# Evaluation of Electromagnetic Information Leakage Incorporating Channel Characteristics

Name: Taiki Kitazawa
Laboratory's name: Information Security Engineering
Supervisor's name: Yuichi Hayashi

Abstract

Electromagnetic (EM) information leakage can occur without causing interference, making it difficult to apply traditional electromagnetic compatibility (EMC) evaluation frameworks directly. Consequently, a new evaluation framework is needed to clarify, from an offensive security perspective, the vulnerabilities that allow information to be reconstructed from EM emissions. In this thesis, the basic decomposition of EMC is adopted as a framework, and EM information leakage is decomposed into three components: *Leakage Source*, *Leakage Channel*, and *Receptor*. Reinterpreting prior studies through this framework reveals that evaluations have predominantly focused on modeling the *Leakage Source*, while the *Leakage Channel* has been treated merely as a signal propagation path.

Against this background, this thesis proposes an information reconstruction approach that incorporates the influence of temporal, frequency, and spatial parameters determining the characteristics of the *Leakage Channel*, in addition to the *Leakage Source*. (1) Chapter 2 systematically evaluates how the characteristics of the *Leakage Channel* affect information reconstruction performance. (2) Chapter 3 addresses cases where a *Leakage Source* couples into multiple channels. By exploiting channel characteristics, algorithmic noise can be separated, revealing vulnerabilities in devices previously regarded as outside the attack surface. (3) Chapter 4 examines situations where information from the *Leakage Source* is intermittently lost or fluctuates during propagation through the channel. By applying probabilistic modeling to such cases, the study demonstrates that information reconstruction beyond conventional measurement limits is achievable. (4) Chapter 5 investigates scenarios involving secondary *Leakage Sources* induced by a primary *Leakage Source*. By actively controlling the *Leakage Channel* and observing emissions from the secondary *Leakage Source*, the study shows that information can be reconstructed from outside conventional security boundaries.

In summary, this thesis clarifies the incompleteness of existing security evaluation frameworks and reveals previously unrecognized threat landscapes that emerge when channel characteristics are taken into account.