CSEC
CYBER SECURITY EDUCATION CONSORTIUM

Cyber Security and Critical Infrastructure Protection

Sujeet Shenoi
Tandy School of Computer Science
University of Tulsa, Tulsa, OK 74104
sujeet@utulsa.edu

NSF

ADVANCED TECHNOLOGICAL EDUCATION

Electronic Assets (Targets)

Principle of Easiest Penetration

"An intruder must be expected to use any available means of penetration, not necessarily the most obvious means, nor the one against which the most solid defense has been installed."

- Hardware
- Software
- Data
- People

Security Goals

Confidentiality

—Assets are KNOWN only to authorized parties

Integrity

—Assets can be modified only by authorized parties in authorized ways

Availability

—Assets are available to authorized parties on demand

CSEC
CYBER SECURITY EDUCATION CONSORTIUM

Major Threats

01001010100101010101010011001010101010000101010101010101010100010100100

Interruption

—Asset is lost, unavailable or unusable

Interception

—Asset is accessed in an unauthorized manner

Modification

—Asset is tampered with in an unauthorized manner

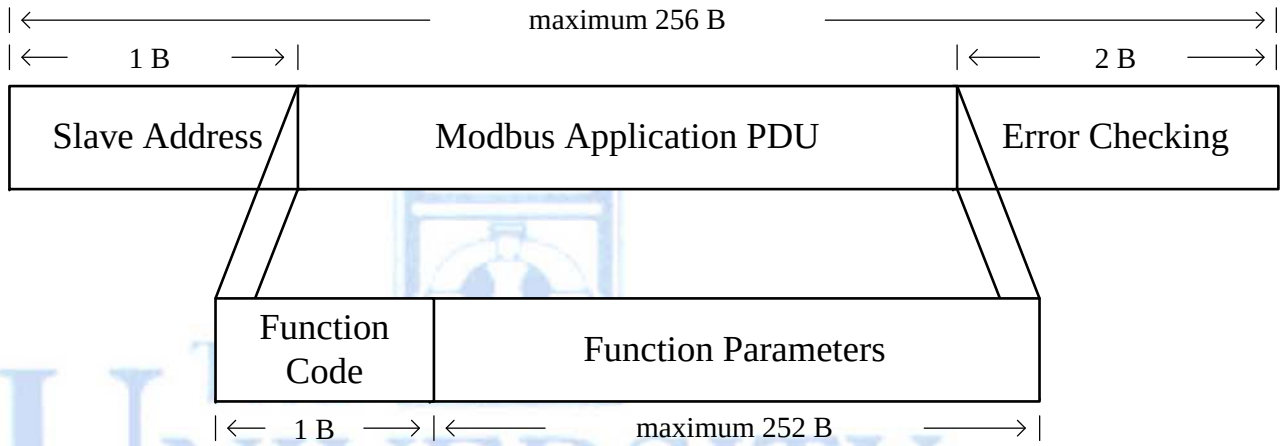
Fabrication

—Asset is counterfeited

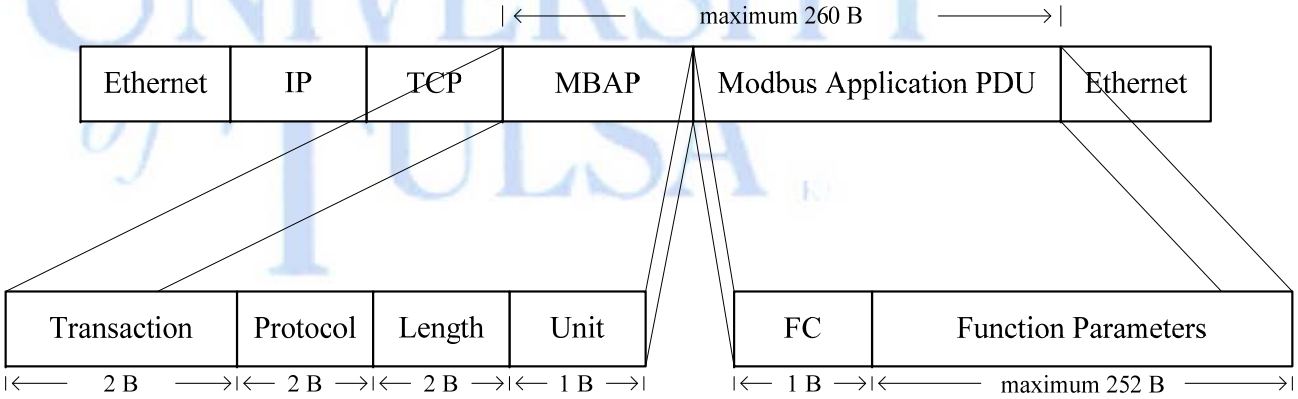
ADVANCED TECHNOLOGICAL EDUCATION

Modbus Messages

- Modbus Serial



- Modbus TCP

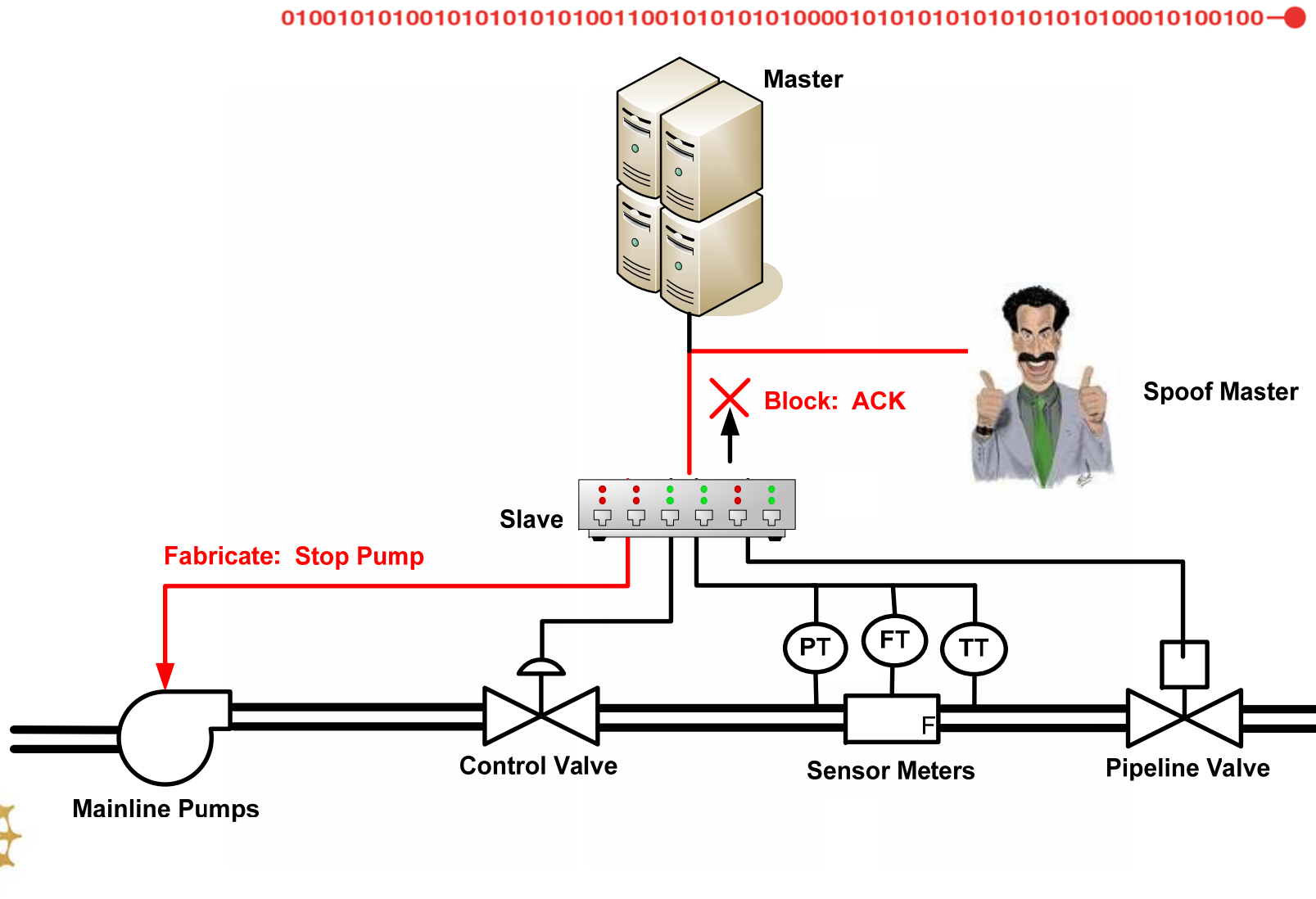


Types of Attacks

- Modbus Protocol Specific Attacks
- Modbus Vendor Implementation Attacks
- Modbus Support Infrastructure Attacks

CSEC
CYBER SECURITY EDUCATION CONSORTIUM

Example Attack



NSF

ADVANCED TECHNOLOGICAL EDUCATION

Attack Preconditions

- Modbus Serial (22 Attacks)
  - Availability of Modbus Sniffer, Packet Injector
  - Access to Control Center, Field Device
  - Access to Communications Link
- Modbus TCP (29 Attacks)
  - Availability of Modbus TCP Sniffer, Packet Injector
  - Access to Control Center, Field Device, Database, Historian
  - Access to Network Segment

CSEC
CYBER SECURITY EDUCATION CONSORTIUM

Modbus Serial Attack Taxonomy

0100101010010101010101001100101010101000010101010101010101000010100100

Low Guarded Elevated High Severe

22 DISTINCT ATTACKS (64 Instances)	Master	Field Device	Com Link	Message
Interception		4 Read Field Device Data	2 Read Com Link Traffic	4 Read Message Data
Interruption	4 DoS Master	11 DoS Field Device	1 DoS Com Link	
Modification	2 Bad Data in Master	8 Bad Data in Field Device 3 Bad Control	2 Bad Traffic	7 Bad Data in Message
Fabrication	1 Full Control			15 Bad Data in Message

ADVANCED TECHNOLOGICAL EDUCATION

CSEC
CYBER SECURITY EDUCATION CONSORTIUM

Modbus TCP Attack Taxonomy

01001010100101010101010011001010101010000101010101010101010100010100100

Low Guarded Elevated High Severe

29 DISTINCT ATTACKS	Master/DB/ Historian	Field Device	Network Segment	Message
Interception		3 Read Field Device Data	3 Read Traffic	3 Read Message Data
Interruption	14 DoS Master	19 DoS Field Device	6 DoS Network Segment	
Modification	3 Bad Data in Master	6 Bad Data in Field Device 4 Bad Control	3 Bad Traffic	14 Bad Data in Message
Fabrication	2 Full Control	1 Fabricated Field Device		18 Bad Data in Message

NSF

ADVANCED TECHNOLOGICAL EDUCATION

Methods of Defense

Principle of Adequate Protection

"Computer items must be protected only until they lose their value. They must be protected to a degree consistent with their value."

Principle of Effectiveness

"Controls must be used -- and used properly -- to be effective. They must be efficient, easy to use and appropriate."

Principle of Weakest Link

"Security can be no stronger than its weakest link."

CSEC
CYBER SECURITY EDUCATION CONSORTIUM

Controls

- Encryption
- Software Controls
- Hardware Controls
- Physical Controls
- Policies and Procedures

NSF

ADVANCED TECHNOLOGICAL EDUCATION

Effectiveness of Controls

- Awareness of Problem
- Likelihood of Use
- Overlapping Controls
- Periodic Review

CSEC
CYBER SECURITY EDUCATION CONSORTIUM

Reactive Security Strategies

- Assurance
- Isolation
- Encryption
- Authorization
- Security Services

NSF

ADVANCED TECHNOLOGICAL EDUCATION

CSEC
CYBER SECURITY EDUCATION CONSORTIUM

Reactive/Proactive Security Strategies

- Threat Awareness
- Situational Awareness
- Anomaly Detection/Prevention
- Intrusion Detection/Prevention
- Incident Response
- Risk Management

NSF

ADVANCED TECHNOLOGICAL EDUCATION

CSEC
CYBER SECURITY EDUCATION CONSORTIUM

Proactive Security Strategies

- Multilayer Protocol Design
- Standards-Driven Design
- Risk-Based Design
- Embedded Security Services
- Defense-in-Depth
- Assurance

NSF

ADVANCED TECHNOLOGICAL EDUCATION

CSEC
CYBER SECURITY EDUCATION CONSORTIUM

Technical Challenges

- Complex, evolving systems
- Theoretical limitations (Halting Problem)
- Complete security is a "Holy Grail"

NSF

ADVANCED TECHNOLOGICAL EDUCATION

CSEC
CYBER SECURITY EDUCATION CONSORTIUM

Law & Policy Challenges

- Laws and public policy cannot keep pace
- Laws and their interpretations differ widely
- Investigation and enforcement are difficult
- Deregulation issues (e.g., telecom industry)
- Shrink-wrapped vs. open source software
- Domestic economic policy

NSF

ADVANCED TECHNOLOGICAL EDUCATION

CSEC
CYBER SECURITY EDUCATION CONSORTIUM

Defense in Depth

01001010100101010101010011001010101010000101010101010101010100010100100

Managing Risk

- Technology
- Law and Policy
- Human Capital

NSF

ADVANCED TECHNOLOGICAL EDUCATION