Cybersecurity Essentials: CIA, IAAA & Zero-Day Exploits

CIA Triad in a Nutshell

- **Confidentiality:** Ensures information is accessible only to authorized users, using encryption, access controls, and data classification to prevent leaks and breaches.
- **Integrity:** Guarantees data remains accurate and unaltered, using checksums, hashing, and digital signatures to detect tampering and ensure trustworthiness.
- **Availability:** Maintains reliable access to systems and data through redundancy, backups, and DDoS protection, preventing costly downtime.

What if CIA is Broken?

That's when the IAAA Framework comes into play.

IAAA Framework Made Simple

- **Identification:** Assigns a unique ID (e.g., username) to entities, establishing who's who in the system.
- **Authentication:** Verifies identity via:
  - Something you know (password)
  - Something you have (token)
  - Something you are (biometric)

  Often combining factors for stronger security.
- **Authorization:** Grants permissions post-authentication, enforcing least-privilege so users access only what they need.
- **Accounting (Audit):** Logs and monitors activities to trace actions back to users, enabling forensics, compliance, and accountability.

Pegasus: My Favourite Zero-Day Attack

Pegasus is the ultimate zero-day exploit, quietly hijacking devices without a trace by chaining unknown flaws in iOS and Android. Its stealthy elegance lies in turning a simple link or call into full device control—harvesting messages, calls, location data, and camera/microphone access before anyone realizes they've been compromised.

The Sneak Attacks

- **2016 Triple iOS Zero-Days**
  - **CVE-2016-4655:** Kernel info-leak reveals protected memory layouts.
  - **CVE-2016-4656:** Kernel memory corruption grants jailbreak privileges.
  - **CVE-2016-4657:** WebKit flaw in Safari executes code via a crafted link.

  Together, they enabled **"click-to-jailbreak"** installs with zero user awareness.
- **2019 WhatsApp Zero-Click (CVE-2019-3568):**
  A missed WhatsApp call alone triggered buffer overflow in the VOIP stack, installing Pegasus with no interaction—proof that even unanswered calls aren't safe.
- **2021 FORCEDENTRY (CVE-2021-30860):**
  Disguising a malicious PDF as a GIF, FORCEDENTRY exploited an integer overflow in Apple's CoreGraphics parser to deploy Pegasus via text message—zero clicks and zero warning.

Why It's Legendary

Pegasus redefined cyber-espionage by blending technical artistry with audacity: multi-vector kernel exploits, zero-click messaging tricks, and everyday file formats weaponized in plain sight. Each exploit raised the bar for attackers and defenders, proving that when adversaries strike first, no device is truly secure. The impact of this software has been immense—numerous high-profile individuals and politicians have been targeted, with their calls intercepted and monitored without their knowledge.

Zero-Day Exploits: When Defenses Don't Exist

A **zero-day exploit** leverages a vulnerability unknown to the vendor, leaving "zero days" to patch before attackers strike. These stealthy flaws bypass signature-based defenses and fetch top dollar on illicit markets.

Hall of Fame: Legendary Zero-Day Attacks

Attack	Year
Stuxnet	2010
Operation Aurora	2009
Heartbleed	2014
WannaCry	2017
NotPetya	2017
Log4Shell	2021

Spotlight: Most Recent Zero-Day Exploits

- **Google Chrome:** CVE-2025-2783
- **CLFS Privilege Escalation:** CVE-2025-29824
- **SAP NetWeaver:** CVE-2025-31324
- **Ivanti Connect Secure & Policy Secure**
- **Apple Core Media:** CVE-2025-24085