Secure Remote Control of Field-Programmable Network Devices

Application 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

Our Solution

Challenges

- Different types of attacks threatening the control channel
  - Eavesdropping
  - Faking control messages
  - Replay attack
  - Denial of Service attacks

Control and configuration must be secure and reliable

Tradeoff between resource consumption and performance

Our Solution

AES Implementation in Xilinx Virtex XCV2000E-6 FPGA

- AES-256
- AES-192
- AES-128

Throughput

- Throughput: 420.6 Mbps
- Timing: 0.92 µs
- Block RAM: 27%
- LUTs: 44
- # Port: 6.2%
- # Port: 2677

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