Web-based Modules for Cyberphysical Systems Security

Janusz Zalewski, Florida Gulf Coast University
Nary Subramanian, University of Texas at Tyler
Andew Kornecki, Embry-Riddle Aeronautical University
Bogdan Czejdo, Fayetteville State University
Fernando Gonzalez, Florida Gulf Coast University
Dawid Trawczynski, Advanced Micro Devices

STC 2014 - 26th IEEE Annual Software Technology Conference Long Beach, Calif., 29 March - 3 April 2014

Talk Outline

- Introduction
- Security Curriculum Development
- Security Modules Development
- Cybersecurity Concentration Program
- Conclusion and Future Work
- Acknowledgments

Introduction

Project Objective:

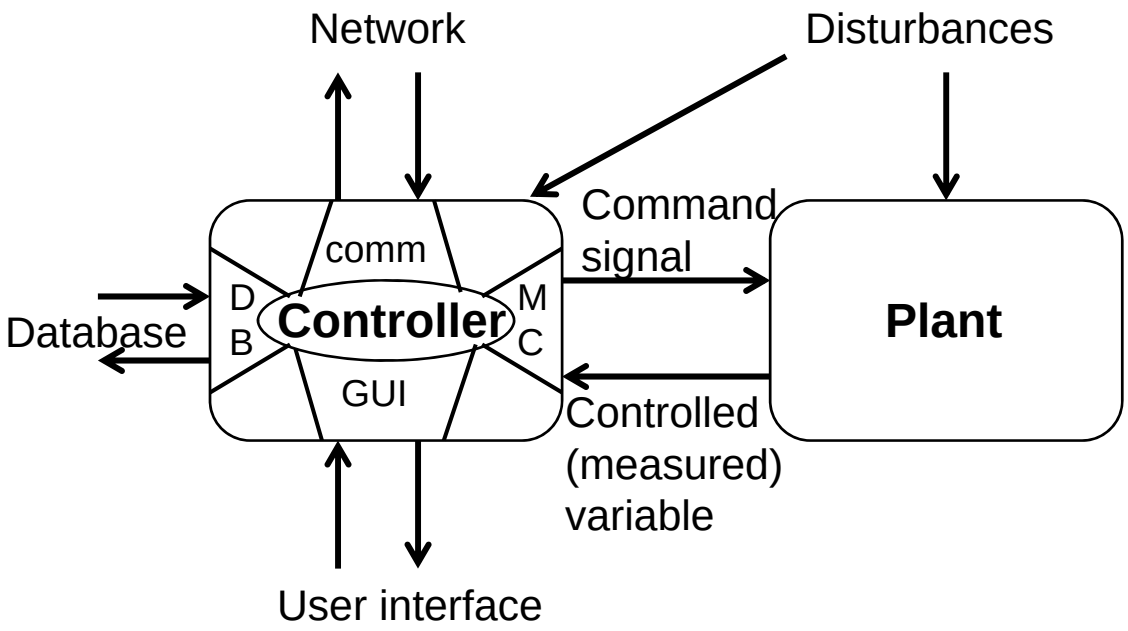
Develop a systematic approach to cyberphysical systems security curriculum.

Systematic approach is based on:

- global view of security as a system property
- strict definitions of security terms
- distinction between theory, experiments and simulations.

Introduction

A *cyberphysical system* is an embedded computer system with Internet connectivity.



Introduction

A *cyberphysical system* is an embedded computer system with Internet connectivity.

Security violations can be viewed as disturbances to the operation and functioning of its interfaces.

Its security surface has four major interfaces:

- Process Interface
- User Interface
- Database Interface
- Network Interface.

Security Curriculum Development

- T. Stapko, Practical Embedded Security, 2008
  - Computer Security: Inroduction and Review
  - Network Comm. Protocols and Built-in Security
  - Security Protocols and Algorithms
  - Data Protection Protocols for Embedded Systems
  - Embedded Security and Wireless
  - Application Layer and Client/Server Protocols
  - Crypto. Algorithms for resource-Constrained Systems
  - Hardware-based Security
  - Misc. Security Issues and Future of Emb. Syst. Security
  - Case Studies (PIC and Rabbot)

Security Curriculum Development

- C.H. Gebotys, Security in Embed. Syst., 2010
  - Where Security Began
  - Intro to Secure Embedded Systems
  - The Key and Using Keys
  - Elliptic Curve Protocols
  - Symmertic Key Protocols Including Cyphers
  - Data Integrity and Message Authentication
  - Side Channel Attacks on Embedded Systems
  - Countermeasures
  - Reliable Testable Secre Systems
  - Summary, Standards, and Ongoing Efforts.

Security Curriculum Development

- D. & M. Kleidermacher

  Embedded Systems Security, 2012
  - Intro to Embedded Systems Security
  - Systems Software Considerations
  - Secure Embedded Software Development
  - Data Protection Protocols for Embedded Systems
  - Emerging Applications

Security Curriculum Development

- The approach is based on the following criteria:
  - Systematic view of security
  - Contents of professional books available
  - Practical timeframe limitations
- The following topic groups have been selected:
  - General education modules:

    Intro to Computer Security; *Elements of Cryptography*
  - Security of specific technologies:

    FPGA Security; *RFID Security*; *SCADA Security*
  - Software aspects of security:

    Java Security; *Threat Modeling*.

Security Modules Development

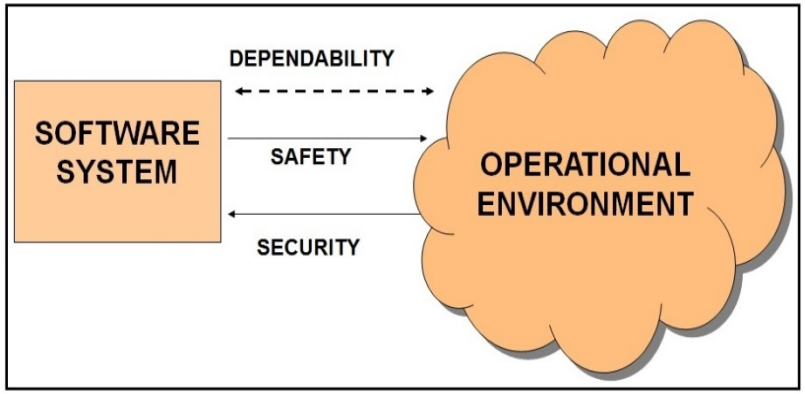
- Pedagogy Consistent with ABET Requiements:
  - Learning Outcomes
  - Learning Objectives
  - Learning Activities
  - Assessment of Progress
- Each Module is structured as follows:
  - Module Objectives
  - Module Introduction
  - Student Activities:

    Suggested Readings & Hands-on Exercise
  - Assessment

Security Modules

- Module #1 General Introduction to Computer Security
  - Definition of security as a system property

security. In computing, the degree to which information is protected from unauthorized access, given that authorized access is not denied.



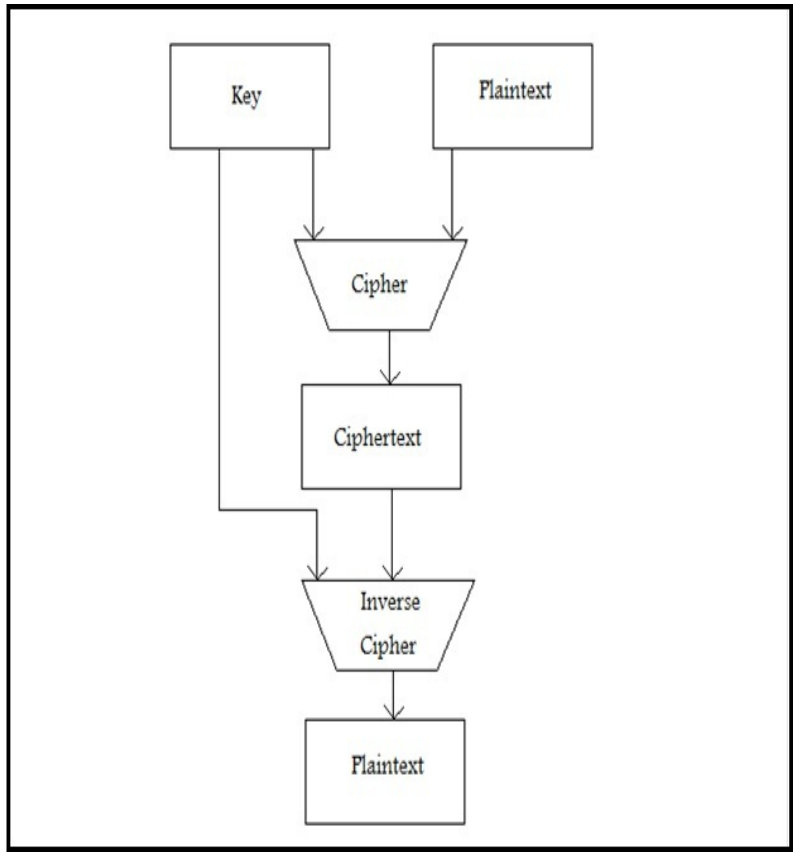
  - Relationship between security, safety, reliability, dependability.
  - Major question

What are the vulnerabilities of a computer (including computer network) and how to prevent the attackers from exploiting them?

Security Modules

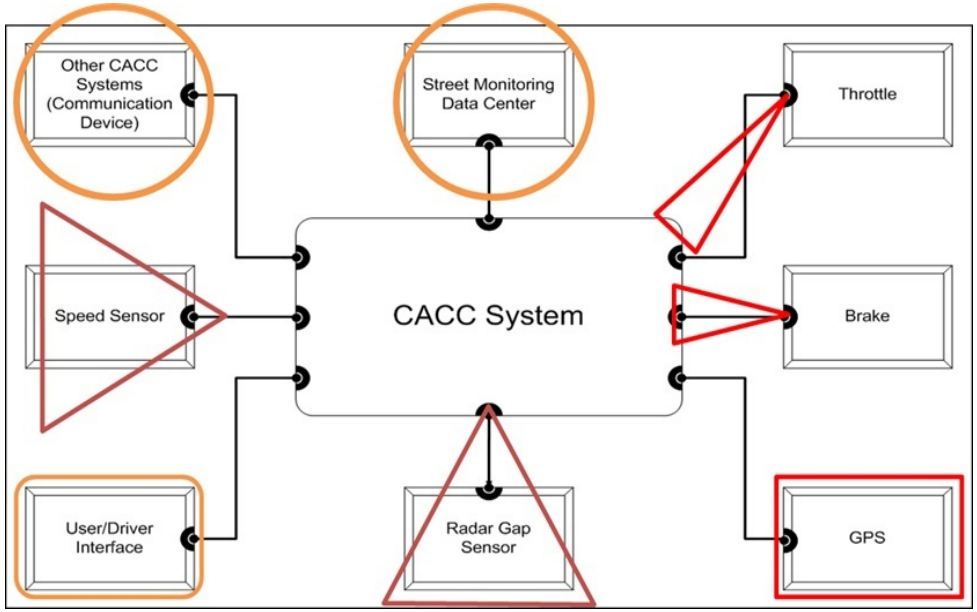
- Module #2 Introduction to Cryptography
  - Major question

    What are the principles of encrypting information, so only designated parties could read it?
  - Principles and major algorithms of encryption: AES, RSA, and others



Security Modules

- Module #3 Embedded Systems Security
  - Major question: What is specific about embedded systems that makes them different regarding security?
  - Specific aspects:
    - Confidentiality of a User Interface
    - Integrity of sensors and actuators
    - Availability of the database interface
    - All 3 for networks

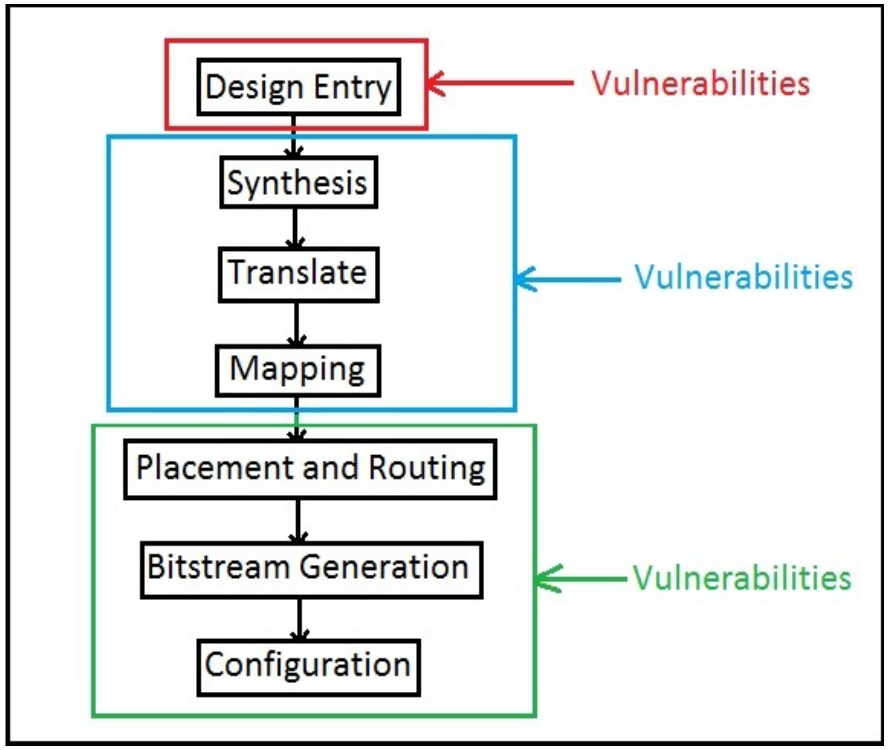


Security Modules

- Module #4 FPGA Security
  - Major question: What are the typical vulnerabilities of FPGA circuits?
  - Specific aspects:

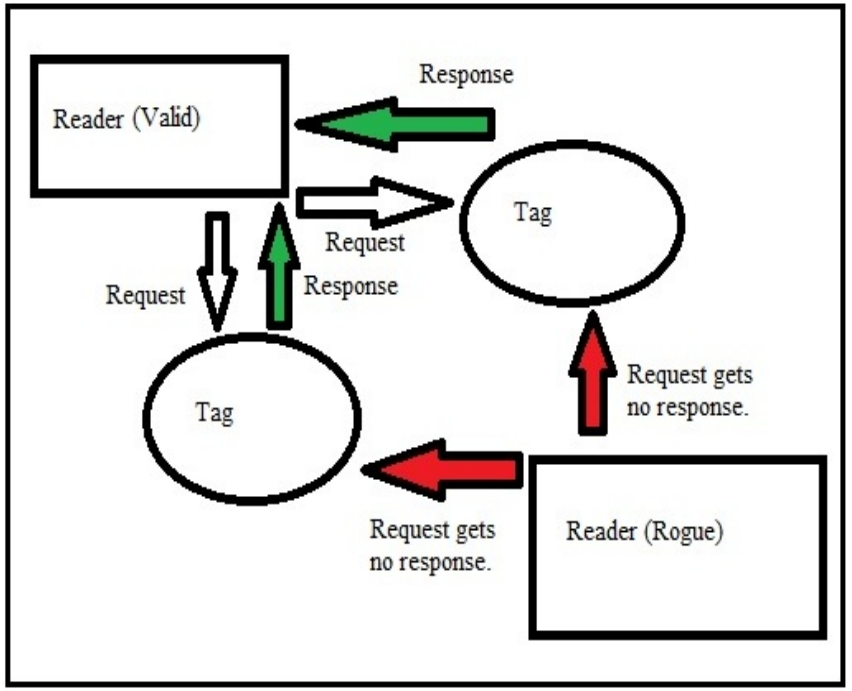
(chances that circuit can be compromised)

- Design
- Manufacturing
- Assembly
- Distribution



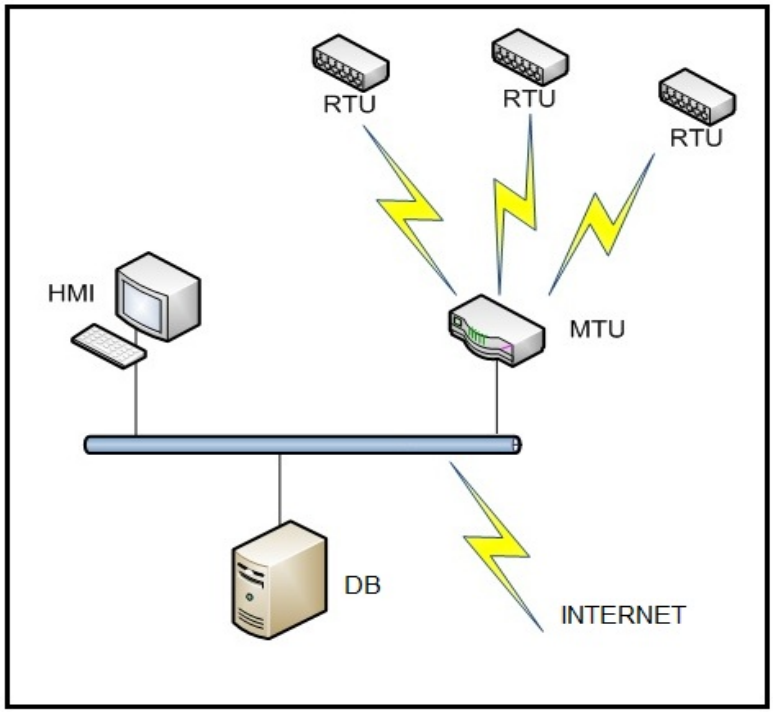
Security Modules

- Module #5 RFID Security
  - Major question: What are the typical vulnerabilities of RFID systems?
  - Specific aspects:
  - Spoofing Identity
  - Data Tempering
  - Repudiation
  - Info Disclosure
  - Denial of Service
  - Elevation of Privilege



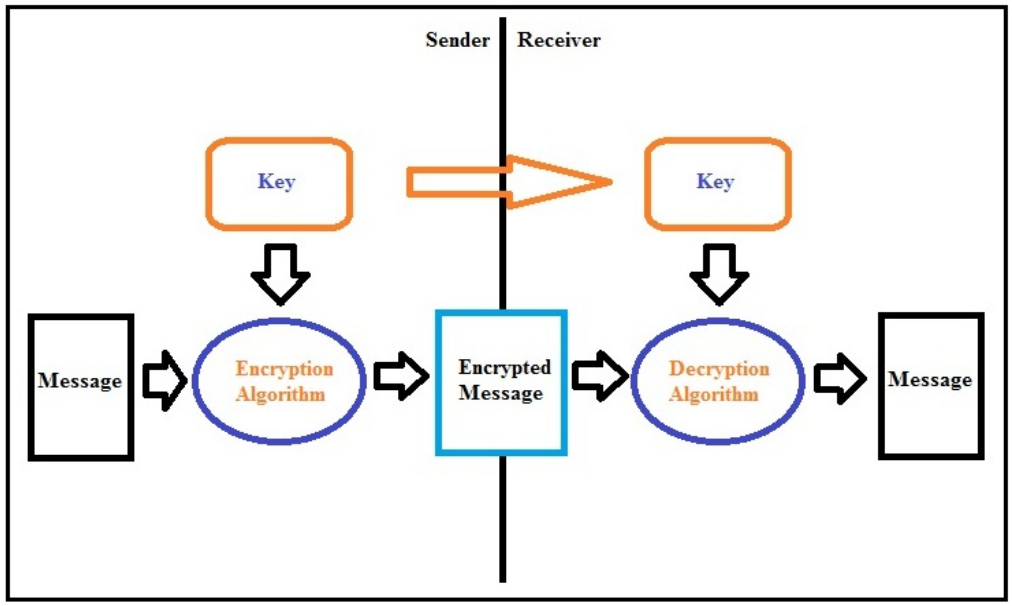
Security Modules

- Module #6 SCADA Security
  - Major aspect: Typical Vulnerabilities.
  - Specific aspects:
  - Spoofing
  - Encryption attacks
  - Signature attacks
  - Protocol attacks
  - Replay of messages
  - Data tempering
  - Eavesdropping.



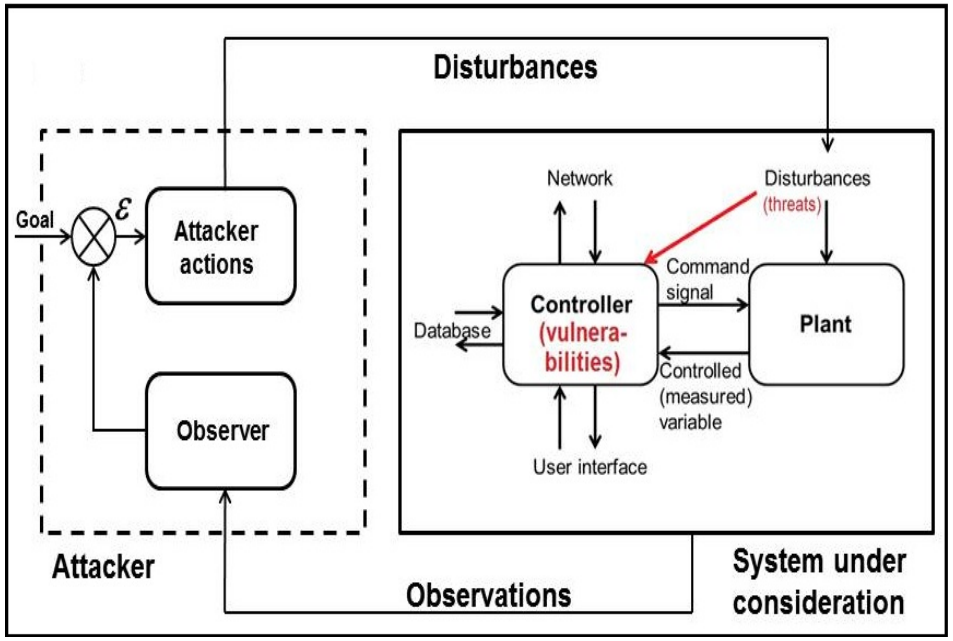
Security Modules

- Module #7Java Security
  - Major question: How to secure Java applications so that messages sent between Java programs cannot be compromised?
  - Some solutions:
  - Use SSL
  - Data Encryption
  - Authentication
  - Authorization.



Security Modules

- Module #8 Threat Modeling
  - Major question: How to capture vulnerabilities for embedded system security analysis using modeling?
  - Typical approach:
    - Understand the Adversary's View
    - Create a Model
    - Determine and Investigate Threats
    - Mitigate Threats
    - Validate Mitigations



Cybersecurity Concentration

- State of Florida is eager to become the Cyber State: http://www.usf.edu/pdfs/final-cybersecurity-report.pdf
- FGCU has submitted a grant proposal to the State to establish a Cybersecurity Concentration:
  - Students may complete the first 2 years at the State College and the next 2 years at FGCU
  - Two concentration paths can be pursued at FGCU:
    - Software Engineering, or
    - Computer Information Systems

Courtesy Dr. Dahai Guo, FGCU

Cybersecurity Concentration

- Concentration in Cybersecurity includes:
  - Cyber Security I and II
  - Secure Software Development
  - Information Assurance
  - Cryptography and Data Security
  - Senior Design in Software Security
  - All in the context of the Software Engineering program.

Courtesy Dr. Dahai Guo, FGCU

Cybersecurity Concentration

- Other highlights:
  - The curriculum includes certifications
  - Resources for students to pursue certifications
  - Support for faculty to pursue certifications
  - The concentration can prepare students for entering graduate schools.

Courtesy Dr. Dahai Guo, FGCU

Conclusion and Future Work

- Eight modules developed
- Availability via the web: http://satnet.fgcu.edu/CEN3213/
- Offered in two courses:
  - CEN 3213 Embedded Systems Programming
  - CNT 4104 Senior Project in Computer Networks
- Considered for adoption at other universities

Conclusion and Future Work

New Modules under Development

- Operating System Security
- Security Protocols for Cyberphysical Systems
- Tools for Security Analysis
- Security Measurement
- others under consideration

Acknowledgments

- Major funding was provided by the National Science Foundation Award No. 1129437
- Supplemental activities:
  - U.S. Air Force Summer Fellowship Program (Subramanian and Zalewski)
  - Software Engineering Institute/Carnegie Mellon (Kornecki)
  - Oak Ridge National Lab (Czejdo).