Atak

Podsłuch elektromagnetyczny

Grzegorz Błoński

stopień trudności

W mediach co rusz słyszymy, że ktoś kogoś podsłuchał. Cały ten szum podsłuchiwania dotyczy raczej specjalizowanych urządzeń podsłuchowych, mini-nadajników zwanych pluskwami – lecz to nie jedyny rodzaj podsłuchu obecny w otaczającym nas świecie. Nie należy zapominać, że podsłuchać można nie tylko człowieka, ale także komputer i to, co w nim najcenniejsze dla właściciela.

Emisja ujawniająca (ang. *compromising emanation*), nazywana także ulotem elektromagnetycznym, to zjawisko występujące w każdym obwodzie, w którym płynie prąd. O ile w wielu przypadkach elektromagnetyzm jest zjawiskiem bardzo przydatnym, to w przypadku emisji ujawniającej jest dokładnie odwrotnie. Każdy podzespół komputera, przetwarzając dane, emituje część energii elektrycznej w postaci pola elektromagnetycznego. To właśnie pole elektromagnetyczne i zawarte w nim informacje będą tematem tego artykułu.

Fakty czy mity

W marcu roku 2004 w Internecie powstał projekt nazwanyEckbox(*http://eckbox.sourceforge.net*), który był rozwijany przez kilka miesięcy.

Jest to jedyny projekt open source teoretycznie pozwalający wykorzystywać technikę podsłuchu elektromagnetycznego. Z premedytacją używam słowa *teoretycznie*, ponieważ nie udało mi się znaleźć potwierdzenia faktu działania tego urządzenia i programu. Projekt powstał na bazie badań i artykułu napisanego przez Wima van Ecka, holenderskiego naukowca z *Neher Laboratories*. Skonstruowane i opisane przez niego urządzenie było odbiornikiem fal elektromagnetycznych, podłączonym do komputera za pomocą specjalnie przerobionego odbiornika telewizyjnego oraz pozwalało na przechwycenie informacji wyświetlanych na monitorze katodowym CRT. Było to rozwiązanie czysto sprzętowe i bardzo rozbudowane. *Projekt Eckbox* jest o wiele prostszą wersją tego rozwiązania – co wcale nie musi oznaczać, że mniej funkcjonalną. Autorzy projektu napisali program, któ-

Z artykułu dowiesz się

- co to jest emisja ujawniająca,
- co to jest ulot elektromagnetyczny,
- czy można wykorzystać te zjawiska do podsłuchiwania.

Co powinieneś wiedzieć

- znać podstawy zjawiska elektromagnetyzmu,
- znać system Linux i umieć pracować w konsoli,
- umieć posługiwać się lutownicą,
- znać podstawy budowy układów elektronicznych.

ry – korzystając z portu równoległego w komputerze PC – potrafi przekształcić dane odebrane przez radioodbiornik podłączony do komputera za pomocą specjalnego interfejsu wykorzystującego przetwornik analogowo-cyfrowy.

Problem ulotu elektromagnetycznego dotyczy każdego urządzenia komputerowego, a mimo to niewiele jest firm, które dbają o zapewnienie pod tym względem bezpieczeństwa swoim wrażliwym danym. W agencjach i instytucjach rządowych sytuacja jest trochę lepsza, ponieważ są one zobligowane do utrzymania określonych informacji w ścisłej tajemnicy.

W USA powstał w latach sześćdziesiątych projekt nazwany TEMPEST (*Transient ElectroMagnetic Pulse Emanation STandard*), który określa dopuszczalne poziomy niepożądanych emisji fal elektromagnetycznych. Projekt uwzględnia trzy klasy (poziomy) bezpieczeństwa:

- Level 1 – AMSG 720 B,
- Level 2 – AMSG 788,
- Level 3 – AMSG 784.

Urządzenia wykonane przy zachowaniu norm zawartych w projekcie TEMPEST są sprzedawane na terenie państw członkowskich NATO. Jednak, aby móc takie urządzenie nabyć lub nimi handlować, trzeba spełnić pewne warunki.

Po dokładniejsze informacje na temat programu TEMPEST odsyłam do Internetu, na przykład na stronę *www.iniejawna.pl*.

Technikalia

Rozpatrując możliwości podsłuchania komputera przy wykorzystaniu kompromitujących emanacji, mamy możliwość zastosowania technik inwazyjnych oraz nieinwazyjnych.

Techniki inwazyjne mogą opierać się na *wstrzyknięciu* w system-ofiarę oprogramowania, działającego w taki sposób, że bez wiedzy użytkownika będzie wykorzystywało układy elektroniczne komputera jako nadajnik i antenę do wypromieniowania informacji, jakie zamierzamy przechwycić.

Przykładem wykorzystania takiej techniki jest program autorstwa Erika Thiele, nazwany dźwięcznie *Tempest for Eliza* (*http://www.erikyyy.de/tempest*). Program ten pozwala – przy wykorzystaniu karty graficznej jako nadajnika i monitora jako anteny – *wysyłać* muzykę w eter – można ją odebrać na standardowym radioodbiorniku fal długich. Program działa w linii poleceń systemu Linux.

Do wydania odpowiedniej komendy potrzebne są nam parametry naszego podsystemu graficznego, takie jak:

- częstotliwość rysowania piksela (*Pixel Clock*),

Listing 1. *Program tempest-cpu autorstwa Berke Duraka*

```
#include <stdlib.h>
#include <stdio.h>
typedef unsigned char u8;
#define BUF_SIZE (1<<18)
void tempest_cpu_pattern (int count, volatile int *buf, int a, int b)
{
   int i, j;
   int x1, x2, x3, x4;
   x1 = 0; x2 = 0; x3 = 0; x4 = 0;
   i = 0;
   while (count --) {
      for (j = 0; j<a; j++) {
         x1 ^= 0x55330fff + i;
         x1 <<= 1;
         buf[i] = x1;
         if (++ i == BUF_SIZE) i = 0;
      }
      for (j = 0; j<b; j++) {
         asm ("nop"); /* this instruction is available on nearly every CPU :
                         ) */
      }
   }
}
int main (int argc, char **argv)
{
   int count1, count2;
   int a1, b1;
   int a2, b2;
   int *c;
   int a, b;
   if (argc != 7) {
      fprintf (stderr, "usage: %s a_low b_low a_high b_high count_low
                        count_high\n");
      exit (EXIT_FAILURE);
   }
   a1 = atoi (argv[1]);
   b1 = atoi (argv[2]);
   a2 = atoi (argv[3]);
   b2 = atoi (argv[4]);
   count1 = atoi (argv[5]);
   count2 = atoi (argv[6]);
   c = malloc (BUF_SIZE * sizeof (int));
   for (;;) {
      for (a = a1, b = b1; a < a2 && b < b2; a += (a2 - a1) >> 4, b += (b2
                        - b1) >>4) {
         tempest_cpu_pattern (count1, c, a, b);
      }
   }
   return 0;
}
```

- rozdzielczość pozioma (*HDisplay*),
- rozdzielczość pionowa (*VDisplay*),
- całkowita rozdzielczość pozioma (*HTotal*).

Po wydaniu przykładowego polecenia:

```
#./tempest_for_eliza 108000000  1280
  1024  1688  10000000  songs/starwars
```

program użyje wartości 108MHz jako częstotliwości rysowania piksela, rozdzielczości okna 1280 x 1024 oraz wartości HTotal równej 1688 pikseli. Kolejne parametry to 10MHz (jako częstotliwość nośna, na której będzie emitowany dźwięk) i wreszcie ścieżka do pliku dźwiękowego. Na ekranie monitora pojawi się dynamicznie zmieniający się obraz czarno-białych linii poziomych, których grubość i szybkość zmian uwarunkowana jest odtwarzanym z pliku dźwiękiem.

Dźwięki emitowane przez monitor są słyszalne także na częstotliwościach harmonicznych. Na standardowym odbiorniku radiowym w zakresie fal krótkich w okolicach częstotliwości 10MHz nadawany dźwięk bardzo dobrze słychać. Oprócz tej częstotliwości odebrałem emitowane dźwięki za pomocą transceivera krótkofalowego na częstotliwościach 26,215 MHz, 26,455 MHz, 26,755 MHz, 27,755 MHz oraz 28,005 MHz – przy czym najsilniejszy sygnał pojawił się na pierwszej z wymienionych częstotliwości. Odległość anteny wynosiła początkowo jeden metr – w tych warunkach siła sygnału była na poziomie 3μV do 6μV (według wskazań transceivera Zodiac Tokyo), bez względu na polaryzację anteny. Przy zwiększeniu odległości do 4 metrów siła sygnału spadła do poziomu 0,39μV. Dźwięki nadal były słyszalne, lecz towarzyszyły im wyraźne szumy, których intensywność zmieniała się w zależności od polaryzacji anteny. Podczas pomiarów używałem anteny MagLoop.

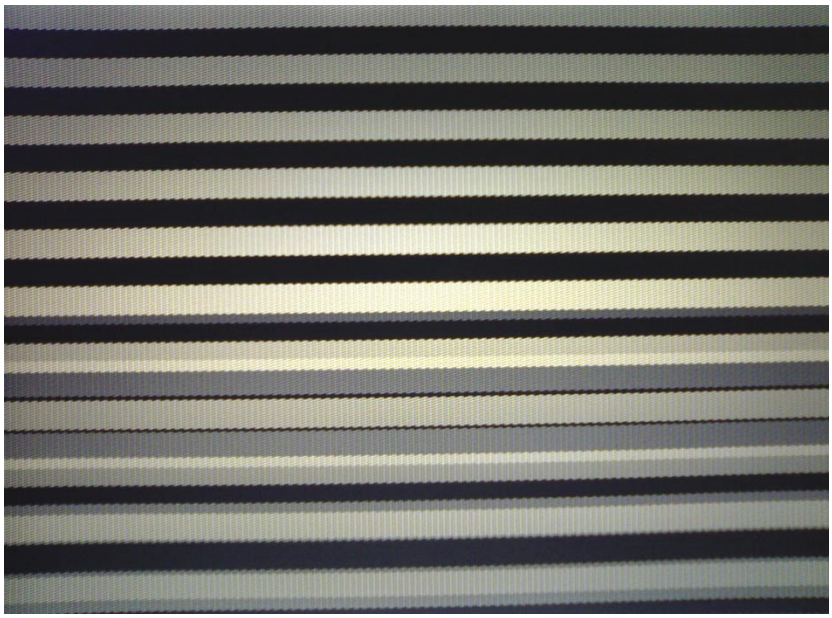
Rysunek 1. *Rozkład pola elektromagnetycznego wokół odcinka przewodnika prądu elektrycznego.*

Przy okazji tych eksperymentów odkryłem, że podłączone do komputera urządzenia typu KVM (*Keyboard Video Mouse*) w trakcie testów emitują tak silnie wzmocnione sygnały z karty graficznej, że bez problemu mogłem odebrać czyste, słyszalne dźwięki w pomieszczeniu znajdującym się za dwoma ścianami w odległości około 8 metrów. Siła sygnału była tak duża, że wskaźnik transceivera Zodiac Tokyo wskazywał 50μV! Sugeruje to, że sygnał mógł być swobodnie odebrany w bardzo dużej odległości, przypuszczalnie kilkudziesięciu, a może nawet kilkuset metrów.

W związku z tym faktem uważam, że używanie przełączników KVM w systemach komputerowych zawierających dane tajne lub wrażliwe jest bardzo ryzykowne. Przełącznik, którego używałem, to dzieło firmy D-link (model DKVM-2K) który, jako urządzenie pozwalające na korzystanie z jednego zestawu klawiatury, myszy i monitora dla dwóch komputerów, sprawuje się doskonale – zgodnie ze swym przeznaczeniem. Bardzo możliwe, że jest na rynku sporo przełączników pozbawionych takiej *przypadłości*. Jednak tak czy inaczej, zanim ktoś zechce użyć jakiegokolwiek przełącznika, powinien się zastanowić nad niechcianym *dodatkiem* w postaci dużej emisji niepożądanych sygnałów lub wykonać testy sprawdzające.

Erik Thiele bazował przy pracy nad swoim programem na innym projekcie (autorstwa Pekki Riikonena), który potrafił tylko emitować pojedyncze tony – ale także pozwolił udowodnić, że podsłuch elektromagnetyczny jest możliwy. Powstało już więcej programów wykorzystujących zjawisko niepożądanego ulotu elektromagnetycznego w komputerach. Autorem kilku takich narzędzi jest Berke Durak (*http://abaababa.ouvaton.org/tempest*). Jego programy wykorzystują do ukrytej transmisji danych drogą radiową zarówno wewnętrzne, jak i zewnętrzne podzespoły komputera.

Pierwszym programem Berke Duraka, o najmniej skompliko-



Rysunek 2. *Ekran monitora podczas pracy programu Tempest for Eliza*

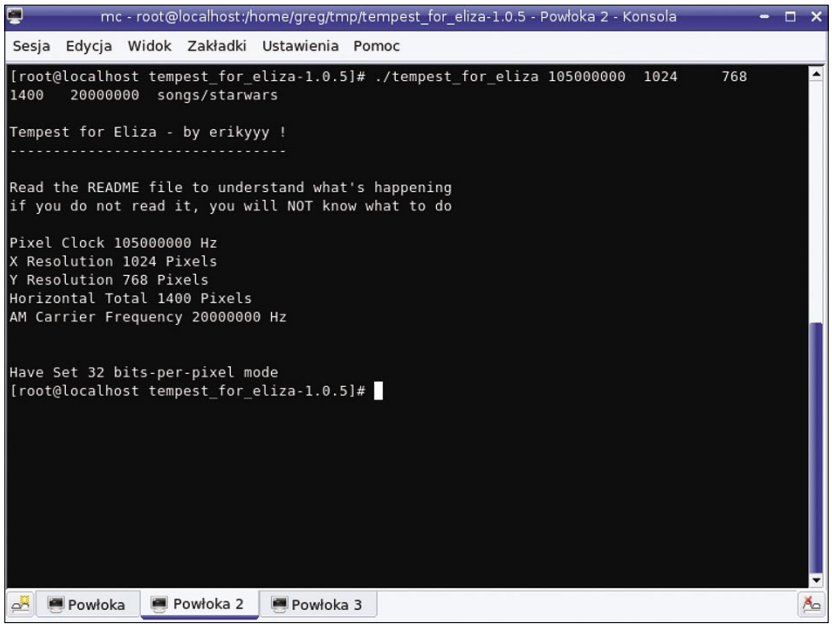
wanej budowie (Listing 1) jest *tempest-cpu*.

Program działający w linii poleceń systemu Linux przyjmuje kilka parametrów określających rodzaj przesyłanych dźwięków, wysokość tonu i czas trwania. Obciąża procesor w 100%, więc nie nadaje się do przeprowadzenia ataku – jego działalność w systemie zostałaby szybko wykryta. Jest jednak dobrym przykładem potwierdzającym fakt istnienia zjawiska ulotu elektromagnetycznego. Procesor emituje niezbyt silne pole elektromagnetyczne, jednak jest ono możliwe do odebrania w odległości do dwóch metrów przy pomocy zwykłego radioodbiornika na fale długie, przy czym odbierany sygnał jest bardzo mocno zakłócany przez szumy oraz interferencje pochodzące od innych pracujących w komputerze podzespołów.

Kolejny program *tempest-crt* tego samego autora wykorzystuje – podobnie jak poprzednie programy Erika Thiele i Pekki Riikonena – monitor jako nadajnik do wysyłania informacji dźwiękowej. Inne dwa programy Berke Duraka – *tempest-pci* oraz *tempest-mem* – wykorzystują jako nadajnik odpowiednio szynę PCI (i urządzenia na niej pracujące) oraz pamięć operacyjną. Ich przydatność do wykorzystania w ataku jest również niewielka, ponieważ pole elektromagnetyczne, które generują wokół siebie urządzenia PCI, jest dużo słabsze niż wytwarzane przez monitory (w szczególności CRT, choć LCD także charakteryzują się dość pokaźnym niepożądanym ulotem).

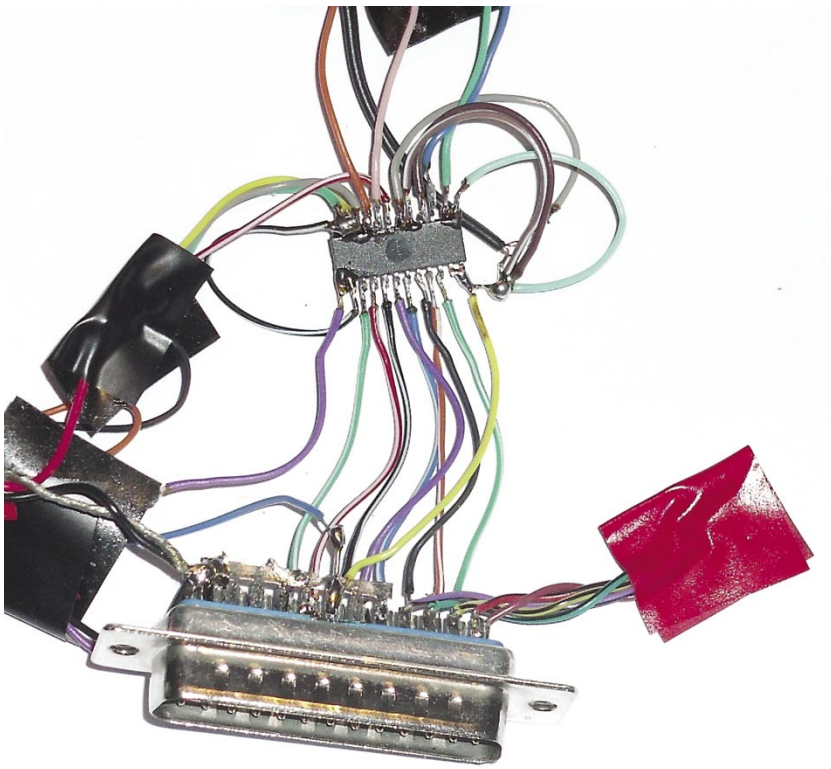
W tym momencie należy wspomnieć, że urządzenia pracujące na szynie SCSI – bardzo wydajnej szynie danych, wykorzystywanej w rozwiązaniach serwerowych – także emitują dość silne pola elektromagnetyczne. Są one dużo bardziej intensywne niż w przypadku szyny PCI i w przypadku braku odpowiedniego ekranowania dają możliwość podsłuchania z dużej odległości.

Programy Duraka są niezaprzeczalnym potwierdzeniem, że można wykorzystać podzespoły komputera w celu wysyłania informacji poprzez zastosowanie odpowiedniego oprogramowania. Wprawny programista, wykorzystując kod źródłowy programów Duraka, teoretycznie może napisać aplikację, która po-



Rysunek 3. *Program Tempest for Eliza po zakończeniu pracy*

Rysunek 4. *Transceiver Zodiac Tokyo w czasie odbierania sygnału emitowanego z komputera*



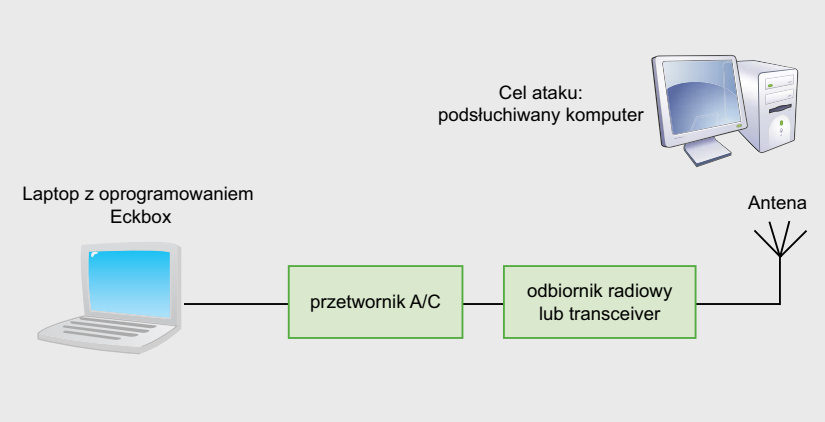
Rysunek 5. *Widok zmontowanego urządzenia*

zwoli mu po zainfekowaniu komputera-ofiary na przechwytywanie informacji, jakie go interesują. Po odpowiedniej modyfikacji programu można go dodać jako załącznik do maila, który automatycznie się uruchomi, jeśli nieuważny internauta w niego kliknie. Choć dotychczas nie ujawniono wirusa czy innego złośliwego kodu wykorzystującego taką technikę do przechwycenia informacji, uważam, że zagrożenie związane z takimi atakami jest dość duże. Całkiem możliwe, że już ktoś napisał taki złośliwy kod i go wykorzystuje, a my o tym po prostu nie wiemy.

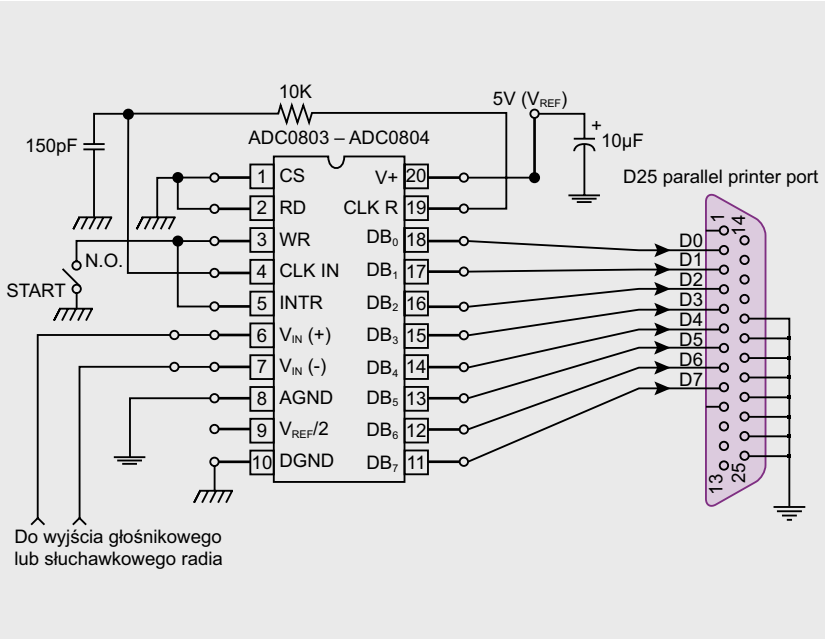
Techniki nieinwazyjne – jak sugeruje nazwa – nie zmuszają nas do *wstrzykiwania* kodu programu do komputera-ofiary. Nieinwazyjność tych metod polega na wykorzystaniu niepożądanej emisji elektromagnetycznej generowanej standardowo przez urządzenia komputerowe. Prekursorem w tej dziedzinie – a jednocześnie naukowcem, który upublicznił informacje o możliwości podsłuchu elektromagnetycznego – był wcześniej wspomniany Wim van Eck.

Podsłuchiwać możemy przeróżne sygnały emitowane przez wiele podzespołów komputerowych – od urządzeń komunikujących się z komputerem bezprzewodowo, takich jak myszy, klawiatury, drukarki itp., aż po te, które są połączone z komputerem kablem. W przypadku słabej jakości filtrowania napięć zasilających w zasilaczach komputerowych część informacji może przedostawać się do sieci elektroenergetycznej i tam może zostać przechwycona.

W roku 1990 Peter Smulders opublikował wyniki badań nad przechwytywaniem informacji z ulotu elektromagnetycznego kabli łączących interfejsy RS-232, na podstawie których możemy przypuszczać, że praktycznie każdy rodzaj transmisji danych, nawet realizowanej przewodowo, jest narażony na podsłuchanie.



Rysunek 6. *Eksperymentalny zestaw do podsłuchu elektromagnetycznego (Eckbox)*



Rysunek 7. *Schemat ideowy urządzenia Eckbox*

Budujemy urządzenie

W związku z tym, że najsilniejsze sygnały emitowane są przez monitory CRT, a zaraz po nich LCD, postanowiłem przeprowadzić własne badania, budując odpowiednie urządzenie. Zaczerpnąłem podstawowe informacje ze strony projektu *Eckbox* i zacząłem od zebrania odpowiednich elementów elektronicznych, aby zbudować interfejs przetwarzający sygnał analogowy z odbiornika radiowego czy też innego transceivera, którym będę próbować odebrać sygnały emitowane przez monitory testowe.

Rozpoczynając pracę nad budową pierwszego układu, podchodziłem do całej sprawy nieco sceptycznie – jednak z odrobiną nadziei, że się uda. Do swojego eksperymentu wykorzystałem odbiornik radiowy w zakresie pasma fal długich, krótkich oraz UKF, a także transceiver Zodiac Tokyo, pracujący w zakresie 25-29MHz. Nasłuchy prowadziłem w modulacji AM oraz FM. Jak wiemy, sygnały nadawane przez różne nadajniki często są słyszalne na częstotliwościach harmonicznych, które są wielokrotnościami częstotliwości nośnej. Liczyłem więc, że gdzieś w końcu usłyszę i zobaczę to, co chcę.

Na Rysunku 6 widać schemat blokowy połączeń poszczególnych elementów zestawu.

W swoim eksperymencie wykorzystywałem radioodbiornik wypo-

sażony w standardową antenę ferrytową oraz zewnętrzną teleskopową. Oprócz tego w przypadku transceivera Zodiac Tokyo korzystałem z anteny dookólnej pętlowej *LoopSkywire* oraz anteny kierunkowej MagLoop własnej konstrukcji. Szczegóły dotyczące budowy tych anten nie zostaną tu zamieszczone – wystarczająco dużo informacji na ten temat można znaleźć w Internecie.

Do zbudowania interfejsu urządzenia dla portu LPT (według informacji ze strony *http://eckbox.sourceforge.net*), potrzebujemy układu scalonego do konwersji sygnału analogowego z odbiornika radiowego na sygnał cyfrowy rozumiany przez komputer PC. Projekt Eckbox zakłada użycie przetwornika analogowo-cyfrowego o rozdzielczości 8 bitów na wyjściu cyfrowym i jednym kanale wejściowym. Układy scalone, które można wykorzystać do tego celu, są dostępne w każdym lub prawie każdym sklepie z podzespołami elektronicznymi.

Dodatkowo będziemy potrzebowali kilku rezystorów, kondensatorów i diod. Przeszukując sklepy natrafiłem na układ ADC0804, niedrogi, spełniający wymogi projektu i posiadający odpowiednie parametry elektryczno-logiczne.

Na Rysunku 7 przedstawiam schemat układu, który zbudowałem, korzystając z informacji zawartych w nocie aplikacyjnej układu ADC0804 i kilku innych rozwiązań wykorzystujących ten przetwornik.

Po zmontowaniu elektronicznej części układu przystąpiłem do połączenia wszystkich elementów zestawu podsłuchowego – tak, jak widać na Rysunku 5.

Program eckbox po skompilowaniu (wraz z odpowiednimi bibliotekami – *svgalib* oraz modułem svgalib_helper) uruchamia się, początkowo wyświetlając tylko czarny ekran. Po chwili, gdy zaczyna działać przetwornik A/C, na ekranie pojawiają się przesuwające się poziome linie – co przedstawia Rysunek 8.

Urządzenie nie wyświetla tego, na co oczekiwałem, ponieważ zastosowany układ ADC0804 przenosi sygnały o częstotliwościach do 10 kHz. Przeoczyłem ten ważny parametr podczas wyszukiwania odpowiedniego układu. Ponieważ w technice nieinwazyjnej zakładamy, że nie mamy możliwości wymuszenia częstotliwości, na jakiej monitor emituje sygnał, musimy próbować odebrać go na częstotliwościach, na których jest emitowany przez podzespoły komputera lub na częstotliwościach harmonicznych (założyłem zakres od 10 do 30 MHz).

Zbudowałem więc kolejny egzemplarz oparty o układ ADC, mogący pracować z częstotliwościami sygnału wejściowego rzędu 18 Mhz, który teoretycznie powinien się sprawdzić lepiej – czyli HI1175 firmy Intersil. Niestety, okazało się, że to także nie pozwala na odebranie sygnału. Zgodnie z informacjami ze strony projektu Eckbox, układ powinien działać na częstotliwości pasma radiowego FM 108MHz.

Taka częstotliwość sugeruje, że program został napisany tak, by odbierać sygnał emitowany przez PixelClock w kartach graficznych. Dość trudne jest zdobycie układu ADC pracującego z sygnałami wejściowymi o takich częstotliwościach.

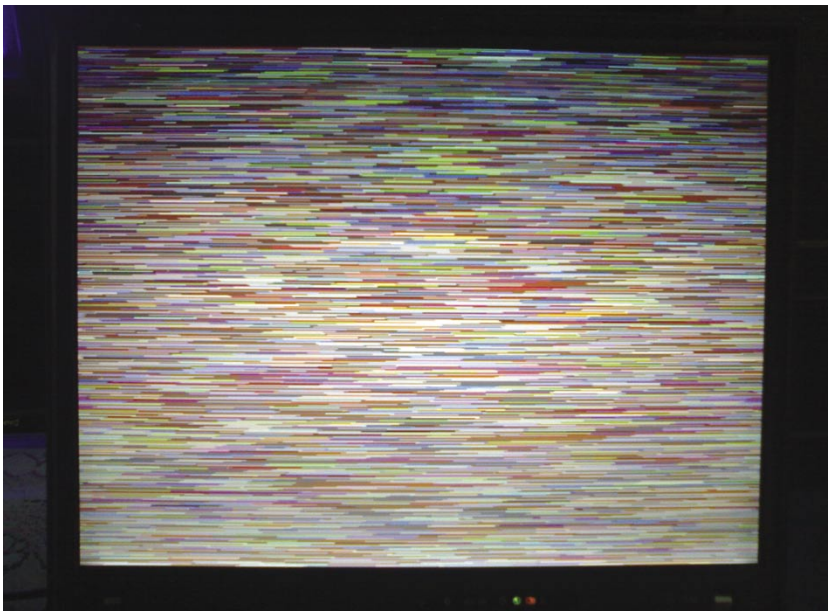
Licząc, że uda mi się podsłuchać coś na częstotliwościach harmonicznych, postanowiłem najpierw zbudować kolejne układy, umożliwiające pracę na wyższych częstotliwościach. Kolejne urządzenie, zbudowane w oparciu o układ HI2302 (także firmy Intersil), podczas pierwszych testów nie chciało działać – czego przyczyną okazało się zaniżone napięcie zasilające. Ponieważ urządzenie jest zasilane z szyny USB, szybko znalazłem przyczynę tej sytuacji. Okazał się nią zewnętrzny dysk twardy podłączony do komputera, który pobierając prąd rzędu 500mA (czyli maksymalny możliwy według specyfikacji USB) powodował spadki napięcia. Po odłączeniu dysku napięcie na szynie USB wróciło do

poziomu 5V, a urządzenie zaczęło pracować.

Niestety, nie powiodło mi się również tym razem. Układ teoretycznie pozwala na odbieranie sygnałów o częstotliwości 100MHz. Program Eckbox, pomimo tego, że wyświetlał zmieniające się w czasie obrazy składające się z linii poziomych, jak na

Brak pozytywnego wyniku działania urządzenia i programu Eckbox wcale nie spowodował w moim przypadku zmiany zdania na temat problemu ulotu elektromagnetycznego i zagrożeń bezpieczeństwa z nim związanych.

Powodem niepowodzenia mogą być zarówno błędy w projektowaniu urządzenia, jak i sam program, który ostatnich poprawek doczekał się w roku jego powstania (2004). Od tamtego czasu na stronie projektu nic się nie dzieje. Być może ktoś już próbował zbudować to urządzenie wcześniej, jednak nie natknąłem się na ślady informacji o działającym egzemplarzu. Jeżeli jest ktoś, kto wykonał taki aparat, chętnie skorzystam z jego wiedzy – o ile zechce się nią podzielić.



Rysunek 8. *Wynik pracy urządzenia i programu Eckbox*

Rysunek 9. *Obraz odbierany przez kolejny układ (HI2302)*

O autorze

Autor, Grzegorz Błoński, z wykształcenia jest informatykiem. Pracuje w dużej firmie produkcyjnej o zasięgu światowym. Zajmuje się administracją i bezpieczeństwem sieciowym. Należy do międzynarodowych organizacji ISOC oraz ISACA, zajmujących się szeroko pojętym bezpieczeństwem IT.

Kontakt: *mancymonek@mancymonek.pl*

Podsumowanie

Po analizie pokaźnych zasobów informacji na temat ulotu elektromagnetycznego, znajdujących się między innymi w Internecie, oraz po przeprowadzonych testach programów Erika Thiele i Berke Duraka uważam, że problem emisji ujawniającej jest kwestią, której nie można pomijać przy tworzeniu polityk bezpieczeństwa w firmach i instytucjach przetwarzających ważne, często tajne dane. Choć w tym artykule opisałem możliwość odbierania sygnałów nadawanych z premedytacją – i to na niewielkie odległości, nie można lekceważyć istoty problemu, która może w wielu przypadkach stanowić o wycieku bardzo cennych danych. Nieudana próba podsłuchania emisji ujawniającej przy pomocy prostych w budowie urządzeń nie przeczy temu, że sam fakt takiego podsłuchu jest możliwy. Przy odpowiednio dużym nakładzie pracy oraz zastosowaniu profesjonalnego sprzętu z dużym prawdopodobieństwem pozwoli nam to na skonstruowanie urządzenia, które będzie działało tak samo dobrze, jak urządzenie Wima van Ecka (lub nawet lepiej). Mam nadzieję, że po przeczytaniu tego artykułu wielu administratorów podejdzie do zagadnienia podsłuchu elektromagnetycznego tak samo poważnie, jak do innych problemów związanych z bezpieczeństwem systemów informatycznych. ●