Exceptional service in the national interest

INFORMATION PROTECTION IN NUCLEAR SYSTEMS

Christopher C. Lamb
cclamb@sandia.gov

Daniel Sandoval
drsando@sandia.gov

International Conference on Computer Security in the Nuclear World

Vienna, Austria, 19-23 June 2023

Sandia National Laboratories is a multimission laboratory managed and operated by National Technology and Engineering Solutions of Sandia LLC, a wholly owned subsidiary of Honeywell International Inc. for the U.S. Department of Energy's National Nuclear Security Administration under contract DE-NA0003525.

SAND2023-07033C

HOW DOES THIS HELP NUCLEAR ENERGY?

Remove blocks to implementing encryption in nuclear control systems

Enable engineers to design systems with timings that can support encryption

Clarify real impacts of encryption over control system communications

METHODOLOGY

1. Define and address arguments against using encryption in nuclear control systems
2. Examine proposed encryption support for control systems
3. Analyze implications of encryption systems
4. Examine real implications of encryption over communications
5. Propose non-encryption solutions

WHY NOT ENCRYPTION?

Limited resources	Timing and Latency	Computational resources and memory
Certificate management	Complexity and easier attacks	PKI, other keying material
Opaque communications	Confidentiality side-effects	Encrypted communications can't be extracted from the wire well

STANDARD SUPPORTED CRYPTOSYSTEMS

Standard	Encryption	Identification	Key Exchange
IEC 60870 with security controls defined by IEC 62351	TLS v1.2 with potential fallback to v1.0 and v1.1	X.509v3	Diffie-Hellman with RC4 and regular/ephemeral exchange
	Note: This is defined by IEC 62351		
IEC 61850 with security controls defined by IEC 62351	TLS v1.2	X.509v3	Diffie-Hellman with RC4 and regular/ephemeral exchange
	Note: This is defined by IEC 62351		
Modbus/TCP	TLS v1.2	X.509v3	TLS with RSA or TLS with ECC
IEEE 1815-2012 with required compatibility with IEC 62351	TLS v1.2	X.509v3	RSA and Diffie-Hellman
	Note: This is compatible with IEC 62351		

TLS 1.2 TIMING ANALYSIS

CLIENT HELLO and SERVER HELLO

- *Three* round trips between server and client

CLIENT KEY EXCHANGE

- Round trip to CA (worst case)
- Verify digital signature
- Digitally sign messages
- Encipher 48-byte public key from the server

SERVER EXCHANGE CIPHER SPEC

- Two single byte encryption

PERFORMANCE EXPERIMENTATION

Three platforms

- INTEL X86 3.5 GHz 64 GB RAM
- ARM Cortex 53 1.4 GHz SoC 1 GB RAM
- ARM Cortex 72 1.5 GHz SoC 4 GB RAM

Three configurations

- HTTP POST requests
- No payload, 512 byte Payload, 1024 byte payload

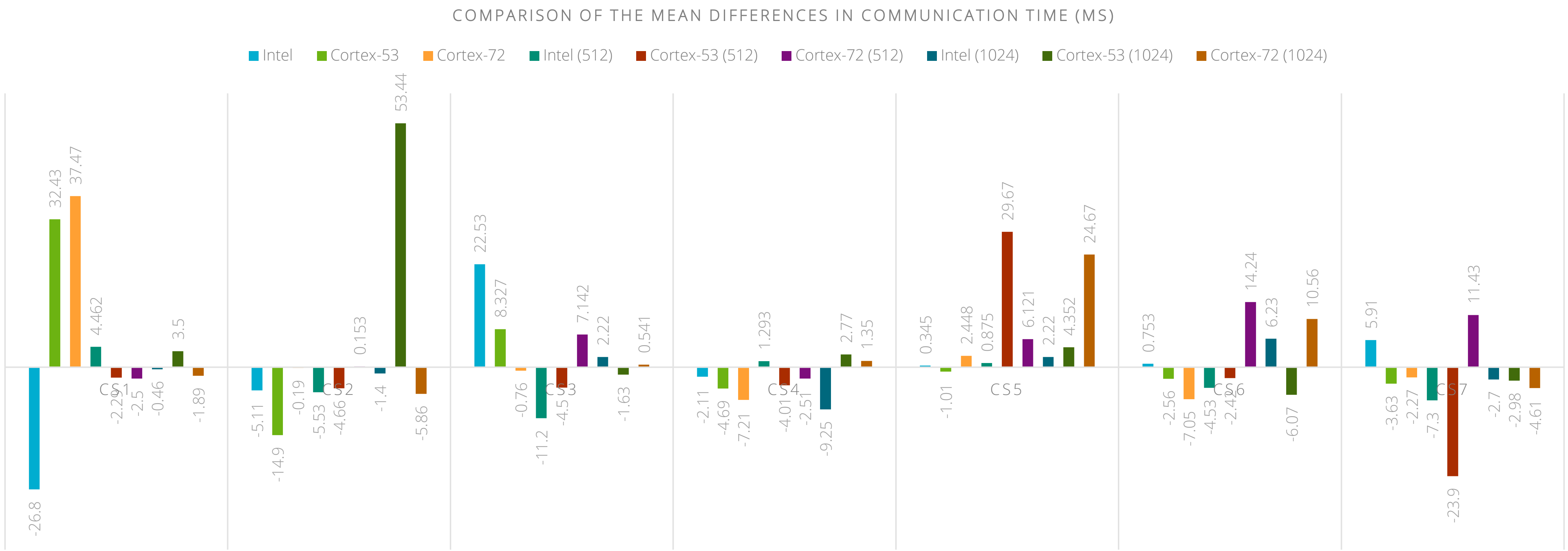
Seven cipher suites

- From simple (AES128-SHA) to complex (ECDHE-RSA-AES256-GCM-SHA384)

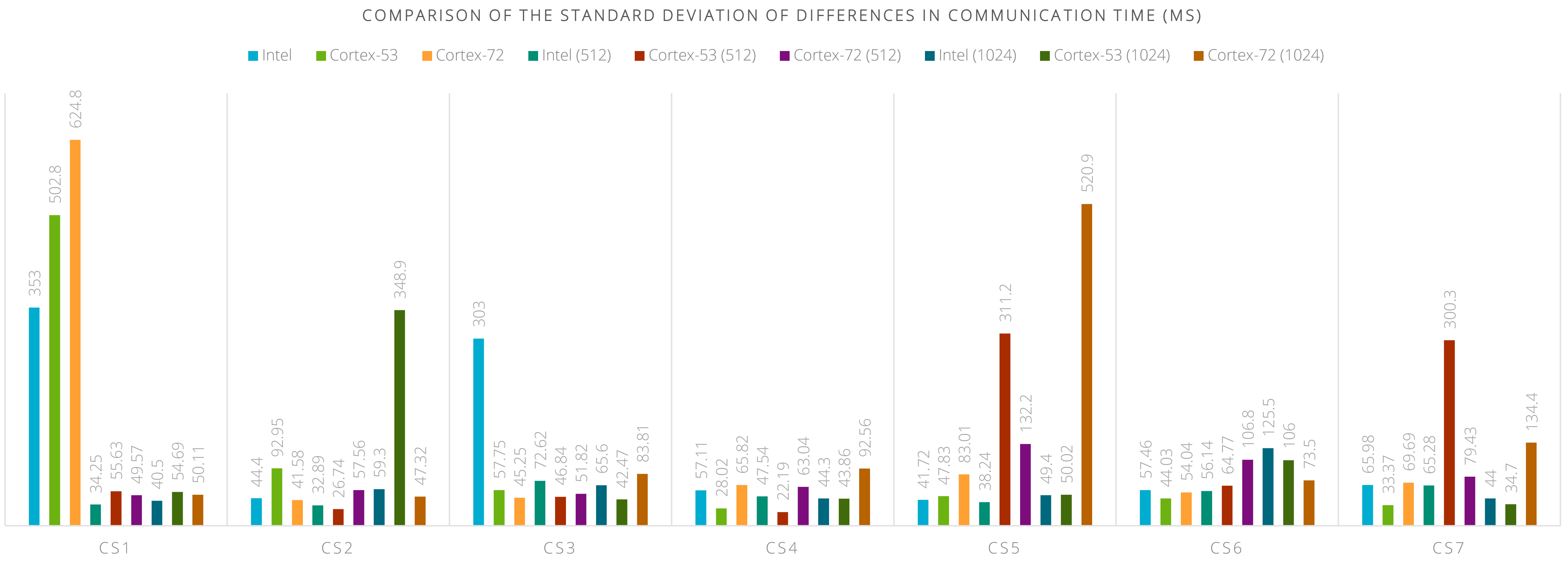
SSL v. cleartext

- Consecutive submissions to https://request.in
- 100 tests per configuration
- Optimization disabled (i.e., no session tickets or compression) to generate worst-case

TLS 1.2 PERFORMANCE ANALYSIS



TLS 1.2 PERFORMANCE ANALYSIS



ALTERNATIVES TO ENCRYPTION

Current Approaches

Network segmentation

- Violates defense-in-depth

Robust perimeter controls

- Violates defense-in-depth

Possible Approaches

Application-level signatures

Integrity-guaranteeing protocols

- Confidentiality and integrity protections are packaged into modern encryption
- Other approaches that only focus on integrity may be useful

THANK YOU!