Beitrag zu INFOS 99

Markus Kuhn, Elsa-Brändström-Gymnasium, Oberhausen
Postanschrift: Christian-Steger-Str. 11 46045 Oberhausen
email: markus.kuhn@elsa.ob.nw.schule.de
http: www.uni-duisburg.de/SCHULEN/EBG/schueler/stega.htm

Steganographie - die Hintertür für den Lauschangriff?

Einleitung

In den letzten Monaten hat eine umfangreiche und kontrovers geführte Diskussion um den "Großen Lauschangriff" stattgefunden. Er erlaubt das Abhören von Personen bei Verdacht auf Beteiligung an schweren Strafdaten. Aktuelle Pläne des Bundesinnenmisteriums sehen erweiterte Abhörtechniken für die computergestützte Kommunikation vor. Spätestens hierdurch wird das Thema auch für Schülerinnen und Schüler im Fach Informatik brisant. Dies ist eine Gelegenheit im Unterricht Programmiermethoden und Zeitgeschehen zu verbinden, die Schülerinnen und Schüler in die Lage versetzen kann, aufbauend auf dem selbst erworbenen Erfahrungshintergrund aktuelle Bestrebungen der deutschen Innenpolitik zu beurteilen.

Der vorliegende Beitrag soll einige Schlaglichter auf die Thematik "Lauschangriff" werfen, Quellen zur Diskussion für Informatikkurse der Oberstufe aufweisen und in einem Praxisbericht zeigen, wie einem Lauschangriff ohne große kriminelle Energie und mit dem Wissen eines Informatikschülers ausgewichen werden kann. Dabei spielt die Steganographie - die Kunst des verdeckten Nachrichtentransportes/Nachrichten zu verstecken - eine entscheidende Rolle. Die eingesetzte Programmiersprache Borland Delphi 2.0 kann dabei durch eine andere Programmiersprache ersetzt werden. Nebenbei wird dabei deutlich, wie der Einsatz der Dialogelemente von Delphi den Schülerinnen und Schülern die Programmierung erleichtert/die Konzentration auf die eigentlichen Aspekte der Problemlösung ermöglicht. Abgerundet wurde die Programmerstellung durch die detalillierte Dokumentation der selbstgeschriebenen Programme.

Praxisbericht

Die im folgenden skizzierte Unterrichtsreihe wurde von mir mit einem Informatik-Grundkurs der Jahrgangsstufe 12 durchgeführt. Sie erstreckte sich über 8 Wochen mit jeweils 2 Unterrichtsstunden. Die Schüler haben aufbauend auf Pascal-Kenntnisse seit einem guten halben Jahr Programmiererfahrungen mit Delphi sammeln können. Die meisten sind sehr interessiert und engagiert. Die Grundprinzipien der Kryptographie wurden bereits vor einem Jahr besprochen, ähnlich wie in Computer + Unterricht Heft 18 von mir vorgeschlagen.

In den **ersten beiden Stunden** der Unterrichtsreihe arbeiteten sich die Schüler anhand einiger Presseartikel in die Thematik "Lauschangriff" ein. (s. Kasten ...) Arbeitsteilig erfassten sie die Inhalte der neuen "Kommunikationsgesetze" und stellten sie einander vor. Die Ergebnisse finden sich im Abschnitt Historie zum Lauschangriff.
In der **nächsten Doppelstunde** wurde die Neufassung des Grundgesetz-Artikels13 hinzugezogen und der Ablauf der damit verbundenen Verfassungsänderung besprochen. Grundlage dafür waren Artikel aus der Tagespresse und "Der Spiegel". Besonders die Diskussionen um auszunehmende Berufsgruppen wurden von den Schülern interessiert verfolgt und zum Teil hinterfragt. Die Frage nach der Effektivität des Lauschangriffes zur Bekämpfung der Organisierten Kriminalität wurde erstmalig angesprochen. Bereits jetzt zeigten sich Zweifel, ob diese Zielsetzung die Einschränkung eines allgemeinen Grundrechtes rechtfertig, zumal wenn die genannte Zielgruppe über ausreichende finanzielle und organisatorische Möglichkeiten verfügt, um Lauschangriffe zu unterlaufen.
In den **folgenden zwei Stunden** wurde die Steganographie von Ihrer Idee her vorgestellt, um den Schülern konkret eine Möglichkeit zu zeigen, wie man den "Augen und Ohren des Gesetzes" entgehen kann:
Der Einstieg in das Thema Steganographie als Hintertür zum "Lauschangriff" erfolgte über ein Rätsel. Die Schüler sollten die versteckte Botschaft dreier Sätze herausfinden. Als Hilfestellung wurde nach einigen Minuten ein vierter Satz aufgedeckt und das Augenmerk der Schüler auf die Gemeinsamkeiten der Sätze gelenkt. Die ersten Stellen der Zahl sind als Wortlänge in diesen Merksätzen versteckt!*

Ein Rätsel zum Einstieg: Worum geht es?

Wie o dies macht ernstlich so vielen viele Müh´

See I have a rhyme assisting my feeble brain its tasks sometime resisting

Que j´aime à faire apprendre un nombre utile aux sages

How I wish I could enumerate pi easily

Dieses erste Beispiel für die Stenographie wurde im folgenden analysiert und auf das Verstecken von Bitfolgen in Bilddateien übertragen. Notwendige Zwischenschritte, um einen Text binär zu codieren, waren den Schülern vertraut. Mühelos wurden verschiedene Strategien entwickelt, um die einzelnen Bits zu verstecken. Vorgeschlagen wurden beispielsweise, jedes 4. Pixel zu verändern, die Bits nur im Zeilenanfang zu verstecken, ausgehend von einem Startpunkt die Folgepunkte über einen vereinbarten Algorithmus zu berechnen, wozu auch der Zufallsgenerator benutzt werden könnte.

In der **vierten Doppelstunde** der Reihe wurde mit der Umsetzung der Ideen in eigenen Programmen begonnen. Eingeführt wurde die TImage-Komponente von Delphi und der Aufbau des BMP-Formates unterstützt durch einen Hexeditor untersucht. Bei der Realisierung entschieden sich die Schüler für zwei grundsätzlich verschiedene Wege. Während die einen den von mir favorisierten Vorschlag aufgriffen und die Bildpunkte über die *Pixels*-Eigenschaft manipulierten, entschlossen sich die anderen, direkt die BMP-Datei gezielt zu verfälschen. Die Vertiefung der kurz zuvor eingeführten *delphischen* Dateidialoge nahm dabei nebenher ihren Lauf. Die Programme schrieben die Schüler innerhalb dieser und **zwei weiterer Doppelstunden** ergänzt sicherlich durch zahlreiche Stunden in ihrer Freizeit. Dabei gingen sie in der Gestaltung der Oberfläche und der Verwendung von Delphi-Komponenten weit über das eigentlich nötige Maß hinaus und arbeiteten sich intensiv und eigenständig in die Delphi-Programmierung ein. Abschließend stellten sich die Schüler ihre Programme gegenseitig vor und testeten ihre Funktionalität: Texte wurden mit einem Programm in einer Grafik versteckt und mit einem der anderen Programme wieder ausgelesen. Die Schülerlösungen können auf unserer Homepage abgerufen werden. Dort findet sich auch eine rudimentäre Lösung, die sich auf die nötigen Programmschritte und Komponenten beschränkt. Sie soll lediglich zur Nachahmung und Erweiterung anregen. Sie sind recht knapp und einfach gehalten, um einen schnellen Überblick meines Lösungsansatzes zu ermöglichen.

Der Zeitaufwand für diese Unterrichtsreihe betrug bis zu diesem Zeitpunkt 6 Doppelstunden. Es folgten **zwei weitere Doppelstunden** zur Ergänzung und Dokumentation der Schülerlösungen:
Erarbeitet wurden zuerst wesentliche Bestandteile einer Programmdokumentation. Recht schnell wurde deutlich das eine Strukturierung und Unterteilung in ein Benutzerhandbuch und in ein Programmiererhandbuch sinnvoll ist. So sollten sich wichtige Informationen zum Aufgabenbereich, zum Leistungsumfang und zur Handhabung im Benutzerhandbuch finden lassen, während dokumentierter Quelltext, Beschreibung der Modularisierung, verwendete Delphi-Komponenten ins Programmiererhandbuch einzubringen sind. Mehrere Schüler schrieben und strukturierten bei dieser Gelegenheit ihre Handbücher mit HTML.

Einschränkung des Grundrechtes auf "Unverletzlichkeit der Wohnung"

Obwohl Kritiker schon seit 1997 wiederholt auf die Problematik der Gesetzesänderungen für den großen Lauschangriff hingewiesen haben, kommt es im Frühjahr 1998 kurz vor den Sitzungen des Bundestages und Bundesrates zur Änderung des Artikels 13 des Grundgesetzes zu großem Aufsehen in den Medien. Grund ist weniger die Gesetzesänderung an sich, die nicht nur breiten Konsens in den Parteien findet. Grund ist vielmehr die Diskussion um bestimmte Berufsgruppen, die vom Lauschangriff verschont bleiben sollen. Als Folge davon werden Erweiterungen der Rechte der Behörden zur Überwachung von Verdächtigen von einer größeren Gruppe in der Bevölkerung wahrgenommen und es entsteht auch bei Schülerinnen und Schülern ein Bedürfnis nach umfassender Information.

Die Verfassungsänderung zur Legitimation des "großen Lauschangriffs", der es den Überwachungsbehörden u.a. erlaubt im Verdachtsfalle Wohnungen zu verwanzen und (Telefon-)Gespräche abzuhören, ist nur ein Element des Staates, um, wie Innenpolitiker sagen, Verbrechensbekämpfung effektiv betreiben zu können. Verbunden mit den gesteigerten Möglichkeiten der Telekommunikation sind auch neue Gesetze entstanden, die den Behörden umfangreiche Zugriffe auf Nachrichten und Daten ermöglichen. Zwar sind diese Zugriffe nur im begründeten Verdachtsfalle rechtens und müssen von Richtern genehmigt werden, aber die Effektivität dieses Kontrollmechanismusses wird gerade von Richtern durchaus kritisch gesehen. Kritisiert wird auch eine fehlende Erfolgskontrolle, die die Verhältnismäßigkeit der eingesetzten Maßnahmen rückwirkend überprüfen könnte, wie sie in den USA praktiziert wird, um Mißbrauch zu vermeiden.

Als Grund für die Verschärfung der Gesetze wird immer wieder die Bekämpfung der organisierten Kriminalität aufgeführt. Dem kommt ein gesteigertes Sicherheitsbedürfnis der Bürger aufgrund der steigenden Kriminalität entgegen. Ob eine wirksame Bekämpfung durch die neuen Befugnisse tatsächlich ermöglicht wird oder die Organisierte Kriminalität nur als Schreckgespenst dient, um die Einschränkung der bürgerlichen Grundrechte leichter durchsetzen zu können, muss letztlich jeder selber beurteilen. Eine intensive Beschäftigung mit den neuen Gesetzen und mit den Möglichkeiten diese zu unterlaufen, kann Schülerinnen und Schülern der Oberstufe dazu verhelfen, sich selbst ein Urteil zu bilden. Eine Zusammenstellung dieser Gesetze ist Bestandteil dieses Beitrags.

Steganographie

Die Steganographie hat als besondere Form der Kryptographie zum Ziel, einen geheimen Nachrichtenaustausch zwischen Sender und Empfänger zu ermöglichen. Während sich die bekannteren Verfahren der Kryptographie darauf konzentrieren, die Elemente der Nachricht so zu verändern, dass sie nur der eingeweihte Empfänger wieder vollständig und richtig rekonstruieren kann, versucht die Steganographie die Nachricht zu verstecken. Ihr Ansatz ist ebenso einfach wie überzeugend: Wenn niemand die Nachricht bemerkt, wird auch keiner versuchen, sie zu entschlüsseln!

Darüber hinaus ist er nicht neu, wie zwei historische Beispiele belegen. Schon der Grieche Herodot berichtet im 5. Jahrhundert v. Chr. von der Übermittlung versteckter Nachrichten. Ein Adliger soll eine Nachricht auf den kahlgeschorenen Kopf eines Sklaven tätowiert haben. Nach angemessener Zeit für das Haarwachstum übermittelte dieser Sklave die Nachricht unbemerkt. Im zweiten Weltkrieg wurden winzige Mikrofilme als i-Punkte meist unbemerkt versandt. Das Verfahren war gegenüber der Tätowierung um einiges schneller und zudem effizienter, da bereits riesige Datenmengen verschickt werden konnten.

Seit dem Aufschwung der Telekommunikation haben sich Form und Träger der steganographierten Nachrichten erneut verändert. Es geht heute darum, möglichst unauffällig einzelne Bits in Datenströme nach einem bestimmten Muster einzubauen, um sie auf Seiten des Empfängers präzise wieder herauszufiltern. Als Träger kommen dafür in besonderem Maße Bild- und Tondateien in Frage, aber auch Texte können benutzt werden. Mit Blick auf ein elektronisches Bild der Mona Lisa schreibt der Spiegel: "Schon der Mundwinkel der Schönen reicht aus, allerlei Heimlichkeiten zu verstecken". Die Vorgehensweise ist bei Bild- und Tondateien sehr ähnlich. Bildpunkte bzw. Tonsignale werden dezent verändert, so dass der lauschende Beobachter nichts bemerkt. Eine Studie, die an der Universität Hildesheim entstanden ist, belegt überzeugend die Möglichkeit, digitale Telefongespräche, wie sie ISDN übermittelt, zum versteckten Nachrichtenaustausch zu verwenden. Die Veränderung der Tonsignale war für die Versuchspersonen nicht auszumachen. In Bilddateien können die Farbwerte der einzelnen Bildpunkte so fein verändert werden, dass es dem Betrachter auch auf den zweiten Blick nicht auffällt.

Zwar gibt es Möglichkeiten durch aufwendige Analysen solche veränderten Signale aufzuspüren, die vielleicht mit einer Häufigkeitsanalyse in Alphabeten vergleichbar ist nun aber beispielsweise auf ungewöhnliche Farbmischungen anzuwenden ist. Dies setzt aber voraus, dass der Lauscher bereits Verdacht geschöpft hat und nun nach dem Versteck sucht!

Eine Schwäche der Steganographie soll nicht verschwiegen werden. Der Vorteil der neueren Kryptographiemethoden liegt ja gerade darin, dass ein Teil des Schlüssel veröffentlicht wird und der Empfänger den wichtigen privaten Schlüssel selber auswählen kann und geheimhält, ohne ihn jemals aus der Hand zu geben. Für die Steganographie müssen Sender und Empfänger sich über den Schlüssel, die Art des Versteckens, zumindest einmal verständigen. Wenn hiervon der Lauscher Wind bekommt, ist das Steganographieren hinfällig. Zwar sind grundsätzlich Kombinationen mit anderen Kryptographiemethoden möglich, aber der eigentliche Vorteil des unbemerkten Datenaustausches ist entfallen.

Für viele Firmen bietet die Steganographie unabhängig von dem bereits Beschriebenen die Chance ihre Produkte mit "digitalen Fingerabdrücken" unauffällig zu kennzeichnen, um Urheberrechts- oder Lizenzverletzungen aufzuspüren und nachzuweisen.

Um Steganographie auszuprobieren bedarf es eigentlich gar keiner eigenen Programmieranstrengungen. Es sind bereits ungefähr ein Dutzend Programme frei im Internet verfügbar und beispielsweise unter www.stego.com abrufbar. Einige mit den wohlklingenden Namen *Hide and Seek, Mandelsteg* und *Pretty Good Envelope* beschreibt Marit Köhntopp in ihrem Artikel. Sicherlich liegt aber ein besonderer Reiz nicht nur für die Schülerinnen und Schüler darin, selbst (re-)aktiv zu werden.

Aber wie funktioniert sie denn nun ...

Da sie in besonderem Maße anschaulich und unter Delphi relativ einfach zu bearbeiten sind, habe ich mich für Bilder als Träger der versteckten Nachrichten entschieden. Bilder bestehen aus einer Folge von Bildpunkten (Pixel) für deren Farbdarstellung auf dem Bildschirm ein RGB-Wert nötig ist. Was sich hier so geheimnisvoll anhört, ist nichts anderes als der jeweilige Farbanteil in Rot, Grün und Blau. Für jede Farbintensität stehen 8 Bit zur Verfügung, so dass sich jeweils 256 Werte speichern lassen. Aus den 256*256*256 Farbintensitäten ergeben sich die rund 16,7 Millionen verschiedene Farben, die ein heutiger Farbmonitor darstellen kann.

Besonders kurz und für das Programmieren wichtig ist die hexadezimale Darstellung der RGB-Werte. Ein weißer Bildpunkt hat die Intensitäten 255 255 255, was auf die hexadezimale Darstellung FF FF FF führt. Entsprechend hat ein schwarzer Bildpunkt die Intensität 00 00 00, während durch FF 00 00 ein roter Punkt entsteht. Zur Speicherung eines Punktes werden also bei 16,7 Millionen Farben 3 Byte benötigt.

Der Einfachheit halber gehe ich nun im folgenden davon aus, eine binäre Nachricht verstecken zu wollen. Jede Nachricht die ich im Computer darstellen kann, lässt sich in diese Form bringen. Als Nachricht wähle ich 01010010, was dem ASCII-Code für den Buchstaben "R" entspricht. Diese Binärnachricht soll in der Pixelfolge*

	FF FF FF	07 07 07	F0 E0 A7	F0 E0 A7	E0 FF 0B	90 A0 00	00 00 00	90 10 A0	

eingebracht werden.

Nun ist zu entscheiden, wo innerhalb der drei Byte die Nachrichtenbits versteckt werden sollen. Für den Anfang soll das niederwertigste Bit des Blau-Anteils jedes Bildpunktes ein Nachrichtenbit tragen. Höherwertige Bits scheiden aus, das sie die Farbintenstiät zu stark beeinflussen. Reduziert auf die Blauanteile ergibt sich folgende Tabelle:*

hex.	FF	07	A7	A7	0B	00	00	A0	
bin.	1111 1111	0000 0111	1010 0111	1010 0111	0000 1011	0000 0000	0000 0000	1010 0000	

Kombiniert mit den Nachrichtenbits ergibt sich:*

	0	**1**	**0**	**1**	**0**	**0**	**1**	**0**	
	1111 111**0**	0000 011**1**	1010 011**0**	1010 011**1**	0000 101**0**	0000 000**0**	0000 000**1**	1010 000**0**	

Und schließlich für die RGB-Werte der Pixel:*

	FF FF F**E**	07 07 0**7**	F0 E0 A**6**	F0 E0 A**7**	E0 FF 0**A**	90 A0 0**0**	00 00 0**1**	90 10 A**0**	

Die Blauwerte des Bildes verändern sich damit allenfalls um eine Farbstufe. Unser Auge kann diese leichte Veränderung nicht bemerken. (Bei einer Analyse der Datei könnten allerdings die zu 00 00 0**1** veränderten schwarzen Bildpunkte auffallen.)

Eine kleine Überschlagsrechnung zeigt welche Datenmengen auf die beschriebene Weise in eine Bilddatei eingebracht werden können. In einem Bild mit 320 mal 240 Pixeln haben so 76800 Bit Platz. Bei einer Zeichenlänge von 8 Bit können 9600 Buchstaben versteckt werden. Allerdings haben wir auch eine Bilddatei die mindestens 320 * 240 * 3 = 230400 Byte groß ist.

Selbstverständlich ist man nicht gezwungen jeden Bildpunkt zu verändern, auch ist können andere oder gleichzeitig verschiedene Farben "geimpft" werden. Dem Einfallsreichtum stehen hier Tür und Tor offen. Im Blick behalten werden sollte lediglich dabei, dass die Vorgehensweise ja auch dem Empfänger zur "Entblätterung" der Nachricht mitgeteilt werden muss. Hier liegt ja, wie oben schon erwähnt, die eigentliche Schwachstelle der Steganographie. Ist dem Lauscher der Schlüssel einmal bekannt, ist der Aufwand zum Herausfiltern sehr gering, auch wenn er viele harmlose Nachrichten bearbeiten muss.

Technische Grundlagen: Hintergrundinformationen zum BMP-Format und zu Delphi-Komponenten

Um die Vorteile zu nutzen, die Delphi für eine einfache Realisierung mit sich bringt, ist es auch nötig, einige Beschränkungen vorzusehen. Die Bearbeitung von GIF- oder JPEG-Bildern ist aufgrund ihres hohen Verbreitungsgrades im Internet zunächst naheliegend. Diese Formate werden aber nicht von den

Standardkomponenten verarbeitet. Mit der Komponente TImage können aber beliebige BMP-Dateien geladen werden.

Eine Verwendung der Standardkomponente TImage von Delphi erfordert allerdings für die Steganographie die Verwendung von BMP-Grafiken mit 16,7 Millionen Farben, da die Grafiken immer im diesem Format abgespeichert werden. Verzichtet man auf die Anzeige der Grafik, entfällt diese Einschränkung selbstverständlich. Jedoch ist es wesentlich motivierender die Grafik vor und nach dem Steganographieren zu sehen. Die Veränderung der Bildinformation durch die selbst erdachten Steganographie-Verfahren kann während der Programmentwicklung anhand eines einfarbigen Bildes kontrolliert werden.

Der Einsatz von Delphi-Sprachelementen bleibt durchaus überschaubar. Neben den üblichen Dialogkomponenten TButton, TEdit, TLabel, den Dateidialogen OpenDialog und SaveDialog, die das Dateihandling komfortabel und übersichtlich machen, genügt es die Komponente TImage einzuführen. Die Eigenschaft Picture liefert die Methoden zum Laden und Speichern. Die Eigenschaft Canvas erlaubt den gezielten Zugriff auf die Bildpunkte über Pixels[x,y]. Allerdings erfordert die Veränderung der Farbinformation auf der Ebene der Bits etwas Vorarbeit.

Quellen:

Markus Kuhn: *"Moderne Kryptographie - Hintergründe und Auswirkungen aktueller Chiffrierverfahren"* in: Computer und Unterricht 18, Friedrich Verlag, Selze Mai 1995

Marit Köhntopp: *"Sag´s durch die Blume"* in: iX 04/96, Heise
Internet: www.netuse.de/~mk/publikationen/steganographie/index.html oder
www.koehntopp.de/marit/ publikationen/steganographie/index.html.

Möller, S./Pfitzmann, A./Stierand, I.: *"Rechnergestützte Steganographie: Wie Sie funktioniert und warum folglich jede Reglementierung von Verschlüsselung unsinnig ist"*, in: DuD, Datenschutz und Datensicherung 18/6 (1994) S. 318-326
Internet: www.informatik.uni-hildesheim.de/FB4/Projekte/sirene/publ/MoePS_94.ps.gz