

Dr Markus Kuhn
University Lecturer



UNIVERSITY OF
CAMBRIDGE

Computer Laboratory

15 JJ Thomson Avenue
Cambridge CB3 0FD
United Kingdom

M Kuhn · Comp Lab · JJ Thomson Ave · Cambridge CB3 0FD · UK

Herrn Willi Beiß

Behörde für Inneres

Landeswahlleiter

Johanniswall 4

20095 Hamburg

Willi.Beiss@bfi-a.hamburg.de

phone +44 1223 334676
fax +44 1223 334678
email Markus.Kuhn@cl.cam.ac.uk
web www.cl.cam.ac.uk/~mgk25/
date 2007-11-04

Bericht über eine Kurzuntersuchung zur Einschätzung des Risikos kompromittierender RF Abstrahlungen eines digitalen Wahlstifts

Am 26. Oktober 2007 besuchte mich Herr Gordian Kaulbarsch von der Hamburger Behörde für Inneres, mit einem dotVote Wahlsystem, bestehend aus einem Laptop-Computer, acht digitalen Wahlstiften und drei USB Dockingstationen. Ich hatte dann einen Tag lang die Gelegenheit, im Beisein von Herrn Kaulbarsch in unserem Labor die Sicherheit des Systems im Hinblick auf das Abhörisiko durch *kompromittierende Radio-Abstrahlungen* zu untersuchen und abzuschätzen.

Hintergrund

Elektronische Signale breiten sich nicht nur entlang elektrischer Leitungen aus, sondern erzeugen dabei immer auch elektromagnetische Wellen. Dieser Effekt wird bei Sendeantennen gezielt ausgenutzt, führt aber auch bei allen anderen Leitungen zu (ungewünscht) abgestrahlten schwachen Radiosignalen, welche beispielsweise Funkempfänger stören können. Mit Hilfe von geeigneten Empfängern und Auswertetechniken ist es manchmal möglich, auf diese Art aus einigem Abstand Informationen über ein Signal aus dem Inneren einer elektronischen Schaltung zu gewinnen, ohne dass dies beabsichtigt war. Wir sprechen von kompromittierenden Radio-Abstrahlungen wenn solche unerwünschten Signale es dem Empfänger ermöglichen vertrauliche Daten zu rekonstruieren.

Die Gefahr der Abhörbarkeit kompromittierender Abstrahlungen wird dadurch gemindert, dass ein Abhörer diese (meist sehr schwachen) Signale zuerst einmal von den vielen anderen Radiosignalen in der Umgebung trennen muss, wie etwa andere Sender, andere elektronische Störsignale, atmosphärisches Rauschen, sowie das thermische Eigenrauschen der Antenne. Dabei kann eine Richtantenne ebenso helfen wie ein möglichst empfindlicher und störtester Radioempfänger der auf einen Frequenzbereich eingestellt ist in dem das Hintergrundrauschen besonders schwach und die kompromittierende Abstrahlung zugleich relativ stark ist.

Darüber hinaus hilft es einem Abhörer erheblich, wenn das abgehörte Signal viel Redundanz enthält, so dass andere Störungen nicht so sehr ins Gewicht fallen. Dies ist insbesondere bei Videosignalen gegeben die, aufgrund ihres häufig und regelmäßig wiederholten Bildinhaltes, mit geeigneter Ausrüstung relativ einfach von Umgebungsrauschen getrennt und ausgewertet werden können. Dies wurde in der Vergangenheit bereits bei verschiedenen digitalen

Displays gezeigt, unter anderem bei zwei bis vor kurzem in den Niederlanden eingesetzten Wahlmaschinen.

Untersuchungsziel

Ich konzentrierte mich in dieser Untersuchung ausschließlich auf die digitalen Wahlstifte, da diese einen Bildsensor enthalten der ähnlich wie eine kleine Infrarot-Videokamera betrieben wird. Daher war zu erwarten, dass dieser Sensor und die ihn betreibende Elektronik ein periodisches (und daher hochredundantes) Videosignal erzeugt. Der Bildsensor betrachtet die unmittelbare Umgebung der Stiftmine auf dem Wahlformular, welches mit einem feinen Punktraster überzogen ist in das die Koordinaten des Papierblattes kodiert wurden. Aufgrund des standardisierten Punktmusters und Layouts des Wahlzettels könnte ein Abhörer, dem es gelänge das Videosignal zu empfangen, die Stelle an der der Benutzer sein Kreuz macht rekonstruieren.

Ich habe im Rahmen dieser Kurzuntersuchung nicht versucht, die USB-Verbindung zwischen dem Wahlstift und dem Laptop abzuhören. Meiner praktischen Erfahrung nach ist es sehr schwierig, von USB-Verbindungen aus mehr als unmittelbarer Umgebung (wenige Zentimeter vom Kabel) Daten zu rekonstruieren wenn diese nur kurzzeitig und einmalig übertragen werden. Eine Ausnahme bestünde lediglich, falls die übertragenen Daten hochgradig redundant wären. Leider stand mir keine Dokumentation darüber zur Verfügung, in welchem Format die vom Stift aufgezeichneten Striche übertragen werden. Sollte es sich dabei nur um eine kurze Folge von als Binärzahlen kodierte Koordinaten von Liniensegmenten handeln, erscheint es mir kaum praktikabel, aus einer kurzen USB-Abstrahlung deutlich mehr Information zu gewinnen als die Anzahl oder Länge der gemachten Striche, wenn diese proportional zur insgesamt übertragenen Datenmenge ist. Sollte dagegen eine wesentlich redundantere Darstellung der Striche übertragen werden, etwa eine unkomprimierte Rastergraphik der mit dem Stift gemalten Striche auf dem Wahlzettel, dann wäre es sinnvoll diesen Aspekt des Systems eingehender zu untersuchen. Dabei kann es einfacher sein, durch Firmware und Treiberänderung gleich den USB-Datenverkehr zu verschlüsseln als eine ausführliche Untersuchung der kompromittierenden Abstrahlung zu beauftragen.

Ich habe im Rahmen dieser Untersuchung ebenfalls nicht den im Stift enthaltenen Bluetooth-Sender untersucht, da mir versichert wurde das dieser durch eine Firmwareänderung durch den Hersteller zuverlässig und dauerhaft ausgeschaltet wird. Des weiteren habe ich nicht das Display des benutzten Laptops untersucht, da mir versichert wurde, dass dies ohnehin öffentlich einsehbar sei und die Software dort keinerlei vertrauliche Daten anzeigen würde.

Zusammengefasstes Untersuchungsergebnis

Ich konnte in Abständen von mehr als einem halben Meter vom Stift in einer normalen Büroumgebung keine Anzeichen kompromittierender Radio-Abstrahlungen feststellen. Erst als ich den Abstand zur Empfangsantenne auf weniger als 30 cm reduzierte wurden potentielle kompromittierende Abstrahlungen erkennbar, die zwar erkennen lassen, wann und wie oft genau die Mine des Stiftes auf das Papier gedrückt wurden, und die auch die Verarbeitung eines Videosignales in der Stiftelektronik erkennen lassen. Aber selbst diese in unmittelbarer Nähe des Stiftes aufgefangenen Signale geben einem Abhörer immer noch keinen klaren und praktisch zuverlässig auswertbaren Hinweis darauf, was der Benutzer des Stiftes gewählt hat, da das Punktmuster nicht erkennbar war.

Zusammenfassend kann ich keinem Angreifer auf das dotVote Wahlsystem die Auswertung kompromittierender Abstrahlungen als praktikable Technik zur Verletzung des Wahlgeheimnisses empfehlen. Selbst wenn es möglich wäre aus den Abstrahlungen des Stiftes die markierten Papierkoordinaten zu rekonstruieren, wofür ich in dieser Kurzuntersuchung keinen Hinweis fand, wäre dies nur in unmittelbarer Umgebung des Stiftes (< 30 cm)

praktikabel. Wenn ein Angreifer aber schon spezielle Abhörelektronik direkt in einer Wahlkabine (z.B. unter der Tischplatte) verstecken könnte, dann gäbe es wesentlich einfachere und zuverlässigere Techniken (insbesondere versteckte digitale Miniaturkameras, ggf. auch Körperschallmikrophone, Drucksensoren, etc.) um an die gleiche Information zu kommen, und diese Abhörtechniken würden ebenso bei traditionellen Wahlen mit normalen Stiften funktionieren. Daher denke ich nicht, dass die im dotVote-System eingesetzten Wahlstifte durch mögliche kompromittierende Abstrahlungen in irgend einer Weise das Wahlgeheimnis im Vergleich zu traditionellen Papierwahlen zusätzlich gefährden. (Sie unterscheiden sich in dieser Hinsicht deutlich von zwei niederländischen Wahlsystemen, bei denen klar auswertbare kompromittierende Abstrahlungen in weit mehr als 10 m Entfernung nachgewiesen werden konnte!)

Technische Einzelheiten meiner Untersuchung sind im folgenden Anhang erläutert.

Markus Kuhn

Anhang

Untersuchte Hardware

Anoto/Logitech/Diagramm Halbacht dotforms pen iO₂ BT (modifizierte dotVote Firmware)

Eingesetzte Messtechnik

Ich benutzte in dieser Untersuchung einen breitbandigen, sehr empfindlichen Meßempfänger (Dynamic Sciences R1250) der speziell für die Analyse kompromittierender Abstrahlungen entwickelt wurde. Diesen verband ich mit einer logarithmisch-periodischen Breitbandmessantenne für den Frequenzbereich 200–1000 MHz, sowie mit einem selbstentwickelten Signalverarbeitungssystem das das Zwischenfrequenzsignal des Empfängers mit frei wählbaren Synchronsignalen versieht und in eine für die Echtzeitausgabe auf einem Computermontor geeignete Rasterform umwandelt. Alle Messungen fanden in einer normalen Büroumgebung statt, also nicht in einem elektromagnetisch abgeschirmten Raum.

Messergebnisse

Ich konnte in unmittelbarer Nähe der Messantenne schnell drei verschiedene Zustände des Stiftes unterscheiden. Mit aufgesetzter Stiftkappe war der Stift deaktiviert, und es waren überhaupt keine Abstrahlungen zu erkennen. Sobald ich die Kappe des Stiftes abzog (was ein Magnetsensorchip im Stift registriert), wurden regelmäßige Taktsignale erkennbar, welche aber im Umgebungsrauschen verschwanden sobald ich den Stift mehr als einen halben Meter von der Antenne entfernte. Die Taktsignale waren in ihrer Frequenz wesentlich weniger stabil als dies zur Erzeugung eines gut erkennbaren Videosignales notwendig ist, was andeutet, dass wesentliche Teile der Stiftelektronik von einem nicht-quarzstabilisierten Oszillator getrieben werden.

Nur während ich die Stiftmine gegen eine Fläche drückte wurde die Videoelektronik des Stiftes aktiv, und es wurde ein periodisches Signal mit einer Wiederholfrequenz von etwa 74.6 Hz sichtbar (13.4 ms Periode). Dieses Signal war an verschiedenen Frequenzen zwischen etwa 510 MHz und 1000 MHz (der oberen Grenzfrequenz des eingesetzten Meßempfängers) sichtbar, und ergab in unserem Labor insbesondere bei etwa 584 MHz (mit einer Bandbreite von 20 MHz) eines der besten erzielbaren Signale (etwa -65 dBm am Antenneneingang, verglichen mit etwa -80 dBm Hintergrundrauschen bei ausgeschaltetem Stift). Innerhalb der 13.4 ms langen Periode befand sich ein etwa 1.74 ms langes Zeitintervall in dem die Ausstrahlung eine für ein Videosignal charakteristische Zeilenstruktur annahm, mit einer Zeilenfrequenz von 58.14 kHz (Zeilenperiode 17.2 μ s) und einer Zeilenlänge von etwa 13.12 μ s. Ich konnte lediglich die Zeilenstruktur eines Videosignales erkennen, aber keinen Bildinhalt, und insbesondere keine Spuren eines für die aktuelle Position des Stiftes charakteristischen Punktemusters.

All diese Signale waren aber nur in unmittelbarer Umgebung der Messantenne (< 20 cm Abstand zum im jeweiligen Frequenzband aktiven Dipol) erkennbar. Bei Abständen größer als 30 cm war von einem Videosignal kaum mehr eine Spur zu erkennen, und im Abstand von 50 cm konnte ich bei den für Videosignalen notwendigen Messbandbreiten (5–20 MHz) keinen Unterschied zwischen einem eingeschalteten und einem ausgeschalteten Stift erkennen. Diese geringen Abstände bedeuten dass die Antenne sich noch im Nahfeld des Senders befand, wo die Signalstärke besonders schnell abfällt. (Da die verwendete Antenne nur für Fernfeldmessungen kalibriert war, aber im Fernfeld keine Signale sichtbar waren, kann ich keine Angaben zur Feldstärke im Fernfeld machen.)

Ich öffnete einen der Stifte, um die Videosignale direkt am Sensor zu vergleichen. Dabei fand ich mit einem Oszilloskop ein analoges Bildsignal an zwei der Pins, was darauf hindeutete, dass zwei Zeilen gleichzeitig ausgelesen werden, womit ein Bild etwa 200 Zeilen hätte.

Mögliche weitergehende Untersuchungen

Die größte Leitungslänge im Stift (inclusive Batterie und Infrarot-LED) liegt bei maximal 15 cm. Die Signalverbindung zwischen dem Bildsensor und dem "Anoto CT50A0" Bildsignalverarbeitungschip ist lediglich etwa 25 mm lang. Daher besteht die Möglichkeit dass einige harmonische Frequenzen der beobachteten Signale überhalb von 1000 MHz besser ins Fernfeld abstrahlen als ich dies mit dem eingesetzte Messempfänger, der nur bis 1000 MHz (30 cm Wellenlänge) reicht, feststellen konnten. Falls weitere Abstrahl-Untersuchungen mit diesem Wahlstift geplant sind, würde sich insbesondere eine Untersuchung mit einem Mikrowellenempfänger im Bereich 1–10 GHz anbieten, da die im Gerät vorhandenen kurzen Leitungen für diese Frequenzen evtl. etwas bessere Sendeantennen bilden. Darüber hinaus wäre eine breitbandige Feldstärkemessung im Fernfeld (≥ 1 m Abstand) sinnvoll, wozu eine Schirmkabine erforderlich ist. Entsprechend ausgerüstete Messlabors existieren in Deutschland beispielsweise beim Bundesamt für Sicherheit in der Informationstechnik oder bei der Firma GBS in Diepholz.