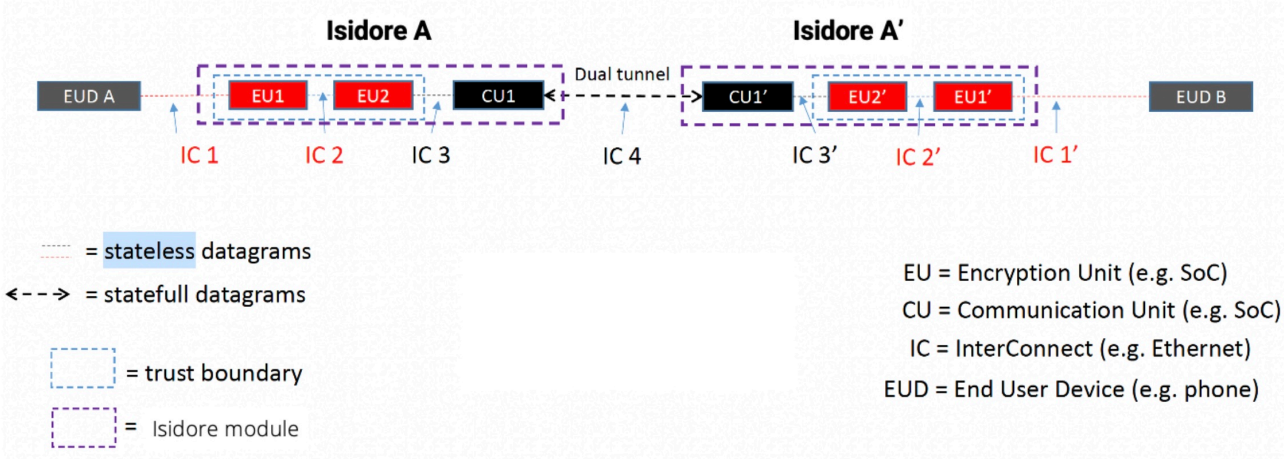
Post Quantum Active Cyber Defense System　後量子主動式網路防禦系統

1. 概述

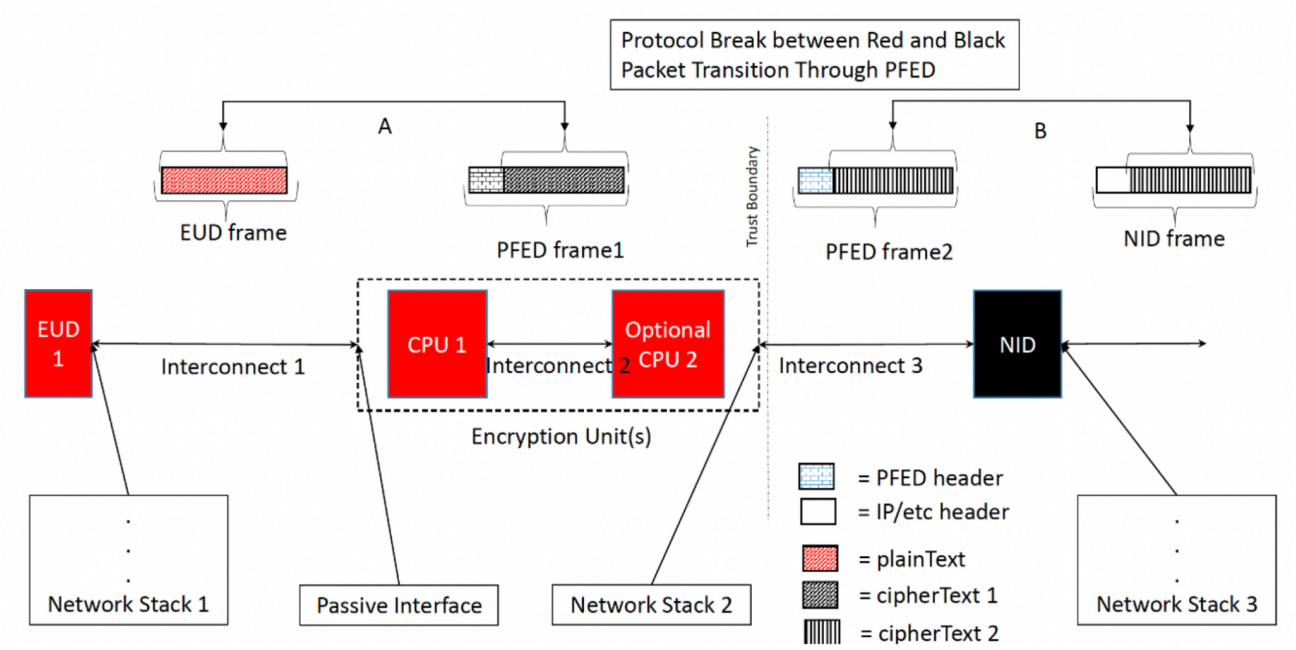
Isidore Quantum 最初是由美國國家安全局 (NSA) 研發並取得專利 (專利號碼：US 11,588,798 B1) 的一項開創性技術。這項新技術完全植基於商用現貨 (COTS) 的硬體與軟體之上。Forward Edge-AI 公司在 NSA 授權下，開發出定製的專利軟體，將NSA獨特的專利架構實現為 Isidore 480 INE (Inline Network Encryptor)：一款可提供 480Mbps 加密速率，既抗量子攻擊、又具入侵防護的主動式網路防禦系統。Isidore 480 INE (簡稱 Isidore) 能對數據流提供從生成到使用(from creative to consumption)整個過程中的量子安全保護，使其免受敵方代理者操作的非本地網路設備(non-indigenous networking equipment) 和不受信任網路的影響。

2. 系統架構

Isidore 係由紅區 (信任區) 和黑區 (非信任區) 兩個子系統組成。兩個Isidore之間的通信單元(CU)，可跨越黑區的U-NAS (Untrusted Network Address Space)，為連接至紅區加密單元 (EU) 的EUD (亦即 Trusted Network Address Space，T-NAS) 建立起點對點的安全連接。系統架構詳如下圖所示。



來自EUD的各類明文(如視頻、語音、文本等)可以任何協定的碼框格式(EUD frame，如Ethernet、RS422、USB、全雙工、半雙工等)送至EU加密成密文，EU為密文加上不受協定限制的PFED (Protocol Free Encrypting Device) 標頭後，再送至CU的NID (Network Interface Device)銜接任何型態的U-NAS (如LAN/WAN、4G、5G、6G、無線電、WiFi等)。EU2變更密文碼框PFED標頭所產生的封包轉換(Packet Transition)，會在紅、黑區之間造成協定斷裂(Protocol Break)，以此建立的信任邊界(Trust Boundary)，安全性等同實體隔離。其工作方式如下圖所示。



Isidore必須配對使用，意即只有彼此綁定的兩個 Isidore 才能互通。除了一對一配對之外，亦可以一對多的方式配對，部署成星型、網狀等各類拓撲結構，這使散置世界各處的多個位於實體隔離之內的機敏終端用戶設備 (EUD)，可經由 Isidore 跨越任何 U-NAS 進行安全通信。

3. 威脅模型

Forward Edge-AI 基於下列威脅模型假設，進行 Isidore 系統架構設計與技術開發，並利用 Forward Edge-AI 專利的異常檢測器來填補威脅模型中的空白。Isidore 利用即時的機器學習系統學習日常流量模式，以此辨識異常流量，並視需要執行免疫系統反應或提供不佔用服務頻寬資源的頻帶外 (out-of-band) 報告。

威脅模型設計假設：

- Isidore 設定 U-NAS 和 CU 為非信任區，T-NAS 雖較為可信但也不可全信。
- Isidore 不排除 T-NAS 的用戶可能會試圖從 T-NAS 攻擊 EU。
- 敵方可以觀察或記錄 U-NAS 上的流量以便其後續分析。
- 敵方可以阻塞、重新排序、修改、延遲和重播 U-NAS 上的任何數據封包。
- 可能遭敵控制的CU為攻擊事件的「緩衝區」，免疫反應機制須能自我修復。
- Isidore 配對設備中的一個可能會被盜或丟失，但不能因此增加遭破解的風險，設備須設計成非管控的加密項目 (non-CCI)，無需權責單位的監管與操作授權 (Authority to Operation, ATO) 即可部署和運用。