SCHWARTZPUBLICRELATIONS

**ERGON PRESSEMELDUNG**

# BESSERER PASSWORTSCHUTZ DANK NEUARTIGER KRYPTOGRAPHIE-TECHNOLOGIE

**Zürich/München, 15.02.2016 –** Airlock Entwickler haben IBM Research – Zürich bei der Entwicklung eines hocheffizienten kryptographischen Protokolls zum Passwortschutz im Falle von Server Kompromittierung unterstützt. Die neue Technologie wurde erfolgreich in Airlock IAM integriert und kann ab sofort als experimenteller Service von Airlock Kunden getestet werden. Mit dem neuen Verfahren wird die Passwort-Verifizierung auf mehrere Server verteilt, so dass ein Angreifer sämtliche involvierten Server kompromittieren müsste, um Informationen über das Passwort zu erhalten.

## Anforderungen an Authentifizierungssysteme

Mit dem wachsenden Angebot digitaler Dienste, die oft persönliche und sensible Daten ihrer Nutzer speichern und verarbeiten, steigen auch die Anforderungen an Authentifizierungssysteme, die den Zugriff auf diese Daten verwalten. Die Systeme prüfen die Identität der Nutzer und sind für eine erfolgreiche Validierung zuständig. Der Schutzbedarf solcher Daten ist über die Jahre deutlich gestiegen, ebenso wie das Interesse von Cyberkriminellen an diesen sensiblen Informationen. Viele Zugänge zu Online-Diensten sind mit Passwörtern geschützt, obwohl Angriffe auf Server und Webapplikationen schon fast an der Tagesordnung sind und Brute-forcing Angriffe selbst Passwörter mit Sonderzeichen knacken können. Eine solche Attacke greift die Hash-Werte der Passwörter an und probiert dank mittlerweile weit verbreiteter grosser Rechenleistung sehr viele Zeichen-Kombinationen in kürzester Zeit aus. Davor kann man sich heute nicht mehr schützen, selbst wenn den Benutzern immer strengere Anforderungen bei der Passwortwahl auferlegt werden, wie zum Beispiel mehrstellige, zufällig gewählte Zahlen- und Buchstabenkombinationen mit Sonderzeichen.

Denn das Problem liegt nicht darin, dass der Benutzer die Passwörter falsch wählt, sondern darin wie Passwörter heute gespeichert werden. Um die Sicherheit digitaler Daten zu verbessern und zu vereinfachen, hat ein Forscherteam von IBM Research – Zürich eine neuartige Passwort-Verifizierung ausgearbeitet, die nun von Ergon Informatik in Airlock IAM implementiert und getestet wurde. Das neue Protokoll geht explizit das Problem kompromittierter Passwortdatenbanken an und hat somit grosses Potenzial, den Ruf von Passwörtern zu rehabilitieren.

## Optimal verteilte Passwort-Überprüfung

Anders als bei bisherigen Systemen, wird mit der neuen Technologie jedes Passwort einzeln mit einem starken kryptographischen Schlüssel geschützt gespeichert. Dieser Schlüssel ist auf mehrere Server verteilt, so dass ein Passwort nur gemeinsam von diesen Servern mittels eines kryptographischen Protokolls verifiziert werden kann. Die Infizierung eines oder gar mehrerer Server oder die Kompromittierung der so geschützten Passwortdatenbank gibt einem Angreifer daher keine Information mehr, um das Passwort knacken zu können. Beim Verifizierungsprozess wird eine Anfrage an alle beteiligten Server gestellt, die Schlüsselfragmente besitzen. Verläuft die Echtheitsprüfung der jeweiligen Server positiv, stellen diese ihre Schlüsselfragmente bereit. Bei korrekter Kombination aus Anmeldenamen und persönlichem Schlüssel bzw. Kennwort, erfolgt die Freigabe der Daten. Das neuartige Protokoll ist auf eine hohe

**Pressekontakt Ergon**

Gernot Bekk-Huber
E-Mail: gernot.bekk-huber@ergon.ch
Phone: +41 44 268 87 21
+41 44 268 87 21

**Kontakt PR-Agentur**

Schwartz Public Relations
Sendlinger Straße 42A
D-80331 München

Sven Kersten-Reichherzer
Tel.: +49 89 211871-36
E-Mail: sk@schwartzpr.de

Praxistauglichkeit ausgelegt und kann auch mit bestehenden Cloud-Systemen wie IBM Softlayer, Amazon EC2, Microsoft Azure oder Google Compute Engine und vergleichbaren Diensten benutzt werden. Ein Kurzvideo erklärt anschaulich das Verfahren.

**Höchstmögliche Sicherheitsstufe**

Das neue Protokoll wurde erstmals im Oktober 2015 einer breiten Öffentlichkeit auf der 22. ACM Conference on Computer and Communications Security (CCS) in Denver, USA, präsentiert. Die Lösung auf höchstem Sicherheitsniveau ist mit nur einer einzigen Elliptische-Kurven-Skalarmultiplikation pro Authentifizierung und pro Server hocheffizient. Durch zukünftige Optimierung des Codes kann die Leistungsfähigkeit und Skalierbarkeit sogar noch weiter gesteigert werden. Eine Umsetzung im Prototyp-Status konnte bereits mehr als 100 Anmeldeversuche pro Sekunde auf einem einzigen Prozessorkern verarbeiten.

Weitreichende Informationen zu dem neuen Protokoll entnehmen Sie dem wissenschaftlichen Hintergrundartikel „Optimal Distributed Password Verification“: http://www.zurich.ibm.com/pdf/csc/CCS15_passwords.pdf

Website: www.ibm.biz/passwordsdoneright

**BILDMATERIAL ZUR MELDUNG**

Das Bildmaterial finden Sie im Internet in hoher Auflösung unter:
http://www.www.schwartzpr.de/de/newsroom/pressemeldung.php?we_objectID=3446&kunde=3201

**ÜBER ERGON**

Die 1984 gegründete Ergon Informatik AG ist führend in der Herstellung von individuellen Softwarelösungen und Softwareprodukten. Die Basis für den Erfolg: 240 hoch qualifizierte IT-Spezialisten, die dank herausragendem Know-how neue Technologietrends antizipieren und mit innovativen Lösungen Wettbewerbsvorteile sicherstellen. Ergon realisiert hauptsächlich Großprojekte im B2B-Bereich.

Die Airlock Suite kombiniert die Themen Filterung und Authentisierung in einer abgestimmten Gesamtlösung, die in punkto Usability und Services Maßstäbe setzt. Das Security-Produkt Airlock ist seit dem Jahr 2002 am Markt und heute bei über 300 Kunden weltweit im Einsatz. Weitere Informationen unter www.ergon.ch sowie www.airlock.com

Schwartz Public Relations · Sendlinger Straße 42A · 80331 München · Tel.: +49(0)89.211871-30 · E-Mail: info@schwartzpr.de