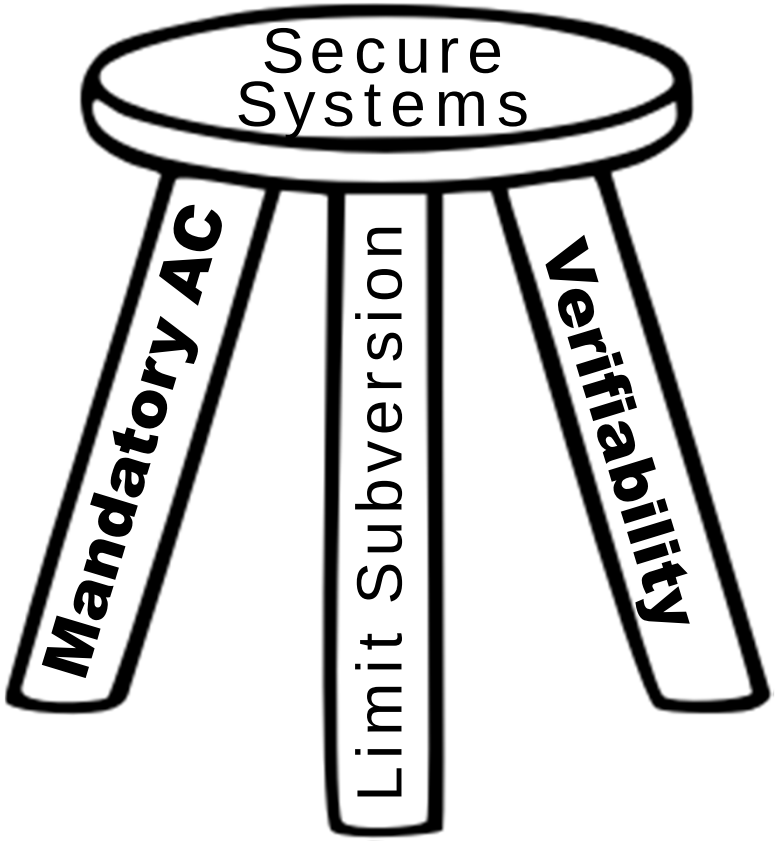
Formal methods

Data base security

Assuring big data cyber security

Legal and policy issues in cyber security

Three Strong Legs of "Stool": USC Applies RM for Secure Systems



1. Subversion is tool of choice for witted adversary
2. Only MAC policy can enforce secure information flow
3. RM is only known verifiable protection technology

Leg 1:Subversion is THE Problem: Likely Choice of Witted Adversary

ACM: "**identifying and addressing security vulnerabilities requires a different mindset from traditional engineering**."

35 years ago: subversion is "tool of choice"

"Key" for repeated, undetected exploits [Irvine]

- E.g., 6 LOC in 40M give total control of Windows
- E.g., 12 LOC in 4M total access to Linux file service

StuxNet demonstrates subversion efficacy

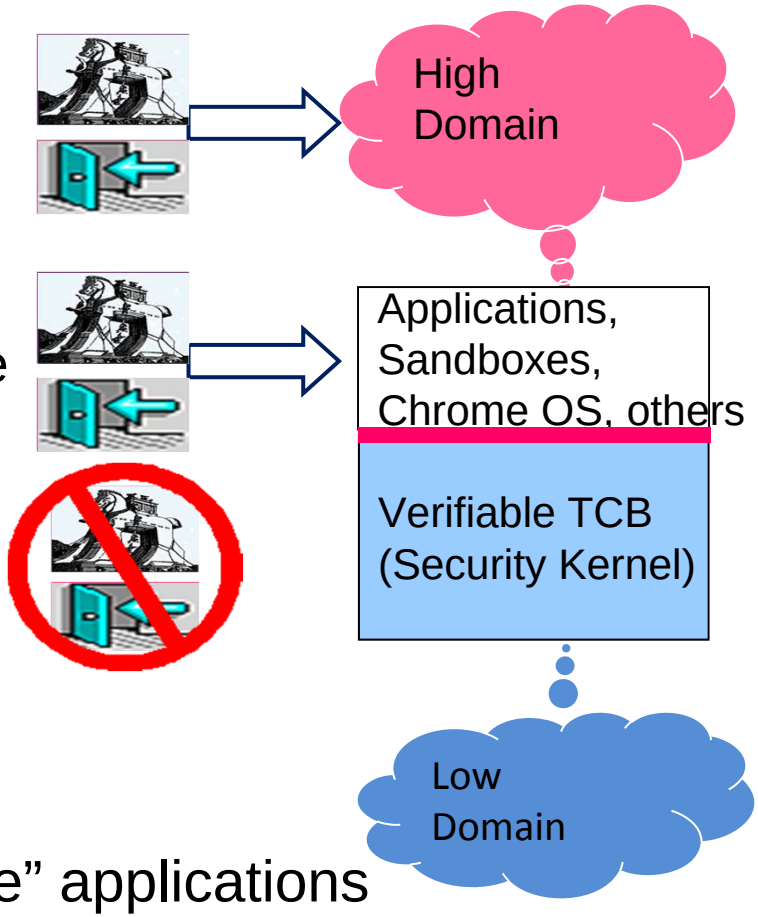
- Remote control, unknown attacker
- Class of serious breaches, e.g., Target, Sony, OPM

RM Proven to Mitigate Subversion

Plant trap door or Trojan horse

Impossible to find or fix
- Computer Science general case
- Application security noncomputable
  - "Arms race we can't win" – IBM

Protects data *despite* apps
- Computer Science special case
- Security kernel is computable
  - Completeness
  - Isolation
  - Verifiability



Security kernel doesn't assume "secure" applications

Leg 2: Use Science of MAC Policy: Explicit Label for Subject & Object

University of San Diego

Mandatory access control (MAC) policy

- Historically call non-discretionary policy
- **Subject** has formal authorization to access a domain
- Access based on sensitivity of information in **object**
  - Specific Information security domain (has “label”)
  - Labels often called “classification” and “clearance”

Fielded secure **system** composition examples

- DBMS, enterprise “cloud”, NSA crypto, UK “guard”

Cannot build security on “foundation of sand”

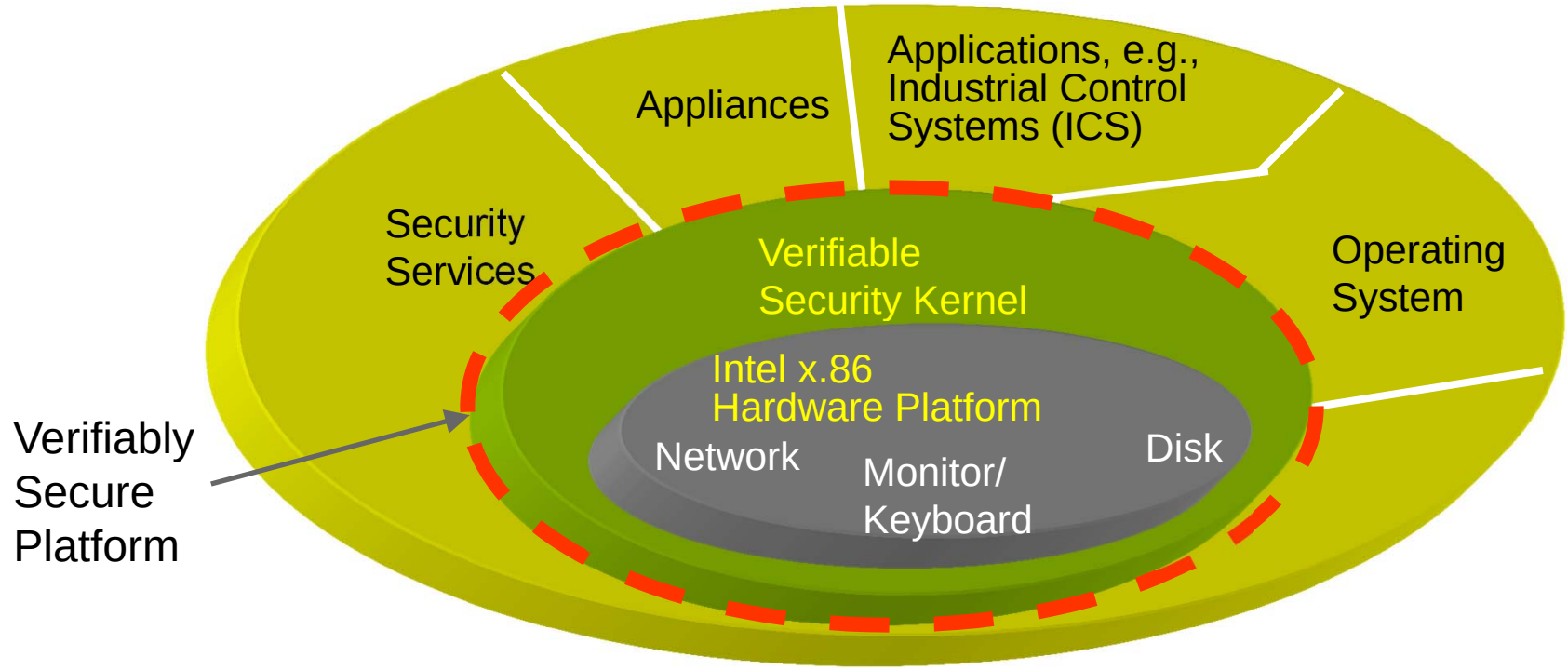
- MAC Kernel ensures subverted apps confinement

Use MAC to Build Systems: On Reusable Security Kernel

University of San Diego

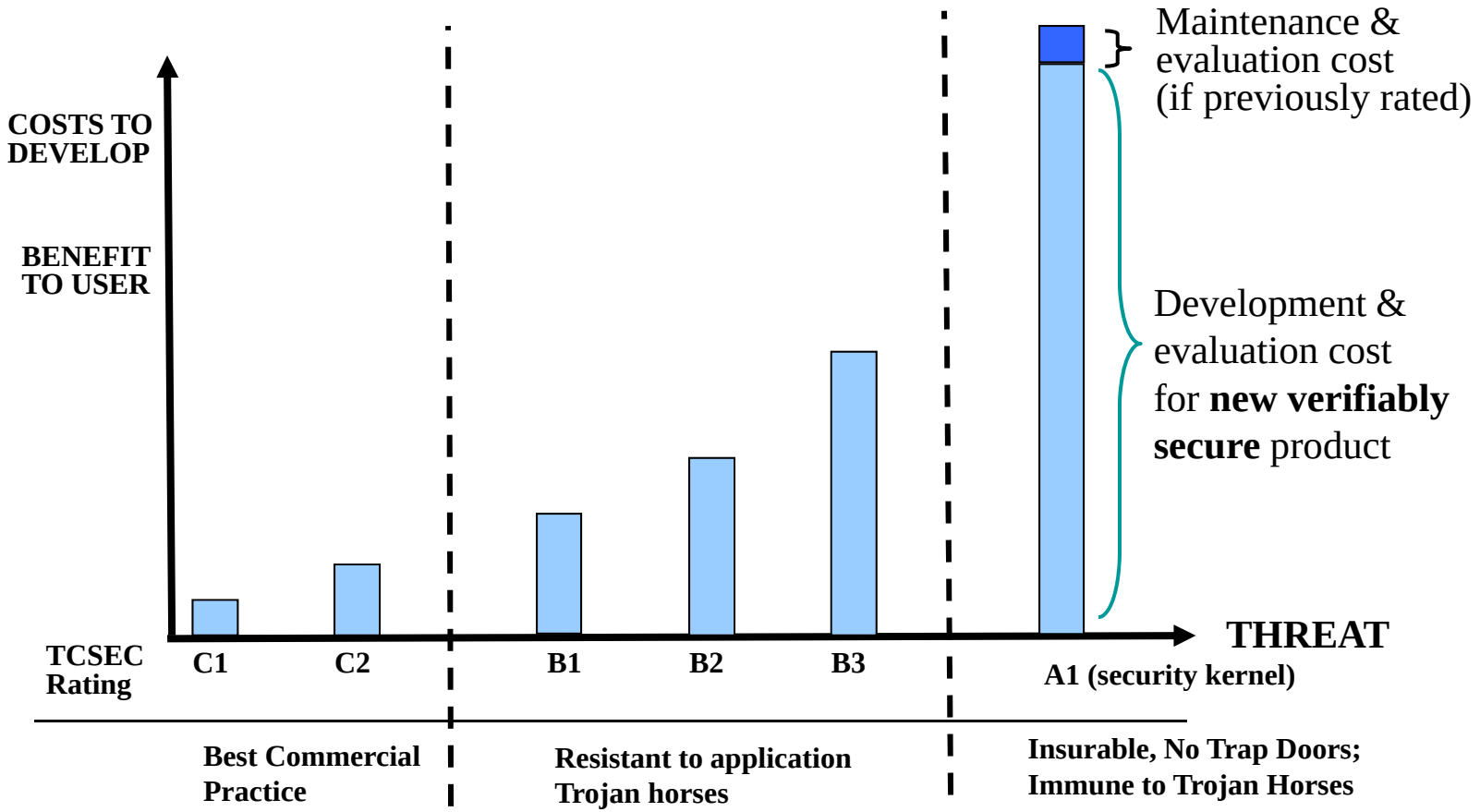
"The only way we know . . . to build highly secure software systems of any practical interest is the kernel approach."

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



Truly a paradigm shift: no Class A1 security patches reported in years of use

New vs Maintenance Cost/Benefit



Verifiable Trusted Systems: OEM Delivery Eco-System

University of San Diego

- Vendor delivers OEM product/support
  - With partners port to domain-specific hardware
- OEMs & manufacturers build platforms
  - Trusted distribution, evaluated configurations
- VARs, ISVs, appliance vendors deliver “box”
  - Add COTS operating system services and apps
- Solution providers and system integrators
  - Customization and integration for customers

Leg 3: RM is Proven Technology: Only Known Verifiable Protection

University of San Diego

Most used highly secure technique [Gasser]

- Not easy to build a security kernel
- Successful examples took 10-15 years to complete

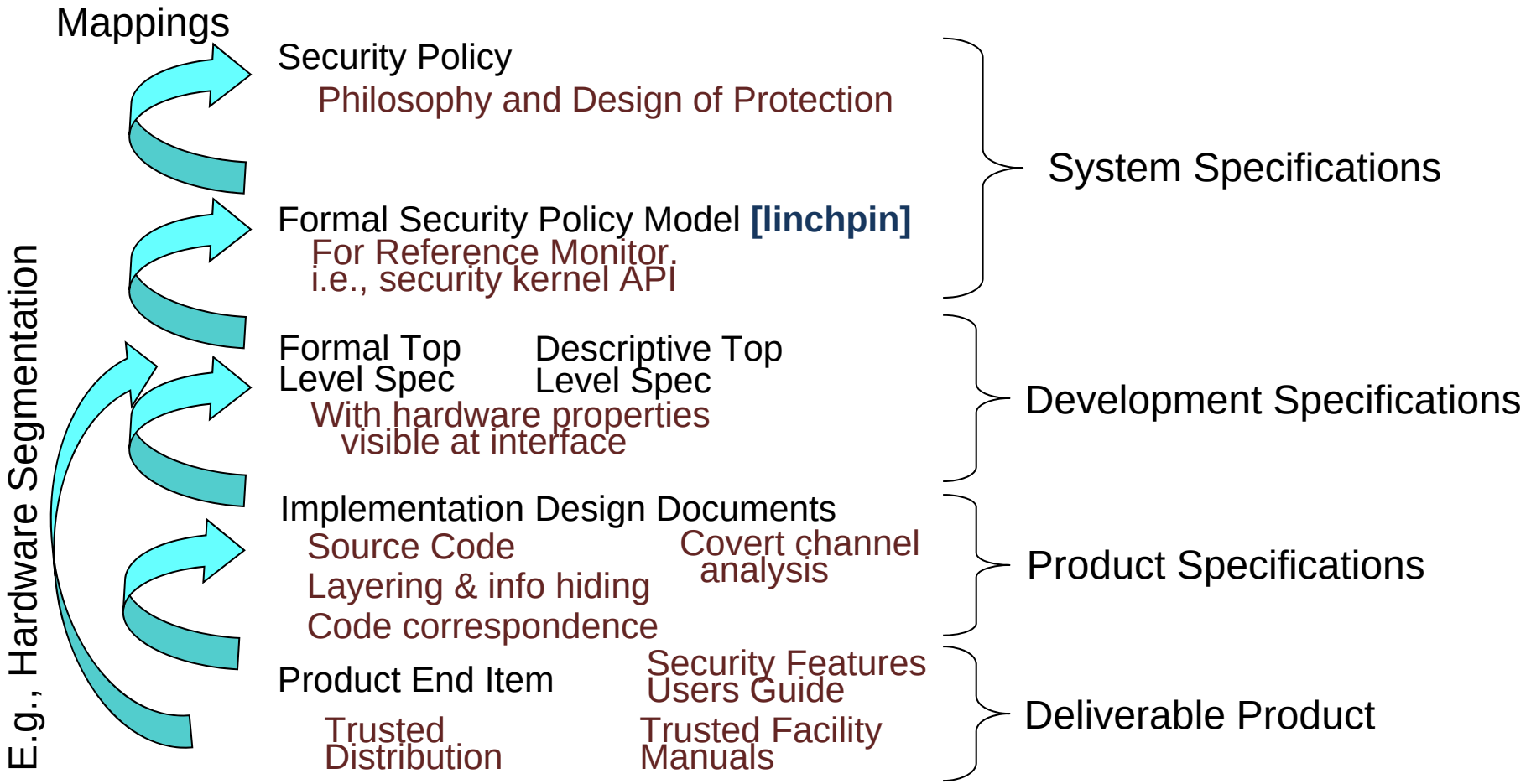
Demands supportive hardware to be practical

- **Segmentation** in instruction set, **protection rings**
- Hardware “root of trust” for trusted distribution

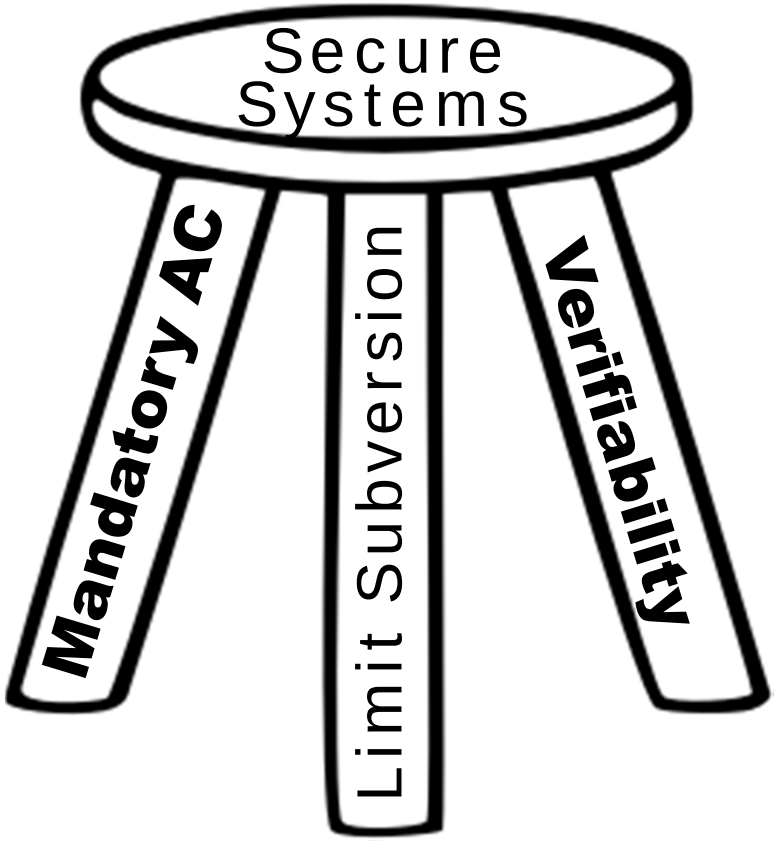
Rigorous **software engineering** enforcement

- Strongly-typed language is essential (prohibit C)
- Information hiding [Parnas], layering [Janson]
- Basis for proof sketch – maintains secure state

Basis for Trusted System Kernel: Systematic Engineering Process



Three Strong Legs for Secure Systems



Reference Monitor

is the

Organizing

Principle

RM Only Approach Proven to Work: Paradigm Shift in Security Education

University of San Diego

1. Witted adversary **subversion** dominant issue
   - Solution not adequate unless mitigates subversion
2. Understand creating overall security policy
   - System is only “secure” WRT a policy, viz., **MAC**
3. Graduates understand **verifiable** science
   - On security kernel that needs **no security patches**

Transformative only if RM permeates education

- Bolting on RM courses is NOT paradigm shift

Transformative Unifying Principle for Cyber Security Education

University of San Diego

IT 'S

UP TO

YOU

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

A University Education
Cyber Security Paradigm Shift

For Engineers of Verifiably Secure Components and Systems

Dr. Roger R. Schell
schellr@ieee.org

- Distinguished Fellow, University of San Diego, Center for Cyber Security Engineering and Technology (CCSET)
- President, Aesec Corporation

National Initiative for Cybersecurity Education (NICE) , 2015
November 3 – 4, 2015
Paradise Point Conference Center
San Diego, CA 92109

The opinions expressed are solely those of the presenter and not necessarily those of any employer, sponsor, or associate.