secorvo
security consulting

Secorvo Security News

März 2019

Die Heuristikfalle

Computer lösen Aufgaben deterministisch: vorhersehbar und wiederholbar. Dafür füttern wir sie mit Lösungsalgorithmen. Für viele Probleme des echten Lebens (man könnte sagen: für alle, die diesen Titel verdienen) gibt es jedoch keine Lösungsalgorithmen. Da helfen uns bestenfalls *Heuristiken*: Dicker-Daumen-Regeln, die meist zum Ziel führen, aber nicht immer. So hindert uns die Heuristik "meide Unbekanntes", giftige Früchte zu verzehren, lässt uns aber auch vor Menschen mit fremdländischem Äußeren zurückweichen.

Nicht anders funktioniert künstliche Intelligenz, die uns jetzt allerorten begegnet. In vielen Fällen genügen da heuristische Ergebnisse - eine überwiegend richtige Übersetzung ist besser als keine, und auch für eine zu 80% zutreffende Rechtschreibkorrektur sind wir dankbar.

Aber es gibt auch Probleme, die heuristische Erfolgsquoten nicht gut vertragen. So veröffentlichte die Bundespolizei am 11.10.2018 eine Studie über die sechsmonatige Erprobung biometrischer Gesichtserkennung von Straftätern durch Videoanalyse am Bahnhof Berlin-Südkreuz. Drei Gesichtserkennungssysteme, die mit Fahndungsfotos trainiert worden waren, erreichten dabei eine durchschnittliche Trefferquote von bis zu 91,2%; die Falschakzeptanzrate (Anteil der fehlerhaft als "Gesuchter" erkannten Personen) lag bei 0,34%.

Würde das System für ein Jahr an allen Bahnhöfen eingesetzt und mit Fahndungsfotos der 175.000 per Haftbefehl gesuchten Personen gefüttert, dann könnte es - sofern die Gesuchten an wenigstens einer dieser Kamera vorbeieilen – fast 160.000 davon entdecken.

Eine beeindruckende Zahl. Allerdings würden auch 0,34% der Bahnreisenden fälschlich als Täter identifiziert: Bei jährlich 4,669 Milliarden Reisenden wären das etwa 15.875.000 Fehlidentifikationen. Die Erkennungsrate läge damit unter 1% aller Identifizierten – keine grandiose Systemleistung. Und in einer freiheitlichen Ordnung eine wohl kaum erträgliche „Unschärfe“.

Inhalt

secorvo
security consulting

Security News

Office 365 und der Cloud Act

Microsoft bietet mit Office 365 Dienste wie Sharepoint, OneDrive, Teams und Exchange sowie Anwendungen wie Outlook, Word oder Excel für Privatanwender und Unternehmen an. Zur Sicherstellung von Datensicherheit und Datenschutz verpflichtete sich Microsoft zur Umsetzung wirksamer Maßnahmen. Ab Ende 2019 wird Microsoft seine Cloud-Dienste aus Deutschland in neuen Cloud-Regionen bereitstellen, die als „deutsche Region" Teil der globalen Cloud-Umgebung von Microsoft Office 365 sein werden. Damit wird das bisherige Modell von Microsoft Office 365 Deutschland abgekündigt. In den neuen Regionen mit Rechenzentren in Berlin und Frankfurt soll die Speicherung in Deutschland erfolgen, während die Cloud-Dienste aber auch an Microsofts weltweites Cloud-Netzwerk angebunden sind. Für Dienste aus seinen neuen Rechenzentrums-Regionen verspricht Microsoft die Einhaltung der DSGVO und will sich dazu vertraglich verpflichten. Wahrscheinlich wird Microsoft durch dieses Vorgehen unter den am 23.03.2018 in Kraft getretenen Cloud Act fallen (Clarifying Lawful Overseas Use of Data Act), der US-amerikanischen Ermittlungsbehörden Zugriff auf Daten einräumt, die US-Unternehmen auf europäischen Servern speichern. Es erscheint zweifelhaft, dass sich damit die Anforderungen der DSGVO erfüllen lassen.

Reverse Engineering – powered by NSA

Am 05.03.2019 stellte Robert Joyce (NSA) auf der RSA Conference („Come Get Your Free NSA Reverse Engineering Tool!") das Reverse-Engineering-Werkzeug Ghidra vor. Das Tool, dessen Existenz 2017 mit den Wikileaks-Enthüllungen Vault 7 bekannt geworden war, steht nun unter der Apache License 2.0 zur Verfügung. Es konkurriert mit seinem Funktionsumfang und der grafischen Benutzeroberfläche mit dem kommerziellen Werkzeug IDA des Herstellers Hex-Rays, dessen Lizenzkosten jenseits der tausend Euro liegen. Natürlich drängt sich bei einer Anwendung, die die NSA entwickelt hat, sofort die Frage nach Hintertüren auf. Innerhalb weniger Stunden nach Veröffentlichung wurden auch erste gravierende Schwachstellen in Ghidra entdeckt – keine Ausnahme bei „jungen" Open-Source-Projekten –, aber bisher keine Hintertüren. Die Bugs betreffen den Umgang mit dem Debug-Server und das Laden nicht vertrauenswürdiger Extensionen. US-Regierungsstellen haben bereits 32 Projekte im Quellcode im Rahmen ihrer Initiative zum Technologietransfer publiziert; sie erhoffen sich davon eine Beteiligung der Community an der Weiterentwicklung. Zwar sollte man mit dem Einsatz von Ghidra in sensiblen Bereichen noch vorsichtig sein – dennoch ist die Veröffentlichung eine Bereicherung, denn bisher stand kein freies Werkzeug mit ähnlichem Funktionsumfang zur Verfügung.

Löchrige Container

Software ohne Abhängigkeiten ist in der heutigen Zeit kaum noch vorstellbar. Wie problematisch das aus Sicherheitssicht ist, belegt das Unternehmen Snyk in seinem diesjährigen „The State of Open Source Security Report" mit konkreten Zahlen: Die Überprüfung von mehr als einer Million Open-Source-Projekten ergab, dass 78 % der dabei erkannten Schwachstellen auf indirekte Abhängigkeiten zurückzuführen sind. Indirekte Abhängigkeiten sind solche, die von explizit eingebundenen Komponenten benötigt und automatisch mitinstalliert werden. Ein Großteil der Abhängigkeiten in Paketverzeichnissen wie npm, Maven Central oder Ruby Gems sind solche indirekten Abhängigkeiten. Deshalb ist ein klarer Blick auf die Abhängigkeiten eigener Software von großer Bedeutung. Erkennen kann man bekannte Schwachstellen in den Abhängigkeiten z. B. mit dem Scanner von Snyk.

Wenn es – wie bei Containerlösungen – darum geht, die Bibliotheken und Programme eines gesamten Betriebssystems als Abhängigkeiten für den Container zu nutzen, zeichnet sich eine ähnliche Problematik ab: Laut Snyk besitzt jedes der Top 10 Docker Images mindestens 30 bekannte Schwachstellen. Sie gehen meist auf veraltete Bibliotheken im verwendeten Docker Base Image zurück. Als Gegenmaßnahme hilft in der Regel ein Upgrade, in vielen Fällen reicht sogar ein einfacher Rebuild. Auch der Einsatz von minimalen Base Images wie z. B. Alpine Linux trägt zu einer grundlegenden Sicherheits-„Hygiene" bei.

ACME wird Standard

Automatic Certificate Management Environment (ACME) ist ein von der Internet Security Research Group (ISRG) entwickeltes Protokoll zum automatisierten Bezug von TLS-Serverzertifikaten. Es wurde am 11.03.2019 in RFC 8555 als IETF-Standard veröffentlicht. Die ISRG ist die Dachorganisation hinter dem gemeinnützigen Trustcenter Let's Encrypt, das seit 2015 über das ACME-Protokoll kostenfreie, öffentlich gültige TLS-Serverzertifikate ausstellt.

ACME-Clients mit Internet-Zugang beantragen, installieren und erneuern ihre TLS-Serverzertifikate selbsttätig und reduzieren so den Administrationsaufwand erheblich. Auch der Nachweis, dass der Antragsteller berechtigt ist, ein öffentlich gültiges

DV-Zertifikat für den gewünschten Host-Namen zu erhalten, ist im ACME-Protokoll bereits vorgesehen.

Die nun verabschiedete Protokollversion (ACMEv2) schafft Planungssicherheit für die Entwickler alternativer Client- und Server-Implementierungen sowie für andere Trustcenter, die es ihren Nutzern ermöglichen wollen, ohne Änderung der bereits etablierten Prozesse und der Client-Software die Zertifizierungsstelle zu wechseln. Proof of Concept: Let's Encrypt selbst hat über ACMEv2 bereits mehr als 70 Millionen TLS-Serverzertifikate ausgestellt.

DSFA leicht gemacht?

Zum 01.03.2019 hat der Bayerische Landesbeauftragte für den Datenschutz (BayLfD) einen Hinweis auf das PIA-Tool (Privacy Impact Assessment) der französischen Datenschutzbehörde CNIL veröffentlicht. Das Tool ist nicht neu, aber inzwischen auch in deutscher Sprache verfügbar und soll Verantwortlichen die Durchführung von Datenschutz-Folgenabschätzungen (DSFA) erleichtern. Die Oberfläche ist recht benutzerfreundlich und man kann die Folgenabschätzung Schritt für Schritt vornehmen. Die CNIL bietet weitere Hinweise zum Tool samt Youtube-Erklärvideo in englischer Sprache. Allerdings gibt es auch andere, teils komplexere Ansätze als die Methodik der CNIL zur Durchführung von DSFAs.

Eine Herausforderung wird durch die Software jedoch nicht gelöst: die Schwellwertanalyse, mit der vor der Durchführung einer DFSA geprüft wird, ob es sich bei dem abzuschätzenden Prozess tatsächlich um eine „Hochrisikoverarbeitung" handelt. Häufig werden DSFA daher vorsorglich durchgeführt. Um diesen Prozess zu erleichtern, hat der BayLfD eine überarbeitete Orientierungshilfe für Datenschutz-Folgenabschätzungen inklusive Prüfschema veröffentlicht. In der Theorie ist eine DSFA samt Vorprüfung also gar nicht so schwierig – ob sich dies auch so einfach in die Praxis umsetzen lässt, muss sich erst noch erweisen.

OWASP ASVS 4.0

Am 01.03.2019 hat das Open Web Application Security Project (OWASP) Version 4 des Application Security Verification Standard herausgegeben. Im Vergleich zur Vorversion haben sich viele Änderungen ergeben; die inhaltlich bedeutendste ist der Bezug auf NIST 800-63-3 Digital Identity Guidelines für die Abschnitte zu Authentisierung und Session Management, sowie PCI DSS – ein Audit nach ASVS Level 1 deckt die Anforderungen in Abschnitt 6.5 aus PCI-DSS 3.2.1 Abschnitt 6.5 ab. Neu ist auch der Bezug aller Prüfpunkte auf die Common Weakness Enumeration Identifier (CWE) – sehr nützlich für Tester, denn die einzelnen Prüfpunkte werden (wie in den vorangegangenen Versionen) nicht näher erläutert, obwohl einige dieser Punkte durchaus erklärungsbedürftig sind. Darüber hinaus wurde der Abschnitt zu Mobile Security gestrichen, da mittlerweile ein eigener Mobile Application Security Verification Standard (MASVS) existiert. Ebenfalls gestrichen wurde Level 0 ("Cursory"). Mit dem ASVS 4 wurden alle Punkte neu durchnummeriert; zusätzlich wurde eine neue Gliederungsebene eingeführt, da einige Abschnitte im Laufe der Zeit stark angewachsen und unübersichtlich geworden sind. Leider wurde auch die farbliche Unterscheidung der Punkte nach zugehörigem Level abgeschafft; für die Zuordnung eines Prüfpunkts zum Level muss man jetzt genauer hinsehen. Dennoch haben diese Überarbeitungen, vor allem die Anbindung an andere bekannte Werke, dem ASVS sehr gut getan und dürften die Akzeptanz bei Auftraggebern und Testern weiter erhöhen.

Secorvo News

T.I.S.P. und T.P.S.S.E.

Mit deutlich über 1.000 Absolventen ist der T.I.S.P. inzwischen eine nicht nur anerkannte, sondern auch weit verbreitete Berufsqualifikation für IT-Sicherheitsexperten. Das nächste T.I.S.P.-Seminar mit anschließender Zertifikatsprüfung bieten wir Ihnen am **13.–17.05.2019**. In der Woche davor (**06.–09.05.2019**) haben Sie die Gelegenheit, sich als T.P.S.S.E. (TeleTrusT Professional for Secure Software Engineering) zu qualifizieren.

Die detaillierten Seminarprogramme und eine Möglichkeit zur Online-Anmeldung finden Sie hier.

Kaltblütig.

Zum Schutz vor unberechtigtem Datenzugriff bieten Microsofts BitLocker und Apples FileVault deren Verschlüsselung – für mobile Geräte im geschäftlichen Umfeld oft eine Compliance-Anforderung. Nur wer das Passwort kennt, kommt an die Daten heran. Dass dies ein Irrglaube ist, haben Sicherheitsforscher bereits 2008 gezeigt: Hatten sie physischen Zugriff auf einen lediglich gesperrten oder „schlafenden" (Bereitschaftsmodus) Computer, konnten sie das Passwort aus dem Arbeitsspeicher auslesen. Zehn Jahre nach dieser Entdeckung sind die sogenannten Cold-Boot-Angriffe noch immer möglich. Beim nächsten KA-IT-Si-Event am **11.04.2019** werden Andreas Sperber und Daniel Matesic (aramido) live einen solchen Angriff auf einen Computer mit Festplattenverschlüsselung vorführen.

Im Anschluss haben Sie, wie gewohnt, Gelegenheit zum fachlichen und persönlichen Austausch beim „Buffet-Networking" (Anmeldung).

Veranstaltungshinweise

Auszug aus http://www.veranstaltungen-it-sicherheit.de

April 2019	
11.-12.04.	Security Forum 2019 (Hagenberger Kreis zur Förderung der digitalen Sicherheit, Hagenberg/AT)
24.-26.04.	DFRWS EU Conference (DFRWS, Oslo/NOR)
Mai 2019	
06.-09.05.	T.P.S.S.E. – TeleTrusT Professional for Secure Software Engineering (Secorvo, Karlsruhe)
13.-17.05.	T.I.S.P. – TeleTrusT Information Security Professional (Secorvo, Karlsruhe)
19.-23.05.	Eurocrypt 2019 (IACR, Darmstadt)
21.-23.05.	16. Deutscher IT-Sicherheitskongress (BSI, Bonn)
22.-23.05.	20. Datenschutzkongress (EUROFORUM Deutschland SE, Berlin)
26.-30.05.	OWASP AppSec Tel Aviv 2019 (OWASP Foundation, Tel Aviv/ISR)
Juni 2019	
03.-05.06.	Entwicklertag 2019 (VKSI, GI, ObjektForum, Karlsruhe)
03.-04.06.	DuD 2019 (COMPUTAS Gisela Geuhs GmbH, Berlin)

Fundsache

Über 140 Mal taucht „ji32k7au4a83“ in Datenbanken kompromittierter Passwörter auf. Was auf den ersten Blick verwundert, hat eine simple Erklärung: Im taiwanesischen Zeichenschema lautet der vermeintliche Zufallsstring übersetzt „Mein Passwort“.

Impressum

http://www.secorvo-security-news.de

ISSN 1613-4311

Autoren: Dirk Fox (Editorial), André Domnick, Dr. Safuat Hamdy (Gastautor), Hans-Joachim Knobloch, Sarah Niederer, Jannis Pinter, Friederike Schellhas-Mende, Christian Titze

Herausgeber (V. i. S. d. P.): Dirk Fox,
Secorvo Security Consulting GmbH
Ettlinger Straße 12-14
76137 Karlsruhe
Telefon +49 721 255171-0

Zusendung des Inhaltsverzeichnisses: security-news@secorvo.de
(Subject: „subscribe security news“)

Wir freuen uns über Ihr Feedback an redaktion-security-news@secorvo.de