Auch biometrische Venenerkennung überwindbar

Sicherheits-attrappe

Jörg Riether

Was bleibt noch, wenn sich selbst die sicher geglaubte Venenerkennung überlisten lässt? Bei der IT-Defense suchte man Antworten.

Die auf IT-Sicherheit fokussierte und mit mehr als 250 Besuchern ausgebuchte Fachkonferenz IT-Defense fand diesmal Anfang Februar in Stuttgart statt. Die alte Frage nach dem Nutzen für bösartige Individuen beantwortete Roger Dingledine vom Tor-Projekt in Stuttgart so, dass die guten Menschen Tor weitaus dringender benötigen würden als die bösen. Überdies hätten Letztere in der Regel völlig andere Anforderungen an ein solches System – etwa ein proprietäres Spezialwerkzeug für wenige Nutzer, das weder global verteilt noch für viele Millionen Nutzer ausgelegt sei. Zudem würden die versteckten Dienste im Tor-Netzwerk (Onion Services) nur etwa 3 % des Datenverkehrs ausmachen, und der meistbesuchte dieser Dienste sei Facebook.

Die Authentizität versteckter Dienste sowie die Verschlüsselung innerhalb von Tor gilt als sicher. Das Ziel von Überwachungsstellen sind daher heute vermutlich verstärkt Informationen über Beziehungen und sämtliche weiteren denkbaren Metadaten des Tor-Datenverkehrs. In den Round Tables am dritten Tag sprach Dingledine über bemerkenswerte Aspekte. So nehme er an, dass etwaige Nachrichtendienste Stand heute entweder gar keine oder wenn überhaupt nur noch sehr wenige Tor-Knoten betreiben würden. Das sei aber keinesfalls eine gute Nachricht, ganz im Gegenteil.

Es könne nämlich bedeuten, so Dingledine, dass man inzwischen andere und deutlich effizientere Möglichkeiten habe, Zuordnungen vorzunehmen, etwa Website-Fingerprinting oder sonstige hochentwickelte Deep Packet Inspection (DPI). Insbesondere Website-Fingerprinting bereite ihm schon länger Sorgen. Die Idee dahinter ist sehr vereinfacht, dass sich Überwacher in einem Labor selbst zu Tor verbinden, Millionen bekannter Webseiten aufrufen und sämtliche denkbaren Charakteristika des Datenverkehrs speichern und mathematisch analysieren. Somit könnte man beim Vergleich relativ treffsicher erkennen, wenn ein Tor-Nutzer eine dieser Seiten abrufe.

Quo vadis, Biometrie?

Jan Krissler, der 2013 durch die Überwindung des iPhone-Fingerabdruckscanners internationale Bekanntheit erlangte, beschäftigt sich derzeit mit der Erkennung von Hand- und Fingervenen. Er hatte dazu bereits auf dem 35C3-Kongress in Leipzig gemeinsam mit Julian Albrecht eine funktionale Attrappe aus einem Ausdruck kombiniert mit Bienenwachs in Form einer menschlichen Hand konstruiert (siehe *iX* 2/2019, S. 10).

Jan Krissler ist wenig optimistisch in Sachen überwindungssichere Biometrie.

Was den eigentlichen Ausdruck auf Papier angeht, das dann von der Wachsattrappe umschlossen wird, sagte Krissler in Stuttgart, dass sich mit der richtigen Wellenlänge nebst passender Kamera sehr einfach erstaunlich detaillierte Fotos der Handvenen ohne Weiteres anfertigen ließen, selbst aus sechs Metern Entfernung.

Laut Krissler kommen solche Venenerkennungssysteme auch beim BND-Neubau in Berlin zum Einsatz. Der BND habe sich nach Krisslers Vortrag Ende Dezember 2018 zahlreiche Nachfragen von Journalisten gefallen lassen müssen, sich aber nicht weiter dazu äußern wollen.

Wenn solche Venenerkennung ergo einfach fälschbar ist, scheint somit eine der letzten Bastionen der biometrischen Authentifizierung gefallen zu sein. Eine Ausnahme könnte eine echte Lebenderkennung sein, die auch tut, was sie behauptet zu tun – nämlich die Venen auf tatsächliche Bewegung des Blutflusses hin untersuchen. Jedoch gebe es auch für solche Ansätze längst Überwindungsmöglichkeiten, etwa mit einer Flüssigkeit, die via Spritze und vorgefertigter Flussbahnen eingebracht wird und so die Bewegung des Blutes simuliert, so Krissler.

Es gebe aber einen Bereich, der sich ab dato als interessant erweisen könne, nämlich die Retina-Erkennung. Bislang scheinen solche Systeme noch nicht kompromittiert oder gebrochen zu sein, zumindest ist nichts dergleichen bekannt. Krissler sagte jedoch in Stuttgart, dass die konkrete Überwindung technisch nicht zu kompliziert sein dürfte, wenn man es schaffe, an das Rohmaterial heranzukommen, das etwaige Systeme für die Verifikation benutzen. Es dürfte also nur eine Frage der Zeit sein, dass jemand auch solche Systeme überlisten wird.

Der Betreiber der Seite ad security.org, Sean Metcalf, sprach über Angriffe auf Microsofts Active-Directory-Strukturen. Er berichtete von teilweise erschreckend trivialen, aber dennoch effektiven Ideen und Methoden von Angreifern.

Angriffe auf AD

In vielen Umgebungen sehe er eine vermeintliche Sicherheit durch Administration ausschließlich über Spezialsysteme, auf die wiederum via RDP (Remote Desktop Protocol) zugegriffen werde, dies außerdem mit Multi-Faktor-Authentifizierung (MFA) abgesichert. All dies sei aber völlig nutzlos, wenn die lokale Workstation sich bereits unter fremder Kontrolle befinde. So könne man sich als Angreifer gängiger PowerShell-Angriffswerkzeuge bedienen, um etwa Tastaturanschläge aufzuzeichnen. Hier höre er oft das Gegenargument, dass man MFA einsetze. Dies sei nach aktuellem Stand zwar sinnvoll, aber bei Weitem nicht immer sicher.

Metcalf sehe in vielen Unternehmen Portale für Mitarbeiterkontaktdaten, die von den Mitarbeitern selbst gepflegt werden. In eben diesen Portalen könne man oft die Kontaktdaten aktualisieren, dazu zähle natürlich insbesondere die Mobilrufnummer. Dummerweise würden sich nicht selten weitere Systeme, so auch ein MFA-System, aus diesem Portal bedienen. So sei es ein Leichtes, die MFA-Antworten auf ein beliebiges Gerät des Angreifers zu lenken. Und selbst wenn dies nicht klappen würde, hätten nahezu alle Installationen, die er in Unternehmen sehe, konfigurierte Rückfallmöglichkeiten beispielsweise SMS oder Rückruf.

Ein weiteres vermeintliches Allheilmittel, das derzeit sehr beliebt sei, nämlich Passwortmanager für Unternehmen, sei häufig ebenso einfach angreifbar. Oft laufe es so, dass sich eine Person zu einem Passwortmanager-Webdienst im Unternehmen verbinde, wo sie dann das gesuchte Passwort herauskopiere, um es woanders wieder einzufügen. Hier könne man als Angreifer schlicht den Inhalt der Zwischenablage abgreifen. (ur@ix.de)