Komprommittierende Emissionen

Vortrag: *Hans Georg Wolf & Markus Kuhn* <keine>

Bericht: *ISCS* <iscs@ailis.com>

Jeder kennt das Problem - eine lange Nacht vor dem Rechner, und das Radio funktioniert nicht, solange der Computer eingeschaltet ist.

Der Rechner stört den Radioempfang - und zwar nicht zu knapp.

Da liegt die Idee nicht fern, diese Signale, die der Rechner aussendet, geschickt auszuwerten, um so ein genaues Bild davon zu bekommen, was auf diesen Rechner gearbeitet wird.

Die Idee, Störgeräusche eines Gerätes auszuwerten, ist nicht sehr neu. Schon die frühen Telegraphensender konnten abgehört werden, da es bei jeder Eintastung Stromschwankungen in der Stromversorgung gab. Ein geübter Morser konnte am Flackern einer Glühbirne mitlesen, was gesendet wurde.

1950 hörte der Londoner Geheimdienst die damaligen mechanischen Krytographiemachinen auf eine ähnliche Methode ab - Praktisch, so ist es nichteinmal notwendig, den Krypto-Code der Maschine zu knacken; einfach nur das Ausgabegerät abhören, was den Text im Klartext zu Papier bringt.

In einer beeindruckenen Demonstration wurde gezeigt, mit welch geringem Aufwand es Möglich ist, aus einer Entfernung von ein paar Metern den Bildschirminhalt eines abgehörten Demonstrationscomputer mitzulesen.

Notwendig war lediglich der belauschte Rechner auf dem groß Text zu lesen war (allerdings in einer Schriftart, die es dem Lauscher besonders leicht macht), und in einigen Metern Entfernung eine Antenne, ein alter Multisync-Monitor, desen Frequenzen frei einstellbar waren, sowie eine kleine Ansteuerung. Und verrauscht und nicht hundertprozentig syncronisiert, aber durchaus lesbar erschien der Text des belauschten Rechners auf dem kleinen alten Monitor.

An dieser Stelle sein erwähnt, daß nicht der Monitor der kritische Teil ist, sondern die Grafikkarte, die einen regelrechten Sender darstellt.

Abhören ist mit guten Anlagen noch aus mehr als 70 Metern Entfernung möglich. Mit teuren digitalen Anlagen wäre eine weitaus größere Distanz denkbar.

Eine andere Schwachstelle stellt die Tastatur da. Auch sie sendet spezifische Signale aus, die sich mehr oder weniger problemlos auswerten lassen. Gefährliche Möglichkeiten tun sich auf, wenn man an Geldautomaten denkt, deren Tastatur sich überwachen läßt. Die Banken (über dieses Problem durchaus informiert), reagieren eher schleppend bis garnicht - die Beweislast bei Schäden liegt nach wie vor beim Kunden.

Drucker, Scanner - alles strahlt unbeabsichtigt ab. Nicht nur über Funkwellen, ebenso über das Stromnetz, Heizungsrohre in der Nähe u.ä.

Wie kann man sich vor diesen Lauschangriffen schützen? Das beste ist natürlich das teuerste. Ein Faradayscher Käfig, der die verräterischen Emissionen innerhalb der eigenen Räume beläßt.

Die andere Möglichkeit ist ein breitbandiger Störsender, der allerdings den Standort des Rechners verrät und bei übermäßiger Benutzung Probleme mit der Regulierungsbehörde für Post und Telekomunikation schaffen wird. Spezielle Verschleierungsgeräte können hier schon eher Abhilfe schaffen, indem die Signale des Computers mit eigenen Signalen überlagert werden. Leider auch nicht ganz billig.

Eine andere Möglichkeit wenigstens den Bildschirm gegen den Lauschangriff zu schützen, stellt eine Softwarelösung da. Das Verwenden spezieller Fonts aus denen die hohen Ortsfrequenzanteile (diese sind besonders anfällig gegen Abhören) herausgefiltert worden - ähnlich wie ein zu stark komprimiertes JPG.

Mit dieser einfachen Maßnahme, die allerdings nur bei Kathodenstrahlröhrengeräten (nicht bei Laptops) Wirkung zeigt, läßt sich das Störsignal schon gewaltig dämpfen, allerdings nicht aufheben.

Interessant auch die Möglichkeit auf diese Weise gezielt Information aus einen Rechner herauszuschmuggeln. Da letztendlich nur die schnellen Änderungen des Helligkeitsverlaufs abgegriffen werden können, ist es relativ einfach hinter das sichtbare Computerbild mit leichten kaum erkennbaren Mustern ein weiteres Bild zu legen. Ein einfaches Dithermuster, was bei flüchtiger Betrachtung wie eine graue Fläche aussieht, jedoch bei genauerem Betrachten eine dichte hell-dunkel-Schwankung beinhaltet. So kann ein völlig anderes Bild abgegriffen und versendet werden als das, was mit bloßen Auge erkennbar ist.

Vorstellbar wäre zum Beispiel ein Trojanischer Screensaver, um so einen Rechner bequem von der Straße aus mit einer Antenne zu observieren.

Es bleibt viel zu tun, da das Bewußtsein für dieses Problem noch lange nicht genügend geweckt worden ist.