Secure Remote Control of Field-Programmable Network Devices

Haoyu Song, Jing Lu, John W. Lockwood, James Moscola website: http://www.arl.wustl.edu/arl/projects/fpx/reconfig.htm

Motivation

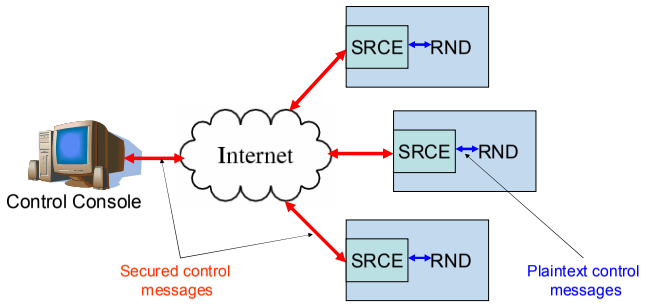
- Distributed, high bandwidth network devices need secure mechanism for remote control and configuration
  - Distributed firewalls
  - Extensible network routers
  - Distributed network intrusion detection and prevention systems
  - Internet-enabled sensors
- Existing software-based security frameworks require a large computational effort to secure the control messages
- Reconfigurable hardware offers high performance and flexibility

Challenges

- Different types of attacks threatening the control channel
  - Eavesdropping
  - Faking control messages
  - Replay attack
  - DoS attack
- Control and configuration must be secure and reliable
- Tradeoff between resource consumption and performance

Our Solution

- A central console controls multiple distributed network devices
- An encryption/authentication circuit secures control messages
- A light-weight protocol provides reliability and enhances security

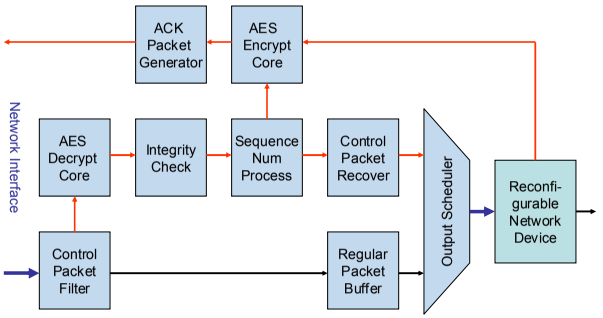


SRCE: Secure Remote Control Engine

RND: Reconfigurable Network Device

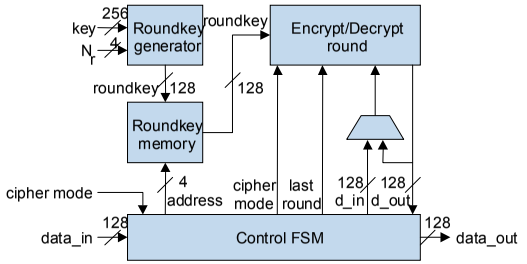
Architecture and Protocol

- AES-encrypted control messages for data confidentiality
- Encrypted digest or checksum for data integrity
- Sequence number against replay attacks
- Go-back-N ARQ protocol for reliable communication
- Transparent to application and modularized for easy integration



Key Components - AES

- Implementation of an AES hardware core
- Supported key size: 128, 192 and 256 bits
- Loop iteration architecture to save hardware resource

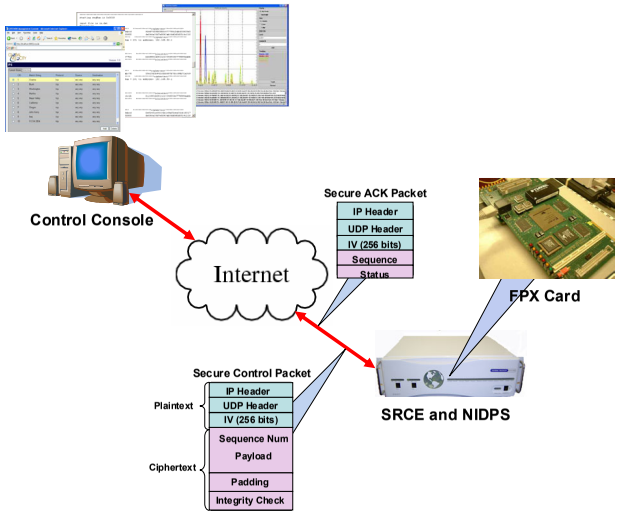


	LUTs		Block RAM		Timing	Throughput
	#	%	#	%	MHz	Mbps
AES-128	2503	5.8%	44	27%	85.6	547.8
AES-192	2610	6.0%	44	27%	86.7	462.4
AES-256	2677	6.2%	44	27%	92	420.6

AES Implementation in Xilinx Virtex XCV2000E-6 FPGA

Application

- A Secure Remote Control Engine (SRCE) in a Distributed Network Intrusion Detection and Prevention System (NIDPS) using Bloom filters for string matching
  - Two stacked FPX cards: one for SRCE, the other for NIDPS
  - SRCE provides NIDPS with a secure and reliable control channel



How SRCE works with NIDPS

- Control messages formatted and encrypted
- Secure control messages converted to UDP packets
- Secure Control packets sent to the system
- Control packets decrypted in SRCE and forwarded to NIDS application
- Encrypted Acknowledgement sent back from SRCE
- NIDPS configuration updated
- Scanning with new configuration begins immediately
- String matches generate alert messages
- Software controller processes alerts and plots statistics

Acknowledgement

This work was supported by a grant from Global Velocity. The authors of this paper have received equity from the license of technology to that company. John Lockwood has served as a consultant and co-founder to Global Velocity.

http://www.globalvelocity.info/