Zur Sicherheit von ATA-Festplattenpasswörtern

Julian Knauer[1] · Harald Baier[1,2]

Hochschule Darmstadt[1]
Fachbereich Informatik
Haardtring 100, D-64295 Darmstadt

Center for Advanced Security Research Darmstadt - CASED[2]
Mornewegstraße 32, D-64293 Darmstadt
{julian.knauer | harald.baier}@cased.de

Zusammenfassung

Festplatten in mobilen IT-Geräten wie Laptops erfordern einen besonderen Schutz der auf ihnen gespeicherten Daten, um im Falle eines Verlusts oder Diebstahls den Zugriff auf die gespeicherten Informationen zu erschweren. Auf Festplattenebene liefert der ATA-Standard die Möglichkeit, durch Vergabe eines ATA-Passworts den Zugriff auf Festplatten einzuschränken. Dieser Beitrag hat zunächst zum Ziel, diese oft ungenutzte Schutzmöglichkeit von Festplatten ins Bewusstsein zu rücken und die unterschiedlichen ATA-Passwortarten vorzustellen. Zentraler Gegenstand dieser Veröffentlichung ist dann eine Diskussion des Sicherheitsniveaus des ATA-Passwortschutzes. Dazu evaluieren wir die verfügbaren Produkte oder Dienstleistungen zu dessen Deaktivierung. Schließlich zeigen wir exemplarisch an Hand einer Festplatte des Herstellers Samsung, dass wir per Zugriff über die Diagnoseschnittstelle der Festplatte ohne weitere Kosten den Passwortschutz ausschalten konnten. Im Ergebnis bedeutet dies, dass ATA-Passwörter im besten Fall Schutz gegen kenntnisarme Angreifer bieten.

1 Einleitung

Im Informationszeitalter kommt dem Schutz von elektronisch gespeicherten Informationen eine immer höhere Bedeutung zu. Gerade Daten auf mobilen Endgeräten müssen geschützt werden, da hier ein unautorisierter physischer Zugriff auf den Datenträger durch Diebstahl oder Verlust wahrscheinlicher ist als bei klassischen stationären IT-Systemen wie Servern oder PCs.

Ein möglicher Weg, Daten auf Festplatten vor unbefugten Zugriffen zu schützen, ist das Einrichten des AT Attachment (ATA) Passwortschutzes. Seit dem ATA-Standard 3 [T1397] existieren mit dem *Security Feature Set* eine Reihe von ATA-Befehlen, die sicherheitsrelevante Funktionen bereitstellen. Sind sie aktiviert, verweigert die Festplatte den Zugriff auf die Daten per ATA-Protokoll. Erst nach Eingabe des korrekten Passworts wird der Zugriff auf den Datenbereich der ATA-Festplatte freigegeben.

Die für das Security Feature Set gespeicherten Datenstrukturen werden in der *Service Area* der Festplatte gespeichert [Rosc03]. Dieser Bereich liegt außerhalb des durch den Nutzer per ATA adressierbaren Speicherbereichs und ist nur für die Firmware der Festplatte les- bzw. schreib-

bar. Neben den Informationen des Security Feature Set speichert die Service Area auch wichtige Geräte-spezifische Informationen wie z.B. Listen über defekte Sektoren [Vids06, Mess99, Tony07] oder Werte der *Self-Monitoring Analysis and Reporting Technology* (SMART). Mit SMART werden wichtige Parameter der Festplatte überwacht. Es kann Aufschluss über die Gesundheit des Gerätes liefern, wie z.B. Lese-/Schreibfehler melden, die Temperatur überwachen und die Anzahl der aktiven Betriebsstunden der Festplatte speichern [T1397].

Ausgangspunkt der vorliegenden Veröffentlichung ist die Frage, wie schwer es ist, auf den Datenbereich einer passwortgeschützten ATA-Festplatte zuzugreifen, wenn das zugehörige Passwort nicht bekannt ist. Als Metrik für den Schwierigkeitsgrad verwenden wir die Kosten in EUR, die zur erfolgreichen Umgehung des ATA-Passwortschutzes notwendig sind. Typische Anwendungsfälle sind neben Angriffen durch unautorisierte Personen auch IT-forensische Untersuchungen oder schlicht das Vergessen des Passworts durch den Besitzer der Festplatte. In diesem Fall ist das ATA-Passwort zu deaktivieren [Vids06].

ATA-Passwörter können relativ einfach gesetzt und verändert werden. Neben dezidierten Software-Lösungen (z.B. `hdparm`) kann man insbesondere für mobile IT-Geräte wie Laptops das BIOS zum Setzen, Verändern oder Deaktivieren des ATA-Schutzes verwenden. Allerdings ist diese Schutzfunktion relativ unbekannt. Nach persönlichen Gesprächen mit praktisch erfahrenen Forensikern und Strafverfolgern, liegt nach deren Einschätzung, die Rate von per ATA-Passwörtern geschützten Festplatten unter 1%. Auch das Fehlen von Publikationen zu diesem Thema zeigt die geringe Verbreitung dieses Schutzmechanismus.

Unser erstes Ziel dieser Publikation ist daher, diesen Schutzmechismus in das Bewusstsein der Nutzer zu rufen. Hintergrund ist, dass der Besitzer der Festplatte sich so gegen kenntnisarme Angreifer (z.B. Diebe, die das entwendete IT-System direkt weiterverkaufen) schützen kann.

Unser zweites Ziel ist die Frage, mit welchen Kosten eine Deaktivierung des ATA-Passwortschutzes verbunden ist. Es gibt verschiedene kommerzielle Produkte oder Dienstleister (z.B. professionelle Datenrettungsunternehmen), die eine Deaktivierung des ATA-Passwortschutzes versprechen. Diese Dienstleister verfügen meist über das technische Equipment und auch das Wissen, den Schutzmechanismus zu entfernen. Für den Auftraggeber (z.B. Angreifer, IT-Forensiker) ist dies mit Kosten für eine erste Analyse des Datenträgers verbunden, für die eigentliche Wiederherstellung der Daten fallen in der Regel zusätzliche Kosten an. Eine spezielle Option sind Online-Services [AFF12], die mit kostengünstigen Angeboten ebenfalls versprechen, den Passwortschutz der gesperrten Festplatte zu entfernen. Bei einmaliger Nutzung fallen dafür ca. $50 an, um ATA-Passwörter zu entfernen. Diese Kosten zeigen, dass ATA-Passworte keinen Schutz für sensible Daten gegen gezielte Angriffe bieten.

Unser dritter und technisch interessantester Beitrag ist die Darstellung einer eigenen Methode zur Umgehung des ATA-Passwortschutzes. Dazu verwenden wir eine undokumentierte Diagnoseschnittstelle, die bei einigen Festplattenmodellen verschiedener Hersteller zu finden ist. Auf die Schnittstelle wurden wir durch Vortrag „*Data Recovery Techniques*“ [Fran10] auf dem 27. Chaos Communication Congress aufmerksam. Per RS-232 Pegelwandler [MAXI] kann eine Terminalverbindung zwischen unserem PC und der zu entsperrenden Festplatte hergestellt werden, die so einen direkten Zugriff auf die Firmwaredaten über eine Eingabekonsole bietet. Mittels Reverse-Engineering ist es uns gelungen, die Konfigurationsstruktur einer Samsung Festplatte zu analysieren und sicherheitskritische Module zu identifizieren und zu manipulieren. Die Kosten für dieses Vorgehen liegen bei unter 10 EUR. Damit wird erneut bestätigt, dass ATA-Passworte keinen Schutz gegen gezielte Angriffe bieten.

Der Artikel ist wie folgt gegliedert: In Abschnitt 1 beschreiben wir die technischen Grundlagen des ATA-Passwortschutzes. Anschließend diskutieren wir in Abschnitt 2 mögliche Angriffsvektoren auf Festplattenpasswörter. Im zentralen Abschnitt 3 evaluieren wir die verschiedenen Deaktivierungsmöglichkeiten für ATA-Passwörter und stellen unseren Zugriff über die Diagnoseschnittstelle vor. Abschließend fassen wir unsere Ergebnisse in Abschnitt 4 zusammen und geben einen kurzen Ausblick.

Dieser Abschnitt erläutert die Grundlagen zu ATA-Passwörtern. Im ATA-Standard [T1308] wird zwischen zwei verschiedenen Passworttypen unterschieden: Dem *User Password* und dem *Master Password*. Jedes der beiden Passwörter kann 32 Zeichen lang sein und für jedes Zeichen kann ein ASCII-Wert zwischen 1 und 255 gewählt werden (d.h. $c \in \{0x01, 0x02, \cdots, 0xFF\}$ für jedes Zeichen c). Der ASCII-Wert $0x00$ ist nicht als Passwortzeichen zulässig, er markiert das Ende der Zeichenkette.

Zusätzlich bestimmt das Sicherheitsniveau (auch *Master Password Capability* genannt), welche der `SECURITY`-Befehle in Kombination mit dem Master Password erlaubt sind. Zum Zeitpunkt der Auslieferung der Festplatte muss der Hersteller ein beliebiges Master Password setzen. Um den Zugriffsschutz zu aktivieren, setzt der Benutzer ein User Password. Nach dem nächsten Aus- und Einschalten der Festplatte ist der Zugriff auf die Festplatte nur stark eingeschränkt erlaubt. Zum Entsperren der Festplatte wird der ATA-Befehl `SECURITY UNLOCK` an die Festplatte gesendet. Der Befehl enthält den Typ des Passworts und das Passwort selbst. Stimmt das Passwort mit dem gespeicherten Passwort überein, wird die Zugriffssperre aufgehoben und der `SECURITY UNLOCK` Befehl wie folgt dargestellt ausgeführt. Tabelle 1 gibt einen Überblick über die sicherheitsrelevanten Befehle, die nach Eingabe des Master Passwords im jeweiligen Sicherheitsniveau ausgeführt werden. Wir erläutern dies im Folgenden.

				SECURITY COMMAND		
Security Enabled	**Master Password Capability**	**Passwords defined**	**Password supplied**	**SET PASSWORD**	**UNLOCK**	**ERASE UNIT**
No	N/A	Master only	Correct Master	N	N	P
No	N/A	Master only	Not Valid	A	A	A
Yes	High	Master and User	Correct Master	P	P	P
Yes	High	Master and User	Correct User	P	P	P
Yes	Maximum	Master and User	Correct Master	A	A	P
Yes	Maximum	Master and User	Correct User	P	P	P

Key: N NOP, do nothing
A Return command aborted
P Process the command (if valid password supplied) otherwise return aborted

Tab. 1: Berechtigungen des *Master Password* [T1308]

Solange die Master Passwort Capability auf *High* gesetzt ist, gibt es im Verhalten zwischen dem User Password und dem Master Password keinen Unterschied. Beide Passworttypen können in diesem Fall dazu eingesetzt werden, die Festplatte zu entsperren oder ein sicheres Löschen mittels `SECURITY ERASE UNIT` des Datenträgers zu veranlassen und damit die Sicherheitsmechanismen zu deaktivieren und zurückzusetzen. Da in diesem Fall alle HDD Blöcke,

beginnend ab LBA 0 bis zum Maximum, das durch den Befehl `READ NATIVE MAX` ermittelt wird, mit dem Wert $0x00$ überschrieben werden. Dadurch gehen alle Benutzerdaten verloren. HDD Blöcke die von der Firmware während des Betriebs als defekt makiert wurden, werden dabei nicht berücksichtigt. Hersteller haben die Möglichkeit einen erweiterten Modus für den `SECURITY ERASE UNIT` zu implementieren. Im Gegensatz zu dem herkömmlichen überschreiben der HDD Blöcke mit $0x00$, steht es dabei dem Hersteller frei mit welchem Wert er die Blöcke überschreibt. Während des löschens werden so alle Blöcke von LBA 0 bis zum Maximum, das per `DEVICE CONFIGURATION IDENTIFY` ermittelt wird, überschreiben. Es wird außerdem versucht alle Blöcke zu überschreiben, die während des Betriebs als defekt makiert wurden.

Ist die Master Password Capability auf *Maximum* gesetzt, unterscheidet sich das Master Password in seinem Verhalten von dem User Password. Das Master Password kann nun nicht mehr dazu verwendet werden, den `SECURITY UNLOCK` Befehl auszuführen. Die einzigen ausführbaren ATA-Befehle sind `SECURITY ERASE PREPARE` und `SECURITY ERASE UNIT`. Der erste Befehl muss vor dem eigentlichen Löschbefehl gesendet werden, um ein versehentliches Löschen zu verhindern.

2 Angriffsvektoren auf Festplattenpasswörter

In diesem Abschnitt stellen wir die aus unserer Sicht relevanten vier Angriffe auf den ATA-Passwortschutz dar und diskutieren jeweils die Machbarkeit: Verwendung eines Default Master Passwords, Austausch des Festplattencontrollers, klassisches Passwortbrechen (z.B. Wörterbuchangriff, Brute-Force) sowie Deaktivierung des Passwortschutzes.

Wir stellen zunächst den Angriff per Default Master Password dar. Da Festplatten zum Zeitpunkt ihrer Auslieferung durch den Hersteller ein gesetztes Master Password haben müssen, finden sich im Internet Listen mit möglichen Standardpasswörtern [anon08], Samsung verwendet als standard Master Password 32 „t“, gängig sind aber auch 32 Leerzeichen. Dabei sind jedoch einige Randbedingungen zu berücksichtigen. Solange das Sicherheitsniveau für das Master Password auf High gesetzt ist, können diese Passwörter zur Entsperrung genutzt werden – ansonsten ist nur noch ein `SECURITY ERASE UNIT` gestattet. Außerdem verlieren die Passwörter ihre Gültigkeit, sobald der Benutzer ein eigenes Master Password setzt. Als letzter Punkt soll auch erwähnt sein, dass sich die Passwörter mit jeder neuen Fesplattenserie und -modell ändern können. Es gibt keine Garantie, dass die Passwörter funktionieren. Die Existenz dieser Standardpasswörter konnte von uns durch die in Kapitel 3.3 dargestellte Analyse der Firmware nachgewiesen werden. Samsung speichert in einigen ihrer Festplatten das Default Master Password im Klartext in der Service Area ab.

Zweiter möglicher Angriffsvektor ist der Austausch des Controllers. Wenn ATA-Passwörter nicht in einem EPROM auf dem Controller der Festplatte gespeichert werden, sondern in der Service Area, ist es nicht möglich, durch den Austausch des Controllers die Festplatte zu entsperren. Für das von uns verwendete Samsung Modell bestätigten wir diese Annahme durch Verwendung von zwei baugleichen Festplatten vom Typ SP2504C P120S. Eine der Festplatten wurde mittels `SECURITY SET PASSWORD` gesperrt. Im Anschluss wurde der Controller der nicht gesperrten Festplatte mit dem der passwortgeschützten Festplatte getauscht. Die Zustände der Festplatten blieb unverändert.

Ein klassischer Passwortangriff (z.B. Wörterbuchattacke oder Brute-Force Angriff) auf Fesplattenpasswörter ist grundsätzlich möglich, die Erfolgschancen in der Praxis aber gering. Der

ATA-Standard bietet einen guten Schutz gegen diese Art des Angriffs. Dies liegt einerseits daran, dass der Festplatten-Controller nur maximal fünf Versuche des `SECURITY UNLOCK` Befehls zulässt – mit jedem Versuch wird ein Zähler inkrementiert; ist das Limit erreicht, werden die Sicherheitsfunktionen der Festplatte eingefroren, bis sie einmal komplett aus- und eingeschaltet wurde (mit jedem Einschalten wird der interne Zähler zurückgesetzt). Andererseits führt ein ständiges Aus- und Einschalten der Festplatte zu einem Verschleiß der mechanischen Bauteile und verringert die Lebensdauer des Gerätes.

Art des Ausschaltens	**Anzahl der Zyklen**
software-controlled	600.000
hard	20.000

Tab. 2: Anzahl der Aus-/Einschaltzyklen (lt. SeagateTechnology2007)

Wichtig für diese Betrachtung ist der Verschleiß durch den Ein-Ausschalte-Prozess. Ein „*software-controlled*“ Ausschalten schont die Mechanik der Festplatte, das Gerät ist in der Lage, sich in einen sicheren Zustand zu begeben, wo Lese-/Schreibköpfe geparkt werden und der Motor der Spindel sich ausschaltet. Bei einem „*hard*“ Ausschalten wird die Stromzufuhr zum Gerät unterbrochen. Die Lese-/Schreibköpfe können so über dem Datenträger verharren. Da nicht alle Hersteller Zahlen darüber liefern, wie viele Zyklen die Festplatte verträgt, werden repräsentativ für gängige Desktopfestplatten in Tabelle 2 Werte genannt, die aus dem Handbuch der Seagate Momentus 7200.2 Serie stammen [Seag07]. Über diese Werte hinaus ist mit einem Versagen der Hardware zu rechnen. Im Falle eines Software-kontrollierten Ausschaltens können statistisch bis zu $5 \cdot 600.000 = 3\,\mathrm{Mio}.$ Passwörter ausprobiert werden.

Neben der physischen Belastung für die Festplatte, sollte auch der zeitliche Aufwand berücksichtigt werden. Die einzelnen Ein- und Ausschaltzyklen benötigen je nach Festplatte mehrere Sekunden. Einen kompletten Zyklus mit unserer Testfestplatte vom Typ SP2504C P120S haben wir einen durchschnittlichen Wert von $6,324$ Sekunden ermittelt. Gemessen haben wir dazu die Zeit bis die Festplatte ausgeschaltet ist, beginnend ab dem ausschalten bis zum abklingen des Motorgeräusches. Dazu haben wir den SMART-Wert *Spin_Up_Time* addiert. Dieser liefert die Zeitspanne, die die Festplatte benötigt um Betriebsbereit zu sein [T1308].

Um die Dauer eines Brute-Force-Angriffs auf ein Passwort mit maximaler Länge zu berechnen, haben wir die folgende Formel 1 aufgestellt.

$$\text{maximum time} = c^l \cdot t + \frac{c^l}{5} \cdot r \tag{1}$$

- c Größe des Alphabets
- l Maximale länge des Passworts
- t Benötigte Zeit per `SECURITY UNLOCK` Befehl
- r Benötigte Zeit per Aus-/Einschaltzyklus

Wie wir bereits zu Beginn des Abschnittes erwähnt haben, kann jedes Zeichen c des Passworts einen Wert $c = \{1, \cdots, 255\}$ annehmen und die maximale Länge l eines Passworts beträgt $l = 32$. Der eigentliche ATA Befehl `SECURITY UNLOCK` benötigt auf unserem Testsystem durchschnittlich $t = 0,006$ Sekunden. Die Dauer des Ein-/Ausschaltzyklus r haben wir bereits

zuvor erklärt ($r = 6,324$). Mit diesen Werten kommen wir auf eine Laufzeit von $1.298 \cdot 10^{77}$ Sekunden. Ein Brute-Force-Angriff ist damit unmöglich, ein erfolgreicher Wörterbuchangriff unwahrscheinlich.

Letzter Angriff ist die Deaktivierung des Passwortschutzes durch Manipulation der Firmware-Daten. Dies ist bei gesetztem User Password die erfolgversprechendste Attacke. Wir stellen diese im Detail in Abschnitt 3 dar.

3 Deaktivierung des ATA-Festplattenschutzes

In diesem Abschnitt evaluieren wir das Sicherheitsniveau von ATA-Passwörtern. In Abschnitt 2 haben wir gezeigt, dass wir den ATA-Passwortschutz mit einfachen Angriffen wie Default-Passwort oder Passwortbrechen typischerweise nicht deaktivieren können. In diesem Abschnitt stellen wir dar, wie dennoch die ATA-Sicherheitsfunktionalität umgangen werden kann und wie teuer dies ist. Neben verfügbaren Online-Services und einer kommerziellen Lösung aus der professionellen Fesplattenanalyse stellen wir auch unsere Methode zum Umgehen der Schutzmaßnahmen von Festplatten vor. Neben den Kosten berücksichtigen wir auch den zeitlichen Aufwand als zusätzliches Kriterium.

Dienst/Lösung	**Kosten pro Dienst/Lösung**	**Kosten für 100-fache Wiederherstellung**	**Daten gelöscht**	**Zeitaufwand pro Datenträger**
HDD Unlock	$ 19,95	$ 664.05	Ja	2 Stunden
Repair Station	$ 49,95	$ 3.393,70	Nein	wenige Minuten
PC-3000	$ 3000,00	$ 3000,00	Nein	wenige Minuten
Eigene Methode	10,00 €	10,00 €	Nein	wenige Minuten

Tab. 3: Kostenübersicht für das Entfernen von ATA-Passwörtern

Tabelle 3 bietet eine Übersicht über die hier vorgestellten Möglichkeiten. Neben dem Preis für einen einzelnen Vorgang, das Passwort zu entfernen, zeigt die Tabelle zusätzlich den Gesamtpreis für das entfernen von 100 Passwörtern. Speziell die Online-Services bieten hier spezielle Rabatte für höhere Kontingente an. Mit der Abschätzung es Zeitaufwands zeigen wir, wie wenig Aufwand zum Entfernen des Passwortschutzes nötig ist, vorausgesetzt der Benutzer hat bereits Erfahrungen mit den vorgestellten Methoden und benötigt keine Einarbeitungszeit. Die Tabelle zeigt, dass der ATA-Passwortschutz höchstens Angriffe durch kenntnisarme Gegner ausschließt.

Zunächst erläutern wir in Abschnitt 3.1 Online-Services, insbesondere für welche Zielgruppe sie geeignet sind. Dabei handelt es sich um reine Softwarelösungen, die über die ATA Schnittstelle herstellerspezifische ATA-Befehle senden. Diese Befehle, auch *Super-On* genannt, sind nicht im ATA-Standard dokumentiert. Sie erlauben einen Zugriff auf die Service Area der Festplatte, die normalerweise in einem nicht durch ATA-Befehle adressierbaren Bereich liegt. Anschließend stellen wir in Abschnitt 3.2 die kommerzielle Lösung *PC-3000* [ACE12] vor. Sie ist als universelles Werkzeug bei Forensikern und Datenrettungsunternehmen im Einsatz und bietet Zugriff auf die Festplatten sowohl per Super-On als auch über eine serielle Schnittstelle. Abschließend beschreiben wir in Abschnitt 3.3 unsere Methode, um über die serielle Schnittstelle den ATA-Passwortschutz auszuschalten, und welcher Aufwand dazu nötig war.

3.1 Online-Services

Als Online-Services untersuchten wir die beiden Dienste HDD Unlock und Repair Station der Firma A-FF Laboratory [AFF12]. Beide Dienste richten sich an jeweils unterschiedliche Zielgruppen.

HDD Unlock richtet sich an Kunden, die zwar die Festplatte wiederverwenden wollen, nicht aber deren Daten. Bezahlt wird nach Festplattenkapazität. Der Anwender erwirbt zunächst eine *Virtual Unlock Card* passend zur Kapazität seiner Festplatte. Der Preis für eine Samsung SP2504C P120S mit 250 GB ist in Tabelle 3 gelistet. Die Software überprüft zunächst online die Gültigkeit des Codes der Virtual Unlock Card und ob die Festplatte unterstützt wird. Anschließend löscht HDD Unlock die Daten der Festplatte und entfernt das ATA-Passwort. Die Dauer des Löschvorgangs ist festplattenabhängig und richtet sich nach der Speicherkapazität und Geschwindigkeit des Laufwerks. Die Dauer für unsere Festplatte ist ebenfalls in Tabelle 3 zu finden.

Die Repair Station richtet sich an Anwender, die an den gespeicherten Daten auf der Festplatte interessiert sind oder eine defekte Firmware reparieren möchten. Wie auch HDD Unlock ist die Repair Station eine reine Softwarelösung. Bei dem Entfernen der Passwörter unterscheidet es sich von HDD Unlock, denn die gespeicherten Daten bleiben unversehrt und bezahlt wird nicht nach Festplattenkapazität, sondern nach Anzahl der zu entsperrenden Festplatten. Das Deaktivieren eines Passworts einer einzelnen Festplatte kostet $49.95. Weil nur die Sicherheitsmaßnahmen deaktiviert werden, vergehen nur wenige Minuten, bis auf die Festplatte zugegriffen werden kann. Das Unternehmen bietet eine *Bulk*-Lizenz an, mit der mehrere Laufwerke wiederhergestellt werden können. Tabelle 3 zeigt exemplarisch die Kosten für 100 Wiederherstellungen laut Webseite [AFF12].

Da es sich in beiden Fällen um reine Softwarelösungen handelt, kann davon ausgegangen werden, dass die Software mit undokumentierten herstellerspezifischen ATA-Befehlen arbeitet. Im Fall von HDD Unlock wird ein `SECURITY ERASE UNIT` ausgeführt, während die Repair Station die Service Area der Festplatte liest und dort den Passwortschutz entfernt.

3.2 Kommerzielle Software

Wenn es sich um professionelle Datenrettung oder Festplattenanalyse handelt, hat sich die PC-3000 [ACE12] als Standardwerkzeug etabliert. Diese Kombination aus Soft- und Hardware bietet, selbst bei stark beschädigten Datenträgern, die Möglichkeit, auf die gespeicherten Daten und die Firmware zuzugreifen. Die Software bietet bereits viele Funktionen die bei der Sicherung der Daten hilft. Diese erlaubt auch ein Deaktivieren der ATA-Schutzmaßnahmen. Zusätzlich bietet die PC-3000 eine Hardwareschnittstelle, die es erlaubt, über die serielle Schnittstelle mit der Festplatte zu kommunizieren. Dokumentationen zu den verschiedenen Festplattenserien helfen dem Ermittler zusätzlich, die Festplatte auszuwerten bzw. wiederherzustellen.

Das Bundeskriminalamt (BKA) gab uns die Gelegenheit unsere Methode, die in Abschnitt 3.3 vorgestellt wird, mit einer PC-3000 zu überprüfen. Auf diese Weise haben wir die Firmwaredaten, die wir mit unserer Methode ausgelesen haben, mit denen der PC-3000 verglichen. Wir konnten so die korrekte Arbeitsweise verifizieren. Weil keine Unterschiede gefunden wurden, die auf Lesefehler hindeuteten, gehen wir von einer korrekten Implementierung aus. Zusätzlich konnten wir bestätigen, dass die Daten, die mittels herstellerspezifischer ATA-Befehle aus der

Service Area gelesen werden, identisch mit denen sind, die über die serielle Terminalverbindung gelesen werden.

Die Kosten für eine PC-3000 sind für eine professionelle Lösung gering. Trotz des eingeschränkten Abnehmerkreises kostet die Standardausführung etwa $3.000,–. Bei der PC-3000 handelt es sich um ein komplexes Hard-/Softwareprojekt, welches einiger Einarbeitungszeit und Erfahrung bedarf, bevor es korrekt bedient werden kann. Die abgeschätzte Dauer in Tabelle 3, um den ATA-Schutz zu entfernen, bezieht sich auf einen erfahrenen Ermittler. So dauert das Entfernen des Schutzes, wie bei der Repair Station, nur wenige Minuten.

3.3 Deaktivierung mittels Diagnoseschnittstelle

In diesem Abschnitt stellen wir unseren eigenen Ansatz zur Deaktivierung des ATA-Passwortschutzes vor. Wir griffen dazu über die Diagnoseschnittstelle einer Festplatte auf die Firmware zu und konnten mittels Reverse-Engineering den Passwortschutz deaktivieren. Mit Kosten von 10 € ist es preislich der günstigste Deaktivierungsansatz.

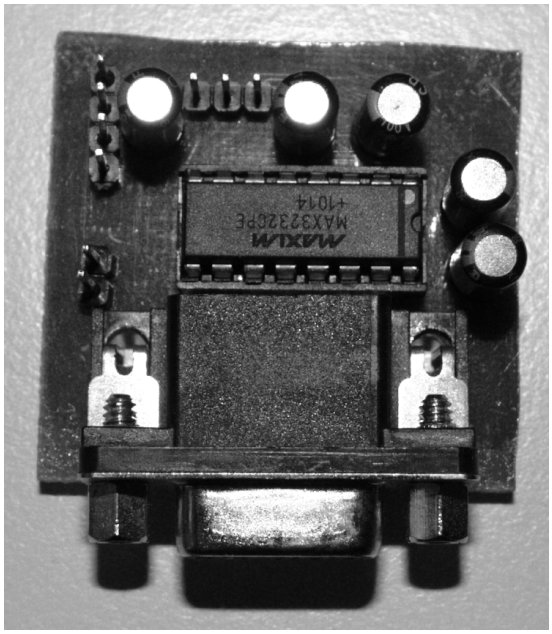

Abb. 1: Beispielkonstruktion eines RS-232 Pegelwandler aus einem MAX-3232 CPE

Um die komplexen Lese-/Schreibalgorithmen zu optimieren und systemunabhängig zu machen, verfügen Festplatten über eine eigene *Microcontroller Unit* (MCU) und eine eigene Betriebssoftware [Mess99]. MCUs verfügen über Schnittstellen, die dazu genutzt werden können, eine serielle Schnittstelle bereitzustellen. Einige Festplattenhersteller nutzen diese Möglichkeit zur Systemdiagnose und haben ein Diagnoseprogramm implementiert, das dann über diese serielle Schnittstelle erreichbar ist. Damit eine Verbindung hergestellt werden kann, muss eine Verbindung nach außen bereitgestellt werden. Samsung versteckt diese Schnittstelle hinter den Jumper-Pins zur Festplattenkonfiguration, Seagate stellt einen eigenen proprietären Anschluss bereit. Um mit der Diagnoseschnittstelle zu kommunizieren, ist es nötig, die Pegel der Logiksignale der Festplatte und des PCs umzuwandeln. Zu diesem Zweck wird zwischen die Verbindung von Festplatte und PC ein RS-232 Pegelwandler (Abbildung 1) geschaltet. Dieser wandelt die höhere Signalspannung des PCs in eine niedrigere Spannung um. Die Verbindung erfolgt

Befehl	Beschreibung
`RM Index`	Lädt das Firmware Module `Index` aus dem Servicebereich in den Speicher der Festplatte.
`MW Offset Word [Word ...]`	Schreibt `Word` an Adresse `Offset` im Speicher der Festplatte.
`WM Index`	Speichert den Inhalt des Speichers als Module `Index` im Servicebereich ab.

Tab. 4: Wichtige Terminalbefehle für Samsungs SP2504C P120S

dann über ein Terminalprogramm, z.B. minicom [SLMS11]. Zusätzlich ist es wichtig, das Terminal korrekt zu konfigurieren und die BAUD Rate in der passenden Geschwindigkeit anzugeben. Für unser Experiment mit der Samsung SP2504C P120S wurde das Terminalprogramm auf `57600 BAUD, 8-N-1` konfiguriert und über die entsprechenden Pins auf der Rückseite der Festplatte mit der Diagnoseschnittstelle verbunden. Die korrekten Werte für die gängigen Festplattenmodelle können im Internet gefunden werden [hdds10].

Beim Einschalten der Festplatte erscheinen im Terminal Statusmeldungen, die der Bootprozess der Festplatte erzeugt. Ist die Initialisierung der Festplatte abgeschlossen, wartet ein Prompt mit der Bezeichnung `ENG>` auf Benutzereingaben. Neben der Einführung in einige Befehle durch [Andr06], haben wir durch ausprobieren herausgefunden das alle Befehle auf ein bis zwei Großbuchstaben reduziert sind und erwarten keinen, bis maximal zwei Argumente. Wird ein Befehl eingegeben und erwartet dieser einen Parameter, gibt das Diagnoseprogramm einen Syntaxfehler aus. So liefert die Eingabe von `HE` eine Übersicht über die aktuell verfügbaren Befehle. Zusätzlich konnten wir herausfinden, dass das Kommando `HE 1` eine etwas ausführlichere Ausgabe liefert und auch ob ein Befehl einen Parameter erwartet. Die für unser Experiment erforderlichen Befehle sind in Tabelle 4 aufgeführt. Die Quelle [Andr06] berichtet über die Verwendung der drei Befehle und erklärt kurz deren Arbeitsweise. Mit diesem Wissen können wir alle Firmwaredaten für unsere Analysen lesen und schreiben.

Die Konfigurationeinstellungen der Festplatte sind in separate Teile (Module) aufgeteilt. Module werden über einen Index referenziert und mit dem Befehl `RM` in den Speicher der Festplatte geladen. Zusätzlich wird der Inhalt des Moduls auf dem Terminal ausgegeben. Die Ausgabe erfolgt als Hexadezimal-String aus einem Offset und den Datenwörtern. Das Modul Adressoffset beginnt immer bei `W:005B00`. Im Speicher kann das Modul nun mit dem Befehl `MW` modifiziert werden. Der Befehl erwartet als Argument den Offset und die zu schreibenden Daten, die an den Offset geschrieben werden sollen. Anschließend kann der modifizierte Speicherinhalt in ein beliebiges Modul mit dem Befehl `WM` zurück geschrieben werden.

Um die Struktur der Firmwaremodule weiter zu analysieren, haben wir zunächst ein Programm geschrieben, dass die Module ausliest und als separate Binärdateien auf dem PC speichert. Module speichern in den ersten vier Datenwörtern den Modulnamen, ähnlich wie ein Dateiname. Das erste wichtige Modul liegt an Index 2. Dort befindet sich das *File Information Table* (FIT). Es beinhaltet ein Inhaltsverzeichnis über alle verwendeten Module; mit Index, Name, Größe und der Cylinder-Head-Sektor Adresse. Um die Bedeutung der Werte zu ermitteln, wurden sie zunächst in Zeichenketten bzw. Dezimalzahlen konvertiert. Mit Hilfe eines *Service Manuals* [SAMS05] für Festplatten vom Typ SP2504C P120S konnten wir den Werten eine Bedeutung zuordnen und unseren eigenen Interpreter für das Inhaltsverzeichnis schreiben.

Durch die FIT konnten wir das Modul 16 als Security-Modul identifizieren und näher untersuchen. Um die Position der Passwörter zu finden, wurde zunächst eine Kopie des Moduls auf dem PC als Referenz gespeichert. Nun wurde zuerst das Master Password gesetzt und anschließend das Modul erneut gespeichert. So konnten wir die beiden Kopien miteinander vergleichen und Änderungen feststellen. Das Master Password wurde im Klartext an Offset `W:005B08` des Modules geschrieben. Beim Auslesen muss lediglich auf die Byte-Reihenfolge der Datenwörter geachtet werden, um die Zeichenfolge in die richtige Reihenfolge zu bringen. Wir haben den Schritt noch einmal wiederholt, nachdem wir das User Password gesetzt haben. Dies wird ebenfalls im Klartext an Offset `W:005B18` gespeichert. Ab diesem Zeitpunkt waren wir in der Lage eine gesicherte Festplatte, durch manuelle Eingabe der Passwörter, zu entsperren.

Eine weitere Möglichkeit ist das Zurücksetzen der Passwörter. Dazu werden die Passwörter mit *Null*-Bytes überschrieben. Dafür wird das Security-Modul einer zuvor gesperrten Festplatte mit dem Befehl `RM 16` ausgelesen. Es genügt das erste Datenwort zu überschreiben. Mit `MW 5B08 0000` und `MW 5B18 0000` werden jeweils die ersten beiden Zeichen der Passwörter ersetzt und werden als Passwörter der Länge 0 gewertet. Im letzten Schritt muss das modifizierte Modul wieder als Modul 16 gespeichert werden. Dazu wird über das Terminal ein `WM 16` gesendet. Beim nächsten Einschalten der Festplatte sind keine Schutzmaßnahmen mehr aktiv, da für die Festplatte keine Passwörter vorhanden sind. Diese einfache Manipulation der Daten ist nur möglich, weil die Firmware keine Prüfsummen vorsieht, um die Integrität der Daten zu überprüfen.

Die letzte Möglichkeit, die in diesem Beitrag vorgestellt werden soll, ist das Überschreiben der *Security Flags*. Diese geben an, ob die Festplatte gesperrt ist und ob das Master Password geändert wurde. Der ATA-Standard gibt vor, dass eine Revisionsnummer angibt, ob das Passwort geändert wurde. Mit jedem Setzen des Master Passwords wird die Revisionsnummer um eins erhöht. Um die Adresse der Security Flags und der Revisionsnummer ausfindig zu machen, wurden die drei Modulkopien aus dem vorangehenden Absatz noch einmal untersucht. Besonders interessant ist hierbei die Beobachtung in der Zustandsänderung vom gesetztem Master Password zu zusätzlich gesetztem User Password. Es zeigen sich in diesem Fall Unterschiede an zwei Datenworten unmittelbar nach dem Modulnamen. Das Adressoffset `W:005B05` bezeichnen wir als Security Flags. Hier konnten wir eine Veränderung feststellen. Das untere Ende des Datenworts hat sich von `0x00` nach `0x01` verändert. An Offset `W:005B06` findet sich die Revisionsnummer des Master Passwords. Um nun den Passwortschutz zu entfernen, laden wir das Modul 16 erneut in den Speicher. Dies erfolgt mit dem Befehl `RM 16`. Der Befehl `MW 5B05 0000 fffe` überschreibt die Security Flags und die Revisionsnummer mit dem Standardwert [T1397] für ein nicht gesetztes Master Password. Bevor die Festplatte ausgeschaltet wird, werden die Änderungen per `WM 16` zurück an Index 16 geschrieben. Wird die Festplatte nun eingeschaltet, sind keine Schutzmaßnahmen aktiv und es kann auf die Benutzerdaten zugegriffen werden.

Der Vorteil unserer Methode, sind die geringen Kosten der Bauteile. Ein selbst gebauter RS-232 Pegelwandler kostet weniger als 10 €, was im Vergleich mit den anderen die günstigste Lösung darstellt (vergl. Tabelle 3). Der Nachteil ist jedoch die eingeschränkte Kompatibilität zu anderen Festplatten. Da die Terminaleinstellungen variieren und nicht alle Festplatten über diese Schnittstelle verfügen, ist dieser Ansatz nicht für alle Festplattentypen geeignet. Zusätzlich entstehen weitere Kosten, wenn das nötige Equipment nicht bereits vorhanden ist. Eine günstige Lötstation inklusive Lötdraht kostet zusammen 15 €. Alternativ kann der Versuchsaufbau auf einem kleinem Experimentier-Steckboard für 2,55 €zusammengebaut werden. Je nachdem ist

also mit einer Kostenspanne von 10 – 25 € zu rechnen.

Unserer Einschätzung nach haben unerfahrene Bastler die Möglichkeit diese Verfahren in wenigen Stunden umzusetzen. Der von uns verwendete RS-232 Pegelwandler ist als Schaltplan im Datenblatt [MAXI] zu finden. Weil die Schaltung wiederverwendet werden kann, entsteht nur ein einmaliger Mehraufwand an Zeit für den Zusammenbau. Der Anwender muss für jeden Festplattentyp nur einmalig das Security-Modul ausfindig machen und die Struktur analysieren.

4 Zusammenfassung und Ausblick

Wir haben gezeigt, dass es sowohl Online-Services, als auch professionelle kommerzielle Lösungen gibt, die jede Zielgruppe abdecken, um den Passwortschutz einer Festplatte zu entfernen. Unsere Methode zeigt, dass es auch für Personen ohne Vorwissen über die interne Funktionsweise von Festplatten möglich ist, die ATA-Sicherheitsmaßnahmen zu entfernen. Neben der einfachen technischen Konstruktion machen die geringen Kosten das vorgestellte Verfahren besonders interessant, weil nun das Untersuchen der Festplattenfirmware nicht mehr nur Experten vorbehalten ist. Dies bedeutet aber auch, dass bei Verlust des Datenträgers ein gesetztes ATA-Passwort keinen ausreichenden Schutz der Daten mehr gewährleistet. Mit wenig Aufwand ist es möglich, die Schutzmaßnahmen zu umgehen.

Es hat sich außerdem gezeigt, dass die Samsung SP2504C P120S über keine Gegenmaßnahmen verfügt, um Manipulationen an der Konfiguration der Firmware festzustellen. Eine einfache Verifikation von Prüfsummen hätte zumindest gereicht, um Änderungen an den Sicherheitseinstellungen zu erschweren. Dass auch sicherheitsrelevante Informationen (wie Passwörter) unverschlüsselt im Klartext abgespeichert werden, weist auf einen erheblichen Sicherheitsmangel bei der Implementierung des Security Feature Set bei dieser Festplattenserie hin.

Der nächste Schritt zur Verbesserung unseres Verfahrens besteht in der Integration des Super-On-Befehls für dieses Festplattenmodell. Die zusätzliche Hardware würde wegfallen und die Geschwindigkeit, mit der die Firmware ausgelesen werden kann, würde drastisch steigen. Mit Super-On-Befehlen können auch Festplatten ausgelesen werden, die über keine serielle Diagnoseschnittstelle verfügen.

Danksagung

Wir danken den anonymen Gutachtern für ihre Kommentare zur Verbesserung des vorliegenden Beitrags. Außerdem bedanken wir uns bei Sven Schmitt, Thomas Willkomm und Gerhard Wagner vom Bundeskriminalamt für die großartige Unterstützung bei unseren Praxistests.

Literatur

[ACE12] ACE Laboratory, PC-3000 for Windows UDMA. `http://www.acelaboratory.com/pc3000.udma.php` (2012), last Retrieved: April, 19th 2012.

[AFF12] A-FF Laboratory, Data Recovery. `http://hdd-tools.com/` (2012), last retrieved: Jan, 30th 2012.

[Andr06] Andrej: Palo does not come with the preparation of safe (translated). http://www.hardw.net/forum/topic6825.htm (2006).

[anon08] anonymous: List of hard disk ata master passwords. http://ipv5.wordpress.com/2008/04/14/list-of-hard-disk-ata-master-passwords/ (2008).

[Fran10] P. Franck: Data Recovery Techniques. http://events.ccc.de/congress/2010/Fahrplan/events/4231.en.html (2010), last retrieved: Jan, 30th 2012.

[hdds10] hddstudio: Seagate Diagnostic Command List. http://forum.javaxtreme.org/showthread.php?t=103 (2010).

[MAXI] MAXIM: True RS-232 Transceivers. MAXIM, Maxim Integrated Products, Inc. 120 San Gabriel Drive Sunnyvale, CA 94086 USA, rev. 5 Aufl.

[Mess99] H. Messmer: The Indispensable PC Hardware Book (3rd Edition). Addison-Wesley (1999).

[Rosc03] W. L. Rosch: The Winn L. Rosch Hardware Bible. Que Corp., Indianapolis, IN, USA, 6th Aufl. (2003).

[SAMS05] SAMSUNG: Hard Disk Drive service manual - P120S Series. SAMSUNG, Samsung Semiconductor Europe GmbH Kölner Strasse 12 65760 Eschborn, Germany, p120s series Aufl. (2005).

[Seag07] L. Seagate Technology: Momentus 7200.2 SATA Product Manual. Seagate, 920 Disc Drive, Scotts Valley, California 95066-4544, USA, revision d Aufl. (2007), publication Number: 100451238.

[SLMS11] M. van Smoorenburg, J. Lahtinen, A. C. de Melo, J. Seymour: minicom - friendly serial communication program (2011).

[T1397] T13: AT Attachment 3 Interface (ATA-3). http://www.t13.org/documents/UploadedDocuments/project/d2008r7b-ATA-3.pdf (1997).

[T1308] T13: AT Attachment 8 - ATA/ATAPI Command Set (ATA8-ACS). http://t13.org/Documents/UploadedDocuments/docs2006/D1699r3f-ATA8-ACS.pdf (2008).

[Tony07] B. J. Tony Sammes: Forensic Computing - Second Edition. Springer (2007).

[Vids06] A. Vidström: Computer Forensics and the ATA Interface. Technical report E7091, FOI, Swedish Defence Research Agency Command and Control Systems Box 1165 SE-581 11 LINKÖPING Sweden (2006).