aesec™

The power of verifiable protection™

Powerful Security Kernel Cyber-defense Reset

Dr. Roger R. Schell, President
Edwards E. Reed, Sr. Director, RIT MS'90

RIT Cybersecurity Seminar Series
ESL Global Cybersecurity Institute
Rochester, NY – December 1, 2023

Arc of Cybersecurity History:
Past, Present, and Future

"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." – Charles Dickens

- Cybersecurity past
- Cybersecurity present
- Cybersecurity future

Cybersecurity Past: 1960s to 1980s
Recognize Computer Security Problem

- Vietnam electronic intelligence-combat operations interface
- USAF ADP Security Program – response to Ware Report challenge
  - MIT Multics Demand for CPU Hardware with **Segmentation & Rings**
- "Tiger team" experience – red team and **subversion**
  - Air University Review 1978 Achilles' heel paper on information warfare
- Foundational research and industry collaboration
  - "Anderson Report" – **reference monitor and security kernel**
  - Multilevel security (MLS) in Honeywell Multics for Pentagon, GM, Ford
  - SCOMP MLS communications: enhanced commercial minicomputer
- NPS research for CIA - open source MLS kernel design
  - Enduring basic reference by Phillip Myers on **subversion**

Cybersecurity Past: 1980s into 1990s
Build on Security Kernel Technology

- NSA DoD Computer Security Center – became "national" NCSC
  - Added third NSA mission – "separate and distinct organization"
  - Unquestioned world leader in cybersecurity technology
  - Formulated DoD policy standards for MLS deployment
- Codified decades of research in a standard: TCSEC (Orange Book)
  - Goal: widespread availability of trusted systems
  - Class A1 (**security kernel**) "substantially addressed **subversion**"
  - Systematic scientific network (TNI) and data base (TDI) interpretation
  - Used in internal NSA development – BLACKER Type 1 crypto
- DDIRNSA William Black ask: Can NSA trust a KGB-produced O/S?
  - Answer: "Yes, if it were built to Class A1 **security kernel** specs."

History of Security Kernel Characteristics

- Seminal concept description (Jun 1972 IDA Workshop)

  "*a compact security 'kernel' of the operating system and supporting hardware – such that an **antagonist could provide the remainder** of the system without compromising the protection provided. Advanced virtual memory techniques of **segmentation and protection rings** (such as those in the Multics system) offer a promising basis for the secure kernel.*"

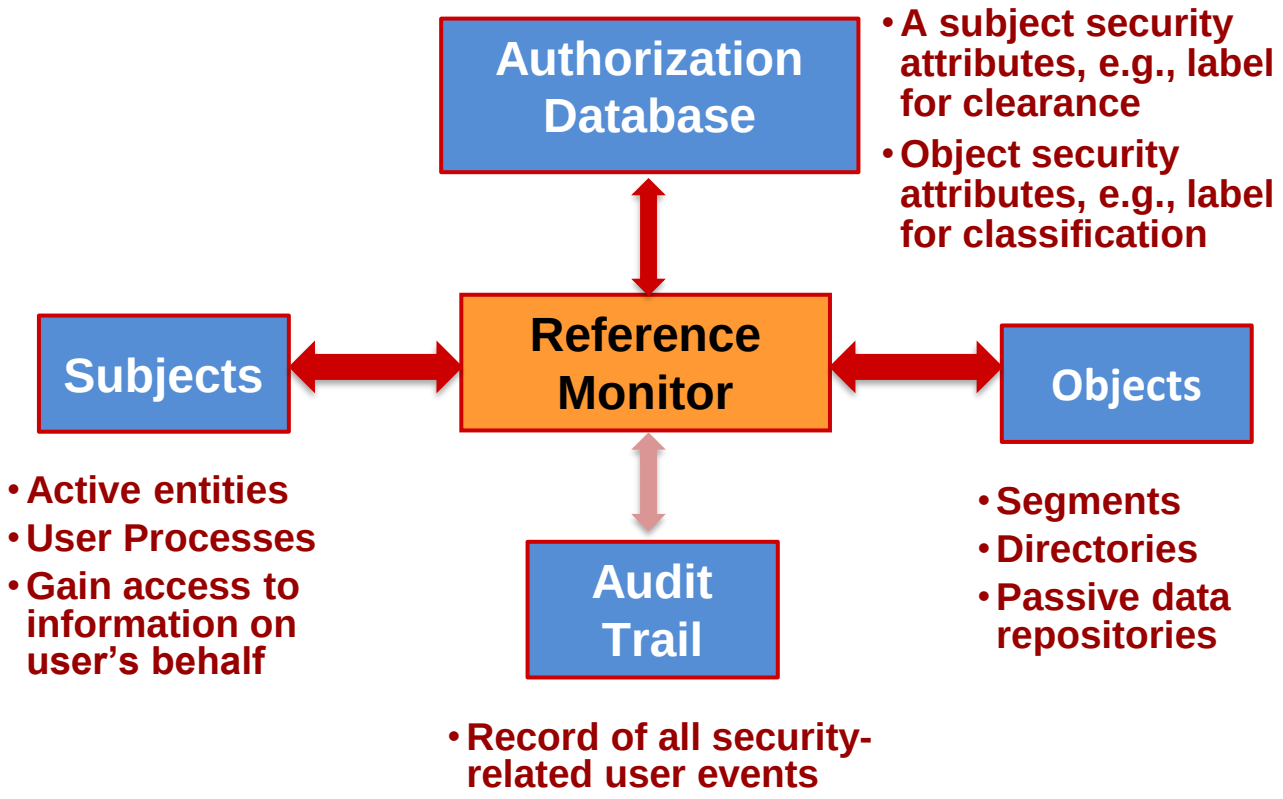
- Early characterization (Jul 1983 IEEE Computer article)

  "*the security kernel approach provides controls that are effective against most internal **attacks** – including some that many **designers never consider**.*"

- Consistent history of mitigating attacks (Nov 2016 CACM article)

  "*half dozen security kernel-based operating systems ran for years (even decades) in the face of nation-state adversaries **without a single reported security patch** "*

Security Kernel Definition
Reference Monitor implementation



Fundamental Properties

Completeness
- Non-bypassable **Segmentation**

Isolation
- Tamper-proof Protection **Rings**

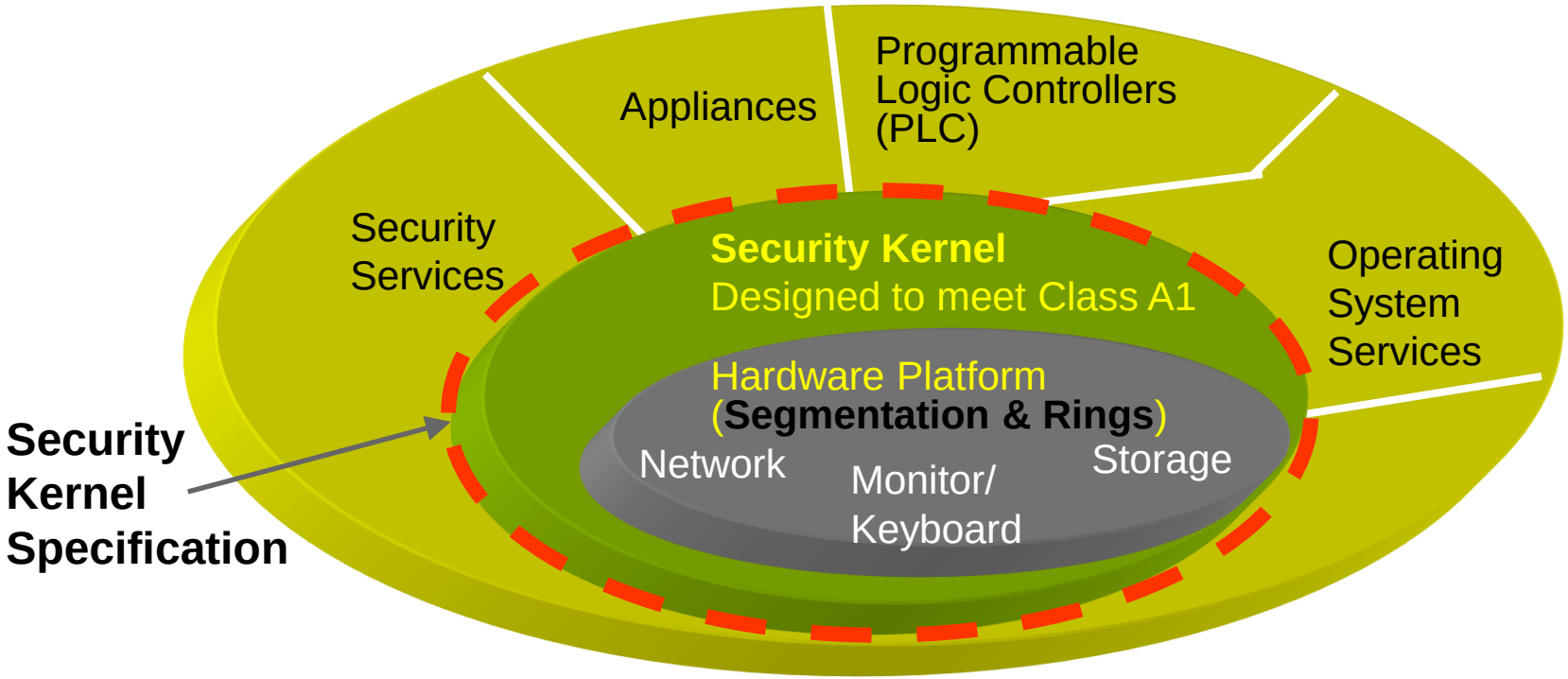
Verifiability
- Model-based Design
  and nothing else
- Formal Security Policy Model

DEFINITION (TCSEC Glossary): "***Security Kernel*** - *The hardware, firmware, and software elements of a Trusted Computing Base that* ***implement the reference monitor*** *concept.*"'

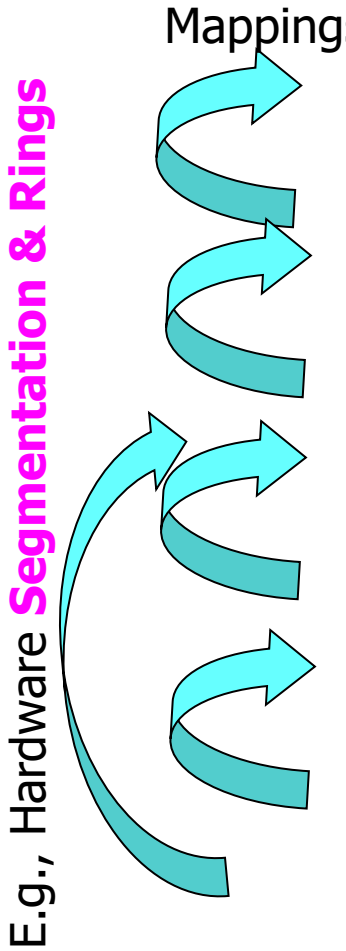
Security Kernel-Based Systems

"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)



Model-based Security Kernel



Security Policy
Philosophy and Design of Protection

Formal Security Policy Model [linchpin]
(**FSPM**) For Reference Monitor.
i.e., security kernel API

Formal Top Level Level Spec (FTLS)

Descriptive Top Level Spec

With hardware properties visible at interface

Implementation Design Documents
Source Code
Layering & info hiding
Code correspondence

Covert channel analysis

Product End Item

Security Features Users Guide

Trusted Distribution

Trusted Facility Manuals

System Specifications

Development Specifications

Product Specifications

Deliverable Product

And nothing else

Explicit TCSEC Subversion Mitigations
Section 4.1 Class A1-unique requirements

1. FTLS precisely defines security kernel API, including hardware
2. Show FTLS is consistent with the Formal Security Policy Model
3. Formal covert channel analysis to both identify and analyze
4. Penetration testing based on the FTLS
5. Hardware and firmware included in FTLS
6. Complete correspondence mapping of all source code to FTLS
7. Strict (inspectable) configuration management
   - Mitigate subversion of toolchain, design, source & objects
8. Trusted distribution of security kernel

Legacy of Security Kernel Deployments

"... 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
  - COTS evaluation as Class A1 TNI M-component
  - MLS Pentagon IBM terminal server for OSD and USAF
  - Published ITSEC evaluation in UK for MOD deployment
- BLACKER "VPN" front-end (Unisys for NSA)

Cybersecurity Past: 1990s to Present
Choice Between Two Divergent Paradigms

"Two roads diverged in a wood, and I — I took the one less traveled"
– Robert Frost

- **Surveillance-based road**
  - Patches attacks surveillance finds
  - **Chosen**: well travelled past road
  - Abolished commercial evaluation
  - Eliminated TCSEC as a standard
  - Reassigned NCSC evaluation staff
  - Led to huge vested $$ interests
- **Model-based road**
  - Security kernel for formal model
  - **NOT chosen**: less traveled road
    - Contributed to "**market failure**"

Cybersecurity Present
Surveillance-based Design

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

- Disastrous 'certain ends' foreshadowed by:
  - Expanding use of low assurance, e.g., cloud, critical infrastructure
  - Lack of market business case incentives for truly trustworthy systems
  - Vested interests, e.g., $200 billion annual cybersecurity market
    - Competing government "products", e.g., MISSI, NetTop, SELinux, MILS
    - Objection that the TCSEC interfered with vested research, "new" products
  - Futile penetrate and patch – "arms race we can't win"
  - Ineffective monitoring and surveillance as defense basis
  - Burdensome "Best practices" miss **subversion** by professional attacks
  - Government "Policy" against full multilevel inhibits high assurance use

Reset for Bright Cybersecurity Future
Model-based design

"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." – Charles Dickens

- 'Ends will change' to dramatically reduce cyber risks by:
  - Leverage security kernel, viz., designed to meet TCSEC "Class A1"
    - Pervasive data labeling policy, confidentiality and integrity
    - Trustworthy components confine layered applications and networks, e.g., TNI
  - "RAMP" to deploy in < 2 years and promptly refresh
    - Apply previously deployed kernel-based products, e.g., COTS OEM RTOS
    - Visible sponsored reference implementations
    - "No-waiver" phased, selective use, e.g., massive databases, and ICS for SCADA
  - Commitment to education, supply chain, evaluation and use
  - Aligns defenses with threat, e.g., APT and **subversion** in supply chain
- Truly a paradigm shift: no security patch for Class A1 – ever

Delivery of Trustworthy Systems
Traditional OEM Eco-System

- Vendor delivers reusable OEM **security kernel** product/support
  - With partners port to domain-specific hardware
- OEMs & manufacturers build trusted platform
  - Trusted distribution, evaluated configurations
- VARs, ISVs, appliance vendors deliver "box"
  - Add COTS operating system services and apps on **security kernel**
- Solution providers & integrators deliver to user

CONCLUSION for Education and Research

Need Security Kernel Cyber-defense Reset

- It is scientifically impossible to build a secure cyber system without a trustworthy operating system, e.g., one highly unlikely to have a zero-day flaws
- Reproducible design pattern, multiple vendors, multiple products – with **NO** security patches, **EVER**
- Can leverage operating system technology designed to meet Class A1. It is commercially available, and previously deployed in high-profile systems for decades without a single reported zero-day flaw or security patch

Potential Research Ideas

- Add Segmentation/Rings to RISC-V ISA
- Equities Question – Analysis and Recommendation
  - What are the consequences of having BOTH security crypto AND end points
- Define a MAC policy for shared hardware fabrics/circuits
  - Identify underlying Reference Monitor that controls all accesses
- Identify & prototype trustworthy 3-tier labeled gateway
  - Trusted network design, classic multi-tenant Information Technology Cloud
- Identify & prototype massive scales – millions of IoT devices
- Leverage Reference Monitor for Resilience to massive attack
  - Role of trustworthy foundries to nation-state resilience

aesec™

The power of verifiable protection™

Powerful Security Kernel Cyber-defense Reset

Dr. Roger R. Schell, President
Edwards E. Reed, Sr. Director, RIT MS'90

RIT Cybersecurity Seminar Series
ESL Global Cybersecurity Institute
Rochester, NY – December 1, 2023

Bibliography

- Cyber defense triad for where security matters
  - http://www.aesec.com/CACM-Schell-Cyber-Defense-Triad-Nov2016.html
- Using Proven Reference Monitor Patterns for Security Evaluation
  - http://www.mdpi.com/2078-2489/7/2/23/htm
- GEMSOS Final Evaluation Report
  - https://www.aesec.com/eval/NCSC-FER-94-008.pdf
- Collected Papers
  - http://www.aesec.com/papers.html
- Seminal Papers
  - https://seclab.cs.ucdavis.edu/projects/history/seminal.html