Trust-based Resillient Intrusion Detection System (TRIDS)

Idee: Der mit Abstand meistgenutzte Angriffsvektor von Schadsoftware zur Infektion eines Systems stellt die sogenannte Binary-Exploitation dar: der Kontrollfluss einer Software (Anwendung oder Betriebssystemteile) wird durch geschickte Manipulation derart modifiziert, dass durch Ausnutzung einer Schwachstelle innerhalb des regulären Programmablaufs in eine zuvor eingebrachte Schadsoftware - ggf. nur einen Teil einer Schadsoftware (Loader) - verzweigt wird; die Integrität des Kontrollflusses einer Software wird verletzt (control flow intergity breach). In diesem Beitrag wird eine Technik präsentiert, die diese Kontrollfluss-Verletzungen erkennt und vermeiden kann. Ziel dieses Beitrags ist es, zu zeigen, wie dieses Verfahren zur Angriffsfrüherkennung und Eindämmung von Schadsoftwareepidemien genutzt werden kann, damit einen signifikanten Beitrag zu einem Cyber-Lagebild liefert und so die Funktion eines verteilten Intrusion Detection Systems (IDS) übernimmt.

Stand der Forschung / Technik: Die Überwachung der Kontrollflussintegrität kann durch eine pro-aktive Erweiterung des etablierten Trusted Computing (TC) Ansatzes erfolgen, das Verfahren wurde bereits unter dem Dachbegriff „Trusted Control Flow Integrity“ [1] [2] vorgestellt und basiert auf der Nutzung von Programmmetadaten: der vollständige Kontrollflussgraph einer Software, welcher zum Zeitpunkt der Kompilierung oder spätestens zum Zeitpunkt des Bindens vorliegt, wird als Metadatum mit dem erzeugten Binary gespeichert, vor der Ausführung eines Prozesses im Trusted Platform Modul (TPM) [3] hinterlegt und während der Prozessausführung lückenlos überwacht; hierdurch wird jede Verzweigung aus dem Programmkontext heraus in eine potentielle Schadsoftware erkannt und kann durch ein angepasstes Betriebssystem unterbunden werden – sprich: herkömmliche Binary-Exploitation funktioniert in diesem Kontext nicht mehr, da der Prozess, welcher den Integritätsbruch verursacht, durch das Betriebssystem gelöscht werden kann; die Schadsoftware kommt dadurch nicht mehr zur Ausführung, gleichzeitig werden Peering-Systeme über den ein adaptiertes Trusted Network-Layer-Protokoll über den erkannten Integritätsbruch informiert. Durch ein darauf erfolgendes Black-Listing des potentiell infizierten Systems kann auch eine weitere Ausbreitung einer Schadsoftwareinfektion bereits im Entstehen eingedämmt werden, das Protokoll selbst ist durch kryptographische Mittel gegen Angriffe geschützt und auch Angriffe gegen die Verfügbarkeit werden zuverlässig erkannt. Als Fortentwicklung dieses Konzepts wurde mit Trusted Forensics [4] ein Konzept vorgestellt, in welchem der infizierte Prozess nicht mehr gelöscht, sondern lediglich angehalten und als Image forensisch gesichert wird. Hierdurch ist es möglich geworden, Schadsoftware zum Zeitpunkt der Infektion zu untersuchen, die Funktionalität zu verstehen und ggf. auf den Hersteller oder Betreiber zu schließen.

Innovation: Die o. a. Technologie kann auch als ein host-based IDS verstanden werden, welches die Integrität eines einzelnen Systems überwacht und im Falle eines erkannten Integritätsbruchs über Notifikationsmechanismen ein zentrales Lagebild speist. Die Vernetzung der Systeme mit pro-aktiven TPM kann somit auch als ein Trusted Cluster sowie bei Skalierung der Technologie auf höhere Netzwerkschichten auch als ein Trusted Network verstanden werden – bei ebenfalls theoretisch beliebiger Skalierbarkeit. Diese Lageinformationen können auf unterschiedlichen Abstraktionsebenen – im militärischen Bereich beispielsweise auf verschiedenen Führungsebenen – in entsprechenden Lagebildern zusammengefasst werden, wodurch präzise Aussagen zu Exploit-basierten Schadsoftwareangriffen und Lateral Movement möglich werden; dies ermöglicht sowohl eine Erkennen von breitbandigen Schadsoftwarekampagnen als auch gezielte Angriffe auf einzelne Systeme. Insgesamt kann somit im Modell die Gesamtheit dieser verteilten IDS auch als ein kollektives verteiltes trusted IDS mit hoher Resilienz verstanden werden – ein Trust-based Resillient Intrusion Detection System (TRIDS).

Reifegrad: SW-Demonstrator in Entwicklung, HW-Implementierung wird ggf. angestrebt, sobald sich eine Finanzierungsmöglichkeit ergibt.

Referenzen:

[1] Maybaum, M. (2015) “Trusted Control Flow Integrity“, Risiken kennen, Herausforderungen annehmen, Lösungen gestalten, SecuMedia Verlag, Gau-Algesheim, pp. 129-144.

[2] S. Z. Mei et al. (2014) "Trusted Control Flow Integrity for JVM-Based Application", Applied Mechanics and Materials, Vols. 511-512, pp. 1219-1224.

[3] Trusted Computing Group (2018) “TPM Main Specification”, [online] URL: https://trustedcomputinggroup.org/tpm-main-specification/.

[4] Maybaum, M. und Tölle, J. (2016) “Future Digital Forensics an an Advanced Trusted Environment“, Proceedings of the 15th European Conference on Cyber Warfare and Security (ECCWS2016), München, pp. 212-220.