23-25 JAN.
2018
—
The EGG
BRUSSELS

Roman Lysecky

Automated threat detection and mitigation in medical devices

A MedTech Europe event
The MedTech Forum
bringing HealthTech stakeholders together

Connected Medical Devices

Connected/Smart Medical Devices

- Connected devices offer tremendous potential to improve healthcare
- Security of medical devices is increasingly a critical concern among all the healthcare stakeholders

Connected/Smart Device Security

- Historically, medical devices systems (and embedded systems in general) were not susceptible to remote hacks and malware
  - Devices lacked network connectivity
  - "*Secured*" by their physical locations
- Network access is now pervasive, and even legacy devices are being connected to the internet
- **For medical devices, the threat of hacks and malware has significant concerns for patient health and costs of recalls**

Impact of Device Recalls

- US FDA recalled ≈500,000 implantable pacemakers and cardiac defibrillators due to security vulnerabilities

  *… which could result in **patient harm** from rapid battery depletion or administration of inappropriate pacing*

- Correcting vulnerabilities requires physician visit for software update or surgery to replace the device
- Potential overall cost of recall: $3 billion

- **Recalls take time and patients are left vulnerable**

Security Doesn’t Stop at Design

Design for Security: Proactive and Reactive

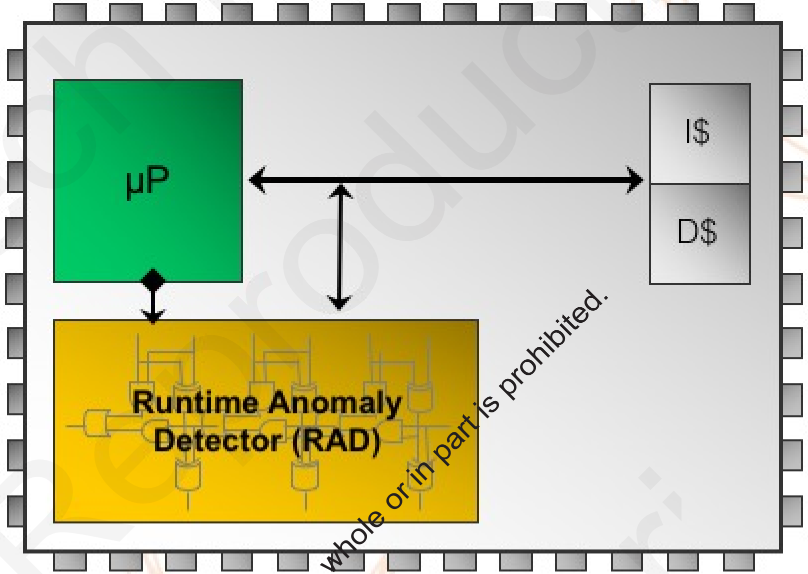
- Security and privacy threats must be addressed throughout the product lifecycle
- Security is shared responsibility of device manufactures and healthcare providers

- **Advocate that a fundamental requirement is to support runtime mitigation**
  - Capable of identifying and safely reconfiguring advice's operation to mitigate vulnerabilities
  - Ensuring the continuity of life-critical operations and patient privacy

Automated Threat Detection

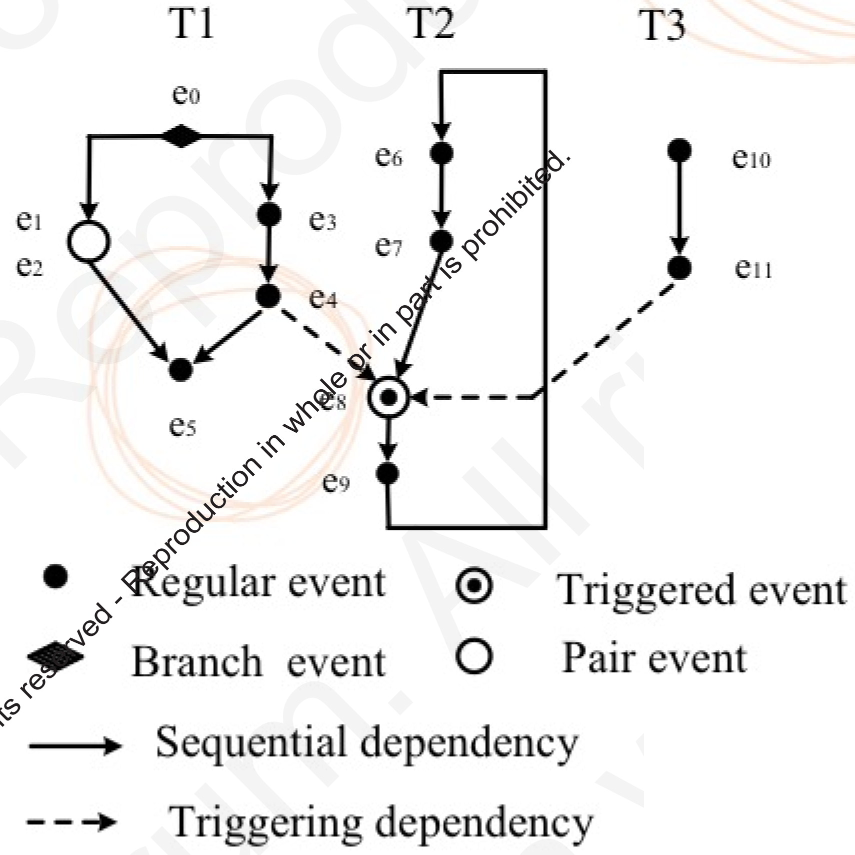
Runtime Anomaly Detection

- Anomaly detection detects attempted hacks, breaches, malware, etc., by continually monitoring the system execution
- Deviations between normal execution and runtime behavior indicate potential threats
- On-chip hardware ensures efficiency (e.g., 1% power overhead)



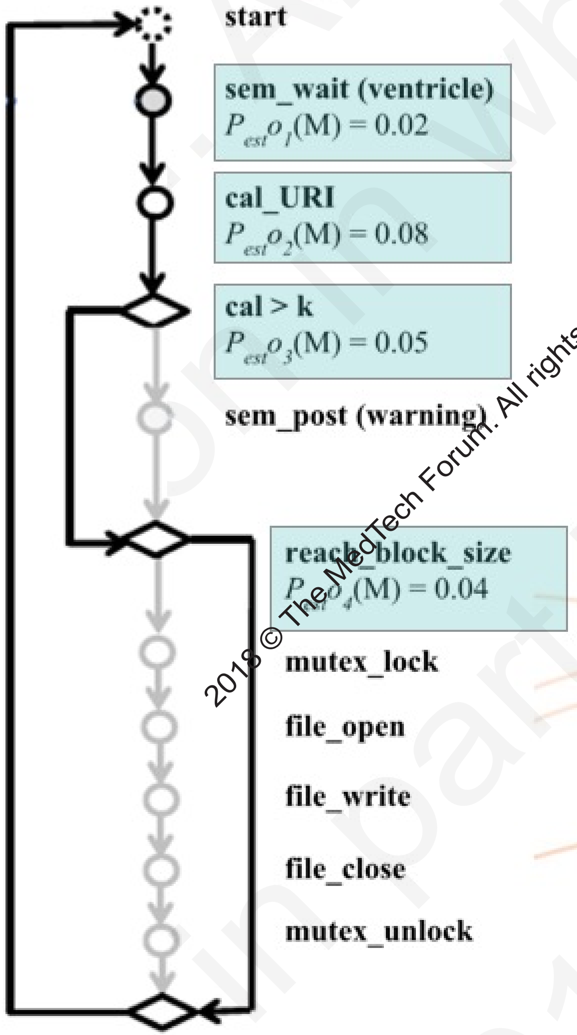
Formal Runtime Security Models

- Formals models incorporate both timing and execution ordering behaviors
- Embedded systems software typically contains precise and well-defined timing requirements
  - Can be used to increase detection rate, accuracy, and speed of runtime threat detection



2018 © The MedTech Forum. All rights reserved - Reproduction in whole or in part is prohibited.

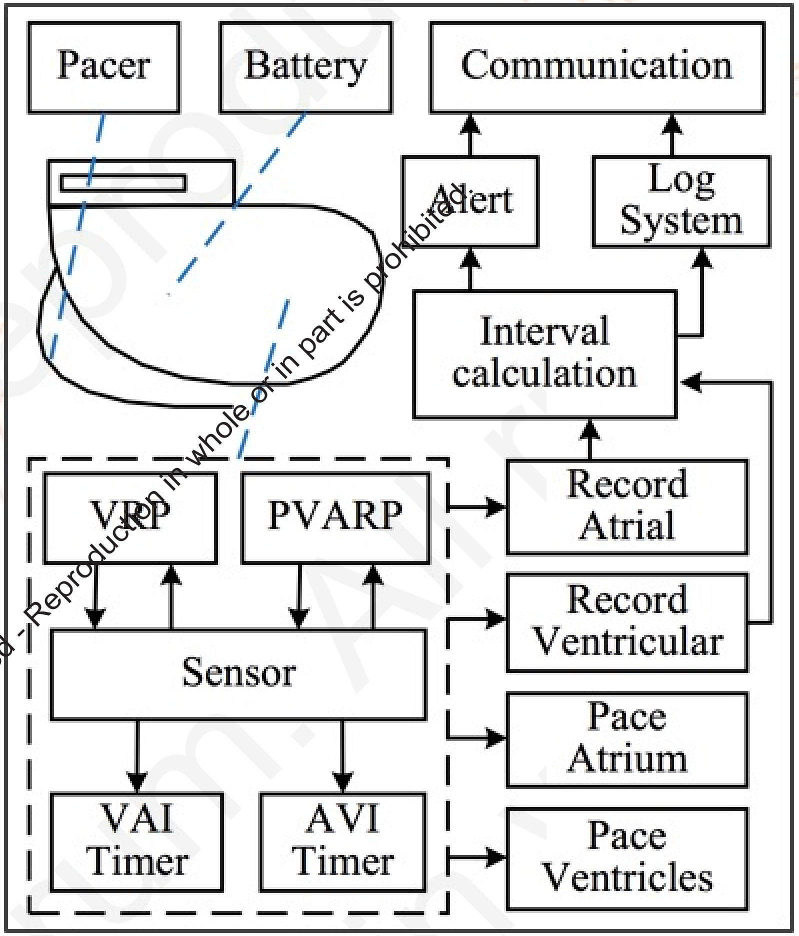
Estimating Threat Probability



$P_{est}p_j(N) = 1 - (1 - P_{est}o_j(M))$

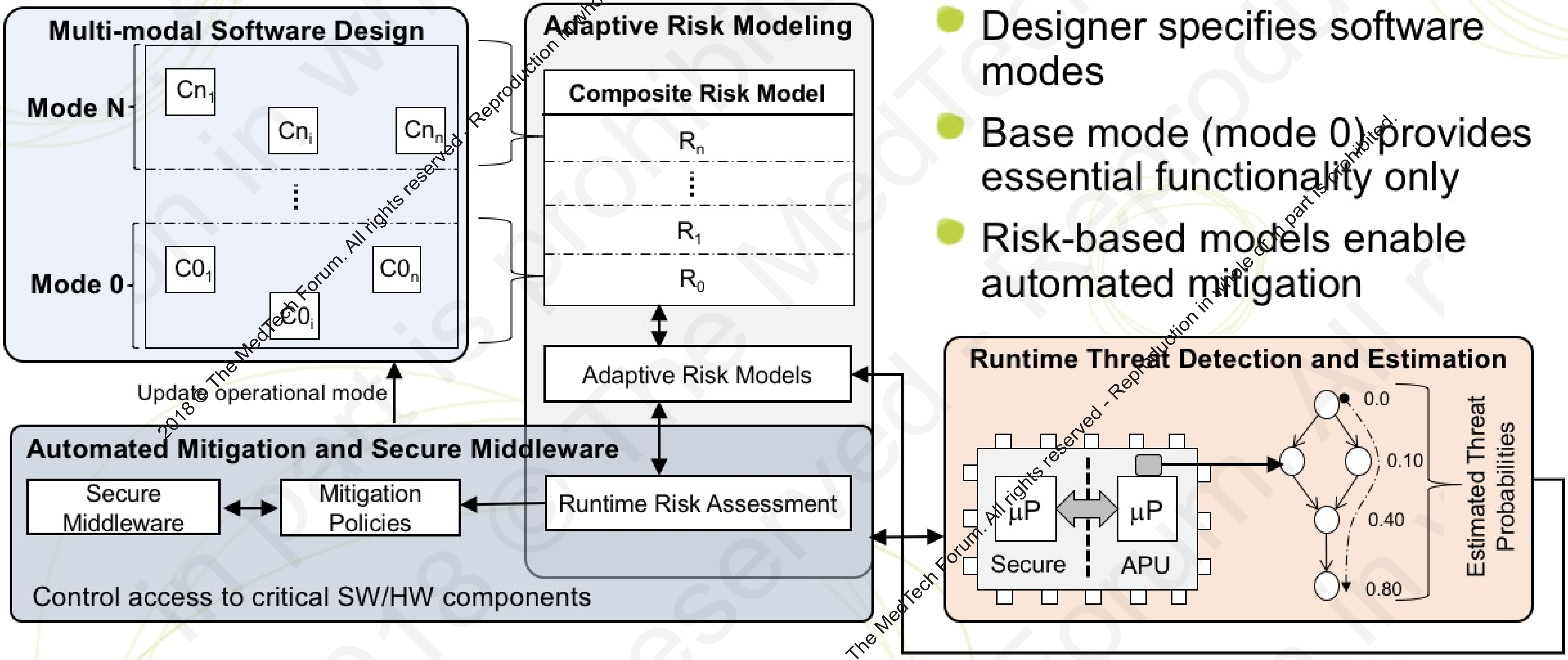
$P_{est}p_j(N) = 0.18$

- Runtime anomaly detection can isolate which components are affected
- Estimate the probability of a threat affecting specific software components, tasks, and applications
- Average detection rate greater than 95%
- Machine learning yields 45% improvement



Automated Runtime Mitigation

Multimodal Adaptive Software Design



- Designer specifies software modes
- Base mode (mode 0) provides essential functionality only
- Risk-based models enable automated mitigation

Concluding Remarks

Concluding Remarks

- Security and privacy threats must be addressed throughout the product lifecycle
- Security is shared responsibility of device manufactures and healthcare providers
- Automated runtime threat detection and mitigation is a fundamental requirement for connected medical devices