MAC Security Kernel-based OS
Dramatically Mitigates Software Supply Chain Attacks [1]

Aesec Corporation Position Paper

The supply chain cybersecurity problem can be solved with inherently secure engineering. Current futile efforts to keep an adversary out of a system can be replaced by a secure architecture that dramatically constrains the ability of an adversary who planted attacks (e.g., Trojan horses) inside a system to compromise sensitive information. Below is a brief analysis of how a Trusted Computer System Evaluation Criteria (TCSEC) Class A1 operating system would solve the four specific cybersecurity vulnerabilities experts say were exploited in the SolarWinds attack These seem reflective of other software supply chain attacks, including massive data breaches and cyber physical on Industrial Control Systems (ICS) in the critical infrastructure. Even if implemented after such an attack, the properly configured Class A1 OS prevents exfiltration of information.

Vulnerability #1: Lack of a threat model for mitigating software subversion attack. "I don't know of any organization that incorporates what a supply chain attack would look like in their environment from a threat modeling perspective," David Kennedy, former National Security Agency (NSA) hacker and founder of security consulting firm TrustedSec, told CSO. “This is not a discussion that's happening in security today.”

> Class A1 OS solves this. Addressing supply chain attacks is a *raison d’etre* for TCSEC Class A1. Because commercial OSs were developed by uncleared personnel, NSA created security criteria and evaluation procedures known as TCSEC Class A1. The core technology is the Reference Monitor, and its hardware, firmware and software implementation is defined as a Security Kernel. Class A1 is so rigorous that it would enable NSA to buy a Security Kernel-based OS from even the KGB (now the SVR), according to George Cotter, founding director of the National Computer Security Center. Class A1 substantially addresses subversion (NIST SP800-160v1), and TCSEC has at least eight specific requirements unique to Class A1 to defeat software subversion (i.e., supply chain) attacks.

Vulnerability #2: Pervasive impact on deployments due to a failure to keep the adversary out. “An attacker could literally select any target that has their product deployed,” Kennedy said.

> Class A1 OS solves this. Pervasive mitigation from a single Class A1 Trusted Device embodies a Class A1 Security Kernel-based OS with trusted distribution for wide availability. Failure at a single installation (e.g., swapped Ethernet cables, or modification of hardware) does not invalidate the Class A1 Trusted Device’s ability to defeat subversion for other deployments.

Vulnerability #3: No security categorization for which to enforce mandatory access control policy. “Not every user or device should be able to access any application or server on the network,” Kennedy continued. Exploiting the lack of categorization was key to the SolarWinds attack, however. The vague, mushy advice that “companies should try to put controls in place that would minimize the impact” the article advocates is hardly actionable mitigation.

> Class A1 OS solves this. Class A1 defines mandatory access controls with mathematical precision and is applicable to many specific categorization policies for users and devices such that it is scientifically possible to put in place systematically enforceable controls. A Class A1 Trusted Device can be configured for the specific categorization policy of an infrastructure or deployment in a trustworthy and inspectable manner. This effort can benefit from the long-recognized need described in FIPS 199 “for categorizing federal information and information systems according to an agency's level of concern for confidentiality, integrity, and availability and the potential impact on agency assets and operations should their information and information systems be compromised through unauthorized access, use, disclosure, disruption, modification, or destruction.” The MAC

[1] A previous version of this Position Paper originally appeared in the Government Computer News, Roger R. Schell, March 01, 2010, “**Inherently secure systems mitigate software supply chain attacks**”

> policy has a formal security policy model with a mathematical proof that no Trojan horse (no matter how ingeniously designed and surreptitiously inserted) can cause information flow in violation of the configured Class A1 Security Kernel-based OS policy.

Vulnerability #4: Cannot verify that no backdoor exists or remains. "Software supply-chain attacks are some of the hardest type of threats to prevent," CSO said. "It's likely that the number of software supply-chain attacks will increase in the future, especially as other attackers see how successful and wide ranging they can be." According to security expert and Harvard fellow Bruce Schneier, the only way to be sure a network is clean is "to burn it down to the ground and rebuild it." Former homeland security adviser Thomas Bossert agreed. "A 'do over' is mandatory and entire new networks need to be built," he wrote in the New York Times. To start over, however, would take decades and many billions, and there would be little basis for confidence that some clever adversary's attack was not already somewhere in the massive attack surface of the rebuilt software.

> Class A1 OS solves this. It renders previously implanted Trojan horses or "backdoors" that remain in application software incapable of exfiltrating data in violation of MAC it verifiably enforces. A Class A1 OS is also specifically designed and constructed so that evaluators can confirm that no backdoor or other malware exists in the OS itself. "The most effective approach to evaluating the security of complex systems is to deliberately construct the systems using security patterns specifically designed to make them evaluable," wrote Mark Heckman, professor of computer science and cyber security at University of San Diego. "Just such an integrated set of security patterns was created decades ago based on the Reference Monitor abstraction . . . repeatedly and successfully used to create and evaluate some of the most secure government and commercial systems ever developed." He is specifically talking about Class A1 OS. Its maturity is demonstrated by at least a half dozen security kernel-based OSs running for years in the face of nation-state adversaries without a single reported security patch. NIST SP800-160v1 recently highlighted examples of "systems that have been verified to be highly resistant to penetration from determined adversaries."

"The magnitude of this national security breach is hard to overstate," Bossert said. But we should not be surprised by this sort of attack, as it is the nearly inevitable consequence of the lack of action for many years. The concern for this eventuality was clearly stated by former NSA Director Lt. Gen. Lincoln Faurer in 2007 when he provided the following conclusion to seniors at NSA:

> "Our team remains convinced that an IC disaster looms (e.g., we discover that an unfriendly state has obtained access to our most sensitive information) unless we proceed post haste to implement what NSA previously defined as a Class A1 Trusted Computing Base (TCB) in our sensitive network components and our electronic credentials. We believe the urgency of this need demands that the first set of solutions directly leverage the designs, architectures and rating maintenance plans which NSA has previously evaluated at the Class A1 level of assurance, as this is the only practical way to be confident the needed solutions can be operationally deployed in the next couple of years."

Conclusion: System-level problems require system-level solutions. Class A1 OS with verifiably enforced MAC provides the basis for the secure composition of systems and networks of systems. Even threats from insider hostile systems and applications can be effectively mitigated with well known, clearly defined, consistently enforced system-level MAC policies. A Government Computer News article published in 2021 describes how massive breaches that lead to disclosures of customer and business information, as well as ransomware attacks can be effectively mitigated using more effective system-oriented architectures. Class A1 MAC is also useful protecting the integrity of critical infrastructure control systems settings and processes against destructive attacks, as revealed in a Purdue CERIAS presentation in 2020.

Point-level design and evaluation criteria (modules, components) are inadequate. System-level criteria, such as TCSEC (including Trusted Network Interpretation) provides, are essential for achieving system-level software supply chain security.