Fig. 1

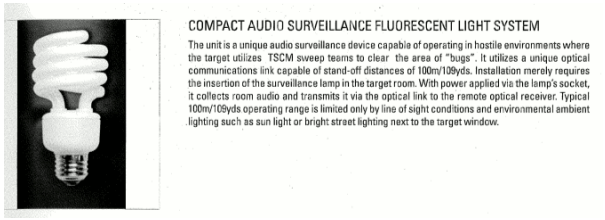

Fig. 2

1. Alles sehen, nix raffen

- Was können die?
- Was können wir dagegen tun?
- Warum haben die uns nicht längst eingedost?
- Was tun?

(cf. Fig. 1)

2. Spielzeug I

(cf. Fig. 2)

(Aus dem elaman-Katalog)

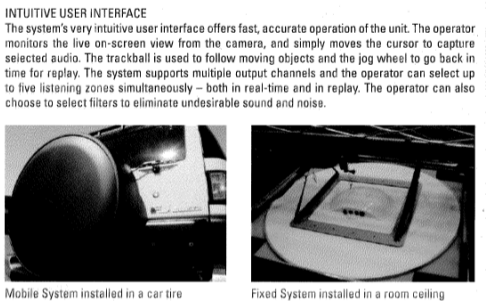

Fig. 3

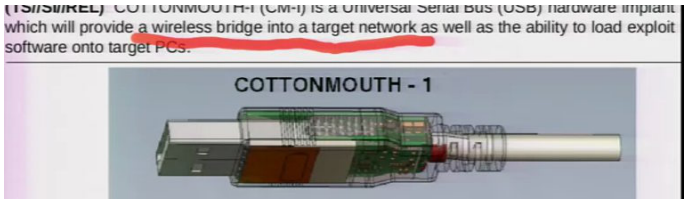

Fig. 4

3. Spielzeug II

(cf. Fig. 3)

(Aus dem elaman-Katalog)

Was dieses Ding tut: Mit vielen Mikrofonen zeichnet das ein komplettes Schallfeld auf; ähnlich wie bei einem Hologramm ist in den aufgezeichneten Daten die komplette räumliche Information im Schallkegel enthalten, so dass auch im Nachhinein noch der Schall an einer bestimmten Stelle rekonstruierbar ist. Damit könnten die Leute z.B. aus dem Gesamtlärm einer Demo einzelne Gespräche rausziehen.

4. Spielzeug III

(cf. Fig. 4)

(Aus den Snowden-Leaks)

Was das Ding tut: An einen Rechner gesteckt versucht es, Sicherheitslücken im Betriebssystem auszunutzen. Findet es sie, kann es auch noch gleich eine WLAN-Verbindung unabhängig vom Wirtscomputer machen – das alles in einem einfachen USB-Stecker.

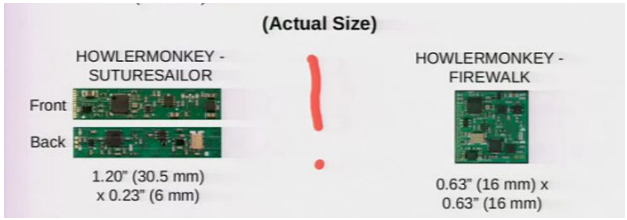

Fig. 5

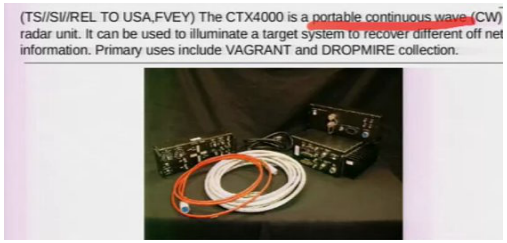

Fig. 6

5. Spielzeug IV

(cf. Fig. 5)

(aus den Snowden-Leaks)

Was die Dinge tun: Im Wesentlichen Ähnliches wie das Cottonmouth von der letzten Folie, nur bauen die die Sachen (in der Größenordnung von Zentimetern) in Computer ein, während sie auf dem Postweg sind. Und diese speziellen Teile haben kein WLAN an Bord, dafür gehen sie aber direkt in die Netzwerkbuchse.

6. Spielzeug V

(cf. Fig. 6)

(aus den Snowden-Leaks)

Das das Ding tut: Das ist ein starker Sender für Mikrowellen etwa im Bereich von Mobiltelefonen (mit externem Verstärker bis zu 1 kW. Damit bestrahlt die NSA Räume, in die sie vorher winzige (Größenordnung Millimeter) Wanzen gebracht hat, die die Reflexion dieser Strahlung moduliert – auf die Weise kann die Wanze fast völlig passiv sein. Solchen Wanzen hat die NSA z.B. für Tastatur- und Monitorkabel.

Und nein, das ist kein paranoider Scherz, die machen sowas wirklich.

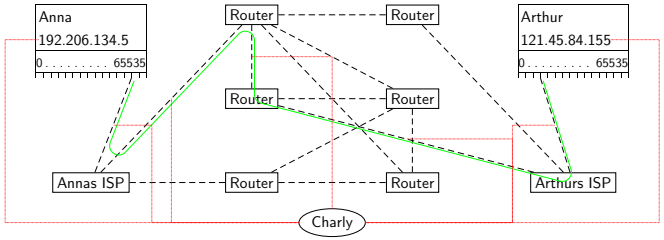

Fig. 7

7. Breit/flach vs. eng/tief

Gezielte Angriffe sind teuer. Massenüberwachung geht mit ihnen nicht. Für sie müssen die Geheimdienste in die Netze.

(cf. Fig. 7)

Anna will mit Arthur reden, der Geheimdienstmann Charly will sie abhören.Die roten Linien zeigen, wo Charly überall abhören kann:

- Direkt in den Rechnern von Anna oder Arthur – das ist der Staatstrojaner. Das ist für die Behörden sehr attraktiv, weil die Daten da in jedem Fall unverschlüsselt vorliegen. Der Aufwand, den Trojaner auf die Rechner zu kriegen ist aber enorm (die BRD-Polizei hat sowas nur ein paar Mal im Jahr versucht und es oft nicht geschafft).
- An den Leitungen von den Leuten zu ihren ISPs: Das ist konzeptionell, was die Polizei beim Abhören macht, und das bei einigen 10000 Anschlüssen im Jahr. Das ist einfacher, aber immer noch recht gezielt und nicht tauglich für Massenüberwachung, weil die ISPs für jede solche Maßnahme eine Einzelanordnung haben wollen. Hier hat man dann schon mit Verschlüsselung zu kämpfen. Die derzeit übliche Infrastruktur kann zudem keine Verbindungen kapern, selbst SSL ist hier also eine Herausforderung.
- An den Übergabepunkten der ISPs ins Internet. So werden, so weit wir wissen, Internet-Abhörschnittstellen derzeit meist realisiert: An diesen Punkten stehen "Black Boxes" der Behörden, die im Prinzip den ganzen Internetverkehr ausleiten, aber nur die Daten aus Einzelanordnungen abgreifen. Für was anderes gibts keine Rechtsgrundlage. Andererseits gibts mindestens einen Fall, in dem BRD-Behörden (für Schweizer Behörden) den kompletten Verkehr eines Servers abgegriffen haben.
- An den Backbones. Polizeien haben auf den großen Internetleitungen keine Rechte, auch der VS nicht. BND und NSA filtern da allerdings durchaus und machen Keyword-Suche und sowas; wenn da was Relevantes rauskommt, geben sie das auch an VS und Polizei weiter, so sie glauben, dass es ihnen nützt. Hier ist allerdings selbst nicht so ultrapralle Verschlüsselung ein ernsthaftes Hindernis.

Noch ein Aspekt: Was, wenn Arthur keine Person, sondern ein Unternehmen ist? Erstaunlicherweise ist die offizielle Zusammenarbeit zwischen Privatunternehmen und Geheimdiensten weniger eng, als mensch meinen könnte – vermutlich fürchten die Dienste, die Unternehmen könnten Dinge über sie herausfinden, während die Unternehmen Imageschäden durch allzu offensichtlichen Abfluss von Daten fürchten. Andererseits ist klar, dass Google, Facebook und ähnliche riesige Mengen hochinteressanter Daten haben, und zumindest halbwegs kompetente Dienste werden nur schwer von diesen Beständen fernzuhalten sein.

Dazu kommen natürlich auch rechtliche Verpflichtungen (z.B. können die sich deutsch Dienste nach Ottokatalog frei in Buchungssystemen von Fluggesellschaften und Fährdiensten umsehen).

Fazit: Daten, die ihr an „große" Läden übertragt, lohnen vermutlich die Verschlüsselung im Hinblick auf ernstzunehmende Dienste nicht.

8. Was können wir tun?

Im Jargon: „Operational Security“ (OpSec) und „Tactical Surveillance Counter Measures“ (TSCM)

Gegen einen gezielten Angriff *würde* helfen:

- Alle Kommunikation stark verschlüsseln mit sorgfältigem Schlüsselmanagement
- Alles Ausführbare (incl. Javascript, Browser-Erweiterungen, OS-Updates) nur von vertrauenswürdigen Quellen mit ordentlicher Krypto beziehen
- Physischen Zugriff durch Behörden auf alle Hardware verhindern, spätestens ab Kauf
- Alles Vertrauliche in stromlosen, schallgeschützten Räumen ausmachen

Im Wesentlichen müssten wir ein Geheimdienst werden, um den Geheimdiensten technisch zu entgehen. Aber das können wir eigentlich nicht, denn

- Das frisst Zeit und Aufmerksamkeit, die wir besser auf andere Dinge lenken (z.B. die Geheimdienste politisch zu bekämpfen).
- Wir sind auf Offenheit angewisen – immerhin ist ja die politische Sozialisation noch Außenstehender mal ein richtig wichtiges Projekt, und da würden wir als Geheimdienst blöd dastehen
- Vor allem aber: Es ist jedenfalls unterhalb sehr heikler direkter Aktionen nicht nötig. Dafür reicht es, der breiten Massenüberwachung etwas entgegenzusetzen, und das ist weit einfacher.

9. Aufgeben?

Wenn die alles können, warum kriegen sie dann nichts auf Reihe?

- Abwegiger Mist in VS-Berichten
- Erfolgreiche Aktionen gegen z.B. Bundeswehrkram, die allenfalls durch Zufall aufgeklärt werden
- Zehn Jahre Suche nach Bin Laden, weitgehend unbehinderte Operationen von Taliban und Freunden, hilfloses Drohnen-Rumgeballere
- Nicht mal Vollamateure wie die Marathon-Bomber werden erwischt.
- V-Mann ist bei Nazi-Mord dabei

10. Malfunction

Mögliche Gründe für Dienste-Murks:

- Wettbewerb in den Behörden und zwischen den Behörden
- Politische gewollte aber abwegige Theorien (z.B. „Extremismus“)
- Quasireligöse Verblendung wichtiger Mitarbeiter („Antikommunismus“), innere Emigration
- Unfähigkeit im Umgang mit Technik
- Ökonomie des sicherheits-industriellen Komplexes
- (In der BRD:) Eher überschaubare Ressourcen (Größenordnung: BfV ca. 3000 Stellen, die Landesämter sind mit zwischen einigen Dutzend und einigen 100 Stellen dabei, Etat das VS BaWü rund 18 Mio Euro).

11. Geheimdienst spielen?

Die Dienste machen nicht viele all-out *Einzelangriffe* (brauchen trotz Computern ≥ 1 Dienstler pro Opfer). Umgekehrt braucht die Abwehr aber auch de facto ≥ 1 Person pro Angriff. Wenn wir das wirklich tun würden, könnten wir nichts mehr sonst machen, wir wären damit beschäftigt, so zu tun, als wären wir selbst ein Geheimdienst).

Aber: Abwehr von *Massenüberwachung* ist realistisch und notwendig:

- Telefon so oft wie möglich funklos machen
- So viel wie möglich verschlüsseln (PGP, SSL wenn möglich mit Certificate Patrol)
- So wenig App- und Download-Mist wie halt möglich
- Verstand verwenden

12. Bringts was?

Die Dienste können die Krypto unter richtig verwendetem PGP und SSL *nicht* brechen.

Wenn überhaupt, können sie die Schlüsselverwaltung angreifen („MITM“). Bei PGP ist das eher schwierig, bei SSL eher leicht.

Die Dienste greifen *sicher* routinemäßig auf Telekom-Metadaten zu. Lange vor einem gezielten Angriff werden sie die nutzen. Oh: Für Raumüberwachung durchs Telefon gibts in der BRD immer noch keinen Beleg.

13. Aber

Die Dienste funktionieren, obwohl sie murksen:

Fear, Uncertainty, Doubt

- Angst: Wenn ich mein Maul aufmache, fliege ich dann?
- Unsicherheit: Können die mich hier hören?
- Zweifel: Ist Arthur vielleicht ein Spitzel?

Die Angst vor dem Handeln der Geheimdienste ist weit schlimmer als das, was sie wirklich tun.

Das panoptische Prinzip

Allein, dass wir hier sitzen und unsere Zeit mit Nachdenken über die Schlapphüte verschwenden müssen, ist ein Erfolg für die Läden. Solange tun wir nämlich nichts gegen eine der vielen Sauereien, die unsere Obrigkeit so organisiert.

14. Die historische Gelegenheit

Die Abschaffung oder Einschränkung der Geheimdienste ist entscheidend für unsere Handlungsfähigkeit.

Die Dienste sind aber nach NSU und Co schon angeschlagen. Auch der Obrigkeit ist aufgefallen, dass sie nicht so funktionieren, wie sie behaupten. Auch die breitere nicht komplett bornierte Öffentlichkeit ist inzwischen sehr skeptisch und hat immer weniger Bock auf Überwachung. Die öffentlich gewordenen Verflechtungen mit konsensfähigen Bösewichten wie der NSA helfen sehr.

Die Macht der Dienste über die Obrigkeit ist aber auch nicht zu unterschätzen.

Es liegt an uns, Druck zu machen, den Skandal Geheimdienste immer weiter zu thematisieren, mit allem, was wir so an Aktionsformen haben.