

---

# Real Time Systems Security Considerations

Prepared by  
Dr. Samuel E. Bowser  
Senior Project Engineer  
The Aerospace Corporation

# Overview

---

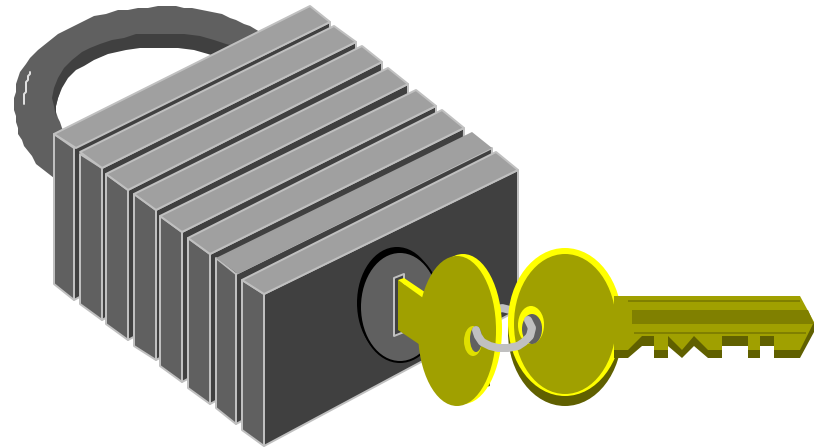
- Many RT processors control critical systems.
- Human lives, mission success, and even national security often depend on RT systems properly functioning as designed – frequently with little margin for error.
- The unique nature of the RT operating environment and the protection of embedded RT systems presents a unique challenge for the system designer.

# RT SECURITY ENVIRONMENT

---

- To adequately protect a RT system, it is necessary to ensure effective:

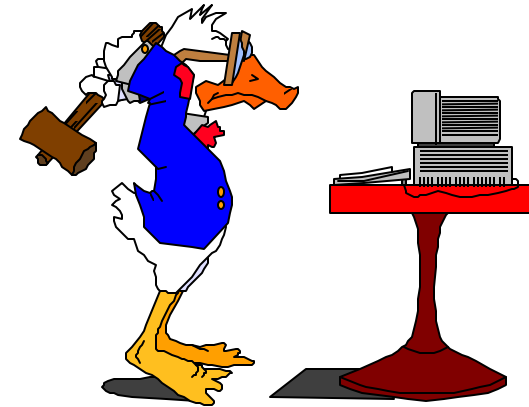
- accountability,
- availability,
- confidentiality,
- access control,
- integrity, and
- non-repudiation.



# Common Threats

---

- Hardware or software design flaws.
- Accidental component failures.
- Damage to components.
- Hardware failures.
- Unauthorized substitution of components.
- Introduction of environmental hazards or negligent neutralization of mechanisms intended to protect against environmental hazards.
- Misuse of systems or components.



# Common Threats - continued

---

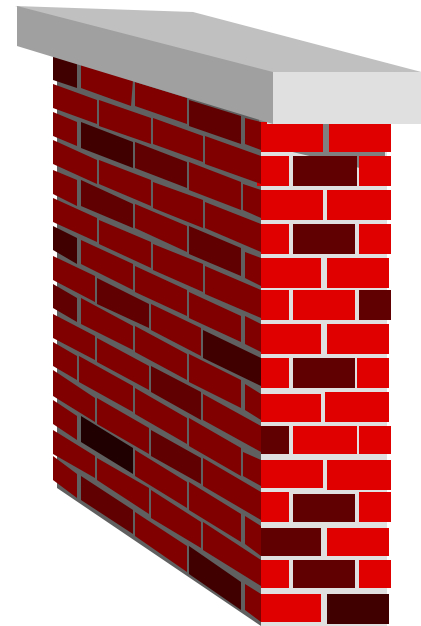
---

- Penetration of systems components, to which the perpetrator is not authorized access.
- Initiation of connections to system components, to which the perpetrator is not authorized access.
- Malicious or negligent tampering with components, to which an embedded application or an individual is not authorized access.
- Probing or performing technical surveillance of classified components.

# DATA Attacks

---

- Examples of data attacks are:
  - data destruction,
  - data modification,
  - data fabrication,
  - interruption or interception of data.
- An attack can result in:
  - disclosure of information,
  - violation of object confidentiality,
  - modification of objects,
  - violation of object integrity.



# The Results of Successful Attacks

---

- There are four fundamental categories of results or conditions that can arise from accidental threats or attacks:
  - **Information Loss or Leakage:** occurs when information is disclosed to an unauthorized person or entity.
  - **Integrity Violation:** occurs when data integrity is compromised due to unauthorized destruction, alteration, or creation of data.
  - **Denial of Service:** occurs when access to information or system resources by legitimate users is deliberately obstructed or impeded.
  - **Illegitimate Use:** occurs when a system resource is used by other than legitimate users in an unauthorized way.

# Real Time Security

---

- System Integrity requires memory protection.
- Subject-object access control mechanism, (non-intrusive).
  - Non-intrusive access control mechanism means that the enforcement of access control does not intrude into the critical time of a Real-time system. An example of such a mechanism is the use of off-line built access control table.

# Real Time Security continued

---

- Data labeling mechanism.
- File System and Network Security  
Guidelines have been established for full function, non-real-time OSs such as UNIX and Windows NT Kernels. However, requirements for Kernels implemented on Real-time OSs (such as LynxOS, VxWorks) are still to be established

# Conclusions

---

Even though the specific subject of this guidance is software security, there are some aspects of the RT operating environment for which the software developer, PM, security officer, and other key project personnel must be aware. RT operating systems, by themselves, frequently cannot contain all the necessary security functionality to adequately protect them. Software security solutions often must work in conjunction with other security safeguards (e.g., physical security) to achieve an acceptable level of risk. Software security cannot be considered in a total vacuum. The developer, and the project administration and security staff, must be aware of these issues in order to ensure that the other critical components to achieving a viable security architecture are not neglected. Bottom line there are no specific RT security standards.