**Cryptography Classes in Bugs Framework (BF):**

**Encryption Bugs (ENC), Verification Bugs (VRF), and Key Management Bugs (KMN)**

Irena Bojanova, NIST; Paul E. Black, NIST; Yaakov Yesha, NIST, UMBC; Farhan Nadeem, NIST

Advances in scientific foundations of cybersecurity rely on the availability of accurate, precise, and unambiguous definitions of software weaknesses (bugs) and clear descriptions of software vulnerabilities. The Bugs Framework (BF) comprises rigorous definitions and (static) attributes of bug classes, along with their related dynamic properties, such as proximate, secondary and tertiary causes, consequences, and sites.

**BF Taxonomy**

**Encryption Bugs (ENC):** The software does not properly transform sensitive data (plaintext) into unintelligible form (ciphertext) using cryptographic algorithm and key(s).

**Decryption Bugs:** The software does not properly transform ciphertext into plaintext using cryptographic algorithm and key(s).

**Key Management Bugs (KMN):** The software does not properly generate, store, distribute, use, or destroy cryptographic keys and other keying material.

**Verification Bugs (VRF):** The software does not properly sign data, check and prove source, or assure data is not altered.

**Cryptography Classes in Bugs Framework (BF):**

**Examples**

- **CVE-2007-5460 → ENC**
  - **Cause:** Weak Encryption Algorithm ( XOR cipher with fixed key )
  - **Attributes:**
    - Sensitive Data: Credentials (PHNs/passwords)
    - Data State: Transferred (over network)
    - Algorithm: Symmetric (that allows obtaining shared key by sniffing or spoiling the docking process and decryption)
    - Security Service: Confidentiality
  - **Consequence:** IX of Sensitive Data (credentials)

- **CVE-2001-5185 → VRF**
  - **Cause:** Missing Verification Step (challenge-response) in public key authentication
  - **Attributes:**
    - Verified Data: Any (Secret/Public)
    - Data State: Transferred (over network)
    - Algorithm: Digital Signature (not using such allows private key not to be verified by public key)
    - Security Service: Integrity Authentication
  - **Consequence:** IX of Sensitive Data

- **CVE-2015-0204, 1637, 1067 (FREAK) → KMN & ENC**
  - **Inner ENC:** An inner KMN leads to an inner ENC, which leads to an outer ENC.
  - **Inner KMN:**
    - **Cause:** Improper Offer of Weak Protocol (Export RSA – offered from MRTM-tricked server and accepted by client)
    - **Attributes:**
      - Cryptographic Data: Keying Material (pair of private and public keys)
      - Data State: Transferred (over network)
      - Algorithm: Export RSA (128-bits key generation based on prime numbers, such that private key can be obtained from public key through factorization)
      - Operation: Generate
  - **Consequence:** IX of Keying Material (private key)

**Model of Cryptographic Store or Transfer Bugs**

**BF Taxonomy**

- **Key Management Bugs (KMN):** The software does not properly generate, store, distribute, use, or destroy cryptographic keys and other keying material.

**Verification Bugs (VRF):** The software does not properly transform sensitive data (plaintext) into unintelligible form (ciphertext) using cryptographic algorithm and key(s).

**Encryption Bugs (ENC):** The software does not properly transform sensitive data (plaintext) into unintelligible form (ciphertext) using cryptographic algorithm and key(s).