Information Exposure (IEX) Class in the Bugs Framework (BF)

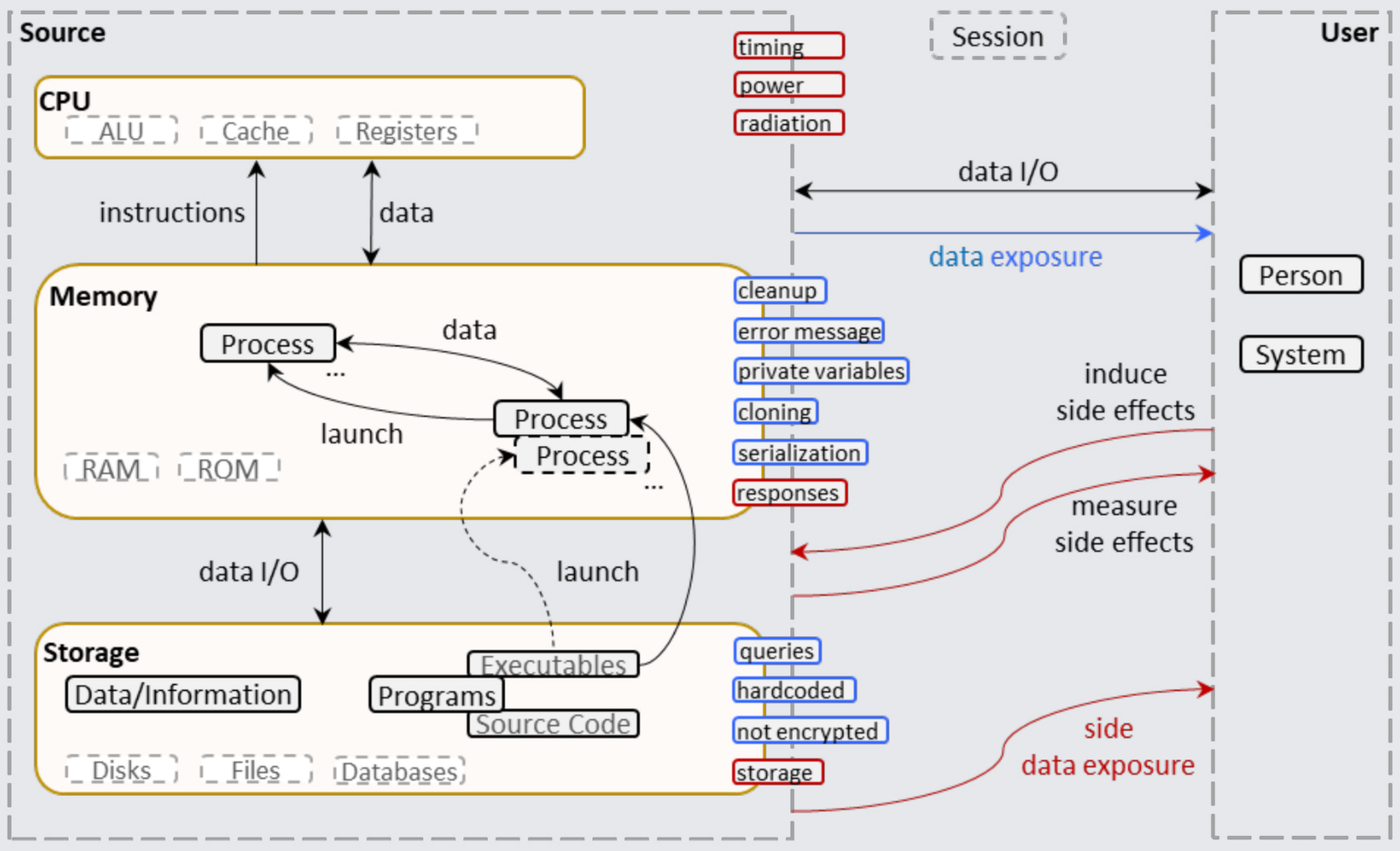
Irena Bojanova, NIST; Yaacov Yesha, NIST, UMBC; Paul E. Black, NIST; Yan Wu, BGSU

https://samate.nist.gov/BF

Exposure of sensitive information can be harmful on its own and in addition could enable further attacks. A rigorous and unambiguous definition of information exposure faults can help researchers and practitioners identify them, thus avoiding security failures. Information Exposure (IEX), a new class in the Bugs Framework (BF). The BF comprises rigorous definitions and (static) attributes of fault classes, along with their related dynamic properties, such as proximate and secondary causes, consequences and sites. ….

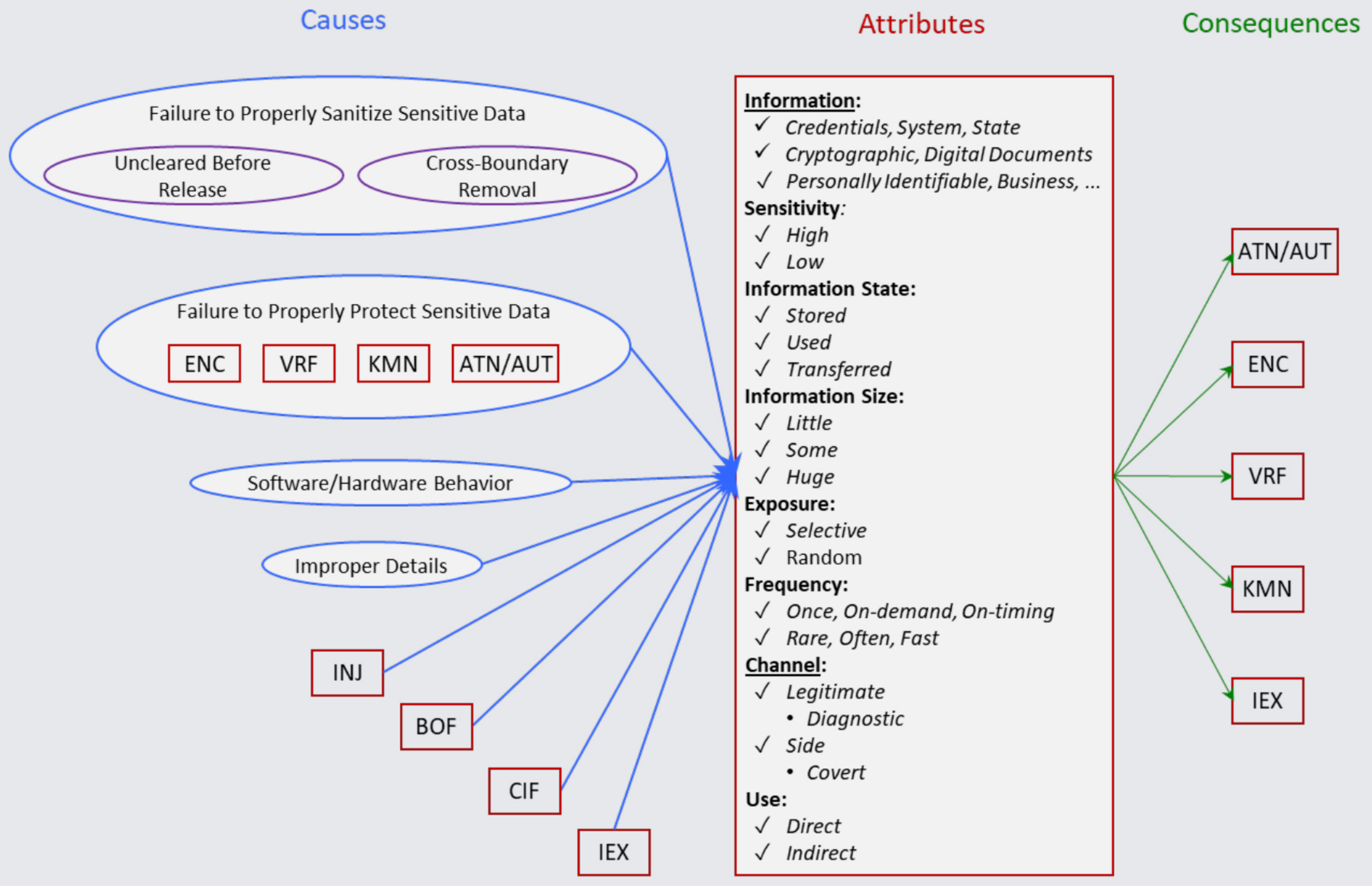
Definition of IEX: *Information is leaked through legitimate or side channels.*

• BF Model of Information Exposure



Note: Legitimate channels are in blue. Side channels are in red.

• IEX Taxonomy



- We use the IEX taxonomy to analyze specific vulnerabilities and provide clear descriptions.
- The following are examples from the MITRE Common Vulnerabilities and Exposures (CVE).

• CVE-2007-5172

IEX 1 of password leads to ATN leads to IEX 2

IEX 1

Cause: Improper Details
(password in error message)

Attributes:
Information: Credentials (password)
Sensitivity: High
Information State: Stored
Information Size: Little
Exposure: Selective
Frequency: On-Demand
Channel: Diagnostic (connection error message)
Use: Indirect

Consequences: ATN.

IEX 2

Cause: Failure to Properly Protect Sensitive Data (password)

Attributes:
Information: Any (user data)
Sensitivity: Low/High
Information State: Stored
Information Size: Huge
Exposure: Selective
Frequency: On-Demand
Channel: Legitimate
Use: Direct (valuable on its own)

Consequences: Any IEX consequence

ATN (to be described later)

• CVE-2017-5754 (Meltdown)

Cause: Hardware Behavior
(CPU out-of-order execution)

Attributes:
Information: Any
(passwords in password manager or browser, personal photos, emails, instant messages, business-critical documents)
Sensitivity: High
Information State: Stored
(in kernel-memory registries of other processes or virtual machines in the cloud)
Information Size: Huge
Exposure: Selective
Frequency: On-Demand
Channel: Covert (cache-based timing)
Use: Any

Consequences: Any IEX consequence

THE NINETEENTH ANNUAL
HIGH CONFIDENCE SOFTWARE AND SYSTEMS CONFERENCE
Annapolis, MD | April 29 - May 1, 2019