CubeSec and GndSec: a lightweight security solution for CubeSat communications

Small Satellite Conference
SSC12-III-4

August 14th, 2012

Authors: Obulpathi Challa, Gokul Bhat, Janise McNair

Wireless and Mobile Systems (WAMS) Lab
Advisor: Dr. Janise McNair
Electrical & Computer Engineering

Presenter: Dante Buckley
Space Systems Group
Department of Mechanical & Aerospace Engineering

WAM

UF UNIVERSITY of FLORIDA
The Foundation for The Gator Nation

CubeSats are going global

1. MoreDB – telemetry decoding software client
2. GENSO – Global Educational Network for Satellite Operators

In our future, we envision a large number of CubeSats and ground stations networked together to perform computational and communication intensive missions like remote sensing, tracking, imaging, image processing etc.,

Current security mechanisms for CubeSat communications

1. CubeSat communication protocols have almost no security features, other than CRC (Cyclic Redundancy Checks)
2. CubeSats use wireless broadcast media which means they are susceptible to eavesdropping.
3. Unauthorized users can intercept and monitor the sequence of commands sent to and received from the spacecraft.
4. After gathering sufficient amount of data and analyzing it, the adversary can perform replay attacks, send spurious commands causing resource consumption, data loss or corrupt satellite function and eventually mission failure.

Components of Data Security

1. Confidentiality: Refers to the property that data can only be read by the authorized parties.
2. Integrity: Ensures data is valid and has not been tampered with.
3. Availability: Refers to the property that data is available when requested.

Our Objective

We want to provide confidentiality, integrity and availability of CubeSat resources and communications data.

Challenges for CubeSat security subsystem

1. Power constraints: CubeSat has limited power generation capability of about 2W.
2. Space constraints: CubeSat volume is limited to 10 x 10 x 10 cm^3.
3. Mass constraints: CubeSat mass is constrained to the CubeSat specifications
4. Time constraints: CubeSat has a constrained 8 minutes window time per pass with an average exposure time of about 25 minutes per day over a singular location.

Block ciphers

1. Block ciphers are fundamental building components in the design of cryptographic protocols.
2. Block ciphers can be treated as a deterministic function that transforms a block of bits into its corresponding ciphertext.
3. This mapping is determined by the symmetric key.
4. Advanced Encryption Standard (AES) and Data Encryption Standard (DES) are are the most prominent block ciphers.

Block ciphers: AES

1. Advanced Encryption Standard (AES) is the de-facto industry standard for symmetric block cipher and is widely deployed.
2. AES has a fixed block size of 128 bits and variable key size of 128, 192, or 256 bits.
3. The AES uses multiple rounds of transformation, to convert the input plaintext into the final output of ciphertext.
4. Each round consists of four steps, namely AddRoundKey, SubBytes, ShiftRows, and MixColumns.

Block ciphers: DES

1. Data Encryption Standard (DES) is another prominent industry standard for symmetric block cipher.
2. The block size in DES is 64 bits. The cipher key size is 56 bits.
3. Core of DES is the Feistel network containing 16 rounds with 8 substitution boxes along with initial and final permutations.
4. DES was proved to be insecure, however DES3 (DES applied three times) is still secure.

Modes of encryption

1. Electronic codebook (ECB)
2. Cipher-block chaining (CBC)
3. Propagating cipher-block chaining (PCBC)
4. Cipher feedback mode (CFB)
5. Output feedback mode (OFB)
6. Counter mode (CTR)
7. Galois/Counter Mode (GCM)
8. and several others ...

Modes Comparison: ECB, CBC, PCBC, CFB, OFB and GCM

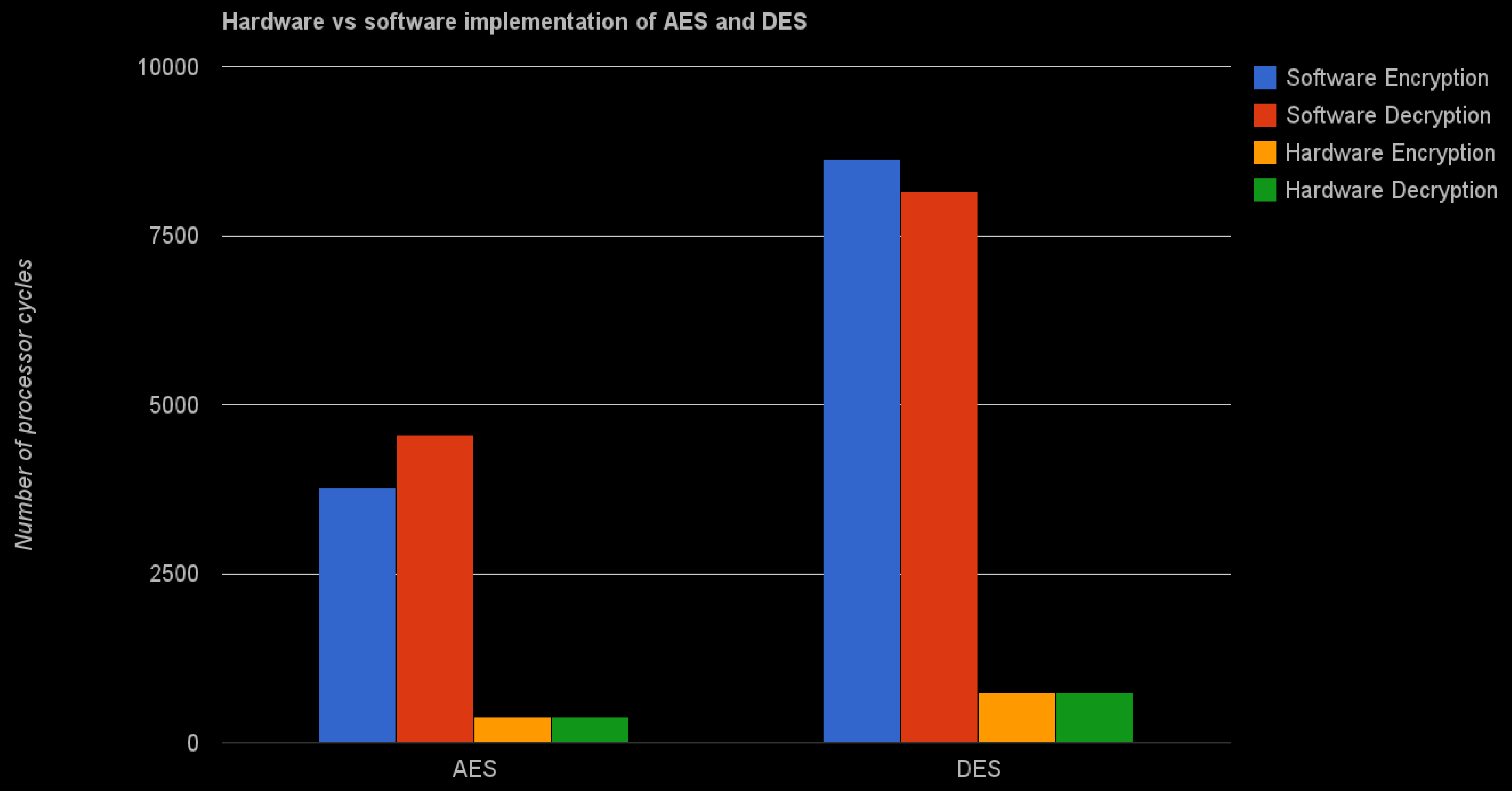
1. CBC, PCBC, CFB and OFB modes do not support parallelism.
2. Modes like ECB and CBC require padding of final block with zeroes to round it to the block size of 128 bits. 256 byte sized packets (AX.25 packet protocol commonly implemented on CubeSats) means an overhead of 3% is the best case scenario. With smaller sized packets, used for control information, this overhead can be as much as 25%.

Galois/Counter Mode (GCM)

1. GCM allows pipelined and parallelized implementations and have minimal computational latency to achieve high encryption speed.
2. Parallel processing enables use of additional microcontrollers, provided for hardware redundancy, for increasing encryption speed.
3. GCM is free from intellectual property rights.
4. GCM has other additional features like being capable of acting as a stand-alone MAC, authenticating messages when there is no data to encrypt, with no modifications. It can be used for incremental message authentication.
5. Due to its speed, ability to parallelize, cost of implementation and aforementioned advantages, we selected GCM mode for CubeSat security subsystem.

Software .vs. Hardware Implementation

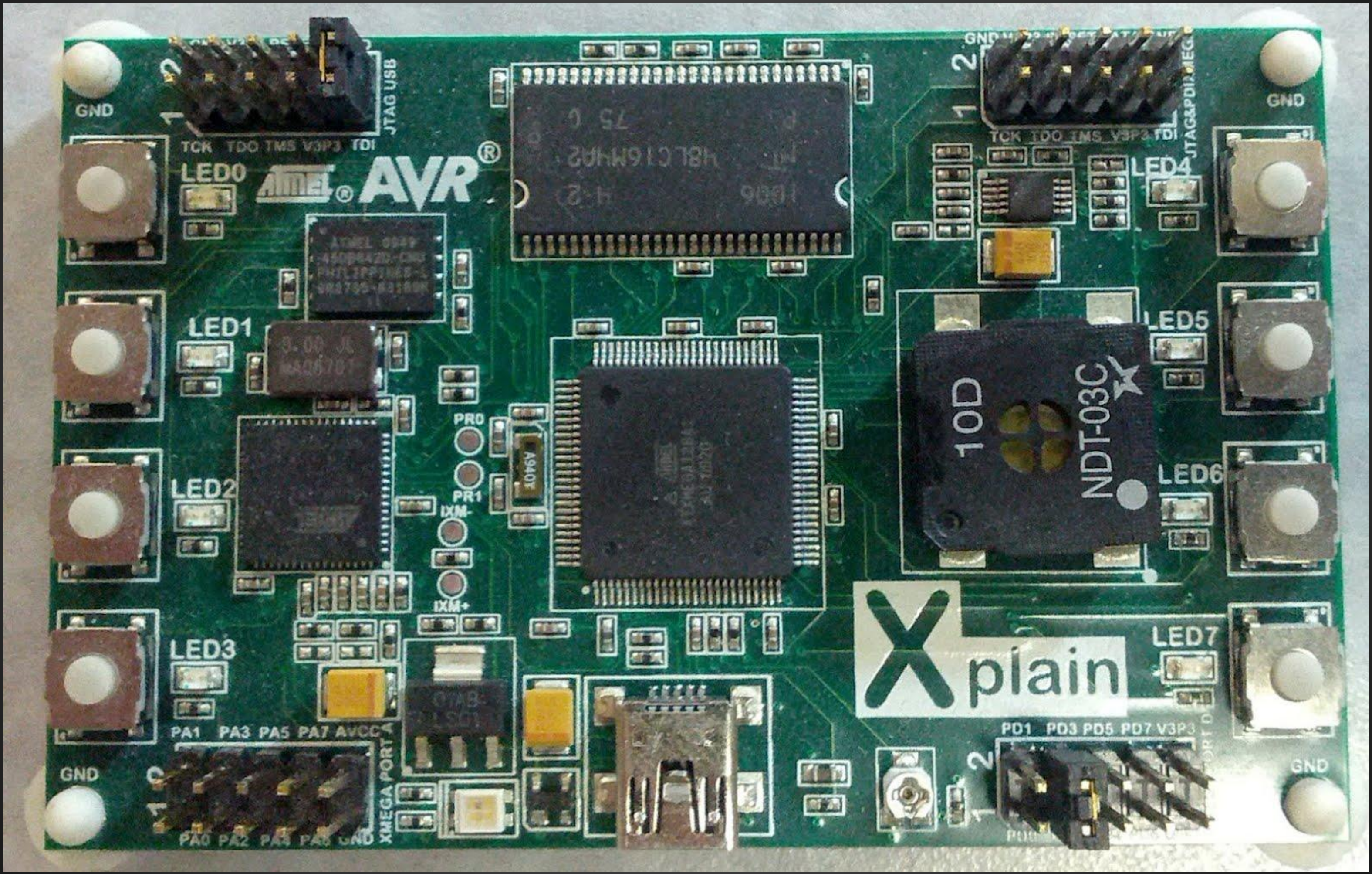
1. Software implementation of AES requires 3766 CPU cycles for encryption and 4558 CPU cycles for decryption per block.
2. Software implementation of DES requires 8633 CPU cycles for encryption and 8154 CPU cycles for decryption per block.
3. Whereas hardware implementation of AES and DES require about few 100’s of CPU cycles (~400) for encryption or decryption on a typical microcontroller.
4. This means hardware implementation of AES and DES is about 10 - 20 times efficient in terms of time and power compared to software implementation.


Hardware vs software implementation of AES and DES
10000
7500
5000
2500
0
Number of processor cycles
AES
DES
Software Encryption
Software Decryption
Hardware Encryption
Hardware Decryption

XMega family of microcontrollers

1. XMega devices are based on 8/16-bit AVR RISC core with 135 RISC instructions.
2. XMegas include features like AES and DES crypto engines, Direct Memory Access, and efficient power management.
3. The DMA controller contains an innovative event system to ensure predictable real time performance even during high loads.
4. AVR XMEGA series operates with just 1.6 Volts with up to 32 MIPS at 32 MHz.

Hardware platform: Xplain platform



Features of XPlain platform

1. ATXMega128: The core of the XPlain board is the ATXMega128 microcontroller.
2. XPlain also features AT90USB1287, as a communication bridge.
3. The kit is powered using USB cable.
4. ATXMega128 can be communicated using UART, USB, UART-to-USB or JTAG.
5. XPlain kit features 4 MB SDRAM, 8 MB serial Dataflash and internal 128 Kb flash of ATXMega128 microcontroller for storing encryption keys.

CubeSec: Proof of concept

1. As a proof of concept, symmetric key encryption using 128 bit AES and DES block ciphers in Galois/Counter Mode (GCM) of encryption has been implemented on XPlain platform hosting the ATXMega128 microcontroller
2. Summary of SWaP (Size, Weight, and Power) analysis
3. CubeSec software is available for download from GitHub (a social online project coding resource)

GndSec

1. GndSec is the terrestrial counterpart of CubeSec. We implemented required encryption software for GndSec in python software.
2. CubeSec and GndSec provide mutual authentication, confidentiality, data integrity between CubeSat and the desired ground station.

SWaP Analysis: Size

1. ATXMega128 microcontroller which forms the core of the application is 2 cm x 2 cm.
2. Other than power connections, it also requires a JTAG programmer for programming and debugging purposes.
3. Mini JTAG connector has size of 6 mm x 3 mm, total footprint is below 3 cm x 3 cm.
4. Size of CubeSec with two microcontrollers, to provide redundancy and increase speed of encryption size, is less than 5 cm x 5 cm.

SWaP Analysis: Weight and Power

1. Weight of PCB is about 0.2 g / cm 2. 5 cm x 5 cm PCB weighs about 5 g.
2. ATXMega128 microcontroller and power circuitry weighs about 2 g.
3. Mini JTAG connector weight about 1.5 g.
4. Miscellaneous components add up to about 1.5 g, leading to total weight of 9.6 g.
5. ATXMega128 in active mode operating at 3.0 V with external clock running at 1 MHz drains 800 µA. As a result, 2.4 mW of power consumed at 1 MHz Operation

Data rate

1. Encrypting a single 16 byte AES block of data requires 375 clock cycles.
2. At a clock rate of 1MHz, data stream can be encrypted at the rate of 43 KBps using AES.
3. In GCM mode of operation data stream can be encrypted at 5.4 KBps.
4. ATXMega128 can be clocked at 12 MHz to encrypt data at 64 KBps.
5. Using 100 mW of power and two microcontrollers, encryption speed can be increased to 256 Kbps.

Conclusion

1. CubeSec can be constructed with minimum requirements: size of 3 cm x 3 cm, weighing 10 grams and power requirement of 2.5 mW to encrypt data stream at a rate of 5.4 KBps.
2. Data encryption speed can be scaled up to 256 KBps by increasing the power consumption to 100 mW and using two microcontrollers.
3. CubeSec features two microcontrollers, to provide reliable operation even if one of the microcontroller fails.
4. Space, weight and power can be traded to get higher speed of encryption. A single microcontroller can be clocked at higher speeds using more power, without sacrificing space or weight, to get higher speed of encryption.

Thanks!

Thanks to Dante Buckley for presenting our work
in addition to all the support from
Professor Norman Fitz-Coy

WAM Lab Website: www.wam.ece.ufl.edu/

Authors Email: obulpathi@ufl.edu; gbhat@ufl.edu; mcnair@ece.ufl.edu

WAM

Wireless and Mobile
Systems (WAMS) Lab

UF | UNIVERSITY of FLORIDA
The Foundation for The Gator Nation