# Attacking Instant Messaging Applications (4 days)

Training description

Vectorize (Iddo ELDOR & Jacob BECH)

**Title**

Attacking Instant Messaging Applications

**Overview**

Few publicly-known hacks have inspired the imagination of security researchers as much as exploits against IM (instant messaging) applications. 0-click attacks aimed against applications such as WhatsApp, iMessage, and Telegram have raised unprecedented interest and have often caused political turmoil.Yet, in sharp contrast with the curiosity that IM exploitation generates, public information about this surface remains scant. This training is our bid to bridge the gap.This course will provide students with the knowledge and hands-on experience in reverse engineering, vulnerability research, and exploitation of real-world IM applications. The target audience is advanced security professionals.

**Course agenda**

### Day 1: Introduction, planning and preparation

- Instant Messaging Overview
- Attack Flow: from Recon Stage to Attack Primitives
- Initial Static & Dynamic Analysis on a Real World IM Application
- Building Attack Blocks
- Advanced Frida Scripting

### Day 2: Discovery

- Protocol(s) Deep Dive
- Understanding and Dissecting Packets
- Re-Inserting Compiled-Out Functions
- Automating Sensitive Information Extraction
- Parameter Tampering
- Userland ftrace

### Day 3: Verification

- Advanced Static & Dynamic Analysis
- Common Classes of Java Vulnerabilities
- In-Memory Fuzzing
- (Applied Symbolic Execution)

- Operational Security

### Day 4: Exploitation

- Common Classes of Native Vulnerabilities
- Exploit Mitigations
- Vulnerability Hunting
- Crashing the Target
- Building Attack Primitives