Active Countermeasure using EMI Honeypot against TEMPEST Eavesdropping in High-Speed Signalling

Kai Yao, Shengchang Lan
Dept. of Microwave Engineering
Harbin Institute of Technology
Harbin, Heilongjiang, China
yaokai@hit.edu.cn;lansc1015@hit.edu.cn

Meng Xia, Lijia Chen
School of Electronic Information Engineering
Harbin Institute of Technology
Harbin, Heilongjiang, China
495762423@qq.com; ljchen@hit.edu.cn

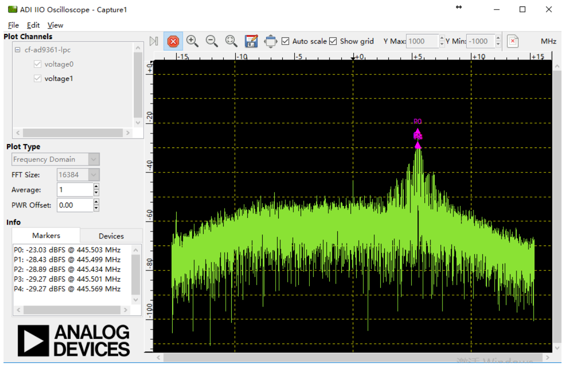
***Abstract*—Current development in TEMPEST and other eavesdropping strategies becomes a critical threat to the information security. To enhance the countermeasures of eavesdropping the electromagnetic radiation leakage in high-speed signalling such as computer monitors and other high-speed peripherals, this paper proposed an active countermeasure solution by interfering the TEMPEST receiver with a honeypot radiation source. Instead of passive noise jamming methods, this honeypot strategy used the multi-carrier modulation to hide the leakage and transmit a pseudo high-speed signal blended with information baits which may lead the eavesdropper uncovered. This system was implemented on a software defined radio platform and verified to be a prospecting application in future information security.**

I. Introduction

Recent development of TEMPEST(transient electromagnetic pulse emanation surveillance technology) is a crucial problem for information security[1]. Equipments such as computer monitors, digital television, and many other high-speed peripherals radiates electromagnetic waves which contain some portion of the information flowing between the peripheral devices. The information can be restored using non-interactive detection methods some distance away with log periodic antenna coupled with a highly sensitive receiver[2]. Since the concept was proposed, there has been an increasing number of researches on the countermeasure against the TEMPEST[3]. The main idea was to use AWGN(Additive White Gaussian Noise) to suppress the receiving quality of the EM waves eavesdropped based on the countermeasure using EMI(Electromagnetic Interference). However, this paper proposed an active countermeasure strategy using honeypot strategy with baits. This concept yielded a multiple carrier modulation to hide the radiation from the high-speed signalling and transmit the pseudo signals containing the bait information deliberately leaked to the eavesdroppers. Hence his location may be exposed if he used the bait information on the internet. Consequently, this paper discussed the feasibility of this active countermeasure against the TEMPEST eavesdroppers and the implementation of this strategy based on a software defined radio platform.

II. EM emission analysis

Using an omnidirectional antenna, spikes in positive or negative polarities at the rising and falling edges of the original high-speed signallings can be detected. With this information, it is possible to reconstruct the pattern of the digital video signal and to distinguish between the rising and falling edges through the peak of the detected signal[4].



Y Max: 1000
Y Min: -1000

Plot Type: Frequency Domain
FFT Size: 16384
Average: 1
PWR Offset: 0.00

P0: -23.03 dBFS @ 445.503 MHz
P1: -28.43 dBFS @ 445.499 MHz
P2: -28.89 dBFS @ 445.434 MHz
P3: -29.27 dBFS @ 445.501 MHz
P4: -29.27 dBFS @ 445.569 MHz

Fig. 1. Frequency domain of leaked signal.

Fig. 1 showed the frequency spectrum of leaked signal radiated by Dell U2417H screen connecting with the desktop computer. The center frequency of the received signal was 445.5MHz. The signal was demodulated to recover the information displayed on the computer monitor with the preliminary knowledge of the accurate screen resolution and the frame per second. Fig. 2 showed the recovered text "APSURSI2018" demodulated by TEMPEST corresponding to the signal represented in Fig. 1 . Each letter displayed on the screen after processing was legible. This system could be used to steal important information and pose a serious challenge to information security.

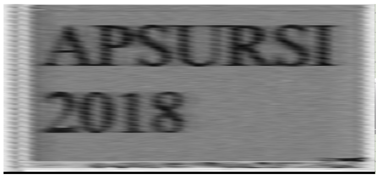


Fig. 2. Display of information recovery of EM emission from HDMI cable.

978-1-5386-7105-4/18/$31.00 ©2018 IEEE

III. Honeypot system and implementation

To avoid being unconsciously attacked by TEMPEST, we proposed an active countermeasure strategy based on the honeypot theory. The system structure was shown in Fig. 3. This honeypot system consisted in a software defined radio platform to generate the waveform, two multiband antennas for sensing the leakage of the high-speed signallings and transmitting honey baits, and a honey bait network server.

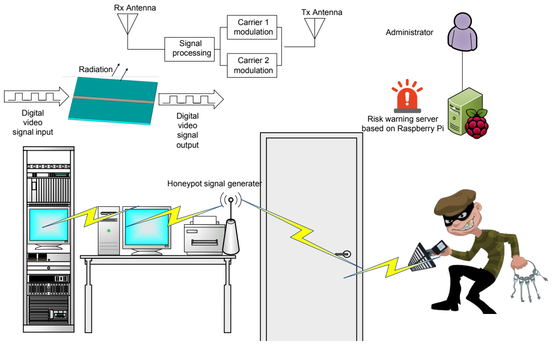

Rx Antenna
Signal processing
Carrier 1 modulation
Carrier 2 modulation
Tx Antenna
Administrator
Radiation
Digital video signal input
Digital video signal output
Risk warning server based on Raspberry Pi
Honeypot signal generater

Fig. 3. The whole structure of the system.

The software defined radio platform can sense the electromagnetic radiations and capture leaked signals with respect to the specified frequency and screen resolution, and furthermore automatically resolve and adjust the refresh rate. We used the multiple-carrier modulation to design the jamming signals and the bait signals shown as in Fig.4. As the result, this multiple carrier modulation may generate at least two spectra peaks, shown as in Fig. 5. On peak could cover the frequency band of the leaked signals and the other peak represented the pseudo signals as the bait. It was recommended that the bait can be generated as a normal screen display with hooks inside, a few Mega Hz next to the real leakage signal frequency spectrum.

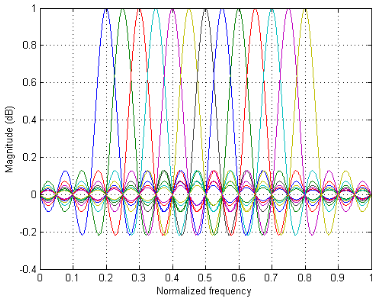


Fig. 4. Multiple carrier modulation.

As shown in Fig. 6, we established a demo system with two omnidirectional antenna connected to the software defined radio platform, PlutoSDR. After deploying the entire honeypot's hardware system in the right place, if someone has already attacked the entire system, he would get the information regarding the specially designed website, and tried to use the information to login to the system. These kind of operations would trigger the alarm, and after that the server would send a message to the system administrator that the honeypot has been under an attack. This active honeypot system can used as probes for attacks can be widely deployed around computers that required electromagnetic protection.

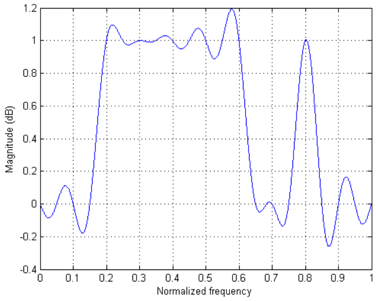


Fig. 5. The designed power spectrum using Multiple carrier modulation.

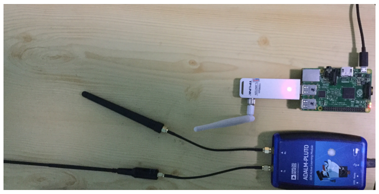


Fig. 6. PlutoSDR and Raspberry Pi of the honeypot system.

IV. Conclusions and future work

An active countermeasure using EMI honeypot against TEMPEST eavesdropping in high-speed signalling was proposed in this paper. The test we set to verify the system can prove that the system can work accurately and efficiently. It can not only hide the EM signal leaked from the user and protect them from attacker, but also would set up a honeypot which could be used as a bait to attract the attacker. Especially, this would be great helpful to get the status of the protection situation. In future, new firmware will be developed, and we will continue to improve the algorithm. New features and more defense logic will be developed. The system will be widely used in future.

References

[1] Y. I. Hayashi, J. G. Yook, K. Sim. "Introduction to a special session on EMC and information security",*Ursi Asia-Pacific Radio Science Conference*, pp. 1275-1276, 2016.

[2] H. S. Lee, J. G. Yook, K. Sim. "Study for possibility of information leakage from digital video display interface", *URSI Asia-Pacific Radio Science Conference (URSI AP-RASC)*, pp. 1102-1103, 2016.

[3] T. L. Song, Y.R. Jeong, H. S. Jo. "Noise-Jamming Effect as a Countermeasure Against TEMPEST During High-Speed Signaling",*IEEE Transactions on Electromagnetic Compatibility*, vol. 57, no. 6, pp. 1491-1500, April 2015.

[4] T. L. Song, Y. R. Jeong, J. G. Yook. "Modeling of Leaked Digital Video Signal and Information Recovery Rate as a Function of SNR",*IEEE Transactions on Electromagnetic Compatibility*, vol. 57, no. 2, pp. 164-172, April 2015.