Dramatic Cyber-Physical Attack Surface Reduction
Leveraging Integrity MAC Security Kernel

Dr. Roger R. Schell, PhD
President and founder of Aesec Corporation
roger.schell@aesec.com
(831) 657-0899

CREDC Seminar
University of Illinois at Urbana-Champaign
Streamed live on the Web
October 1, 2019
2:00pm to 3:00pm CDT
Presentation Outline

• Problem: national existential risk

• Available solution technology: security kernel

• EDS delivery path: PLC technology transfer
Presentation Outline

• Problem: national existential risk
  – Poor energy delivery systems (EDS) resilience
  – Vulnerable critical cyber-physical EDS components

• Available solution technology: security kernel

• EDS delivery path: PLC technology transfer
National Existential Risk
Poor EDS Resilience

• Leon Panetta, former SecDef & CIA Director
  – “Biggest nightmare is of a computer virus
    - that attacks and disables US infrastructure”
  – “Could result in millions of lost lives” [Mar 2019]

• Both current and former Federal CISOs
  – “what keeps them up at night”
  – “Exposure of critical infrastructure to attacks
    - against industrial control systems [PLCs]” [Sep 2019]

• U.S. government claims Russian subversion
  – “power grid hackers left behind tools needed to
    - later disrupt grid by shutting off vital systems.” [Jun 2019]
Computer systems all use operating system (OS)
- Programmable Logic Controllers (PLC) have an OS
Science: secure system requires trustworthy OS
- Must withstand witted adversary cyber attacks
EDS cyber physical PLCs use untrustworthy OSs
- One of a few common OSs – none trustworthy
- Evident by stream of regular “security patches”
Cyberattacks inflict permanent physical damage
- STUXNET destroyed Iranian enrichment centrifuges
- Crash Override for physical Ukraine EDS destruction
- Triton aimed for Saudi refinery destruction
• Problem: national existential risk

• Available solution technology: security kernel

• EDS delivery path: PLC technology transfer
Security Kernel Technology
Solution Concept Introduction

• Seminal (1972) concept description
“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.”

• Early (1983) IEEE article characterization
“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
“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”
“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 today. Codified in TCSEC Class A1

TCSEC Glossary: “Security Kernel - The hardware, firmware, and software elements of a Trusted Computing Base that implement the reference monitor concept.”

Security Kernel
Designed to meet Class A1

Hardware Platform (Segmentation & Rings)

Network
Monitor/Keyboard
Storage

Trusted Device
“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 for kernel in years of use
• NIST calls out “kernel” in flagship SP-800-160v1
  - “Electric Grid – Industrial/process control systems”

• PLC typically controls critical physical component
  “Trustworthy components within ICS, including for example, highly assured, kernel-based operating systems in Programmable Logic Controllers” [PLC]

• Kernel MAC controls integrity security domains
  “can help achieve a high degree of system integrity and availability through domain separation with control over cross-domain flows and use of shared resources.”
Controlled sharing between integrity domains
- Enforce Mandatory Access Controls (MAC) policies

Verifiable Design required for MAC enforcement
- **Add on** security by test and analysis has failed
  - Threat/vulnerability detection & response never finish
- **Build in** security by Construction is successful
  - Reference Monitor basis of the TCSEC Class A1 approach

Mitigate subversion, e.g., malware (STUXNET)
- To protect distribution of software & commands
  - Protect installed code, configuration settings & data

All three required for Secure Operating System
Security Kernel Technology
Cyber Defense Triad

- MAC policies required
  - To secure information flows
- Reference Monitor
  - Only known verifiable protection technology
- Deal with Subversion
  - Tool of choice for witted adversaries
Presentation Outline

• Problem: national existential risk

• Available solution technology: security kernel
  – Integrity Mandatory Access Controls (MAC) policy
  – Verifiable design for MAC enforcement
  – Mature subversion mitigation

• EDS delivery path: PLC technology transfer
Four distinct **hierarchical** integrity domains

1. Cyber physical system (CPS) control
   - **Only** domain with I/O access to physical hardware
   - Enforces “Pierson Safe Region” for physical device
2. Supervisory Control and Data Acquisition
   - SCADA domain – main PLC “Logic Loop”
3. Distributed control
   - Integrity-protected network interfaces
4. Untrusted public networks (e.g., Internet)
Integrity MAC policy
MAC Reduces Attack Surface

- Network access of any kind gives adversaries a huge attack surface
- Distributed control is vulnerable to insider attack
- SCADA and other adaptable control systems can be sabotaged
- Cyber Physical Control requires protection of Safe Regions that only Mandatory Access Controls provide
Integrity MAC policy
Prototype OPLC Integrity Domains

High Integrity
“Pierson Safe Region” Hardware Control

Medium Integrity
Update Current State
Program Logic
Command New State

Medium-Low Integrity
SCADA Modbus Server
TCP/IP Network

Low Integrity
Serial I/O Network
Ethernet/Fiber/Radio

= Cross-Domain Service (CDS)
Integrity MAC policy
OPLC Physical CPS Device Control

High Integrity

Mockup Diagram

Medium Integrity

Key:
Information Flows
Processes
Databases

Buffer Management
Pierson Safe Region
Physical Device

Cross Domain Service

Update Buffers In
Program Logic
Update Buffers Out

Logic Loop

Update Buffers Out

scada_modbus_server

Remainder of OpenPLC

Data input
Data output

Data input
Data output

mb_db
Modbus Database

R/W Mutex
R/W Mutex
R/W Mutex
R/W Mutex
R/W Mutex

R/O Mutex
R/W Mutex
R/W Mutex
Presentation Outline

• Problem: national existential risk

• Available solution technology: security kernel
  – Integrity Mandatory Access Controls (MAC) policy
  – Verifiable design for MAC enforcement
  – Mature subversion mitigation

• EDS delivery path: PLC technology transfer
• NIST highlights in flagship SP-800-160v1
  “Trustworthy Secure System Development”

• Reference Monitor Concept
  “provides an abstract security model of the necessary and sufficient properties that must be achieved by any system mechanism claiming to securely enforce access controls.”

• Security Kernel defined as its implementation

• Integrity-MAC is access control policy
Verifiable Design for MAC
Secure by Construction

Mappings

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

Product End Item
Trusted Distribution

System Specifications
Development Specifications
Product Specifications
Deliverable Product

E.g., Hardware Segmentation

Covert channel analysis

Security Features
Users Guide
Trusted Facility Manuals
Verifiable Design for MAC
Ineffective Shortcuts

• Reference Monitor & **FSPM** are long, hard work
  – Omitted by unwary/lazy for “plausible” shortcuts
• “Verified OS” – for functionality, not policy FSPM
  – Example: seL4 – need to verify info flow outside OS
• “Partition Kernel” lacks FSPM for kernel API
  – Example: MILS – explicitly excludes from kernel
• “Verified capability hardware” – missing a FSPM
  – Examples: DARPA-sponsored CRASH and CHERI
• Static code analysis – lacks FSPM for API of OS
  – Example: LDRA Testbed
• Shortcuts cannot **enforce** Integrity MAC for PLC
Intel x86 Architecture
Hardware Protection Levels (Protection Rings)

- Essential Hardware Properties
  - Hardware Rings – more than 2
  - Memory Segmentation vs Paging
  - Strong Process Model
- NSA TCSEC/TNI Class A1 – Verified Design

Presentation Outline

- Problem: national existential risk

- Available solution technology: security kernel
  - Integrity Mandatory Access Controls (MAC) policy
  - Verifiable design for MAC enforcement
  - Mature subversion mitigation

- EDS delivery path: PLC technology transfer
Mature Subversion Mitigation
NIST: Class A1 for Subversion

- NIST cites “Class A1” in flagship SP-800-160v1
  - “Application . . . to Commercial Products”

- Products are worked examples and use cases
  - “highly trustworthy components and systems that have been verified to be highly resistant to penetration from determined adversaries”

- TCSEC **Class A1** distinguished
  - “by substantially dealing with the problem of subversion of security mechanisms.”
Mature Subversion Mitigation
Trusted Device Protects Itself

- Trusted Boot for software/configuration settings
- Vet Trusted Devices for unauthorized behavior
- Code Correspondence stop “dead code” malware
- Trusted Distribution avoids supply chain attacks
- Media integrity mitigates “parking lot” attacks
Mature Subversion Mitigation
Stopping Malware Attacks

### Attack technique

- Design process
- Development process
- Industry standards
- Parking lot USB drives
- Network attacks
- Phishing attacks
- Deliver network map
- Find OS/RTOS
- Tailor attacks
- Install tailored attacks
- Alter config settings
- Bypass safety limits
- Bypass safety limits
- Send damaging commands
- Erase audit logs

### Attempt

- Subvert the design
- Install discovery tools
- Send data to malware controller
- Install code on device controller
- Trigger attack on physical device

### Class A1 Stopper

- Formal Sec Policy Model
- Formal Top-Level Spec
- Minimization
- Code Correspondence
- Trusted Distribution prevents unauthorized installation of code
- MAC Secrecy prevents data transfers to public networks
- MAC Integrity prevents unauthorized data transfers to physical device
- MAC Integrity prevents unauthorized access to I/O connections to physical devices

### Value Proposition

- Verifiable Design substantially mitigates subversion
- Trusted Distribution prevents toe-hold
- MAC Secrecy prevents data exfiltration
- MAC Integrity defeats targeted attacks
- MAC Integrity over Composable* domains (hierarchy) prevents damage to physical device

*Composition per TNI Class A1

26
Mature Subversion Mitigation
Illustrative STUXNET Mitigation

Class A1 Trusted Distribution rejects installation of untrusted software (malware)
by checking for authorized cryptographic seal
Parking Lot USB, phishing payload, etc.

Trusted Device Supplier
Trusted OEM Supplier: e.g., Siemens

Trusted Device
Crypto-Sealed
Lacks Seal
Crypto-Sealed

Trusted Device Software
Physical Device (e.g., Generator)

= Trusted Hardware Root of Trust (e.g., Intel TPM or custom FPGA)
= Trusted Device Distribution Keys
= OEM Distribution Keys

Class A1 Evaluation included use of a suitable Trusted Distribution Cryptographic Algorithm (e.g., Simmons)
Suppliers AND Customers BOTH get Trusted Device updates via Trusted Distribution;
OEM Supplier’s Keys not exposed
Presentation Outline

- Problem: national existential risk

- Available solution technology: security kernel

- EDS delivery path: PLC technology transfer
  - Original Equipment Manufacturer (OEM) model
PLC Technology Transfer
Traditional OEM Model

- **Security kernel vendor offers Trusted Device**
  - Hardware & software domain-specific platform, e.g., motherboard, SOC
  - Trusted distribution, system security certification

- **OEMs & manufacturers build PLC platforms**
  - Trusted Device is part of any hardware product configuration

- **VARs, ISVs, appliance vendors**
  - Add applications and system services software, use OpenPLC source

- **Solution providers and system integrators**
  - Customization and integration for customers
  - Deliver complete solutions

10-15 yrs

OEMS & Manufacturers

VARs, ISVs, Appliance Vendors

Systems Integrator Solutions

2-3 yrs
Former DIRNSA LtGen Linc Faurer note [2007]

“very high priority problem area”
- “vulnerability of our network components and
electronic credentials to software subversion”
- “convinced that an IC disaster looms”

“demands that the first set of solutions”
- “directly leverage the designs, architectures and
rating maintenance plans [RAMP] which NSA has
previously evaluated at the Class A1 level of assurance”
- “this is the only practical way to be confident the
needed solutions can be operationally deployed in the
next couple of years.”
Problem: national existential risk
- Poor energy delivery systems (EDS) resilience
- Vulnerable critical cyber-physical EDS components

Available solution technology: security kernel
- Integrity Mandatory Access Controls (MAC) policy
- Verifiable design for MAC enforcement
- Mature subversion mitigation

EDS delivery path: PLC technology transfer
- Original Equipment Manufacturer (OEM) model
Verifiable CPS Bottom Line

- Critical *physical* components need verifiable PLC
  - Limited system risk from remaining components
- Kernel makes CPS attack surface much smaller
  - Each *integrity MAC* domain protected from lower
  - Security kernel *verified design* for unknown attacks
  - Deals with *subversion* of security mechanisms
- PLC performance & functionality retained
  - OEM host PLC on *trusted device* with secure OS
  - PLC manufacturers can use OpenPLC prototype
- Mature OEM business model & support approach
  - Successful security kernel OEM delivery history
EDS clear **NEED** for resilient CPS

Commercial **TECHNOLOGY** available

Lack PLC manufacturer **ADOPTION**
Dramatic Cyber-Physical Attack Surface Reduction
Leveraging Integrity MAC Security Kernel

Dr. Roger R. Schell, PhD
President and founder of Aesec Corporation
roger.schell@aesec.com
(831) 657-0899

CREDC Seminar
University of Illinois at Urbana-Champaign
Streamed live on the Web
October 1, 2019
2:00pm to 3:00pm