OUT-OF-BAND RADIATION IN INFORMATION PROCESSING EQUIPMENT MEASUREMENT USING SOFTWARE TOOLS

Kadatskaja O., Yerrafiq Muad, Martynchuk A., Saburova S.

V.V. Popovsky Dep.Engineering Infocommunication HNURE,
Ukraine

E-mail: olha.kadatska@nure.ua,
muad.errafik@nure.ua,
oleksandr.martynchuk@nure.ua,
svitlana.saburova@nure.ua

Abstract

The purpose of work is which includes addressing the concern of OBR as a potential cyber-attack vector, exploring the potential of software-defined radio (SDR) receivers, evaluating the effectiveness of SDR-based solutions, identifying vulnerabilities in information processing equipment, and contributing to the existing knowledge on OBR and its impact on cybersecurity. The suggested approach revolves around leveraging SDR receivers to detect and analyze OBR signals, developing new security mechanisms, conducting experiments and simulations to evaluate effectiveness, identifying vulnerabilities, and proposing robust security measures.

In the wireless communication systems, OOB-EME can interfere with the intended sig-nal, leading to reduced signal quality and decreased range. The extent of OOB-EME interference depends on the frequency range of the OOB signal, the strength of the signal, and the susceptibility of the affected electronic device or system. OOB-EME can also be used as a vector for cyber-attacks, making it a potential cybersecurity threat. The interference caused by OOB-EME can be conducted or radiated. Conducted interference is caused by OOB-EME signals that are coupled onto power or signal lines, while radiated interference is caused by OOB-EME signals that propagate through space and couple onto other electronic devices or systems.

Importance of measuring OOB-EMR levels. The measurement of OOB-EMR levels can help to identify sources of interference and to evaluate the effectiveness of mitigation strategies. In the con-text of electronic devices and systems, OOB-EMR can cause significant interference and can lead to operational errors or even complete system failure, this can be particularly problematic in critical infrastructure sectors, where system failures can have significant consequences [1].

This can be particularly important in situations where OOB-EMR interference is suspected, but the source of the interference is not immediately apparent. By measuring OOB-EMR levels, it is possible to determine whether the interference is within acceptable levels and to identify potential solutions to reduce the interference. The measurement bandwidth required for measuring OOB levels de-pends on the frequency range of the OOB signal and the specific application of the electronic device or system. In the case of wireless communication systems, the OOB signal is typically in the range of a few MHz to several GHz, requiring a measurement bandwidth of at least a few GHz.

SDR receiver (fig.1) offer a wider measurement bandwidth, typically ranging from a few MHz to several GHz, making them suitable for measuring OOB levels in high-frequency applications. The measurement bandwidth of SDR receivers can be easily adjusted through software, allowing for more flexible and precise measurements. By exploring the potential of SDR receivers to detect and prevent OBR-based cyber-attacks on information processing equipment, this research aims to contribute to the development of effective and practical solutions that can be implemented by the electronics industry to protect against the risks associated with OBR in information processing equipment [2]. Thus, there arose a need for a more effective and flexible solution. This comprehensive approach addresses both technical and cybersecurity aspects, ensuring a holistic solution.

Is proposed solution, emphasizing the usage of SDR receivers for signal detection and analysis with the integration of machine learning algorithms within a centralized control system to identify potential OBR-based cyber-attacks and trigger alerts or countermeasures as necessary.

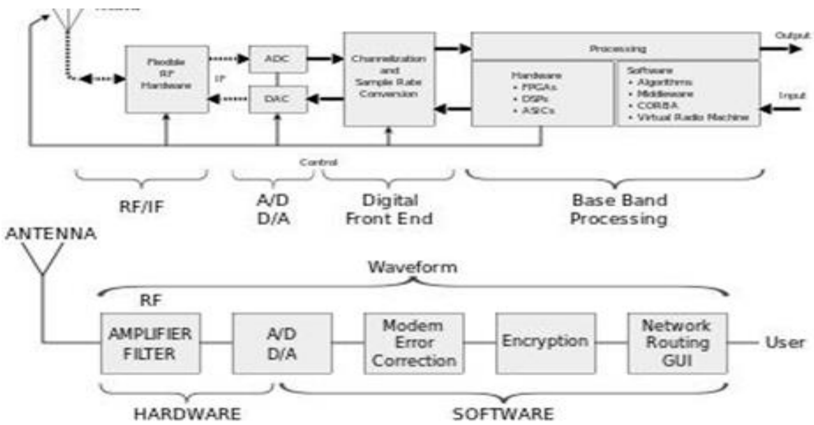

Fig. 1- Software-defined radio structure

This integrated approach holds tremendous potential in fortifying information processing equipment against OBR-based threats.

Tools and software for signal analysis and processing using SDR technology.

● SDRSharp: User-friendly interface for signal analysis and processing. It can be used to visualize and analyze RF signals in real-time, and also supports recording and playback of signals.

● MultiPSK: Digital modes decoding and allows for decoding a wide range of protocols, such as PSK31, RTTY, and CW. It can also decode ACARS, AERO, and many other modes used in aviation and maritime communications. MultiPSK for screening purposes, requiring software installation, configuration, mode selection, and input/output settings. Connecting the SDR receiver allowed for screening and analysis of detected signals displayed in the PSK format.

● VAC Driver, a virtual audio device software, to transfer audio signals between applications, then facilitated the connection between the SDR receiver and signal decoding software, enhancing the ac-curacy and speed of the analysis. It ensured a seamless transfer of audio data from the SDR receiver software to the digital signal decoder software for precise analysis of OBR in information processing equipment.

● Sorcerer: Signal identification and classification software that can recognize over 600 signal types, including both analog and digital signals. It supports automatic signal detection and classification, as well as manual analysis of signals.

● RTL433: Command-line based tool that decodes signals from various devices and sensors using an RTL-SDR dongle It supports decoding of over 300 protocols used in home automation, weather. stations, and other devices.

With its ability to analyze digital signals received by the SDR receiver, Sorcerer played a role in decoding various modulation schemes, visualizing signals, and identifying potential issues such as noise, interference, or distortion, all vital in analyzing OBR. As a command-line tool, RTL433 collected data from sensors operating at the 433 MHz frequency range, enabling analysis and identification of potential sources of OBR when used with the SDR receiver. The detailed analysis of OOB-EMR emissions from information processing equipment using SDR receivers yielded valuable insights into the frequency spectrum, amplitude and phase values, and waveform patterns of these emissions. OOB-EMR levels remained within FCC limits, with sporadic spikes in the 500 MHz to 1 GHz range.

Was a detailed analysis of OBR prevention in information processing equipment using SDR technology and software programs, existing solutions, highlighting the limitations of the latter. Exist the limitations of study, such as the small sample size and limited scope of frequencies tested and suggested expanding the study area and exploring temporal variations in OOB-EMR levels.

Research has practical implications, offering tangible steps to improve the security and reliability of information processing equipment. Overall, the study's results have practical implications for preventing out-of-band radiation in in-formation processing equipment, which can contribute to improving the overall security and reliability of these systems. There were some limitations that need to be considered. Firstly, the study was conducted in a specific study area, and the results may not be generalizable to other areas with different electronic devices and electromagnetic environments. Secondly, the study only measured OOB-EMR levels at a particular point in time and did not account for temporal variations in these levels. Finally, the study did not assess the potential impact of OOB-EMR on specific information processing equipment, such as computers or servers, which would require further investigation.

Table.1. -SDR software result

Software	Frequency range	Bandwidth	Step size	Center frequency	Sampling rate	Decoding parameters
Frequency scanner	120MHz 225MHz	75KHz	30000	-	-	-
MultiPSK	88MHz	2 KHz	-	-	48 Hz	PSK mode
Sorcerer	-	-	-	614.0 Hz	-	CISMSK-16, 31.0sym/s
RTL433	433MHz	45 KHz	-	105.5 MHz	2.4 MHz	-

Results measurement - capturing and analyzing OOB-EMR signals using virtual cables and software tools is as follows.

● Virtual cables and software tools effective for capturing and analyzing OOB-EMR signals
● Detailed analysis of OOB-EMR emissions from information processing equipment using an SDR receiver.
● Identification of frequency spectrum, amplitude, and phase values, and waveform patterns of emissions
● OOB-EMR levels within FCC limits, with some spikes observed in the 500 MHz to 1 GHz range
● Improved equipment reliability and stability
● Enhanced data security and integrity

Future research could investigate temporal variations in OOB-EMR levels to provide a more comprehensive understanding of the potential threat posed by this radiation to data security and privacy. Future studies could assess the impact of OOB-EMR on specific information processing equipment, such as computers o servers, to provide more detailed insights into the mechanisms by which OOB-EMR can affect data security and privacy.

Conclusion

The research focused on investigating the possibility of preventing the use of out-of-band radiation in information processing equipment using software-defined radio (SDR) receivers. The study utilized several software tools, including MultiPSK, Sorcerer, VAC Driver, VBCABLE Driver, and RTL433, to detect and measure the radiation field at different frequencies and distances. The findings of the research revealed that MultiPSK was effective in screening out-of-band radiation, while Sorcerer and RTL433 were useful in identifying digital signals from sensors.

Future research could investigate temporal variations in OOB-EMR levels to provide a more comprehensive understanding of the potential threat posed by this radiation to data security and privacy.

References

1. Grout, V., & Clayton, R. (2016). *A survey of out-of-band channels in mobile devices.* IEEE Communications Surveys & Tutorials, 18(1), 764-790.
2. Kang, Y., & Kim, H. (2016). Detection of wireless out-of-band emissions using software-defined radio. IEEE Transactions on Electromagnetic Compatibility, 58(3), 702-711.