Cyber Security Body of Knowledge

Applied Cryptography

12.07.2021

Kenny Paterson

ETH Zurich

University of
BRISTOL

CyBOK

bristol.ac.uk

About the Presenter

Bio sketch:

- Ph.D. in Mathematics (London, 1993).
- Postdoctoral research, 1993-1996 at ETH Zurich and London
- HP Research Laboratories, 1996-2001: internal mathematical consulting
- Lecturer, Reader, Professor at Royal Holloway, University of London, 2001-2019
- Professor of Computer Science, ETH Zurich, 2019 – now

Wikipedia: https://en.wikipedia.org/wiki/Kenny_Paterson

Research group: https://appliedcrypto.ethz.ch/

Twitter: @kennyog

APPLIED CRYPTO GROUP

ETH zürich

Applied Cryptography – Overview

- Introduction
- Algorithms, Schemes and Protocols
- Implementation
- Key Management
- Consuming Cryptography
- Applied Cryptography in Action
- The Future of Applied Cryptography

Applied Cryptography – Overview

- **Introduction**
- Algorithms, Schemes and Protocols
- Implementation
- Key Management
- Consuming Cryptography
- Applied Cryptography in Action
- The Future of Applied Cryptography

Introduction

- Cryptography is a Mongrel
- Cryptography ≠ Encryption
- Cryptography is Both Magical and Not Magical
- Cryptography is Political
- The Cryptographic Triumvirate

Applied Cryptography is a Mongrel

- Applied cryptography draws on a broad range of disciplines: mathematics, theoretical computer science and software and hardware engineering.
- Almost no-one understands all aspects of the field.
- This leads to gaps.
  - Between theory and practice;
  - Between design, specification and implementation;
  - Between implementations and their eventual use by potentially non-expert developers.
- These gaps lead to security vulnerabilities.
- Cryptography usually fails for **indirect** reasons, not because of a direct failure of a cryptographic algorithm.

Cryptography ≠ Encryption

- Integrity as important as confidentiality in secure communications systems.
- Increasing deployment of more advanced cryptographic techniques.
- Zero-knowledge proofs in anonymous cryptocurrencies,
- Multi-Party Computation (MPC) techniques to enable computations on sensitive data in environments with mutually untrusting parties.
- Fully Homomorphic Encryption (FHE) for privacy-preserving machine learning.

Cryptography is both Magical and Not Magical

- Using cryptography, we can achieve very surprising results, e.g. efficient solutions to the millionaire's problem.
- But cryptography alone cannot make an insecure system secure.
- It can make certain attack vectors infeasible or uneconomical.
- Example:
  - TLS protects communications between clients and servers, limiting what an eavesdropper can see.
  - But TLS cannot prevent traffic analysis, remove all metadata leakage, nor secure the endpoints themselves.
- Cryptography can be brittle and fail ungracefully.
- Cryptography in general is *non-composable*.

Cryptography is Political

- Cryptography is used by many kinds of people for many kinds of things.
- Governments and their agencies have long sought to control the spread of cryptographic technology.
- Broad export control regulations applicable to cryptography are still in place.
- Yet strong cryptography is now in everyone's hands – literally.
- There has been a long-running debate on how to balance potential benefits and harms arising from the spread of strong cryptography.

The Cryptographic Triumvirate

- A useful classification for thinking about how cryptography is used.
- Data in transit – secure communications (TLS, IPsec,…).
- Data at rest – secure storage.
- Data under computation – FHE, MPC, searchable encryption,…

Applied Cryptography – Overview

- Introduction
- **Algorithms, Schemes and Protocols**
- Implementation
- Key Management
- Consuming Cryptography
- Applied Cryptography in Action
- The Future of Applied Cryptography

Algorithms, Schemes and Protocols

- Basic concepts: keys, asymmetric vs. symmetric cryptography
- Introducing the basic building blocks of cryptography:
  - Hash functions
  - Block ciphers
  - Stream ciphers
  - Message Authentication Code (MAC) schemes
  - Authenticated Encryption (AE) schemes
  - Public Key Encryption Schemes and Key Encapsulation Mechanisms
  - Diffie-Hellman Key Exchange
  - Digital Signatures

Algorithms, Schemes and Protocols

- Common aspects:
  - Each building block comes with a well-defined syntax.
  - Each building block comes with formal security definitions which concretely quantify the adversary's resources.
  - Each building block can be securely realised under suitable computational assumptions.
  - Security proof consists of showing that any adversary breaking the formal security definition can be used to construct an algorithm that breaks an underlying computational assumption.
  - We still have to rely on cryptanalysis: the absence of attacks invalidating the assumptions.
- These ideas are *informally* introduced and discussed for each building block.
- Common instantiations of each building block are briefly discussed.

Algorithms, Schemes and Protocols

- Further aspects:
  - Cryptographic diversity.
  - Modelling the adversary, conservatively.
  - The importance of formal security definitions and proofs in providing assurance.
  - The limitations of proofs in cryptography.

Algorithms, Schemes and Protocols

Further aspects:

- Key sizes.
- Cryptographic agility.
- Standardisation of cryptography – NIST, ISO, IETF and their contrasting approaches, strengths and weaknesses.
- Post-quantum cryptography and the NIST “competition”.
- Quantum Key Distribution.

Algorithms, Schemes and Protocols

- Combining building blocks: going from low-level schemes to higher-level interactive protocols.
- Example: TLS combining Diffie-Hellman key exchange, signatures, Key Derivation Functions, AEAD (and more).
- Extending the provable security approach to more complex systems is challenging, and we are reaching the limits of human comprehension.
- Common in analysis of protocols to focus on a “cryptographic core” and abstract away many details.
- Mechanised tools and symbolic tools as complementary approaches to hand-written proofs.

Applied Cryptography – Overview

- Introduction
- Algorithms, Schemes and Protocols
- **Implementation**
- Key Management
- Consuming Cryptography
- Applied Cryptography in Action
- The Future of Applied Cryptography

Implementation

- In an ideal world, a developer would start from a cryptographic specification (written in, e.g., pseudocode) and refine it to a lower-level programming language (or hardware).
- Most developers consume cryptography via a library and its APIs.
- Crypto libraries vary widely in quality, maintenance, support, functionality,…
- Most developers are not cryptographically expert, nor should we expect them to be.
- API design is critical: hard to understand, non-intuitive, insecure-by-default APIs lead developers into making mistakes.

Implementation

- Beyond standard software development issues like bugs, cryptographic implementation challenges include:
  - Length side channels
  - Timing side channels
  - Error side channels
  - Attacks arising from shared resources (Caches, CPU contention,…)
  - Attacks arising from improper composition of building blocks
  - Additional hardware side channels (EM, power consumption, acoustic side channels,…)
  - Fault attacks

Implementation

- Defences come from the fields of software and hardware security.
- They include:
  - Blinding, masking, threshold techniques and physical shielding in hardware.
  - Formal specification and verification of software and hardware designs.
  - Static and dynamic analysis of code.
  - Fuzzing.
  - Information flow analysis.
  - Domain-specific languages for cryptography.
  - Strongly typed languages.
  - Constant-time programming techniques.

Implementation

- Randomness plays a crucial role in cryptography.
- Many cryptographic algorithms can be derandomized using state or other mechanisms.
- Some cannot, e.g. key generation.
- Most OSes provide access to a cryptographically strong source of random bits, with entropy gathered from local sources.
- Some CPUs provide access to bits from true random big generators but the designs are not fully open.
- Using OS-provided randomness sources is recommended over attempting to design one’s own mechanism.

Applied Cryptography – Overview

- Introduction
- Algorithms, Schemes and Protocols
- Implementation
- **Key Management**
- Consuming Cryptography
- Applied Cryptography in Action
- The Future of Applied Cryptography

Key Management

- Cryptographic schemes shift the problem of securing data to that of securing and managing keys.
- So a full treatment must address how those keys are generated, distributed, secured, destroyed,…: the *key lifecycle*.
- This forms the core of the topic of *key management*.
- It includes technical and non-technical aspects, as well as special considerations for managing public keys and the associated infrastructural requirements.

Key Management

- Key derivation:
  - The process of making (many) new keys from existing keys.
  - Main requirement is that new keys should be computationally indistinguishable from random bit string.
  - Done using a special-purpose function called a Key Derivation Function (KDF).
  - Making many keys from one makes it easier to comply with the **Principle of Key Separation**: each key should only be used for one well-defined purpose.
  - Violations of the Key Separation Principle can lead to attacks, several well-documented cases.

Key Management

- Key derivation:
  - The process of making (many) new keys from existing keys.
  - Main requirement is that new keys should be computationally indistinguishable from random bit strings.
  - Done using a special-purpose function called a Key Derivation Function (KDF).
  - Making many keys from one makes it easier to comply with the **Principle of Key Separation**: each key should only be used for one well-defined purpose.
  - Violations of the Key Separation Principle can lead to attacks, several well-documented cases.

Key Management

Other considerations include:

- Key Generation: how to securely generate keys?
- Key Storage: where to store keys and how to do so securely?
- Key Transportation: how to arrange for keys to be where they are needed?
- Key Refreshing and Forward Security: how to limit effects of key compromises?

Key Management

- In order to use a public key (to perform public key encryption or to verify a signature) we need to know whose key it is.
- Public Key Infrastructure (PKI):
  - Provides mechanisms to enable parties to verify the authenticity and validity of other parties' public keys.
  - Provides bindings between public keys and identities of key owners.
  - Main mechanism used is digital certificates: cryptographically secured assertions by trusted third parties called **Certification Authorities** about bindings between public keys and identities.
  - Example: the Web PKI.

Key Management

- PKI brings many challenges:
  - Needs associated mechanisms to determine whether a certificate is still valid, aka revocation status.
  - Requires trusted sources of time.
  - Requires confidence in CA operations (e.g. to avoid certificate mis-issuance).
  - Needs unbroken cryptography and correct software (cf. SHA-1 and Apple “goto fail”).
- Rival approaches (web-of-trust, identity-based cryptography, certificateless cryptography) strike different sets of trade-offs in addressing these challenges.

Applied Cryptography – Overview

- Introduction
- Algorithms, Schemes and Protocols
- Implementation
- Key Management
- **Consuming Cryptography**
- Applied Cryptography in Action
- The Future of Applied Cryptography

Consuming Cryptography

- Cryptography has significant exposure in popular culture.
- This may lead people to believe they are qualified to design new cryptographic algorithms and systems when they are not.
- Many personal experiences of having to help inventors, investors, and others to understand the limitations of their designs.
- Kitchen-sink, large keys and friendly cryptanalysis fallacies.
- Developers regularly “roll their own” cryptographic systems/protocols in the absence of existing solutions and/or due to over-confidence in their abilities.

Consuming Cryptography

Remedies:

- There is no cryptographic “free lunch” – if something looks too good to be true, it probably is.
- Try to detect cryptographic snake-oil by looking for instances of the standard fallacies.
- Look for independent analyses by reputable experts.
- Look for peer-reviewed publication in respectable research venues.

Consuming Cryptography

Remedies:

- Large companies, or smaller ones for whom cryptography is a core technology, should employ qualified cryptographers and give them a role in system specification and development.
- Developers should rely on existing algorithms packaged in cryptographic libraries.
- Developers should rely on existing design patterns and standards for more complex cryptographic systems/protocols.
- When a new application demands a new cryptographic system or protocol, and expertise is not locally available, seek external advice.

Applied Cryptography – Overview

- Introduction
- Algorithms, Schemes and Protocols
- Implementation
- Key Management
- Consuming Cryptography
- **Applied Cryptography in Action**
- The Future of Applied Cryptography

Applied Cryptography in Action

Three case studies exemplifying different aspect of applied cryptography:

- Transport Layer Security version 1.3 (TLS 1.3) – an harmonious collaboration between academia and industry.
- Secure Messaging – comparing and contrasting Apple iMessage, Signal and Telegram.
- Digital contact tracing à la DP3T (and GAEN) – speed of development and simplicity of design combined to combat Covid19 in a privacy-preserving manner.

Applied Cryptography – Overview

- Introduction
- Algorithms, Schemes and Protocols
- Implementation
- Key Management
- Consuming Cryptography
- Applied Cryptography in Action
- **The Future of Applied Cryptography**

The Future of Applied Cryptography

- The debate around lawful access to encrypted data will continue.
- Cryptocurrency and blockchain space should mature and leave behind a raft of useful cryptographic technologies.
- Cryptography for data under computation is a new frontier that is quickly opening up, driven by desire to outsource data processing couple with legal and regulatory considerations, especially relating to handling of personal data.
- Privacy-preserving techniques for data-mining and data aggregation have huge potential and are seeing rapid adoption.
- Electronic voting will continue to face usability challenges as well as public scepticism.
- Cryptographic thinking has a wider role to play in security research, for example in the analysis of adversarial machine learning.

Contact:
Professor Kenny Paterson
Applied Cryptography Group
kenny.paterson@inf.ethz.ch

ETH Zurich
Applied Cryptography Group
Department of Computer Science
Universitätstrasse 6
8092 Zurich, Switzerland

https://appliedcrypto.ethz.ch/

APPLIED
CRYPTO
GROUP

ETH zürich