



# Institute for Development and Research in Banking Technology

(Established by Reserve Bank of India)

Castle Hills, Road No. 1, Masab Tank, Hyderabad-57, India.

---

e-Programme on

## INTRODUCTION TO HARDWARE SECURITY FOR BANKS

December 07 – 10, 2021

---

### Introduction

Computer security vulnerabilities involving hardware are under-represented within the security industry. With a growing number of attackers, malware, and researchers moving beyond pure software attack scenarios and into scenarios incorporating a hardware element, it is important to start laying a foundation on how to understand, characterize, and defend against these types of hybrid attacks.

The goal of this e-program is to start seeding hardware security concepts and discussions into the banking security community and to start laying a foundational understanding that can be leveraged if/when hardware security topics start coming to the forefront of their security concerns. Many of these concepts are already established and recognized in hardware-centric private forums (within hardware, BIOS, and OS vendors, etc.), so it is a matter of expanding the audience of these concepts. It is high time to start including hardware-specific elements and accommodations into the established security understanding and practices. This will, in turn, naturally lead to a unified view & management of security risk found within a platform without distinction for software elements vs. hardware elements.

### Objective

The objective of this e-Programme is to introduce and describe a starting taxonomy of security attacks called hardware-involved software attacks in an effort to further security community awareness of hardware security and its role in upholding the security of the PC platform.

### Contents

- Hardware Trojan
- Hardware involved software attacks
- Hardware and Firmware vulnerabilities
- Critical vulnerabilities in modern processors (Meltdown and Spectre)
- ATM Logic Attacks (<https://www.ptsecurity.com/ww-en/analytics/atm-vulnerabilities-2018/>)
- HSM, Key logger

### Mode of Teaching

Online teaching plus learning inputs through reading material, videos, webinars, assignments, quizzes, online interactions and clarifications. Each e-Programme will have four live webinars and course material will be made available in advance for study.

## Who Can Participate?

Bank officials working in IT Department, cyber Security Operations Centre, Network Operations Centre and related activities.

## End Use:

This e-Programme will help the participant strengthen their knowledge and awareness of hardware security, ATM attacks, and different vulnerable hardware components and help the banks improve their security provisions.

## Programme Coordinator:

**Dr. Dipanjan Roy**, Assistant Professor, IDRBT; e-mail: [droy@idrbt.ac.in](mailto:droy@idrbt.ac.in)

## Fees:

### **For Indian Participants**

- RRBs & Coop Banks: Rs. 8,850/-(Rs. 7,500/- + 18% GST)
- All Other Banks & FI's: Rs. 11,800/-(Rs. 10,000/- + 18% GST)

### **For International participants**

- US \$ 175 (per participant, All inclusive)

## Bank Account Details for Remittance of Fees

The fees for this e-programme can be remitted to the following accounts:

### **For Indian Participants**

Account Name : IDRBT  
Bank & Branch : Axis Bank Limited, Humayun Nagar, Mehdiapatnam, Hyderabad  
Account No. : 426010100018823  
MICR Code : 500211012  
IFSC Code : UTIB0000426

### **For International participants**

Receiver's Correspondent Bank : JP Morgan Chase, New York, USA  
Swift Code : CHASUS33XXX  
Fed Wire Routing Number : ABA 021000021  
Beneficiary Bank & Branch : Axis Bank Ltd., Mumbai, India  
Account Number : 0011407376  
Beneficiary Bank Swift Code : AXISINBB

### **Ultimate Beneficiary**

Account Name : IDRBT  
Customer ID : 030021632  
Account No. : 426010100018823  
Bank & Branch : Axis Bank Ltd., Jubilee Hills, Hyderabad, India. (AXISINBB030)

## Nominations

Banks may nominate any number of participants to these e-Programmes, which may be accepted on a first-cum-first-served basis. While nominating, please provide the details of the participants (Name, Designation, Bank, Mobile No/Phone No, email address, fees billing address, GST No. of the Bank).

Apart from nominations by banks, staff members of banks can self-nominate themselves for these e-Programmes by providing their employee credentials and paying the programme fee latest by **December 06, 2021**.

### How to Register

The nominations for these e-Programmes, and queries if any, may please be sent to [eprogram@idrbt.ac.in](mailto:eprogram@idrbt.ac.in). Please visit <https://www.idrbt.ac.in/eprogrammes> for more details about these programmes.

\*\*\*\*\*

### e-Programmes in December 2021

S. No.	Name of the e-Programme	Date	e-Programme Coordinator	Last Date for Nomination
1	Re-imagining Customer Engagement with Conversational Chatbots	06 – 09	Dr. Mridula Verma	<b>Dec 03, 2021</b>
2	Awareness on Payment Systems Vision 2021	06 – 09	Dr. N.V.Narendra Kumar	<b>Dec 03, 2021</b>
3	Explainable AI/ML for Banking	06 – 09	Dr. V. Ravi	<b>Dec 03, 2021</b>
4	Introduction to Hardware Security for Banks	07 – 10	Dr. Dipanjan Roy	<b>Dec 06, 2021</b>
5	Technologies for Financial Inclusion	14 – 17	Dr. M. V. N. K. Prasad	<b>Dec 13, 2021</b>
6	Security in Cloud Computing	14 – 17	Dr. P. Syam Kumar	<b>Dec 13, 2021</b>
7	Workshop on Registration Authority Operations	20 – 23	Dr. N. P. Dhavale	<b>Dec 17, 2021</b>
8	Privacy and Security Risks in Machine Learning	21 – 24	Dr. Rajarshi Pal	<b>Dec 20, 2021</b>
9	Targeted Attacks - Detecting in early stages	21 – 24	Dr. B. M. Mehtre	<b>Dec 20, 2021</b>
10	API Development	27 – 30	Dr. V. Radha	<b>Dec 24, 2021</b>
11	Basics of IT Vendor Management	28 – 31	Dr. Abhishek Thakur	<b>Dec 27, 2021</b>

\*\*\*\*\*