Review of the Advanced Encryption Standard

Nicky Mouha

October 16, 2020

National Institute of Standards and Technology
U.S. Department of Commerce

NSUCRYPTO 2020

About Me

- Cryptanalysis
  - MILP, SAT for differential and linear cryptanalysis
- Design
  - Chaskey, Simpira, PRIMATEs
- Standardization
  - ISO/IEC 29192-6: Chaskey-12

Standards Review

- NIST commitment:
  - Regular review of standards
- First review: FIPS 197
  - Advanced Encryption Standard (AES)
- Next review: SP 800-38 series
  - Block cipher modes of operation

Methodology

- Retrospection on AES competition
- Understand how AES is used
- **Focus on attacks**

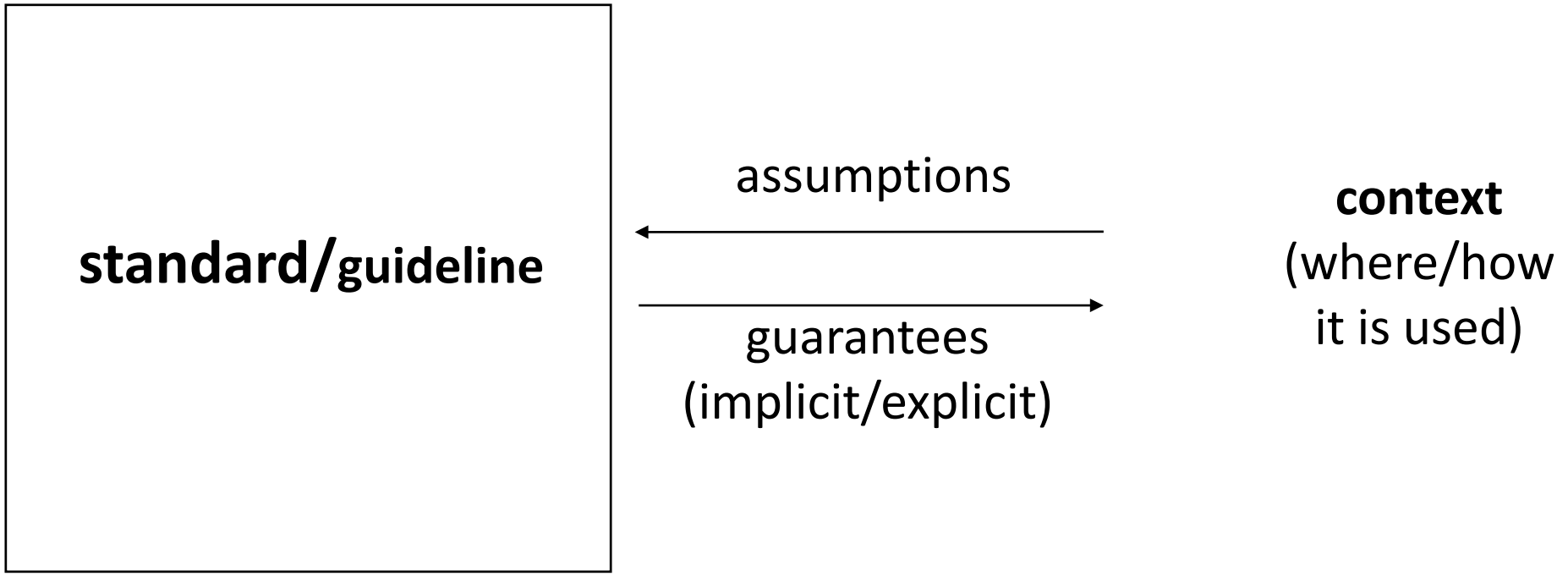
Review Perspectives

- Managerial
  - E.g., decision to renew standard?
- Technical
  - E.g., is it cryptographically secure?
- Editorial
  - E.g., is the standard complete? Unambiguous?

Resources to Consider

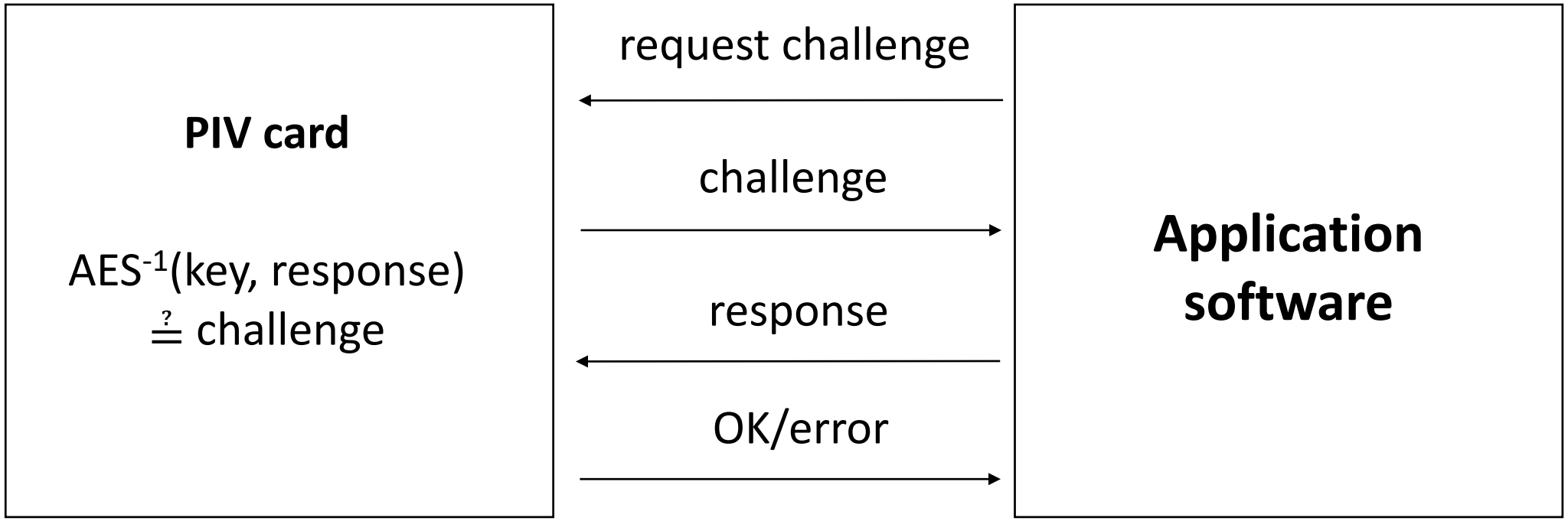
NIST-maintained	External
Primitive Higher-level operation Scheme Conformance testing (algorithm) Conformance testing (module) Configuration guidelines Vulnerability database	Publications, comments,… from public

Reviewing: Standard vs Context



Example: PIV Authentication

(NIST SP 800-73-4 Part 2)



Considerations

- Security model
  - Evolution: AES competition vs today
  - Black-box security (incl. related-key, multi-key, quantum,…)
- Parameters
  - Key size, block size, data limits and attack probabilites
- Use of standard
  - Typical applications, implement securely (incl. side-channel)

Key Takeaways

- Technical
  - Response to related-key/biclique attacks?
  - Security margin?
  - Side-channel and fault attacks?
- Editorial
  - Mostly minor feedback
- Decision: renew?

Conclusion

- Insights for standards review
  - Where is it used?
  - Assumptions and guarantees
  - Focus on attacks

- Good luck to participants!