The new Cryptographic Store/Transfer (CST) Class from Bugs Framework (BF)
Irena Bojanova, NIST; Paul Black, NIST; Yaacov Yesha, NIST, UMBC

This is the BF of the new Cryptographic Store/Transfer (CRY–ST) fault class. It shows causes, attributes, and consequences of CST faults. CST incorporates Encryption (_ENC), Verification (_VRF), and Key Management (_KMN).

Cryptographic Store/Transfer (CST): The software does not properly manage keys, or encrypt/decrypt or verify data for secure store/transfer.

**Causes**

- Improper Cryptographic Algorithm/Step
- Weak Key
- Missing Keys (inadequate) or Risky/Broken Keys

**Attributes**

- ENC: The software does not properly transform sensitive data (plaintext) into unintelligible form (ciphertext) using cryptographic algorithm and key(s).
- _VRF: The software does not properly sign message, check and prove origin, or assure message is not altered.
- _KMN: The software does not properly generate, store, distribute, use, or destroy cryptographic keys (keying material).

**Consequences**

- **Process**: Encryption (_ENC), Verification (_VRF), Key Management (_KMN)
- Data State: Process Specific
- Process Specific

**Examples**

- **CVE-2015-0204, 1637, 1067 (FREAK)**
  - _KMN & _ENC CRY:
    - Inner _KMN CRY leads to inner _ENC CRY, which leads to outer _ENC CRY.
    - Inner _KMN CRY: Client accepted improper offer of weak protocol (SSL with Export RSA) from MITM-tricked server, which generates 512-bit RSA key-pair that is transferred over network, leads to IEX of sensitive data (private key*)
    - Inner _ENC CRY: Known private key for asymmetric encryption (RSA) for transferred sensitive data (Pre-Master Secret**), allows confidentiality failure and decryption, which leads to IEX of that data.

- **CVE-2002-1946**
  - _ENC CRY: Use of weak algorithm for symmetric encryption (specifically, one-to-one mapping) for stored in registry sensitive data (passwords) allows confidentiality failure and decryption, which leads to and IEX of that data.

- **CVE 2001-1585**
  - _VRF CRY: Missing cryptographic step in public key authentication (specifically, challenge-response verification of private key using digital signature) allows client identity authentication failure, which leads to ATN.

**Model**

- **Key Generation**
  - Generate key
  - Store key
  - Destroy key

- **Third party certificate authority (CA) distributes public keys with signed certificate.**