Network Security and Lightweight Cryptography

Dr. Kerry McKay, NIST

Cybersecurity Innovation Forum
September 9, 2015

From Math to Practice

- Crypto algorithms are composition of mathematical functions
  - Evaluated in stand-alone fashion for desired properties
  - If algorithm cannot withstand this, it cannot provide security in practice
- Crypto is deployed in practice as part of a system or protocol
  - There are factors that were not accounted for in stand-alone analysis
  - May degrade or even destroy security properties
  - Have to consider algorithms in context

A [Brief] Tale of Two Application Areas

- Want to highlight two areas
  - Network security (specifically TLS)
  - Crypto for constrained environments (lightweight crypto)

TLS

- Most widely used cryptographic protocol on the Internet
- Multiple versions
  - TLS 1.0, 1.1, 1.2
  - TLS 1.3 currently under development
- More features are constantly developed, increasing complexity
  - Extensions
  - Cipher suites
- Additional complexity increases attack surface

TLS Pitfalls

- Violating crypto assumptions
  - BEAST
- Support for weak cipher suites
  - FREAK, Logjam, RC4 bias attacks, etc.
- Opening up side channels
  - CRIME, TIME, Lucky 13, BREACH
- Implementation flaws
  - Heartbleed, POODLE-TLS
- Supporting too much in the name of interoperability
  - How many servers really needed that heartbeat extension?
- And more

NIST's Role

- TLS is an IETF standard
  - Quynh Dang in TLS WG
- NIST SP 800-52 project
  - Guidelines for the Selection, Configuration, and Use of Transport Layer Security (TLS) Implementations
    - General purpose, but focus is on most common use case: HTTPS
    - Intended audience is admins and users of non-DoD federal IT systems
  - Goldilocks problem between ensuring broad interoperability and limiting attack surface

TLS Plans

- Minor update in 2016
  - Complete list of changes not yet finalized, but will include:
    - Require TLS 1.2 support
    - Require support for ECDHE cipher suites
    - Discussion on recent attacks
    - Move stuff from “future capabilities” into main body that is available now
- Larger update once TLS 1.3 is finalized and widely available

Lightweight Crypto

- What is lightweight cryptography?
  - ???
- Some ideas on meaning
  - AES doesn't always meet requirements, such as memory, circuit size, energy consumption, or latency
    - Think RFID tags, embedded devices, and IoT devices
    - IoT is problematic due to wide range of "things"
  - "Lightweight" seems to mean designed specifically to fit a particular performance constraint
    - Tends to mean hardware implementations rather than software
  - People often talk about block ciphers, but can be other primitives as well

Lightweight Crypto Project

- New game for NIST
  - In past have approved algorithms for general purpose use
    - Lightweight algorithms may be tailored to and approved only for specific environments and applications
  - Potential for portfolio of many algorithms, not just one
  - It's been 15 years since AES selected, and we've learned a lot since then
    - Are there algorithms that fit constraints and are appropriate for general use?
- Held workshop in July
  - Figure out what the needs and requirements are
  - Identify path forward

Challenges

- Identify constrained environment profiles
  - Idea is to have algorithm selections for classes of target devices
- Timeline
  - Market will change quickly
  - Unlikely enough time for competition
- Algorithm maturity
  - Is the literature mature enough for standardization?
- Misuse prevention
  - If there are limitations due to design, can we prevent algorithm from being used in inappropriate application/environment?
- Public perception
  - Make selection open, transparent, and fair

Plans

- Prepare a survey of applications and algorithms
  - Will help us scope next steps
- Talk to stakeholders to find out where lightweight is truly needed
- Have a second workshop
- Keep in touch with the community

Thanks!

- Contacts
  - TLS
    - kerry.mckay@nist.gov
  - Lightweight
    - lightweight-crypto@nist.gov
    - Workshop papers and presentations at http://www.nist.gov/itl/csd/ct/lwc_workshop2015.cfm