Information Assurance Laboratory

Dr. Perry Alexander
Interim Director
Information and Telecommunication Technology Center
alex@ittc.ku.edu
Assuring Information Properties

Confidentiality
- Protection against unauthorized disclosure

Integrity
- Protection against unauthorized modification

Availability
- Protection against unauthorized disruption

Accountability
- Enforcement of bindings between agents and actions
Example: SDR Architecture

TX
- Compression
- Encryption
- Error Cntl
- Spreading
- Modulation
- Transmit

Receive Data
- RX
- Decompress
- Decryption
- Error Cntl
- De-Spread
- De-Mod
- Receive

Channel
Example: SDR Architecture

TX
- Compression
- Encryption
- Error Cntl
- Spreading
- Modulation
- Transmit

RX
- Decompress
- Decryption
- Error Cntl
- De-Spread
- De-Mod
- Receive

Channel

confidentiality
integrity
availability
Example: SDR Architecture

TX
- Compression
- Encryption
- Error Cntl
- Spreading
- Modulation
- Transmit

Send Data

confidentiality

integrity

encryption key

availability

RX
- Decompress
- Decryption
- Error Cntl
- De-Spread
- De-Mod
- Receive

Receive Data

authentication

Channel
Example: SDR Architecture

TX
- Compression
- Encryption
- Error Cntl
- Spreading
- Modulation
- Transmit

RX
- Decompress
- Decryption
- Error Cntl
- De-Spread
- De-Mod
- Receive

Channel

confidentiality
integrity
availability

coding scheme
Example: SDR Architecture

TX
- Compression
- Encryption
- Error Cntl
- Spreading
- Modulation
- Transmit

Send Data

confidentiality

integrity

availability

Channel

RX
- Decompress
- Decryption
- Error Cntl
- De-Spread
- De-Mod
- Receive

Receive Data

frequency, hop rate, hop set
Example: SDR Architecture

TX
- Compression
- Encryption
- Error Cntl
- Spreading
- Modulation
- Transmit

RX
- Decompress
- Decryption
- Error Cntl
- De-Spread
- De-Mod
- Receive

Send Data -> TX -> RX -> Receive Data

confidentiality
availability
integrity
authentication
coding scheme
encryption key
frequency, hop rate, hop set

set-up
Channel
tear-down

power
cost
form factor
evaluation and certification
evaluation and certification
confidentiality
integrity
availability
authentication
coding scheme
encryption key
frequency, hop rate, hop set

TX
- Compression
- Encryption
- Error Cntl
- Spreading
- Modulation
- Transmit

RX
- Decompress
- Decryption
- Error Cntl
- De-Spread
- De-Mod
- Receive
Information Assurance Lab Activities

- **IA Research Programs**
  - Network stability, availability and security
  - Access control over information at rest and in transit
  - Security as a system-level property
  - Trust modeling and assurance

- **IA Educational Programs**
  - MSIT in Information Assurance
  - MS and PhD Focus Area in Information Assurance (pending)
  - Information Assurance Education Brownbag

- **IA Implementation**
  - ITTC and EECS information security policies
  - KU information security policies

Application pending for NSA/DHS Center of Excellence Designation
Information Assurance Lab Technologies

- Formal specification and verification
  - Rosetta and Raskell
  - PVS, Isabelle, SAL verification
  - Graph theoretic modeling
- Synthesis and principled development
  - Worker/Wrapper
  - InterpreterLib and ASG
  - Static analysis and compilation techniques
- Implementation tools
  - Access control
  - Virtualization and virtual machines
  - TPM/vTPM based protection schemes

A highly interdisciplinary approach to assurance