Dr. Markus Knasmüller
Allgemein beeideter und gerichtlich zertifzierter Sachverständiger für Informations- und Kommunikationstechnologie; Abteilungsleiter Entwicklung, BMD Systemhaus GmbH, Steyr

Zur Echtheit und Manipulation von SMS

1. Einleitung

SMS sind Kurznachrichten mit maximal 160 Zeichen, die (im Regelfall) per Mobiltelefon jederzeit einfach an einen Empfänger (im Regelfall ein anderes Mobiltelefon) versendet werden können. Aufgrund der Einfachheit auf der einen Seite und der hohen Akzeptanz auf der anderen Seite haben sie eine hohe Verbreitung; so wurden alleine in Österreich 2011 laut RTR[1] etwa 7,28 Milliarden SMS versendet. Dabei ist die Tendenz immer noch stark steigend, im Vergleich zu 2007 ist dies etwa mehr als das Doppelte.

Aufgrund dieser hohen Anzahl (das sind pro Einwohner beinahe 1.000 versendete SMS pro Jahr) ist es nicht verwunderlich, dass SMS auch in Gerichtsverfahren immer wieder eine bedeutende Rolle zukommen. Als Beispiel seien etwa nur eine Reihe von OGH-Urteilen[2] genannt.

Meist geht es dabei um die Dokumentierung von privaten Nachrichten, etwa Drohungen, aber durchaus werden auch Geschäfte per SMS abgeschlossen. Vielfach stellt sich dann im Verfahren die Frage, ob eine SMS echt ist. Ähnlich einer Mail oder einem Fax ist dies natürlich vor allem eine Frage der Beweiswürdigung; rein subjektiv ist aber klar, dass ein Fax mittels eines Druckers und eines Grafikprogramms sehr einfach gefälscht werden kann, bei einer SMS ist dies nicht so offensichtlich. Wenn bei Verhandlungen oder auch bei Vernehmungen vor den Ermittlungsbehörden ein Handy mit einer SMS, die die Telefonnummer des Senders, die Sendezeit und den Text anzeigt, vorgezeigt wird, so sieht dies für einen technischen Laien nachvollziehbar aus. Dies umso mehr, da auch durch erste einfache Änderungsversuche (etwa mit Bearbeiten, Weitersenden etc) die SMS ganz offensichtlich nicht manipuliert werden kann.

In mehreren Gutachten hat der Autor als Sachverständiger dabei schon die Echtheit von SMS überprüfen müssen; auch wurde ihm dabei die Frage gestellt, ob es überhaupt grundsätzlich möglich wäre, SMS zu fälschen, und falls ja, ob dies nur Experten möglich wäre oder auch ein durchschnittlicher EDV-Anwender dies durchführen könnte.

Dies sind sicherlich interessante Fragestellungen, die im Folgenden untersucht werden. Dabei werden zuerst Manipulationsmöglichkeiten aufgezeigt und dann vorgestellt, wie derartige Manipulationen nachgewiesen werden können.

2. Mögliche Manipulationen

Es ist wahrscheinlich nicht überraschend, dass es tatsächlich möglich ist, SMS zu manipulieren. Dafür gibt es verschiedene Möglichkeiten, die vor allem darin unterschieden werden können, ob der Zeitpunkt der Manipulation vor oder nach dem (angezeigten) Sendedatum der SMS liegt. Soll eine SMS etwa beweisen, dass vor einer Tat eine Drohung geäußert wurde, so muss das Sendedatum der SMS klarerweise auch vor der Tat sein. Jemand, der eine SMS manipulieren möchte, die so eine Drohung beinhaltet, kann dies entweder vor der Tat tun, indem er eine SMS unter Vortäuschung einer falschen Nummer versendet oder danach indem er den SIM-Karten-Speicher manipuliert.

2.1. Vortäuschung einer falschen Nummer

Sofern das Ziel einer Manipulation einer SMS nur ist, dass vorgetäuscht werden soll, dass ein bestimmter Absender eine Nachricht übermittelt und die Sendezeit dabei keine Rolle spielt, so ist dies jedem Internetanwender sehr ein-

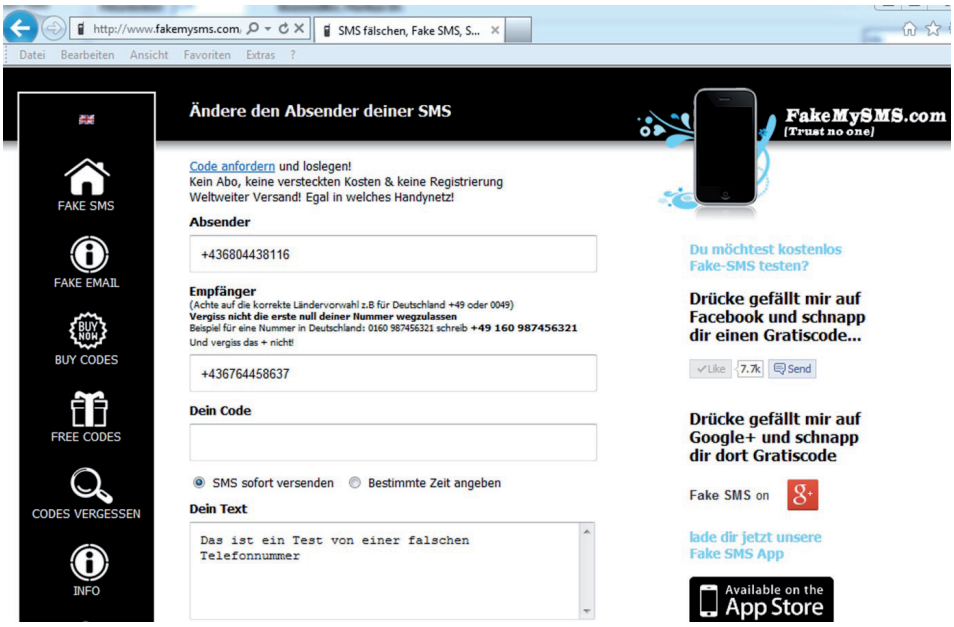

Abbildung 1: Absenden einer gefälschten SMS über die Internetplattform fakemysms.com

fach möglich. In diesem Falle muss die SMS nur über eine einschlägige Internetplattform, wie etwa http://www.fakemysms.com, versendet werden.

Derartige Plattformen ermöglichen das Versenden an beliebige Telefonnummern, wobei aber auch die Absendernummer erfasst werden kann. Abbildung 1 zeigt dabei die Erfassungsmaske.

Es muss dabei also nur im Feld „Absender" die gewünschte Telefonnummer eingegeben werden, am Handydisplay sieht es dann so aus, als wäre tatsächlich die SMS von dieser Nummer versendet worden. Die Kosten dafür sind minimal, für wenige Cent können Freischaltcodes gekauft werden, die für das Versenden der SMS notwendig sind.

Mit dieser Methode kann natürlich auch die Manipulation von einem Dritten, der gar keinen Zugang zu beiden Mobiltelefonen (Absender und Empfänger) hat, vorgenommen werden.

2.2. Nachträgliches Manipulieren einer SMS

Anders sieht dies natürlich aus, wenn es auch notwendig ist, den Zeitpunkt der SMS zu manipulieren. Dabei ist zuerst festzuhalten, dass der bei einer SMS angezeigte Zeitpunkt sich immer auf den Sendezeitpunkt bezieht – es ist daher exakt jener Zeitpunkt, zu dem das SMS vom Absendergateway versendet wurde. Dieser ist – von der Zeitzone abgesehen – vollkommen unabhängig davon, wann die SMS tatsächlich empfangen wurde bzw welche Uhrzeit am empfangenden (oder auch am sendenden) Mobiltelefon eingestellt ist. Einzig die Zeitzone wird berücksichtigt, weil immer der tatsächliche Zeitpunkt in der Zeitzone des anzeigenden Mobiltelefons angezeigt wird. Durch Umstellen der Zeitzone kann daher die angezeigte Sendezeit minimal (eben um die Differenz zwischen den Zeitzonen, also im Regelfall nur um ganze Stunden) geändert werden.

Sollte aber eine bestimmte Uhrzeit vorgetäuscht werden, so kann eine SMS manipuliert werden, indem die SIM-Karte manipuliert wird. Diese SIM-Karte ist jene kleine Chipkarte, die in einem Mobiltelefon ist und einerseits für die Identifizierung gegenüber der Mobiltelefongesellschaft verantwortlich ist (also angibt, mit welcher Telefonnummer jemand erreichbar ist) und andererseits aber auch als (zumindest kleiner) Speicher dient. Auf einer SIM-Karte können dabei bis zu 20 SMS gespeichert werden. Mittels eines einfachen Kartenlese- und -schreibgeräts, im Internet um weniger als € 20,– erhältlich, kann der Inhalt der SIM-Karte ausgelesen werden. Unter Kenntnis des Formats einer SMS, also wie die einzelnen Hexadezimalzahlen angereiht werden, ist es dann (mehr oder weniger einfach) möglich, sowohl den Text als auch Datum und Uhrzeit einer SMS zu manipulieren.

3. Format einer SMS

Für SMS-Textnachrichten werden jeweils 7 Bit als ein Zeichen interpretiert. Damit können mit 1.120 Bit (7 Bit/Zeichen * 160 Zeichen = 1.120 Bit) 160 Zeichen dargestellt werden, wobei der Vorrat an darstellbaren Zeichen grundsätzlich auf 128 beschränkt ist. Dabei wird beim Format zwischen Header und Body unterschieden. Im Header sind die wichtigen Sendeinformationen enthalten. Dazu gehören etwa: Handelt es sich um eine ein- oder ausgehende SMS, mit welchem zweiten Telefonnetzteilnehmer wurde kommuniziert und wann ist dies erfolgt? Im Body ist ganz einfach der Text der Nachricht enthalten. Nachfolgend wird nicht das vollständige Format einer SMS präsentiert,[3] sondern nur diejenigen Informationen, die zu einer Manipulation nötig sind.

3.1. Header der SMS

Im Regelfall geht es bei der Manipulation einer SMS um eine, die empfangen wurde. Relevant ist dabei, von welcher Telefonnummer wurde und wann die SMS gesendet; diese Informationen sind im Header der SMS gespeichert und dies sogar (mit kurzer Anleitung) relativ gut lesbar. So beginnt beispielsweise eine SMS, die von der Nummer +43 664 2127574 am 16. 6. 2012 um 19:59:48 Uhr versendet wurde, mit folgender Bytefolge:

01 06 91 34 66 04 05 F1 04 0C 91 **34 66 24 21 57 47** 00 00 **21 60 61 91 95 84** 80

Die relevanten Bytes sind dabei fett markiert, wobei die Informationen BCD-kodiert sind, also je 4 Bit ergeben eine Ziffer der Nummer und die Nummer beginnt jeweils im zweiten Halbbyte, das heißt, „34" ist also als „43" zu lesen, „57" als „75" etc.

Damit ist „34 66 24 21 57 47" also als „43 66 42 12 75 74" zu lesen, womit die Sendenummer sehr gut aus der Bytefolge erkennbar ist. Sollte nun eine andere Absendernummer vorgetäuscht werden, etwa die Nummer +43 676 4458367, so muss die Zeichenfolge „34 66 24 21 57 47" einfach durch „34 76 46 54 38 76" ausgetauscht werden.

Ähnlich ist dies bei Datum und Uhrzeit. Die Zeichenfolge „216061" steht für „120616" und gibt das Datum also im Format „JJTTMM" an. Die Zeichenfolge „919584" steht für „195948" und gibt also die Uhrzeit im Format „HHMMSS" an. Sollte also etwa der 10. 3. 2011 vorgetäuscht werden, so muss nur die Zeichenfolge „210661" durch „113001" ausgetäuscht werden.

Zusammenfassend würde also nur die Bytefolge am Anfang durch diese ersetzt werden müssen:

01 06 91 34 66 04 05 F1 04 0C 91 **34 76 46 54 38 76** 00 00 **11 30 01** 91 95 84 80

Schon würde dementsprechend angezeigt werden, dass die SMS am 10. 3. 2011 von der Nummer +43 676 4458367 gesendet worden ist.

Eine derartige Manipulation wäre also relativ einfach möglich, wahrscheinlich sogar ohne spezifische Kenntnisse zu haben, da tatsächlich die Daten relativ leicht erkenn- und austauschbar sind.

3.2. Body der SMS

Dadurch, dass für ein Zeichen jeweils nur 7 Bit und nicht – wie normalerweise üblich – 8 Bit (bzw ein Byte) verwendet werden, ist der Body etwas schwerer zu lesen. Vom Aufbau her ist es aber grundsätzlich dennoch sehr einfach; es ist zuerst ein Längenbyte, das angibt, wie viele Zeichen Nutzdaten folgen, und dann folgt der Text. Nur sind die Zeichen eben gepackt, die Zeichenfolge „Das" wäre etwa „03 C4 F0 1C", wobei eben „03" die Anzahl der Zeichen angibt und dann die Zeichen enthalten sind. Diese 7-Bit-Codierung zu lesen ist dabei aber ziemlich kompliziert und es muss dafür wahrscheinlich ein Programm geschrieben werden. Mit Hilfe eines derartigen Programmes kann etwa der Text „Richtig gemein" dargestellt werden. Dieser entspricht der Zeichenfolge „0E D2 F4 18 4D 4F 9F 41 E7 72 BB 9C 76 03", wobei 0E (hexadezimal 14) eben angibt, dass es 14 Zeichen sind und die restlichen Bytes den Text beinhalten. Auch hier kann durch Ersetzen der Bytefolgen jeweils also der Text ausgetauscht werden, wobei dies wesentlich komplizierter ist, als die Manipulation des Headers. Dafür ist sicherlich eine Programmunterstützung notwendig, wobei der Autor trotz intensiver Internet-Recherche kein Programm finden konnte, dass hier eine ganze SMS einfach umgewandelt hätte. Zwar gibt es einige ähnliche Programme, jeweils sind dann aber doch gute Programmierkenntnisse notwendig, um diese entsprechend zu adaptieren.

Eine einfache Möglichkeit, dennoch den gewünschten Text zu erzeugen, ganz ohne Programmkenntnisse, ist es aber, sich selbst von einem beliebigen Mobiltelefon eine SMS mit dem gewünschten Text zu senden und dann einfach Datum und Uhrzeit entsprechend auszutauschen.

3.3. Vollständiges Beispiel

Zusammenfassend kann also eine bestehende SMS auf einer SIM-Karte leicht editiert werden, auch kann etwa eine ganz neue geschaffen werden. Durch minimale Änderungen der Bytefolgen kann dabei sowohl Nummer, Datum als auch Inhalt geändert werden. Abbildung 2 zeigt dabei im Vergleich die beiden oben erwähnten SMS im Byteformat. Zuerst die SMS 0A von der Nummer +43 664 2127574 vom 16. 6. 2012 um 19:59:48 Uhr mit dem Text „Das". Danach die SMS 0B von der Nummer +43 676 4458367 vom 10. 3. 2011 um 19:59:48 Uhr mit dem Text „Richtig gemein".

Auf einem handelsüblichen Handy würden die SMS am Display so dargestellt werden, dass hier die jeweils gewünschte Nachricht angezeigt wird. Dies zeigt Abbildung 3.

An dieser Stelle sei aber angemerkt, dass die Manipulation in diesem Falle nicht vollständig war, weswegen sie in einer gutachterlichen Untersuchung auffallen würde, damit wird sich der nächste Abschnitt beschäftigen.

4. Erkennen von Manipulationen

Nachdem in den ersten Abschnitten gezeigt wurde, ob und wie es möglich ist, SMS zu manipulieren, beschäftigt sich dieser Abschnitt damit, ob derartige Manipulationen erkennbar sind. Dabei ist einmal zu unterscheiden, ob nur eine falsche Nummer vorgetäuscht wurde (etwa durch Portale wie http://www.fakemysms.com) oder aber wirklich die SIM-Karte ausgelesen und manipuliert worden ist.

Im Falle der reinen Vortäuschung einer falschen Nummer ist eine derartige Manipulation auf jeden Fall zu erkennen, da in der SMS auch das sogenannte SMS-Gateway gespeichert ist. Wird eine SMS etwa von einer Nummer des Mobilfunkbetreibers A1 gesendet, so ist die Nummer des SMS-Gateways von A1 in der SMS enthalten. Zurückkommend auf den im Vorabschnitt verwendeten Header

01 06 91 **34 66 04 05 F1** 04 0C 91 34 66 24 21 57 47 00 00 21 60 61 91 95 84 80

gibt dabei die Zeichenfolge „34 66 04 04 F1" das SMS-Gateway von A1 „43 66 40 40 1F" an (das letzte „F" ist ein Platzhalter). Diese Information über das SMS-Gateway wird zwar im Regelfall nicht am Display des Mobiltelefons angezeigt (auch nicht über weitere Optionen), kann aber eben durch Auslesen der SIM-Karte bestimmt werden. Wird nun aber eine SMS etwa über http://www.fakemysms.com versendet und etwa eine A1-Nummer vorgetäuscht, so stimmt die Nummer des SMS-Gateways nicht, wodurch derartige Manipulationen einfach erkannt werden können.

Anders sieht dies aber im Falle einer direkten Manipulation im Speicher der SIM-Karte aus. Werden hier die Daten vollständig geändert und nötigenfalls auch das SMS-Gateway entsprechend angepasst, dann ist eine derartige Manipulation nicht erkennbar.

Ein Indiz kann dann der Einzelnachweis sein, hierbei wird vom Mobilfunkbetreiber gespeichert, wann SMS versendet worden sind. Sind hier etwa diese SMS nicht enthalten, so

```
0A: 01 06 91 34 66 04 05 F1 04 0C 91 34 66 24 21 57
    47 00 00 21 60 61 91 95 84 80 03 C4 F0 1C FF FF
    FF FF FF FF FF FF FF FF FF FF FF FF FF FF FF FF
    FF FF FF FF FF FF FF FF FF FF FF FF FF FF FF FF

0B: 01 06 91 34 66 04 05 F1 04 0C 91 34 76 46 54 38
    76 00 00 11 30 01 91 95 84 80 0E D2 F4 18 4D 4F
    9F 41 E7 72 BB 9C 76 03 FF FF FF FF FF FF FF FF
    FF FF FF FF FF FF FF FF FF FF FF FF FF FF FF FF
```

Abbildung 2: Zwei verschiedene SMS im Byteformat im Vergleich

Abbildung 3: Visualisierung der beiden SMS mit einem handelsüblichen Handy

wäre dies ein Indiz dafür, dass diese SMS nicht versendet worden ist. Dies muss aber auch genau betrachtet werden, denn viele Mobilfunkbetreiber (etwa T-Mobile in Österreich) führen nur kostenpflichtige SMS auf dem Einzelnachweis an. Werden etwa bei T-Mobile SMS über das WebSMS-Portal versendet, so sind diese SMS nicht im Einzelnachweis enthalten. Durch die Vorratsdatenspeicherung[4] wären diese Daten seit 1. 4. 2012 auf jeden Fall verfügbar, jedoch maximal sechs Monate lang.

Auch erwähnt werden sollte, dass eine SMS etwa auch über Dienste wie Skype versendet werden kann. Auch dort kann meist die eigene Telefonnummer mitgesendet werden, nur kann dabei im Gegensatz zu http://www.fakemysms.com nicht einfach eine beliebige Nummer angegeben werden, sondern diese muss mittels eines Codes bestätigt werden. Derartige SMS wären wiederum über das verwendete SMS-Gate identifizierbar.

5. Zusammenfassung

Zusammenfassend kann festgehalten werden, dass SMS einfach manipuliert werden können. Besonders einfach können dabei andere Nummern vorgetäuscht werden, die Manipulation von Text und Uhrzeit ist mittels eines SIM-Karten-Schreibgeräts, das um weniger als € 20,– im Internet erhältlich ist, aber auch möglich. Während erster Fall durch Auslesen des Speichers der SIM-Karte auf jeden Fall erkennbar wäre, ist dies aber im zweiten Falle nur bedingt bzw eventuell gar nicht möglich. Eine Garantie, dass eine bei Gericht vorgezeigte SMS also echt ist, ist auf keinen Fall gegeben.

Anmerkungen:

1 *RTR*, RTR Telekom Monitor Jahresbericht 2011, RTR GmbH, 2011, S 33, online abrufbar unter http://www.rtr.at/de/komp/TK_Monitor2011/TM_Jahresbericht_2011.pdf.

2 ZB OGH 15. 11. 2012, 12 Os 127/12m und OGH 22. 8. 2012, 15 Os 101/12k.

3 Siehe dazu *3GPP*, Spezifikation 23.040, Technical realization of the Short Message Service (SMS), online abrufbar unter http://www.3gpp.org/ftp/Specs/hmtl-info/23040.htm.

4 Siehe zB *Klaushofer*, Die Verpflichtung zur Vorratsdatenspeicherung ist am 1. April 2012 in Kraft getreten, JusIT 2012, 62.

Korrespondenz:
Dr. Markus Knasmüller
Edelhof 45, 3350 Haag
E-Mail: knasmueller@bmd.at