Appears in
IEEE Transactions on Electromagnetic Compatibility (TEMC), Vol. 59, No. 1, Pages 34-42, February 2017.

A Method for Finding Frequency-modulated and Amplitude-modulated Electromagnetic Emanations in Computer Systems

Milos Prvulovic *Senior Member, IEEE*, Alenka Zajić *Senior Member, IEEE*, Robert Callan *Student Member, IEEE*, and Christopher Wang

***Abstract*— This paper presents an algorithm for finding carriers of frequency-modulated (FM) and amplitude-modulated (AM) electromagnetic (EM) emanations from computer systems. Computer systems create EM emanations across the RF spectrum making it difficult, error-prone, and time-consuming to find the relatively few emanations that expose sensitive information. One of the most common and simplest mechanisms for information leakage occurs when an amplitude or a frequency of an existing strong signal (e.g. a processor or memory clock) is amplitude or frequency modulated by a system activity. If the system activity can be linked to sensitive information, this results in information leakage. We present an algorithm for automatically finding these AM and FM modulated signals, demonstrate the algorithm's performance on several different types of processors and systems (desktop, laptop, and smart phone), and compare the results to an exhaustive manual search. We also verify that all signals identified by the algorithm can be traced to plausible unintentional modulation mechanisms to illustrate that these signals can potentially cause information leakage. This algorithm can be an important tool for system designers to quickly identify circuits that are leaking sensitive information.**

***Index Terms*— electromagnetic emanation security, electromagnetic information leakage, modulated signals in computer systems.**

I. Introduction

Security vulnerabilities caused by EM emanations have been reported as early as 1966 [1], though much of the early work was classified. Open publication of attacks exploiting EM emanations from computer monitors [2], [3] brought attention to the issue, and techniques such as differential power analysis [4] have been adapted for use with EM emanations. Researchers have used EM emanations to compromise the security of many types of devices [5] from ASIC design primitives [6], to keyboards [7], smartcards [8], [9], and desktop computers [10]. Some of the strongest and farthest-propagating signals are created when an existing strong periodic signal (e.g. a clock signal) becomes amplitude or frequency modulated depending on processor or memory activity and examples of using modulated signals to compromise the security of different devices have been in [11], [12], [13], [14]. Several countermeasures for EM leakage have been proposed for smartcards [15], [16], [17], [18], [19], [20], [21], [22], [23], including the use of asynchronous circuits [15], low-cost shielding (e.g. metal foil) [16], transmission of jamming signals [17], and so on.

However, all these attacks and countermeasures rely on ad-hoc approaches that find a range of frequencies where EM emanations depend on secret key bits by observing program activities in the time/frequency domain for a long time. This approach is application specific and does not identify the circuits or computer architecture mechanisms causing the leakage. One possible systematic approach would be to use EM interference/compatibility (EMI/EMC [24], [25]) techniques to find emanations sources but these methods cannot determine which signals leak information.

To address these issues, we have developed a method for identifying AM modulated signals called FASE (Finding Amplitude-modulated Side-channel Emanations) [26]. The advantage of FASE is that it finds information leakage in general, not just from a specific application such as cryptography algorithm. Furthermore, it allows us to find the root cause of the observed signal (i.e. the carrier frequency), the circuit generating the carrier, and the mechanism that modulates sensitive information onto the carrier. FASE greatly improves the detection of AM modulated EM emanations however it is not fully automated and still requires exhaustive visual search of the RF spectrum for specific intentionally generated spectral patterns. This can be very time consuming and error prone.

In this paper, we present a fully automated measurement and analysis method for finding AM and FM modulated EM emanations. Note that the goal of this paper is to develop a measurement technique that automatically identifies all frequencies at which at least some information about software activity will leak (the proof is the fact that software activity gets modulated onto the existing carriers), determine the type of modulation (so that it is easy to determine type of demodulation needed to extract the information) and determine quality of the modulated signals (SNR) which will determine if the information extraction will be successful or not. The proposed measurement method is an important tool for both those who want to demonstrate attacks or those who want to defend against the attacks because it allows them to identify mechanisms that lead to EM information leakage.

To find carrier frequencies at which at least some information about software activity will leak we use our SAVAT benchmarks [27] to generate an artificial leakage signal at a specific "baseband" frequency and for a specific duty cycle and

This work has been supported, in part, by NSF grants 1563991 and 1318934, AFOSR grant FA9550-14-1-0223, and DARPA LADS contract FA8650-16-C-7620. The views and findings in this paper are those of the authors and do not necessarily reflect the views of NSF, AFOSR, or DARPA.

record several spectra, generating a different baseband signal in each spectrum. It is not surprising that the real alternation frequency differs from the one set in the benchmarks, because the execution time of a program varies from run to run and cannot be adjusted precisely. Hence, we first propose a method to estimate the real alternation frequency, before we can proceed in finding carrier frequencies. Next, we propose a probabilistic method for separating carrier frequencies from all measured frequencies, then propose a method for identifying if the carrier is AM or FM modulated. To verify the performance of our algorithm, we tested it on a laptop, desktop, and smartphone and found that the algorithm finds the spectral patterns caused by modulated carriers with an accuracy of 99%.

The rest of this paper is organized as follows. Section II describes the unintentional AM/FM signals in computer systems, Section III describes benchmarks that create system activity at controlled frequencies, Section IV describes an algorithm for finding AM/FM unintentional carriers in computer systems, Section V describes experimental setup, Section VI presents experimental results, and Section VII concludes the paper.

II. Unintentional FM and AM Carriers in Computer Systems

AM and FM modulations are well-studied [28] and are used in numerous communication systems. Traditional communications rely on carefully designed transmit and receive signaling (i.e. carrier and baseband signals) and thoroughly regulated allocation of the frequency spectrum to optimize communication. In contrast, unintentionally modulated signals in computer systems are generated by many possible "transmitters." Note that many periodic carrier signals in computer systems are generated by digital circuits and clocks, and therefore have sharp transitions that are best approximated by rectangular pulses instead of the sinusoidal waves used as carriers in communications systems. The spectrum of a pulse train with an arbitrary duty cycle is equivalent via Fourier analysis to a set of sinusoids with various amplitudes at f_c and its multiples (harmonics). In other words, for each carrier signal generated by a digital circuit or clock, additional carrier signals will also be present at $2f_c$, $3f_c$, $4f_c$, $5f_c$, etc. As the duty cycle of a signal approaches 50%, the amplitudes of the odd-numbered harmonics (f_c, $3f_c$, $5f_c$, etc.) reach their maximum, while amplitudes of the even harmonics ($2f_c$, $4f_c$, etc.) trend toward zero. For a small duty cycle (i.e. $< 10\%$) the magnitudes of the first few harmonics (both even and odd) decay approximately linearly. Finally, note that these observations imply the amplitudes of all the harmonics are a function of the duty cycle. If program activity modulates the duty cycle of a periodic signal while keeping its period constant (i.e. causes pulse width modulation), all of the signal's harmonics will be amplitude-modulated. Whether the signal is AM or FM modulated can be determined by tracking the carrier signal as the duty cycle of the baseband signal changes. For baseband signals with the highest frequency component much lower than the carrier frequency, the AM and FM spectra look very similar, but FM carrier shifts in frequency with different duty cycles, while AM carrier does not shift.

The reception of unintentional modulation "signals" differs from traditional communication receivers in several ways. Since unintentional signals occur at the frequency of the unintentional carrier, they are mixed in with all the other noise generated by the computer system (other clocks and switching noise) and other communications signals. Unintentional signals are subject to EMC restrictions which impose a maximum noise power (signal power from our point of view). Therefore unintentional signals are typically weaker, and may be diffused across the spectrum by spread spectrum clocking or by using clock sources with inherent variation such as RC oscillators. Also, since the carriers are typically generated by non-sinusoidal sources, the carrier signals may have harmonics. Finally, communication signals have direct and obvious control of the baseband (modulation) signal, while unintentionally modulated signals from computer systems do not. We may be interested in several different system activities (baseband signals). For example, a baseband signal may be caused by processor activity and another baseband signal may be caused by memory activity. In some cases, multiple baseband signals may even modulate the same carrier.

These effects complicate the detection of unintentionally modulated signals. The presence of noise generated by the system makes it difficult to determine which signals are AM or FM carriers. Some of the unintentional AM or FM carriers are generated by spread spectrum clocked signals, making them harder to recognize. Existing methods to find AM and FM modulation based on its spectral properties (i.e. without knowing the baseband signals) are not designed to deal with these issues, and are not able to identify which carriers are modulated by a specific system activity.

III. Creating System Activity at Controlled Frequencies

The first step to finding unintentionally generated signals is to create a simple identifiable baseband signal. These baseband signals are generated by system activity such as the execution of particular instructions, memory accesses, etc. While we do not know the exact effect a particular activity will have on a particular carrier's baseband signal, we can create low frequency f_{alt} variations in a particular activity, and then expect that in aggregate these variations will generate a low frequency component in the baseband signal at f_{alt} frequency.

In [11], [27], [26], we have introduced such micro-benchmarks for generating such periodic activity. Here, we just briefly summarize the approach. The loop beginning on line 2 of Fig. 1 performs one activity (activity X), and the loop beginning on line 8 performs another activity (activity Y). The outer loop repeatedly alternates activities X and Y, creating periodically changing activity whose period equals the execution time for one iteration of the outer loop. This alternation period T_{alt} is the inverse of the frequency $f_{alt} = \frac{1}{T_{alt}}$. Note that prior uses of similar micro-benchmarks [27], [11] used this alternation to *generate a carrier* signal at some chosen frequency f_c, while we use this alternation at f_{alt} to measure FM- and AM-modulation of any potential *carrier signals intrinsically generated* (and emanated) by the system.

```
1  while(true){
2    // Execute the X activity
3    for(i=0;i<inst_x_count;i++){
4      ptr1=(ptr1&~mask1)|((ptr1+offset)&mask1);
5      // The X-instruction, e.g. a load from L2
6      value=*ptr1;
7    }
8    // Execute the Y activity
9    for(i=0;i<inst_y_count;i++){
10     ptr2=(ptr2&~mask2)|((ptr2+offset)&mask2);
11     // The Y-instruction, e.g a store from L2
12     *ptr2=value;
13   }
14 }
```

Fig. 1. Pseudo-code to generate the X/Y alternation activity.

It is important to emphasize that while the effect of a single event (i.e. execution of a single memory access or processor instruction) on the baseband signal is unknown, as long as there is some difference between the X and Y activities, there will be a signal generated at the frequency f_{alt} and also at some of the harmonics of f_{alt} ($2f_{alt}, 3f_{alt}, ...$). Furthermore, we can change the duty cycle of the benchmark activity (i.e. (i.e. the percentage of time spent in activity X vs. activity Y) by changing how long the activity X is executed versus activity Y.

IV. An Algorithm for Finding AM and FM Unintentional Carriers in Computer Systems

In this section, we use the benchmarks described in Section III to create predictable spectral patterns in the sideband of any carrier modulated by the benchmark activity. The benchmarks are run at several different alternation frequencies $f_{alt_1}, f_{alt_2}, ..., f_{alt_N}$, for several duty cycles $d_1, d_2, ..., d_m$, and every combination of alternation frequencies and duty cycles is recorded K times. The frequency spectrum for each run is recorded, the repeated runs are averaged, and the result we denote as $S(f, f_{alt_i}, d_j)$, where f is the frequency range at which the spectrum is recorded, f_{alt_i} denotes the chosen alternation frequency, and d_j denotes the chosen duty cycle. In contrast to our work in FASE [26], where $f_\Delta = f_{alt_{i+1}} - f_{alt_i}$ was small and constant, here we chose alternation frequencies such that $f_{\Delta_i} = f_{alt_{i+1}} - f_{alt_i}$ is larger and not constant. This is an important step to allow robust automated detection of both AM and FM modulations. Please note, that from this point, the proposed algorithm significantly differs from one in [26]. The algorithm presented in [26] only generates signals at different alternation frequencies to find AM modulations as described in III, but after that, the user needs to visually look for patterns to determine carrier frequencies. In contrast, the algorithm presented in this section can find AM and FM modulations automatically.

To illustrate what measured $S(f, f_{alt_i}, d_j)$ looks like, Figure 2 plots a part of one spectrum around a carrier frequency at 382 kHz. This spectrum was recorded with $f_{alt} = 23$ kHz, so it shows a lower and upper sidebands around 359 kHz and 405 kHz, respectively.

The rest of the section describes several steps in our algorithm needed to identify unintentional AM and FM modulated carriers.

A. Identifying Actual Alternation Frequency

It is not surprising that the real alternation frequency differs from the one set in the benchmarks, because the execution time of a program varies from run to run and cannot be adjusted precisely. Hence, we need to estimate the real alternation frequency f_{alt}, before we can proceed in finding carrier frequencies. First, for every duty cycle, we average spectra with different alternation frequencies, i.e.,

$$S_{avg}(f, d_j) = \text{mean}_{f_{alt_i}} S(f, f_{alt_i}, d_j), \quad (1)$$

and create new spectra as a difference between the original and averaged spectra, i.e.

$$S_{new}(f, f_{alt_i}, d_j) = S(f, f_{alt_i}, d_j) - S_{avg}(f, d_j). \quad (2)$$

This attenuates most spectral features that are not related to modulated signals we are looking for, while preserving most of those that are activity-modulated.

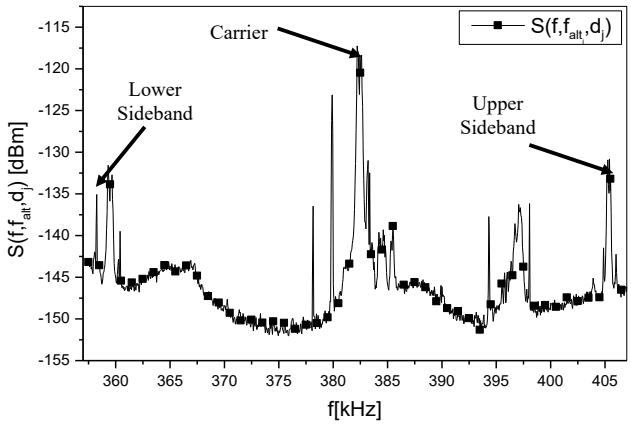

Fig. 2. A measured spectrum $S(f, f_{alt_i}, d_j)$ at a carrier frequency at 382 kHz and a lower and upper sidebands around 359 kHz and 405 kHz, respectively.

To find the true alternation frequency, we shift all points in the spectrum $S_{new}(f, f_{alt_i}, d_j)$ by $\pm f_{alt_i}$, and take the pointwise minimum between two shifts i.e. we compute

$$M(f, f_{alt_i}, d_j) = \min\Big[S_{new}(f + f_{alt_i}, f_{alt_i}, d_j), S_{new}(f - f_{alt_i}, f_{alt_i}, d_j)\Big]. \quad (3)$$

Figure 3 plots the spectrum $S_{new}(f, f_{alt_i}, d_j)$ shifted up by $f_{alt_i} = 23$ kHz (black square curve) and shifted down by $f_{alt_i} = 23$ kHz (red circle curve), their pointwise minimum $M(f, f_{alt_i}, d_j)$ (blue triangle curve). Also shown (magenta diamond curve) is the pointwise minimum computed in the same way (shifting by 23 kHz) for another spectrum whose alternation frequency is different (e.g. 29 kHz). We observe that, when the spectrum contains sidebands that correspond to f_{alt_i}, the shift in frequency aligns these sidebands at the frequency that corresponds, in the original spectrum, to the carrier that produced the sidebands (382 kHz in this case).

At points that do not correspond to the modulated carrier or its sidebands, the pointwise minimum will only have a peak if two prominent spectral features (e.g. two radio unrelated signals) happen to be separated by exactly $2f_{alt_i}$. Finally, when the spectrum is shifted by an amount that does not match the alternation frequency, the sidebands do not align and the pointwise minimum is unlikely to have a peak even at the carrier's frequency.

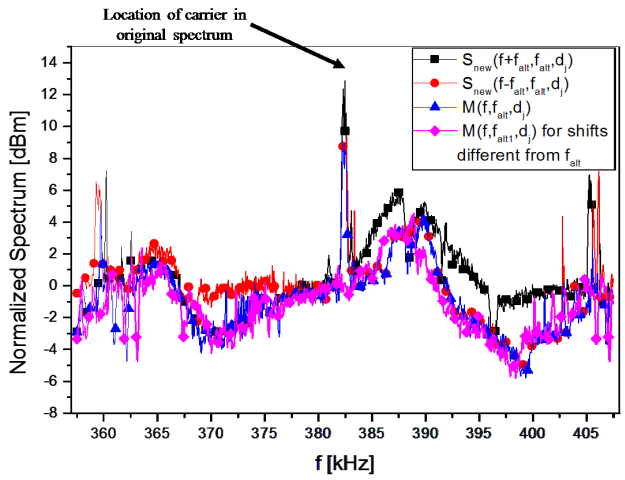

Fig. 3. A spectrum $S_{new}(f, f_{alt_i}, d_j)$ shifted up and down for 23 kHz, the pointwise minimum between these two spectra, and the pointwise minimum between two spectra with shift different from $f_{alt_i} = 23$ kHz.

Instabilities in program execution can cause the actual alternation frequency to be different from the intended one. To find that actual alternation frequency, we compute this minimum-of-shifted-spectra operation with all frequency shifts that are within 25% of the intended one, in 50 Hz increments. For each of these $M(f, f_{alt_i}, d_j)$ we compute the average across f, and the shift that produced the largest average it taken as the actual alternation frequency. The intuition behind this is that shifts that correspond to the true alternation frequency will produce the stronger peaks at frequencies that correspond to modulated carriers, and will possibly have other peaks that come from aligning unrelated signals. In contrast, incorrect shifts will only have the peaks that come from aligning unrelated signals, but their sideband-induced peaks will be attenuated (or completely eliminated). Thus the shift that corresponds to the actual alternation frequency tends to produce more (and stronger) peaks, which increases its average-over-f relative to other shifts.

In our experiments we found that the actual alternation frequency is often 150 to 300Hz away from the intended one. This difference may seem small, but some sidebands are sharply defined, e.g. the peak is only 100 to 200Hz wide, so use of the intended rather than true alternation frequency may cause our approach to completely miss the actual sideband signals and thus not report the corresponding modulated carrier signals.

B. Identifying Carrier Frequencies

To find the frequencies of carriers that are unintentionally modulated by program activity, we perform the following steps for each duty cycle d_j. First, for every alternation frequency f_{alt_i}, where $0 < i < N$, the spectrum $S(f, f_{alt_i}, d_j)$ (that corresponds to that alternation frequency) is shifted by $-f_{alt_i}$ to the left and by f_{alt_i} to the right. This creates $2N$ spectra that all correspond to the same duty cycle and whose sideband signals are shifted to the frequency of the carrier that produced that sideband signal. Then, the pointwise minimum among all these shifted spectra is found, i.e.

$$\begin{aligned} &M_{\text{true}}(f, d_j) = \\ &\min\Big[S(f + f_{alt_1}, f_{alt_1}, d_j), S(f - f_{alt_1}, f_{alt_1}, d_j), \\ &\quad S(f + f_{alt_2}, f_{alt_2}, d_j), S(f - f_{alt_2}, f_{alt_2}, d_j), \\ &\qquad\qquad \vdots \\ &\quad S(f + f_{alt_N}, f_{alt_N}, d_j), S(f - f_{alt_N}, f_{alt_N}, d_j)\Big]. \end{aligned} \quad (4)$$

Intuitively, at a frequency that corresponds to a modulated carrier, the sidebands that correspond to different f_{alt} will all align and the minimum will have a peak. At other frequencies, the minimum will have a peak only if other stronger-than-usual signals happen to be present in the original spectra at *every* one of the $2N$ positions, which becomes increasingly unlikely as we increase N.

However, it is still possible that other signals happen to align and create peaks in $M_{\text{true}}(f, d_j)$. To suppress these peaks, for every alternation frequency, we also compute $M_{\text{false}}(f, k, d_j)$ by taking each spectrum (collected with f_{alt_i}) and shifting it by $\pm f_{alt_{i+k_{k\neq 0}}}$, then taking the point-wise minimum among such spectra:

$$\begin{aligned} &M_{\text{false}}(f, k, d_j) = \\ &\min\Big[S(f + f_{alt_{1+k}}, f_{alt_1}, d_j), S(f - f_{alt_{1+k}}, f_{alt_1}, d_j), \\ &\quad S(f + f_{alt_{2+k}}, f_{alt_2}, d_j), S(f - f_{alt_{2+k}}, f_{alt_2}, d_j), \\ &\qquad\qquad \vdots \\ &\quad S(f + f_{alt_k}, f_{alt_N}, d_j), S(f - f_{alt_k}, f_{alt_N}, d_j)\Big]. \end{aligned} \quad (5)$$

The key property of $M_{\text{false}}(f, k, d_j)$ is that it is computed in exactly the same way as $M_{\text{true}}(f, d_j)$, but the use of incorrect f_{alt} causes none of the sideband signals to be aligned with each other. This is repeated for different non-zero values of k and compute the permutations of $f_{alt_{i+k}}$, and we compute $M_{\text{false}}(f, d_j)$ as the point-wise average among $M_{\text{false}}(f, k, d_j)$ across all non-zero values of k.

Figure 4 plots $M_{\text{true}}(f, d_j)$ and $M_{\text{false}}(f, d_j)$ for the experiment where there is an activity-modulated carrier at 382 kHz. We can observe that the $M_{\text{true}}(f, d_j)$ has a distinctive peak at the carrier frequency, while $M_{\text{false}}(f, d_j)$ does not. However, accidental alignment of other (non-sideband) signals would produce similar peaks in $M_{\text{true}}(f, d_j)$ and $M_{\text{false}}(f, d_j)$. Thus we compute a "modulated carrier score" $MCS(f)$ as the point-wise ratio between $M_{\text{true}}(f, d_j)$ and $M_{\text{false}}(f, d_j)$:

$$MCS(f) \quad = \quad 10 * \log_{10}\left(\frac{M_{\text{true}}(f, d_j)}{M_{\text{false}}(f, d_j)}\right). \quad (6)$$

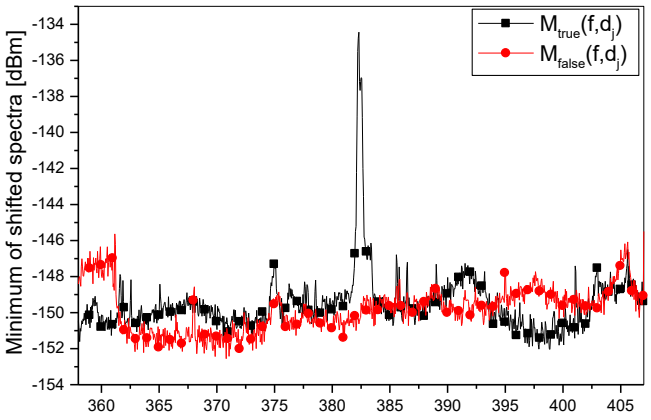

Fig. 4. Minimums of shifted spectra, i.e., $M_{\text{true}}(f, d_j)$ and $M_{\text{false}}(f, d_j)$, with the carrier frequency at 382 kHz and the alternation frequency of 23 kHz.

Intuitively, at each frequency the value of the MCS corresponds to how much stronger (in dB) is the signal that corresponds to the sidebands of that (potential) carrier, relative to the signal that would be computed for that frequency even if no sideband present. To illustrate this, Figure 5 shows the $MCS(f)$ that corresponds to $M_{\text{true}}(f, d_j)$ and $M_{\text{false}}(f, d_j)$ from Figure 4.

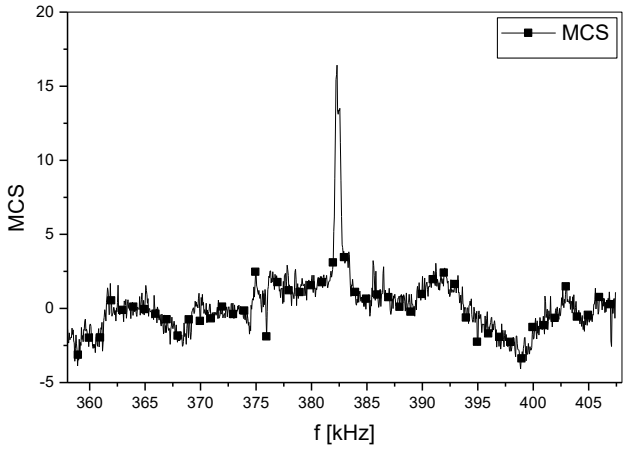

Fig. 5. Modulated carrier score as a function of frequency for a spectrum with the carrier frequency at 382 kHz and the alternation frequency of 23 kHz.

The $MCS(f)$ shown in Figure 5 has a strong peak that strongly suggests that a modulated carrier is present at 382 kHz, the $MCS(f)$ varies and has many other, smaller, peaks, so it is not easy to determine what value of MCS should be treated as the threshold for reporting a modulated carrier. If the MCS threshold is set to some manually selected value, it will need to be adjusted for each evaluated computer system, environment in which the experiment is carried out, antenna position, etc.

Instead, it is highly desirable to set a threshold in terms of the probability that a reported carrier is a false positive, and then automatically determine the corresponding threshold for MCS. To accomplish this, we note that $M_{\text{true}}(f, d_j)$ and $M_{\text{false}}(f, d_j)$ should be statistically equivalent for frequencies that are *not* modulated carriers, so for those frequencies the values of $MCS(f)$ should have a zero mean and a CDF that is symmetric around that mean. In contrast, for frequencies that correspond to modulated carriers, the $MCS(f)$ will have a bias toward positive values, and the magnitude of that bias increases as the power of sideband signals increases. Thus the problem of deciding how likely it is that a particular frequency has a modulated carrier becomes the problem of determining how likely it is that the $MCS(f)$ value for that frequency belongs to the positive-biased "modulated carrier" distribution rather than the symmetric "baseline" (no modulated carrier) distribution.

Although empirical data for the baseline distribution is not available (the $MCS(f)$ contains points from both distributions), the baseline distribution can be closely approximated by noting that 1) the baseline distribution is symmetric around zero and 2) negative values of $MCS(f)$ are very likely to belong to that distribution. The negative-values part of the baseline distribution is thus approximated by simply using the negative-values part of the empirical joint distribution, while the positive side of the baseline distribution is approximated by using the "mirror image" of the empirical joint distribution. Figure 6 shows the empirical joint distribution and the approximated baseline distribution.

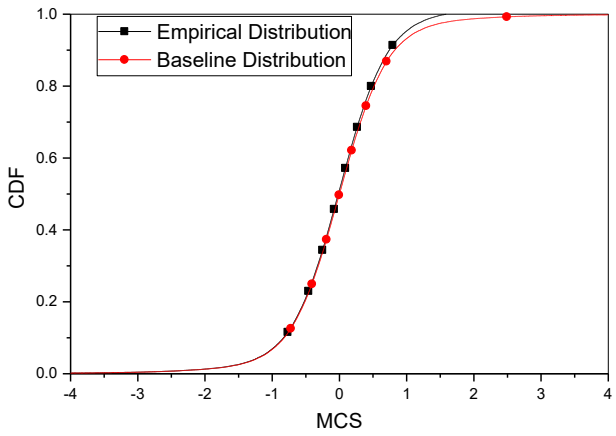

Fig. 6. Empirical joint and baseline cumulative distribution functions for MCS score.

It can be observed that the empirical joint distribution has more high-magnitude points than the approximated baseline distribution. Thus we can now set the probability-of-false-positive threshold (p_{fp}) to a desired value, e.g. $p_{fp} \leq 0.02$, look up the MCS value that corresponds to $1-p_{fp}$, and report carriers whose MCS is no less than that value. For reported MCSs, we than read the actual CDF value and report it as the confidence level. For example, for $p_{fp} \leq 0.02$, we find all MCSs that have value larger than MSC that corresponds to CDF=0.98. Then, for each MCS that satisfies this criteria, we read their actual CDF value. All values should be larger than 0.98.

C. Identifying Modulation

Section IV-B described how to identify modulated carrier frequencies for a given duty cycle d_j. To identify if the carrier has AM or FM modulated signal, we observe how the carrier's frequency and sideband power change as the duty cycle changes. Note that an amplitude-modulated carrier should have the same frequency for all duty cycles (although the magnitude of the carrier and baseband signals will vary as the duty cycle changes). For a frequency-modulated carrier, however, the change in the duty cycle changes the DC-value of the baseband signal, which results in shifting the frequency of the carrier and its sidebands in proportion to the duty cycle. Intuitively, if we plot the modulated carrier's frequency on the Y-axis and the duty cycle on the X-axis, a horizontal line corresponds to AM, while a a line with a non-zero slope corresponds to FM whose Δf corresponds to the line's slope.

To reduce the number of spectra that must be collected, however, we only get discrete points on this line that correspond to duty cycles used in the experiments. Furthermore, the AM/FM identification (and the estimate of Δf for FM) relies on estimating the slope of the frequency-vs.-duty cycle line, so the duty cycles used in the experiments should not be too close to each other. Finally, the linear fit is imperfect - the actual duty cycle may differ from the intended one, the empirically determined frequency of the modulated carrier may contain some error, etc. Thus the key problem in identifying modulation is how to group together likely-carrier points from different duty cycles, i.e. for a likely-modulated-carrier point found for a given duty cycle, determining which likely-carrier points from other duty cycles belong to the same modulated carrier. Unfortunately, simply using the points that produce the best goodness-of-fit (e.g. squared-sum-or-errors) for the frequency-vs-duty-cycle produces poor results when several modulated carriers that do not have a very sharply defined central frequency are present in the same frequency range. To overcome this, we note that the sideband power produced by a carrier is also a function of the duty cycle, i.e. the points that belong to the same carrier but with different duty cycles should all have the sideband power $P_j = P_{max}\sin(d_j\pi)/\pi$, so their $M_{\text{true}}(f, d_j)$ should also be proportional to $\sin(d_j\pi)/\pi$. Thus our modulation-finding consists of finding, for each likely-carrier point, the linear fit (that uses one point from each duty cycle) that produces the smallest *product* of the squared sum of error for the frequency fit and the squared sum of errors for the (M_{true}) fit.

Because the slope of the linear fit is estimated, it is highly unlikely to be exactly zero. Thus we also determine the 95% confidence interval for the estimated slope, and report the carrier as AM if this confidence includes the zero value. Intuitively, we report a carrier as FM-modulated only if there is a high enough (95%) confidence that its frequency change is duty-cycle-induced rather than caused by other (duty-cycle-unrelated) variation in estimated frequencies of modulated carriers. The flow chart of the algorithm is presented in Fig. 7.

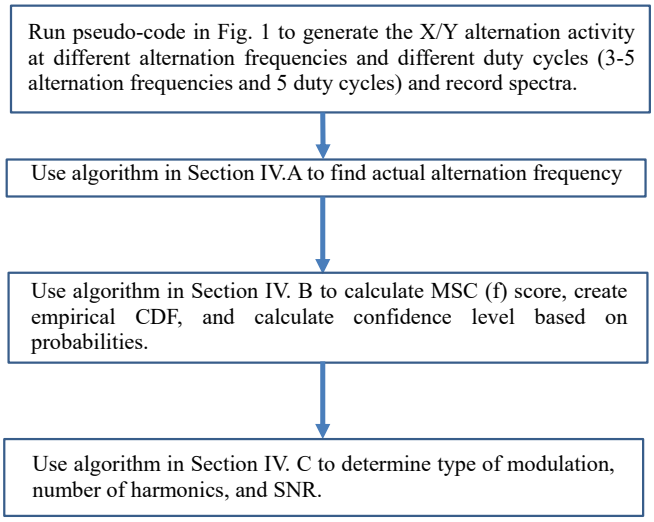

Fig. 7. Flow chart of the proposed algorithm.

V. Experimental Setup

We have evaluated the algorithm by testing it on spectra from a desktop, a laptop, and a smartphone system described in Figure 8. The signals are recorded using the spectrum analyzer (Agilent MXA N9020A). The desktop and laptop measurements are collected with a magnetic loop antenna (AOR LA400) at a distance of 30 cm as shown on the left of Figure 9. To receive weaker signals from smartphones, EM emanations were recorded using a small loop probe with 20 turns and a 4 mm radius positioned on top of the cellphone as shown on the right of Figure 9. The spectra were measured from 0 to 4 MHz with a resolution bandwidth of 10 Hz.

Type	Device	Processor
Laptop	Lenovo	Intel Core 2 Duo
Phone	LG P705	Snapdragon S1
Desktop	Dell	Intel i7

Fig. 8. Description of measured devices.

The benchmarks are run at several different alternation frequencies $f_{alt} = \{23000, 29000, 37000, 53000\}$ Hz with duty cycles $d = \{20, 40, 50, 60, 80\}\%$. The alternation frequencies were chosen to ensure sufficient separation between sidebands of modulated signals, i.e. separation between f_{alt_1}, f_{alt_2}, etc. and their harmonics has to be sufficient to prevent overlapping. For example, if $f_{alt_1} = 23$ kHz is chosen, frequencies in the vicinity of the harmonics of f_{alt_1} should be avoided. Aside from this consideration, the choice of f_{alt} is arbitrary. We have found that four alternation frequencies are sufficient in the algorithm to identify carrier frequencies. To identify if the modulation is AM or FM, we need all five duty cycles.

The benchmarks were run on the laptop and desktop systems as single-threaded Windows 7 32-bit user mode console applications, and as normal Android applications on the smartphone. When possible all unrelated programs and activities were disabled, CPU frequency scaling was disabled, and screens were turned off. We measured two alternation activities. The first activity alternated between a load from

Fig. 9. Measurement setup for laptop or desktop (left) and measurement setup for cell-phone (right).

DRAM memory and a load from the on-chip L1 cache, which we abbreviate as LDM/LDL1. This alternation is useful in exposing modulated carriers related to memory activity. The second activity alternated between loads from the on-chip L2 and L1 caches, which we abbreviate as LDL2/LDL1. This activity exposes carriers modulated by on-chip activity. We tried other instruction pairs (e.g. arithmetic, memory stores, etc.) and found that that all known modulated carriers could be found using just these two activities.

VI. Experimental Results

We tested three devices described in Figure 8, with two measurements per device (one for LDM/LDL1 and one for LDL2/LDL1). Table I summarizes carrier frequencies found using our algorithm, type of modulation, signal to noise ratio (SNR) of the received carrier, and the confidence level that the found carrier is correctly identified from a laptop. Here, we define SNR as a difference in decibels between $M_{\text{true}}(f, d_j)$ and $M_{\text{false}}(f, d_j)$, as defined in equation (6). Our algorithm has found one FM carrier and it's two harmonics with confidence level above 99%. We can also observe that SNR for all three FM modulated frequencies is above 10 dB which indicates that these carriers are strong and will carry signal to some distance away from the laptop. Our algorithm has also found one AM modulated carrier but the observed SNR is only 4 dB, which indicates that this is a weak carrier. Please note that our algorithm finds all carriers independently and then we check for possible harmonic relationship among found frequencies and if found, we report the harmonic order.

TABLE I
Carrier frequencies found in a laptop.

Carrier Frequency [Hz]	Harmonic No.	SNR [dB]	Type of Modulation	Confidence Level
383010	1	16	FM (Δf=2275 Hz)	99.8%
765949	2	12	FM (Δf=4700 Hz)	99.9%
1148959	3	10	FM (Δf=7225 Hz)	99.8%
448071	1	4	AM	99.1%

Table II summarizes carrier frequencies found using our algorithm, type of modulation, signal to noise ratio (SNR) of the received carrier, and the confidence level that the found carrier is correctly identified from a cell phone. Here, our algorithm has found one AM carrier and its second harmonic with confidence level above 99%. The SNR for these two frequencies is above 20 dB, i.e. they are excellent candidates to carry signal outside of the cell phone. Our algorithm has also found two FM modulated carriers, but the observed SNR is only 1 dB, which indicates that these are weak carriers.

Finally, Table III summarizes carrier frequencies found using our algorithm, type of modulation, signal to noise ratio (SNR) of the received carrier, and the confidence level that the found carrier is correctly identified from a desktop. Here, our algorithm has found one AM carrier and its 11 harmonics with confidence level above 99%. The SNR for first seven harmonics is above 10 dB, while SNR for other five harmonics is above 5 dB. Furthermore, we have found one more AM carrier and its seven harmonics all with SNR above 10 dB. Finally, we have found one FM carrier with SNR of 5 dB. To verify the accuracy of the algorithm, we have visually

TABLE II
Carrier frequencies found in a cell phone.

Carrier Frequency [Hz]	Harmonic No.	SNR [dB]	Type of Modulation	Confidence Level
110543	1	1	FM (Δf=3100 Hz)	98.6%
1599990	1	30	AM	100%
3200000	2	22	AM	99.98%
3257391	1	1	FM (Δf=96002 Hz)	99.98%

inspected all spectra and confirmed that carriers found by the algorithm exist in the spectrum. From the results, it can be observed that there are only 2 or 3 fundamental frequencies and the rest are their harmonics. The fundamental frequencies that were reported are all attributable to voltage regulator and memory refresh activity on the measured system. For example in Figure III we can observe that the two strongest sources are voltage regulator (315 kHz) and memory refresh (software activity in the system at 511 kHz). The voltage regulator emanations can be reduced by better shielding of coils, and the memory refresh can be eliminated by creating different scheduling pattern for memory refresh. Alternatively, program code can be changed to avoid power-fluctuations and memory activity that depends on sensitive information. Please note that carrier frequencies can be found at higher frequencies as well (here we have tested only up to 4 MHz). They are typically above 500 MHz and belong to processor or memory clock. While our algorithm can find these frequencies as well, information about processor and memory clocks is readily available. Finding carrier frequencies at lower frequency range is more challenging because there is much more noise-like activity in the spectrum and it is difficult to identify information caring signals.

Automatic identification of potential carriers in the system has several benefits. From the security prospective, it allows us to quickly identify frequencies of interest for observing RF emanations, it allows prediction of distances from which we can expect to receive good quality signal (based on observed SNR), and the type of demodulation needed to correctly receive signals. From the system designer prospective, finding carrier frequencies helps us identify leaky circuits. For example, the unintentional FM and AM carriers found for a desktop and laptop were caused by voltage regulators and memory refresh commands. For a cell phone, several carriers were found to be caused by voltage regulators. The remainder of the carriers found on the cell phone were traced to particular IC packages or modules and were likely caused by either voltage regulators or an unknown periodic memory activity. However, smartphones integrate many system components into System

on Chip (SoC) modules and often use Package on Package (PoP) technology to integrate both the processor and memory into the same package and little information is publicly available describing these components. More information would be needed to definitively determine the circuits and mechanisms modulating these carriers.

TABLE III
CARRIER FREQUENCIES FOUND IN A DESKTOP.

Carrier Frequency [Hz]	Harmonic No.	SNR [dB]	Type of Modulation	Confidence Level
315488	1	28	AM	99.8%
631006	2	28	AM	99.99%
946654	3	22	AM	99.7%
1262312	4	21	AM	99.8%
1566849	5	19	AM	99.9%
1893447	6	18	AM	99.8%
2209415	7	13	AM	99.9%
2840661	9	5	AM	99.8%
3156239	10	6	AM	99.8%
3471917	11	8	AM	99.9%
3787705	12	6	AM	99.8%
451581	1	5	FM (Δf=550 Hz)	99.92%
511653	1	17	AM	99.96%
1023306	2	13	AM	99.97%
1534938	3	24	AM	100%
2046601	4	25	AM	100%
2558214	5	23	AM	100%
3069877	6	20	AM	100%
3581530	7	11	AM	99.99%

VII. CONCLUSIONS

This paper presented an algorithm for finding carriers of frequency-modulated (FM) and amplitude-modulated (AM) electromagnetic (EM) emanations from computer systems. Computer systems create EM emanations across the RF spectrum making it difficult, error-prone, and time-consuming to find the relatively few emanations that expose sensitive information. One of the most common and simplest mechanisms for information leakage occurs when the amplitude or a frequency of an existing strong signal (e.g. a processor or memory clock) is amplitude or frequency modulated by a system activity. If the system activity can be linked to sensitive information, this results in information leakage. We have presented an algorithm for automatically finding these AM and FM modulated signals, demonstrated the algorithm's performance on several different types of processors and systems (desktop, laptop, and smart phone), and compared the results to an exhaustive manual search. We have also verified that all signals identified by the algorithm can be traced to plausible unintentional modulation mechanisms to illustrate that these signals can potentially cause information leakage. This algorithm can be an important tool for system designers to quickly identify circuits that are leaking sensitive information.

REFERENCES

[1] H. J. Highland, "Electromagnetic radiation revisited," *Computers and Security*, pp. 85–93, Dec. 1986.

[2] M. G. Khun, "Compromising emanations: eavesdropping risks of computer displays," *The complete unofficial TEMPEST web page: http://www.eskimo.com/˜joelm/tempest.html*, 2003.

[3] W. van Eck, "Electromagnetic radiation from video display units: an eavesdropping risk?," *Computers and Security*, pp. 269–286, Dec. 1985.

[4] P. Kocher, J. Jaffe, and B. Jun, "Differential power analysis: leaking secrets," in *Proceedings of CRYPTO'99, Springer, Lecture notes in computer science*, pp. 388–397, 1999.

[5] D. Agrawal, B. Archambeult, J. R. Rao, and P. Rohatgi, "The EM side-channel(s)," in *Proceedings of Cryptographic Hardware and Embedded Systems - CHES 2002*, pp. 29–45, 2002.

[6] T. Sugawara, D. Suzuki, M. Saeki, M. Shiozaki, and T. Fujino, " On measurable side-channel leaks inside ASIC design primitives," *Proceedings of the 15th international conference on Cryptographic Hardware and Embedded Systems - CHES 2013*, pp. 159–178, 2013.

[7] M. Vuagnoux and S. Pasini, "An improved technique to discover compromising electromagnetic emanations," in *Electromagnetic Compatibility (EMC), 2010 IEEE International Symposium on*, pp. 121–126, IEEE, 2010.

[8] T. Kasper, D. Oswald, and C. Paar, "Em side-channel attacks on commercial contactless smartcards using low-cost equipment," in *Information Security Applications*, pp. 79–93, Springer, 2009.

[9] K. Gandolfi, C. Mourtel, and F. Olivier, "Electromagnetic analysis: concrete results," in *Proceedings of Cryptographic Hardware and Embedded Systems - CHES 2001*, pp. 251–261, 2001.

[10] D. Genkin, I. Pipman, and E. Tromer, "Get your hands off my laptop: physical side-channel key-extraction attacks on PCs," in *Proc. Crypto. HW and Emb. Sys. (CHES)*, 2014.

[11] A. Zajic and M. Prvulovic, "Experimental demonstration of electromagnetic information leakage from modern processor-memory systems," *Electromagnetic Compatibility, IEEE Transactions on*, vol. 56, pp. 885–893, Aug 2014.

[12] D. Genkin, L. Pachmanov, I. Pipman, and E. Tromer, "Stealing keys from PCs using a radio: cheap electromagnetic attacks on windowed exponentiation," in *Proc. Crypto. HW and Emb. Sys. (CHES)*, 2015.

[13] O. Meynard, D. Real, F. Flament, S. Guilley, N. Homma, and J.-L. Danger, "Enhancement of simple electro-magnetic attacks by pre-characterization in frequency domain and demodulation techniques," in *Design, Automation and Test in Europe Conference and Exhibition (DATE) 2011*, pp. 1–6, 14–18 March 2011.

[14] G. Perin, L. Torres, P. Benoit, and P. Maurine, "Amplitude demodulation-based EM analysis of different RSA implementations," in *Proceedings of the Conference on Design, Automation and Test in Europe (DATE) 2012*, pp. 1167–1172, EDA Consortium, San Jose, CA, USA, 2012.

[15] J. J. A. Fournier, S. Moore, H. Li, R. Mullins, and G. Taylor, "Security evaluation of asynchronous circuits," in *Proceedings of Cryptographic Hardware and Embedded Systems - CHES 2003*, pp. 137–151, 2003.

[16] T. Plos, M. Hutter, and C. Herbst, "Enhancing side-channel analysis with low-cost shielding techniques," in *Proceedings of Austrochip*, 2008.

[17] F. Poucheret, L. Barthe, P. Benoit, L. Torres, P. Maurine, and M. Robert, "Spatial EM jamming: A countermeasure against EM Analysis?," in *Proceedings of the 18th IEEE/IFIP VLSI System on Chip Conference (VLSI-SoC)*, pp. 105–110, 2010.

[18] J. J. Quisquater and D. Samyde, "Electromagnetic analysis (EMA): measures and counter-measured for smart cards," in *Proceedings of E-smart*, pp. 200–210, 2001.

[19] H. Tanaka, "Information leakage via electromagnetic emanations and evaluation of Tempest countermeasures," in *Lecture notes in computer science, Springer*, pp. 167–179, 2007.

[20] H. Tanaka, O. Takizawa, and A. Yamamura, "Evaluation and improvement of Tempest fonts," in *Lecture notes in computer science, Springer*, pp. 457–469, 2005.

[21] Y. Hayashi, N. Homma, T. Mizuki, H. Shimada, T. Aoki, H. Sone, L. Sauvage, and J. L. Danger, "Efficient evaluation of EM radiation associated with information leakage from cryptographic devices," *IEEE Transactions on Electromagnetic Compatibility*, vol. 55, pp.555–563, June 2013.

[22] H. Sekiguchi and S. Seto, "Study on maximum receivable distance for radiated emission of information technology equipment causing information leakage", *IEEE Transactions on Electromagnetic Compatibility*, vol. 55, pp.547–554, June 2013.

[23] Y. Hayashi, N. Homma, T. Mizuki, T. Aoki, H. Sone, L. Sauvage, J. L. Danger, "Analysis of electromagnetic information leakage from cryptographic devices with different physical structures", *IEEE Transactions on Electromagnetic Compatibility*, vol. 55, pp. 571–580, June 2013.

[24] Henry W. Ott, *Electromagnetic Compatibility Engineering*. Wiley, 2009.

[25] C. R. Paul, *Introduction to Electromagnetic Compatibility*. Wiley, 2nd ed., 2006.

[26] R. Callan, A. Zajić, and M. Prvulovic, "Fase: finding amplitude-modulated side-channel emanations," in *Proc. of the 42nd Annual International Symposium on Computer Architecture*, pp. 592–603, ACM, 2015.

[27] R. Callan, A. Zajic, and M. Prvulovic, "A practical methodology for measuring the side-channel signal available to the attacker for

instruction-level events," in *Proc. 47th Int'l Symp. on Microarchitecture*, 2014.
[28] T. Rappaport, *Wireless Communications: Principles and Practice*. Dorling Kindersley, 2009.

Milos Prvulovic (S'97-M'03-SM'09) received the B.Sc. degree in electrical engineering from the University of Belgrade in 1998, and the M.Sc. and Ph.D. degrees in computer science from the University of Illinois at Urbana-Champaign in 2001 and 2003, respectively. He is an Associate Professor in the School of Computer Science at the Georgia Institute of Technology, where he joined in 2003. His research interests are in computer architecture, especially hardware support for software monitoring, debugging, and security.

He is a past recipient of the NSF CAREER award, and a senior member of the ACM, the IEEE, and the IEEE Computer Society.

Alenka Zajic (S'99-M'09-SM'13) received the B.Sc. and M.Sc. degrees form the School of Electrical Engineering, University of Belgrade, in 2001 and 2003, respectively. She received her Ph.D. degree in Electrical and Computer Engineering from the Georgia Institute of Technology in 2008. Currently, she is an Assistant Professor in the School of Electrical and Computer Engineering at Georgia Institute of Technology. Prior to that, she was a visiting faculty member in the School of Computer Science at Georgia Institute of Technology, a post-doctoral fellow in the Naval Research Laboratory, and a design engineer at Skyworks Solutions Inc. Her research interests span areas of electromagnetics, wireless communications, signal processing, and computer engineering.

Dr. Zajić received the Neal Shepherd Memorial Best Propagation Paper Award, the Best Paper Award at ICT 2008, the Best Student Paper Award at WCNC 2007, and was also the recipient of the Dan Noble Fellowship in 2004, awarded by Motorola Inc. and IEEE Vehicular Technology Society for quality impact in the area of vehicular technology. Currently, she is an editor for IEEE Transactions on Wireless Communications.

Robert L. Callan (S'14) received the B.Sc. degree in electrical engineering from the University of Pennsylvania in 2007 and the M.Sc. degree in electrical engineering from the University of Southern California in 2008. Since 2014, he has been a Graduate Research Assistant with the Electromagnetic Measurements in Communications and Computing (EMC^2) Lab, pursuing the Ph.D. degree in the School of Electrical and Computer Engineering, Georgia Institute of Technology focusing on side-channel information leakage in computer systems. Previously, he characterized high speed serial interfaces at IBM and Altera. His research interests span areas of electromagnetics, VLSI, and computer engineering.

Christopher J. Wang anticipates to graduate from Georgia Tech in Spring 2016 with a B.S. in Computer Engineering. He has been an Undergraduate Research Assistant with the Electromagnetic Measurements in Communications and Computing (EMC^2) Lab since 2014, focusing on side-channel information leakage in computer systems. Previously, he worked on the WEAMs health monitoring system as a member of the GT-Bionics Lab under Maysam Ghovanloo.