The No-Go-* Solutions in 1-Page: Eliminating Cyberwar

Erland Wittkoetter, PhD., Aug 29th 2022

Power distribution applies the concept of circuit breakers and fuses to avoid device damage. So far, we don't have equivalent ideas for mitigating security threats in IT devices. We propose separate, non-bypassable hardware **Watchdogs (WDs)** within IT devices. Executive Watchdogs (EWD) are used against malware, Content Watchdogs (CWD) against ransomware or data sabotaging, and Network Watchdogs (NWD) against spyware/backdoors. These watchdogs separate security-relevant tasks from untrusted CPUs/RAM and OS.

Watchdogs check data operations to see if the used app conforms with known/disclosed features or capabilities. An Executable Watchdog is binary hashcoding executables (incl. scripts and software libraries) and locally caches these hashcodes to protect apps against covert code modifications. Data from servers enrich these binary hashcodes, either inferred from statistics, making them graylisted, or via voluntarily shared registration data from manufacturers, making these hashcodes whitelisted.

Content Watchdogs protects user files from being overwritten by default. They focus on early damage detection, rapid threat notification, and damage mitigation with late repair for maliciously damaged user content. A Network Watchdog detects covert or unknown network utilization by apps and stops data exchange as an independent device firewall; it checks for unknown patterns to reveal covert data piggybacking on existing data exchange protocols.

Watchdogs isolate security-relevant algorithms. They are being put outside the reach of regular (versatile/ dynamic) algorithms. Because only binary hashcoded, white-/graylisted executables are allowed, unknown code is not accepted in RAM or by the CPU. Therefore, only known and trusted software could (theoretically) exploit vulnerabilities, which would have severe consequences for manufacturer's reputation once detected.

Sent or received watchdog data must be trustworthy, i.e., authentic and unmodifiable during transmission to/from servers and during execution. This goal can only be accomplished if we are certain that used crypto-keys/devices cannot be stolen, misused, or simulated. Crypto-key protection implies that any cleartext key within a CPU must be flagged as compromised immediately, including public keys. Keys are stored in key safes accessible/processed by protected Encryption/Decryption Units only. Secret public keys require hashcode references to be downloaded. Only hardware with keys to trusted key repositories can access these keys. Key secrecy is thereby be used as (irrefutable) proof that watchdogs have dedicated hardware and are not a (perfect) software simulation.

With Multi-Unit Security, security components are watching each other, inter-guarding themselves if their software was modified or misused. Because of Multi-Unit-Security, software updates happen safely and transparently. With a basic key safe encryption, we are assured of data exchange security and watchdog's code integrity. Unbreakable communication between humans is facilitated with enhanced key safe encryption, but court-issued warrants must provide a side door for legitimate eavesdropping. Additionally, irrefutable evidence is generated/logged to allow the protection of eCommerce and logistics to prove that transactions were validly done by or for users.

All watchdog and key-safe-related activities are fully automated. These processes provide low-cost/effort auto-reporting and investigations of suspicious events without human involvement. Cybersecurity should guide/help/protect people with inherent (often unavoidable) vulnerabilities and not involve humans in operational security tasks, including software updates. Software developers can be trusted for automation; their disclosures about their products could be used to help detect (redundantly) malware.

Hardware watchdogs are primarily required to protect crypto-keys and ensure that software on the CPU related to the watchdog is not being bypassed or manipulated by attackers. Software-based watchdog units on the CPU are feasible but less safe. They are likely sufficient as (quick) retrofits against human criminals and potentially against nation-states' cyber-warfare efforts. Software-based watchdogs are realized as hypervisors similar to hooksafe technology that has successfully eliminated rootkits. Software-based watchdogs are likely insufficient against advanced adversaries like Artificial Superintelligence. At least an external hardware retrofit, e.g., within a Security Stick on an external USB port, would need to be used to protect crypto-keys and to confirm the integrity of the hypervisor software using raw/low-level validation interfaces. This Security Stick is linked to other Multi-Unit-Security components, preventing covert modification from any tool used in cyber-warfare or later by super-smart AI.

More info: https://NoGoStar.com

© **Erland Wittkoetter, PhD.** MMXXII **info@nogostar.com**