

Workshop "Paranoia für Fortgeschrittene"

Jan Schejbal

7. Oktober 2009

- 1 **Einleitung**
 - Ziele des Workshops
 - Was nicht behandelt wird
 - Praktische Vorführung: TEMPEST
- 2 **Angriffe**
 - Elektromagnetische Angriffe
 - Akkustische Angriffe
 - Optische Angriffe
 - Hardware
- 3 **Abschluss**
 - Schutz
 - Abschluss

- 1 Einleitung
 - Ziele des Workshops
 - Was nicht behandelt wird
 - Praktische Vorführung: TEMPEST
- 2 Angriffe
 - Elektromagnetische Angriffe
 - Akkustische Angriffe
 - Optische Angriffe
 - Hardware
- 3 Abschluss
 - Schutz
 - Abschluss

Sinn des Workshops

- Interessante Angriffe vorstellen
- Zeigen, dass effektiver Schutz für privat nicht möglich
- NICHT: Paranoia auslösen, Schutzmaßnahmen empfehlen
- Existenz der Bedrohungen „im Hinterkopf behalten“
 - falls im Beruf zuständig für Hochsicherheitssysteme
 - falsches Sicherheitsgefühl vermeiden
- Kein Sicherheitslehrgang

Sinn des Workshops

- Unvollständig
 - viel Forschung nichtöffentlich (auch Geheimdienste)
 - nur grober Überblick über Angriffe
- Nur belegte Fakten, keine Verschwörungstheorien
 - deklassifiziertes Material der NSA ¹
 - Öffentliche Forschung
 - gleiches Thema vermutlich nichtöffentlich schon lange erforscht

¹David G. Boak: A History of U.S. Communications Security,

1 Einleitung

- Ziele des Workshops
- **Was nicht behandelt wird**
- Praktische Vorführung: TEMPEST

2 Angriffe

- Elektromagnetische Angriffe
- Akkustische Angriffe
- Optische Angriffe
- Hardware

3 Abschluss

- Schutz
- Abschluss

Schwachstelle Mensch

- Dummheit (Phishing, Viren-Anhänge)
- Bequemlichkeit
- Social Engineering
- Bestechung, Erpressung
- Verrat aus Rache
- „Gummischlauch-Kryptoanalyse“
- Infiltration
- Sekretärin oder Putzfrau kann reichen!
- Schutz sehr schwierig
- Wirtschaftsspionage: 70% durch eigenes Personal ²

²<http://www.heise.de/newsticker/--/meldung/146259>

Schwachstelle Software

- Zahlreiche Sicherheitslücken
 - Updates aktuell halten ist schwer
 - Viele Lücken unbekannt
 - Versierte Angreifer dürften genug kennen
 - viele Angriffswege (Browser, Plugins)
- Angriffe auf Updates oft möglich
- Bewusste Hintertüren?
- Weitreichendes Themenfeld
 - genug für eigene Vortragsreihe
- langweilig

Physikalische Sicherheit

- Wind verweht Dokumente
 - Fangnetze!
- Müll durchsuchen
- Einbruchsdiebstahl
- In der Bahn vergessene Geheimdokumente ³
 - Speichermedien oder Papier
- Bei Ebay verkaufte Festplatten
 - Festplatten sind auch in Kopierern
- Installation von Wanzen

³<http://www.welt.de/politik/article3594254/Minister-laesst-geheime-Dokumente-im-Zug-liegen.html>

- 1 Einleitung
 - Ziele des Workshops
 - Was nicht behandelt wird
 - **Praktische Vorführung: TEMPEST**
- 2 Angriffe
 - Elektromagnetische Angriffe
 - Akkustische Angriffe
 - Optische Angriffe
 - Hardware
- 3 Abschluss
 - Schutz
 - Abschluss

Praktische Vorführung

- Vorführung eines TEMPEST-Angriffs
- Normaler Röhrenmonitor
 - unmanipuliert
- Normales Weltempfänger-Radio
 - unmanipuliert, evtl. aber leicht defekt
- Einfaches animiertes Bild
 - Animation um Effekt besser erkennen zu können
 - Nur schwarz-weißes Bild, keine „magischen Eigenschaften“
- Erklärung folgt

- 1 Einleitung
 - Ziele des Workshops
 - Was nicht behandelt wird
 - Praktische Vorführung: TEMPEST
- 2 **Angriffe**
 - **Elektromagnetische Angriffe**
 - Akkustische Angriffe
 - Optische Angriffe
 - Hardware
- 3 Abschluss
 - Schutz
 - Abschluss

Abgrenzung

- Bewusste Funkausstrahlung nicht betroffen
 - Funktastaturen (unsicher)
 - DECT-Telefone (unsicher)
 - <https://dedected.org>
 - Leute von der TUD beteiligt
 - WLAN (unsicher wenn schlecht verschlüsselt)
 - Angriffe auch auf WPA-TKIP
 - GSM (unsicher)
 - Forscher haben Arbeit daran teilweise unter komischen Umständen abgebrochen
- Wanzen etc. nicht betroffen

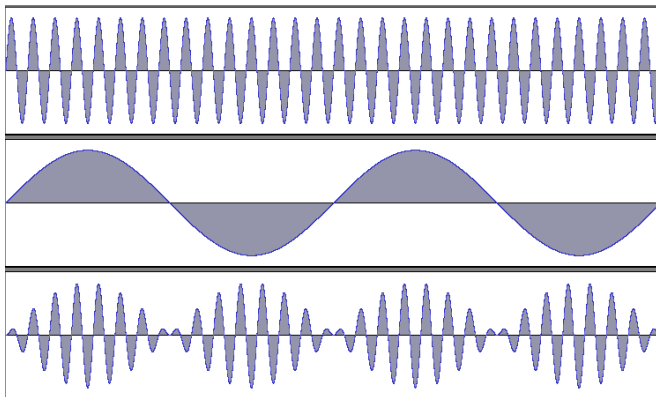
Physikalische Grundlagen

- fließender Strom erzeugt elektromagnetische Abstrahlung
- Induktion in Leitern
- kann gemessen/aufgefangen werden
- Durchdringt Wände
- Wird von Leitungen transportiert
- Abschirmung möglich, nicht einfach

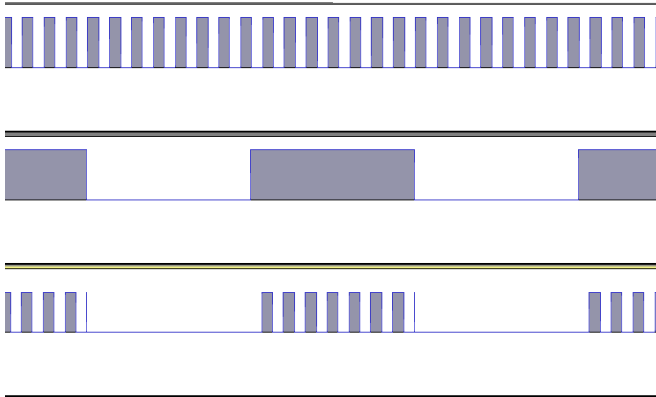
Erklärung der Vorführung

- Röhrenbildschirm
 - Elektronenstrahl tastet Bildschirm ab
 - Wird hell/dunkel (bzw. hier ein/aus) geregelt
- Amplitudenmodulation
 - Hochfrequente Trägerwelle
 - Frequenz am Radio
 - Schallwelle
 - Modulation (Multiplikation/“Begrenzung”)

Amplitudenmodulation



Amplitudenmodulation



- Annäherung mit Rechteckschwingung
- Modulierte Welle entspricht Pixelfolge beim Abtasten

TEMPEST: Ausnutzung der elektromagnetischen Abstrahlung von Geräten

- Röhrenbildschirm besonders anfällig
 - Bildschirminhalt vollständig rekonstruierbar
 - umgebauter Fernseher reicht
 - Reichweite: dutzende Meter
- Alle Geräte betroffen
 - Wahlcomputer
- Meist: besseres Equipment = höhere Reichweiten
- Der NSA und den Soviets bekannt mindestens seit 50ern
 - militärische Codierfernseher
 - real ausgenutzt

Verwendungsmöglichkeiten

- Abhören von Informationen
- Gezielt gebaute/manipulierte Geräte
 - unbemerkte Datenübertragung/Hintertüren
 - gut mit Versehen erklärbar

Leitungen

- Strom- und Datenleitungen betroffen
- Signaleinspeisung durch Induktion
- sehr hohe Reichweite
- können selbst wieder abstrahlen
- Filtern, wo das Kabel die Abschirmung verlässt
- Ferritkerne, Filter

Stromverbrauch

- Stromverbrauch schwankt mit Aktivität/Schaltvorgängen
 - teilmechanische Kryptogeräte: Motoren/Relais
 - Mikroelektronik: Transistoren
- Smartcard-Angriffe
 - können geheime Schlüssel bestimmen
 - z. B. Stromverbrauch
 - gezielte Gegenmaßnahmen
- Filter/Glättung (Kondensatoren)

Schutz

- Abschirmung (Faradayscher Käfig)
 - Gewichtsprobleme
 - Filterung von Strom- und Signalleitungen nicht vergessen
- Abstand
 - Sensible Räume im Gebäudeinneren
 - Zone rund um Gebäude kontrollieren
- TEMPEST-sichere Geräte
 - entsprechend entworfen und gebaut
 - viel mehr als nur Abschirmung/Filter

Schutz

- Störsender
 - Nicht sehr empfehlenswert
 - meist illegal
- Betrieb vieler Geräte gleichzeitig
 - Signalvermischung
 - legale Form des Störsenders
 - vermutlich nicht sehr sicher
 - früher von NSA empfohlen

Beispiele

- TEMPEST
 - (Röhren-)Bildschirme
 - Missbrauch als Radiosender ⁴
 - Diverse Kabel
 - z. B. auch Kabel zum Flachbildschirm
 - Wahlcomputer ⁵
 - billig (Laptop + 50-EUR-Funkscanner)
 - Kabel zum Display
 - PS/2 und USB-Kabeltastaturen ⁶

⁴ <http://www.erikydy.de/tempest/>

⁵ <http://www.heise.de/newsticker/meldung/>

Hacking-at-Random-CCC-demonstriert-TEMPEST-Messung-bei-Wahlcomputern-751445.html

⁶ <http://lasecwww.epfl.ch/keyboard/>

Beispiele

- Stromleitungs-TEMPEST
 - PS/2-Tastaturen ⁷
 - billig (150 \$)
 - nicht bei Notebooks
- Stromverbrauch
 - SmartCards ⁸
 - alte Kryptogeräte ⁹

⁷ <http://cansecwest.com/csw09/csw09-barisani-bianco.pdf>

⁸ http://www.sec.informatik.tu-darmstadt.de/pages/lehre/SS07/itsec/uebungen/ueb08_folien.pdf#page=7

⁹ http://www.governmentattic.org/2docs/Hist_US_COMSEC_Boak_NSA_1973.pdf#page=88

- 1 Einleitung
 - Ziele des Workshops
 - Was nicht behandelt wird
 - Praktische Vorführung: TEMPEST
- 2 **Angriffe**
 - Elektromagnetische Angriffe
 - **Akkustische Angriffe**
 - Optische Angriffe
 - Hardware
- 3 Abschluss
 - Schutz
 - Abschluss

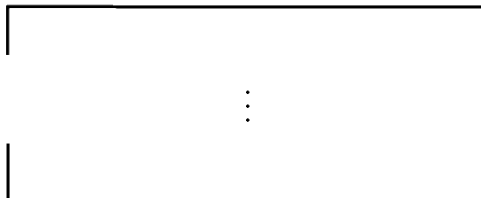
Grundlagen

- Viele Geräte erzeugen Schall
 - Tastaturen
 - Nadeldrucker/Fernschreiber
 - Festplatten
- Schall kann teilweise analysiert werden
- Abhören auf vielfache Art und Weise möglich
 - Lasermikrofone
 - Wanzen
 - Bestehende Audioverbindungen (Hintergrundgeräusche)
 - meist hohe Qualität nötig

Erschütterungen

- Erschütterungen scheinen auch relevant zu sein¹⁰
 - vermutlich ähnlich wie normaler Schall, schwerer abschirmbar

Seismics



(b) (1)
(b) (3)-50 USC 403
(b) (3)-P.L. 86-36

SECRET - Handle via COMINT channels only

¹⁰ http://www.nsa.gov/public_info/_files/cryptologic_spectrum/tempest.pdf#page=3

Tastaturen

- Abgreifen über Wanzen, Lasermikrofon (Fenster oder Laptop)
- Abgriff am Laptop, einfache Mittel ¹¹
 - Reichweite über 30 Meter
 - unter 100\$
- Statistische Analyse möglich
 - liefert nicht direkt z. B. gute Passwörter
 - aber genug um Passwort erratbar zu machen
 - auch ohne Kalibrierung brauchbare Ergebnisse
- Nur ein Beispiel genannt
 - viele Varianten
 - recht effektiv

¹¹<http://cansecwest.com/csw09/csw09-barisani-bianco.pdf#page=43>

Nadeldrucker

- Nadeldrucker stark betroffen ¹²
- Kalibrierung nötig
- nicht komplett zuverlässig
- Immer noch relevant
 - Arztpraxen
 - Kontoauszugsdrucker
- wurde aktiv genutzt im Militärbereich
 - Fernschreiber etc.

¹²<http://www.heise.de/newsticker/meldung/>

- 1 Einleitung
 - Ziele des Workshops
 - Was nicht behandelt wird
 - Praktische Vorführung: TEMPEST
- 2 **Angriffe**
 - Elektromagnetische Angriffe
 - Akkustische Angriffe
 - **Optische Angriffe**
 - Hardware
- 3 Abschluss
 - Schutz
 - Abschluss

(eigentlich) Offensichtliches

- Window Transparency Information Disclosure ¹³

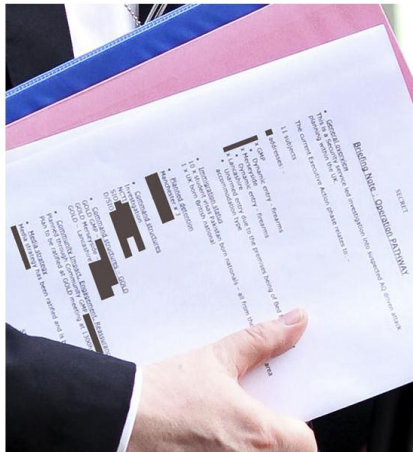
An information disclosure attack can be launched against buildings that make use of windows made of glass or other transparent materials by observing externally-facing information through the window.

¹³<http://www.caughq.org/advisories/CAU-2007-0001.txt>

(eigentlich) Offensichtliches

- Window Transparency Information Disclosure
 - auf Deutsch: durchs Fenster schauen
 - Bildschirme, offen liegende Dokumente
 - aber auch Wandkalender, Post-Its, Telefondisplays etc.
- auch ein Problem bei Besuch im Büro
 - Root-Passwort an der Tafel der Admin-Kammer

(eigentlich) Offensichtliches



(eigentlich) Offensichtliches

- Das war der geheime Plan für die Anti-Terror-Razzia ¹⁴
 - Razzia eilig vorgezogen
- Bob Quick (Chef der Anti-Terror-Einheiten)
 - zurückgetreten
- Kameras werden immer besser

¹⁴ <http://www.tagesschau.de/ausland/scotlandyard102.html>

(eigentlich) Offensichtliches

- auf Tastatur schauen
 - auch mit Hilfsmitteln (Kamera/Teleskop)
- Handbewegungen können auch schon verräterisch sein

weniger Offensichtliches



- Das ist der Schlüssel für Diebold-Wahlcomputer ¹⁵
- Schlüssel können aufgrund von Fotos nachgebaut werden

¹⁵

<http://www.netzpolitik.org/2007/spass-mit-wahlcomputern-einfach-schluesel-nachbauen/>

Spiegelungen

- Brillengläser, Augen, Teekannen etc. spiegeln ¹⁶
 - klein und verzerrt
 - Teleskop und Entzerrungssoftware
 - Für 1000 EUR Reichweite von 10 m
 - Für 20.000 EUR Reichweite von 30 m

¹⁶ <http://www.infsec.cs.uni-sb.de/projects/reflections/>

- 1 Einleitung
 - Ziele des Workshops
 - Was nicht behandelt wird
 - Praktische Vorführung: TEMPEST
- 2 **Angriffe**
 - Elektromagnetische Angriffe
 - Akkustische Angriffe
 - Optische Angriffe
 - **Hardware**
- 3 Abschluss
 - Schutz
 - Abschluss

Chip-Hintertüren

- öffentlich bekannte Arbeiten eher theoretisch
- viele - auch offizielle - Verschwörungstheorien
- Chip kann unbemerkt „Zusatzfunktionen“ bekommen
- Kaum auffindbar
- Befürchtungen vor „Cyberkrieg“¹⁷
 - Lahmlegen kompletter Infrastruktur
 - China!

¹⁷

<http://www.gulli.com/news/pentagon-nationale-sicherheit-2008-05-04/>

Handies

- Software!
 - Blackberry-Vorfall in den Vereinigten Arabischen Emiraten
 - Spionagetrojaner stümperhaft flächendeckend eingespielt ¹⁸
 - Backdoors?
 - Unbemerkte Firmwareupdates?
 - Manipulation bei physikalischem Zugriff möglich
- Hardwaremanipulation möglich

¹⁸<http://news.bbc.co.uk/2/hi/8161190.stm>

Computer

- Computer und Zubehör manipulierbar
- Viren für Apple-Tastaturen ¹⁹

¹⁹ <http://www.netzwelt.de/news/80413-apple-tastatur-hoert.html>

Spionagehardware

- Wanzen
- Keylogger (Keyghost)
- Kameras
- ...
- Hotels oft verwandt!

- 1 Einleitung
 - Ziele des Workshops
 - Was nicht behandelt wird
 - Praktische Vorführung: TEMPEST
- 2 Angriffe
 - Elektromagnetische Angriffe
 - Akkustische Angriffe
 - Optische Angriffe
 - Hardware
- 3 Abschluss
 - Schutz
 - Abschluss

Abwägung

- Absolute Sicherheit nicht möglich
- sehr hohe Sicherheit nicht praktikabel
- Abwägung Schutzaufwand - Gefahrenpotential
- Angriff teuer genug machen reicht
- Sicherheit nur so gut wie schwächstes Glied
 - Abschirmung sinnlos wenn Personal Geheimnisse verrät
 - Es gibt viel wichtigere Probleme!

Einfache Maßnahmen sinnvoll

- Kryptographie (z. B. TrueCrypt) schützt immer noch gut
 - Diebe
 - Festplatte bei Reparatur
 - Polizei
 - Geheimdienste behalten ihre Geheimnisse gern
 - erschwert auch professionelle Spionage deutlich
 - geringer Aufwand
 - auch für private Computer wichtig
 - E-Mails, Browser, Dokumente
- Angriffe ohne Kryptographie viel zu leicht
 - gerade bei E-Mail, Chat
 - PGP/GPG, OTR
- Ordentliche Systeme verwenden
 - eigener Vortrag

Schutzmaßnahmen (theoretisch)

- strengste Sicherheitsüberprüfung für Personal inkl. Hilfskräfte
- Nur sichere Software verwenden (unrealistisch), kein Netzwerk
- Hardware aus vertrauenswürdigen Quellen beziehen
 - Theoretisch kann Hintertür überall sein (China!)
- Abschirmung
 - Fensterloser Raum
 - Kupferverkleidung
 - Leitungsfiler
 - Schalldämmung
 - Kontrolle ein- und ausgebrachter Geräte
 - manipulierte Handies
 - unbemerkt in Kleidung versteckte Wanzen

- 1 Einleitung
 - Ziele des Workshops
 - Was nicht behandelt wird
 - Praktische Vorführung: TEMPEST
- 2 Angriffe
 - Elektromagnetische Angriffe
 - Akkustische Angriffe
 - Optische Angriffe
 - Hardware
- 3 Abschluss
 - Schutz
 - Abschluss

Weiterführendes

- Englischsprachige Wikipedia
 - viele Infos über Geheimdienste
 - Arbeitsweisen
 - Verweise auf Bücher
- Wikileaks
 - Seite zum anonymen Veröffentlichen „geleakter“ Dokumente
 - immer wieder gute Sachen dabei
- Governmentattic
 - Sammlung via FOIA befreiter Dokumente
- Vorträge diverser Veranstaltungen
 - CCC-Kongresse
 - Blackhat
 - ...
- Google

Vielen Dank für die Aufmerksamkeit

- Folien gibt es im Netz
 - inklusive Quellcode
 - erstellt mit \LaTeX Beamer Class
 - und eigenem Programm outlinebeamer
 - <http://outlinebeamer.sourceforge.net>
- Fragen?