Work in progress

This is an early draft of the table of contents of a book on the foundations of cryptographic authentication being coauthored by Francisco Corella, Sukhi Chuhan and Veronica Wojnas. Please send comments to the authors.

Book title: Foundations of Cryptographic Authentication

Part I: Introduction

Chapter 1: Introduction

- Motivation
    - Vulnerabilities of traditional multifactor authentication
    - Worldwide emergence of digital government services
- Book audiences
- Terminology
- Organization of the rest of the book

Part II. Cryptographic foundations

Chapter 2: Cryptographic primitives

- Preliminaries
    - Cryptographic assumptions and security reductions
    - System parameterization
    - Cyclic groups and discrete logarithms
        - Mathematical background on cyclic groups and discrete logarithms
        - Security strengths provided by discrete logarithm assumption
            - Group order and subgroup structure
                - Pohlig-Hellman algorithm
                - Small subgroup attacks
            - NIST classification of cryptographic primitives
            - Strength of the discrete log assumption in ECC primitives
            - Speed of generic discrete-log algorithms
            - NIST’s comparison of security strengths
    - Galois fields
    - Elliptic curves
        - The projective plane
        - Algebraic plane curves
        - Weierstrass curves

        - Jacobian coordinates
        - Group law
        - Montgomery and Edwards curves
            - Montgomery curves
            - Curve25519
            - Edwards curves
            - Twisted Edwards curves
- Primitives used in cryptographic authentication
    - Hash functions and hash trees
        - Cryptographic properties of hash functions
        - Choosing a hash function
        - Structured cryptographic digests: lists, chains, trees
    - Symmetric signatures and HMAC
        - The Merkle–Damgård construction
        - The length extension attack
        - How HMAC avoids the length extension attack
        - Should HMAC be used with SHA-3?
    - Asymmetric signature schemes
        - EUF-CMA vs SUF-CMA security
        - Discrete-log signature schemes in cyclic groups
            - Unified notation for comparison of different discrete log signature schemes
            - The Schnorr signature scheme
            - DSA and ECDSA
            - EdDSA
                - Cofactor clearing and clamping
                - Generation of the private key and the per-message secret
                - The Ed25519 signature scheme
- The many uses of cryptographic primitives in authentication

Chapter 3: Traditional cryptographic credentials

- Using a key pair for challenge-response authentication
- Public key and attribute certificates
- Hash-of-public-key certificates
- Selective disclosure public key certificates
- From zero knowledge protocols to anonymous credentials
    - Zero knowledge (ZK) proof of a fact (PoF)
        - Example: zero knowledge proof of quadratic residuosity
    - Honest-verifier zero-knowledge (HVZK) proof of knowledge (PoK) of a secret
        - Sigma protocols
            - Example: The Schnorr identification protocol
    - Non-interactive zero-knowledge proof of knowledge of a secret
        - From NIZK PoK to challenge-response authentication
        - From NIZK PoK to a signature scheme

        - Two versions of Schnorr signatures
        - The Fiat-Shamir transform
        - Fiat-Shamir transformation of a Sigma identification protocol into a signature scheme
        - Fiat-Shamir transformation of a general three-move protocol into a general one-move protocol
        - Fiat-Shamir transformation of a sequence of three-move protocols into a single one-move protocol
    - Honest-verifier zero-knowledge proof of knowledge of a signature
    - Non-interactive zero-knowledge proof of knowledge of a signature
        - Secret signatures as anonymous credentials
        - Signature by the anonymous subject of a credential
    - Example: BBS signatures as anonymous credentials
    - The role of zero knowledge in anonymous credentials

Chapter 4: Phishing resistant authentication with cryptographic credentials

- Authentication across a communication channel
- <<< secure channels, key agreement, DH, ECDH, authenticated encryption…
- Credential presentation protocols
- Countermeasures against man-in-the-middle phishing attacks
- Authentication with a symmetric signature
- Returning-user authentication with a key pair credential
- Third-party authentication with a public key certificate
- Cardholder authentication and transaction confirmation with a credit card certificate
- Authentication with unlinkable credentials

Part III: Technological foundations

Chapter 5: Web technology

- The World-Wide Web
    - HTTP and TLS
    - JavaScript
    - Redirection
    - Same-origin policy
- Web APIs
    - Web Cryptography API
    - Web Storage API
    - IndexedDB API
    - Web Authentication API
    - Service workers
- Federated identity management
    - OAuth2
    - OpenID Connect

Chapter 6: Mobile technology

- Native apps
- Web apps
- Progressive web apps
- Wallets

Chapter 7: Secure storage

- Browser enforcement of the same origin policy
- Cryptokey objects
- Secure enclaves, TEEs, TPMs
- Hardware security modules

Chapter 8: Email and texting security

- Email authentication protocols
  - SPF, DKIM, DMARC
- Text messaging vulnerabilities

Chapter 9: Blockchains and distributed ledgers

- Bitcoin
- Ethereum
- Hashgraph
- Cryptocurrencies
- Fungible and non-fungible tokens
- Payment wallets

Part IV: Browser-based cryptographic authentication

Chapter 10: FIDO

- FIDO2 specifications
  - Web Authentication API
  - Client to Authenticator Protocol
- Security keys
- Platform authenticators
- Passkey synchronization
- Authentication with third-party certificates

Chapter 11: Fusion credentials

- The concept of fusion
- Biometric fusion
- Biometric cryptosystems and revocable biometrics
- Fusion a key pair with a password
- Fusion a key pair with a revocable biometric
- Fusion of a selective disclosure certificate with a password and a biometric

- Fusions of zero-knowledge credentials with biometrics
- Threats and opportunities arising from AI

Part V: Wallet-based authentication

Chapter 12: Mobile wallets

- Types of mobile wallets
    - Payment wallets
    - Cryptocurrency wallets
    - Government wallets
    - SSI wallets
- Communication methods
- Management of wallet credentials
    - In-wallet storage
    - Online storage
    - Credential revocation

Chapter 13: ISO/IEC wallet credentials

- ISO/IEC 18013-5
    - Extensible data model
    - Terminology
    - Selective disclosure
    - Age attestations
    - Session encryption and mdoc authentication
    - Authentication of the mdoc reader
    - Transaction flows
    - Innovative use of OpenID Connect
    - Security posture
        - Vulnerability to cloning and man-in-the-middle attacks
            - Mitigation and attack prevention
        - Unauthorized access attacks, mitigations, and prevention
            - Active attack against NFC activation
            - Eavesdropping attacks on NFC device engagement
            - Eavesdropping attacks on the QR code
            - Prevention of unauthorized access attacks
    - Privacy
    - User experience --- NOT WRITTEN YET
        - Device activation and engagement
        - Holder authentication
        - Attribute selection and holder consent
        - Accessibility

Chapter 14: Decentralized identifiers

- Early constructions of decentralized identifiers

    - Namecoin
    - Decentralized PKI
- W3C decentralized identifiers
    - did:btcr
        - DID document
        - DID creation
        - DID update
            - The “controller” concept
            - Key rotation in did:btcr
            - DID deletion
            - DID resolution
    - did:key
        - A glossary of “25519” terminology
    - KERI
        - Key rotation and pre-rotation in KERI
    - did:peer
        - Generation methods
- DIDComm
    - Message encoding and transport
    - Message signing and encryption

Chapter 15: Verifiable credentials and self-sovereign identity

- Origin, scope, and “verifiability” of verifiable credentials
- Using verifiable credentials for authentication
- Protection against man-in-the-middle attacks
- Self-sovereign identity
    - Definition
    - SSI with existing technology
    - Benefits of SSI
    - Privacy implications of SSI
- Anoncreds
- W3C BBS cryptosuite

Chapter 16: Combining ISO/IEC credential and verifiable credentials

TBD

Part VI: User experience

Chapter 17: User experience

- Introduction
    - Why UX matters in these things: A potential case study to highlight the importance
    - Usability issues in historical authentication methods

- High level overview of user experience
    - User research basics
- Existing research (“user research that has been done to this point”)
    - Literature review of existing papers
- Review of Cryptographic Authentication Methods
    - Web authentication patterns
        - Potential implementation examples: Secure Keys, Passkeys, Fusion Credentials
    - Wallet authentication patterns:
        - Potential implementation examples, BC Wallet, Mobile Drivers Licenses, Diia
- UX considerations for cryptographic authentication [working set of key themes - subject to change]
    - Mental models and understanding
        - What it is: Definition of the heuristic
        - Examples of implementation patterns that speak to that theme
        - Why it matters
        - Tips to keep in mind/thinking to explore
    - Value proposition
        - What it is: Definition of the heuristic
        - Examples of implementation patterns that speak to that theme
        - Why it matters
        - Tips to keep in mind/thinking to explore
    - Accessibility:
        - What it is: Definition of the heuristic
        - Examples of implementation patterns that speak to that theme
        - Why it matters
        - Tips to keep in mind/thinking to explore
    - Delight/interactions
        - What it is: Definition of the heuristic
        - Examples of implementation patterns that speak to that theme
        - Why it matters
        - Tips to keep in mind/thinking to explore
    - SSI-specific: double-edged sword of responsibility
- Conclusion
    - Summary of key points