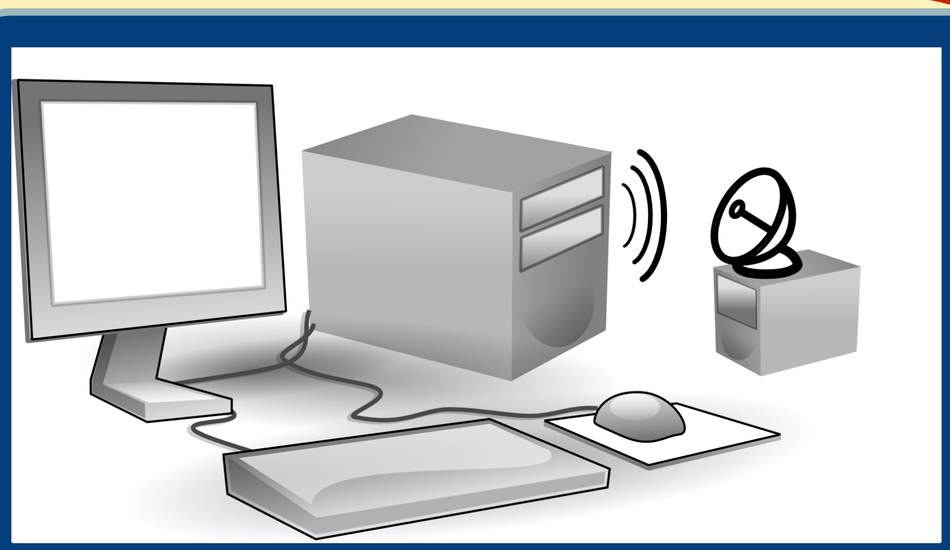
Quantitative Analysis and Reporting of Electromagnetic Covert and Side Channel Vulnerabilities

PIs: Alenka Zajic (PI) and Milos Prvulovic (Co-PI) Georgia Tech
www.ece.gatech.edu/~alenka

The major goals of the project are:

1) perform a systematic investigation of the relationship between software activity and the resulting EM emanations,
2) create software analyses that will identify activity that may result in information-carrying EM emanations, and
3) create a quantitative reporting framework that programmers can use to refactor their code in ways that alleviate or eliminate leakage of specific information



Wirelessly Monitor Emanations from Computers

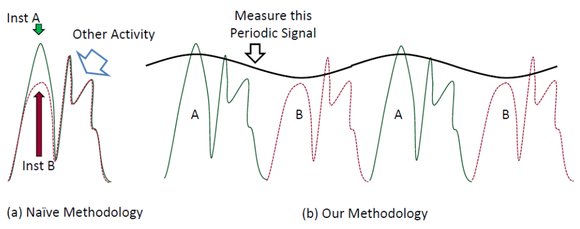
Approach

- ❑ Develop understanding of underlying physical effects that lead to side-channel emanations
- ❑ Develop understanding of relationship between software and hardware activities that lead to side-channel emanations
- ❑ Use it to create a quantitative reporting framework.

SAVAT: A Practical Methodology for Measuring the Side-Channel Signal Available to the Attacker for Instruction-Level Events

```
1  while(1){
2    // Do some instances of the A inst/event
3    for(i=0;i<inst_loop_count;i++){
4      ptr1=(ptr1&~mask)|((ptr1+offset)&mask);
5      // The A-instruction, e.g. a load
6      value=*ptr1;
7    }
8    // Do some instances of the B inst/event
9    for(i=0;i<inst_loop_count;i++){
10     ptr2=(ptr2&~mask)|((ptr2+offset)&mask);
11     // The B-instruction, e.g. a store
12     *ptr2=value;
13   }
14 }
```

The A/B alternation pseudo-code.

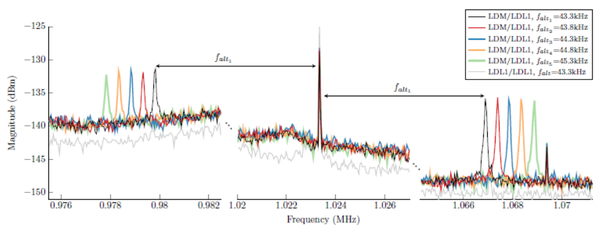


(a) Naïve Methodology (b) Our Methodology

	LDM	STM	LDL2	STL2	LDL1	STL1	NOI	ADD	SUB	MUL	DIV
LDM	1.8	2.4	7.9	11.5	4.6	4.4	4.3	4.2	4.4	4.2	5.1
STM	2.3	2.4	8.8	11.8	4.3	4.2	3.8	3.9	3.9	4.3	4.2
LDL2	7.7	7.7	0.6	0.8	3.9	3.5	4.3	3.6	4.8	3.8	6.2
STL2	11.5	10.6	0.8	0.7	5.1	6.1	6.1	6.1	6.1	6.2	10.1
LDL1	4.4	4.2	3.3	5.8	0.7	0.6	0.7	0.7	0.7	0.7	1.3
STL1	4.5	4.2	3.8	4.9	0.7	0.6	0.7	0.6	0.6	0.6	1.2
NOI	4.1	3.8	4.1	6.4	0.7	0.7	0.6	0.6	0.7	0.6	1.0
ADD	4.2	4.1	4.1	7.0	0.7	0.7	0.6	0.7	0.6	0.6	1.0
SUB	4.4	4.0	3.8	7.3	0.7	0.6	0.7	0.6	0.6	0.6	1.1
MUL	4.4	3.9	3.7	5.7	0.7	0.7	0.6	0.6	0.6	0.6	1.1
DIV	5.0	4.6	6.9	9.3	1.3	1.2	1.0	1.1	1.1	1.1	0.8

SAVAT values (in zJ) for the Core 2 Duo laptop at the 10 cm distance and at the 80 kHz alternation frequency

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



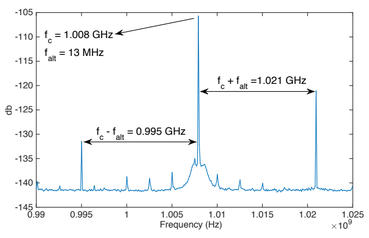
CARRIER FREQUENCIES FOUND IN A DESKTOP.

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%

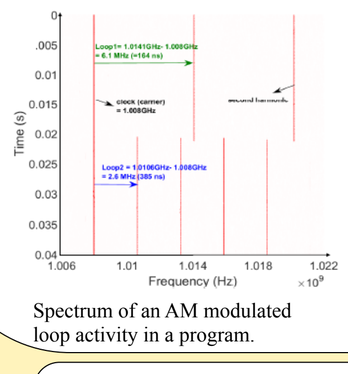
CARRIER FREQUENCIES FOUND IN A LAPTOP.

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%

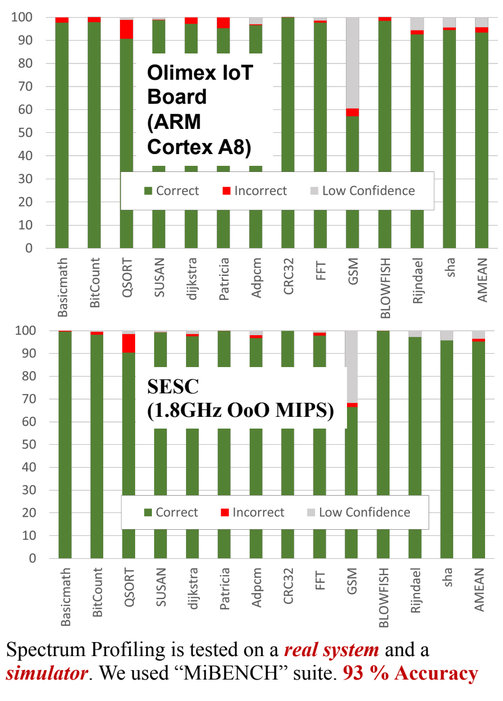
Spectral Profiling: Observer-Effect-Free Profiling by Monitoring EM Emanations



Spectrum of an AM modulated loop activity. The carrier (clock) signal and the side bands (loop activity) can be seen in this figure.

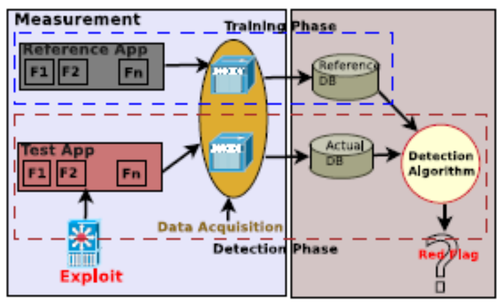


Spectrum of an AM modulated loop activity in a program.

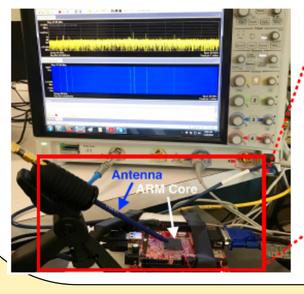


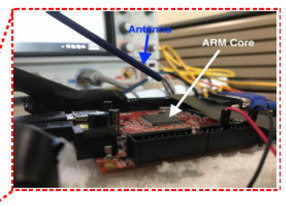
Spectrum Profiling is tested on a ***real system*** and a ***simulator***. We used "MiBENCH" suite. **93 % Accuracy**

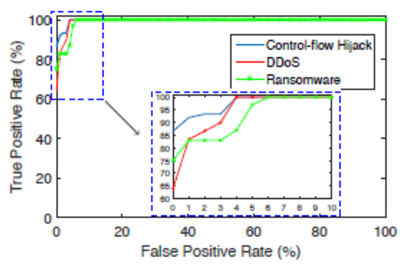
SAFEM: Spectral Analysis for Finding Execution of Malware

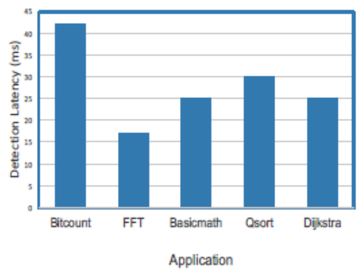


Overview of SFEEM









Accuracy and latency of SAFEEM for different types of attacks

Interested in meeting the PIs? Attach post-it note below!

NSF Secure and Trustworthy Cyberspace Inaugural Principal Investigator Meeting
Jan. 9-11th 2017
Arlington VA

National Science Foundation
WHERE DISCOVERIES BEGIN

Georgia Institute of Technology