Training Course on Over-the-Air (OTA) Update Forensics

Professional Development Training Course Outline

Category	Digital Forensics	**Duration**	5 Days
Base Fee	$1,500 USD	**Delivery Mode**	Online / On-site Hybrid

Course Introduction

Introduction

This specialized training course is designed to equip digital forensic investigators, cybersecurity analysts, and incident response professionals with the crucial skills to conduct Over-the-Air (OTA) update forensics. In today's interconnected world, nearly every mobile device, IoT gadget, and even vehicles receive firmware and software updates wirelessly. These OTA updates, while convenient, represent a significant and often overlooked attack vector, capable of delivering malware, backdoors, or malicious firmware that can compromise devices and exfiltrate sensitive data. Training Course on Over-the-Air (OTA) Update Forensics delves into the intricate mechanisms of OTA update processes across diverse platforms, enabling participants to intercept, analyze, and forensically examine update packages for signs of tampering or malicious intent.

The curriculum provides a deep dive into the technical intricacies of OTA update protocols, cryptographic signing mechanisms, file system patching, and rollback procedures. Through intensive hands-on labs and real-world case studies, participants will learn to identify compromised update servers, analyze firmware differences, detect supply chain attacks, and extract crucial digital evidence related to malicious updates. The course emphasizes both proactive threat intelligence gathering and reactive incident response, ensuring graduates are proficient in protecting systems from OTA-borne threats and meticulously investigating incidents where OTA updates have been weaponized, contributing vital expertise to the evolving landscape of supply chain security and advanced persistent threat (APT) analysis.

Programme Curriculum

Training Course on Over-the-Air (OTA) Update Forensics

Introduction

This specialized training course is designed to equip digital forensic investigators, cybersecurity analysts, and incident response professionals with the crucial skills to conduct Over-the-Air (OTA) update forensics. In today's interconnected world, nearly every mobile device, IoT gadget, and even vehicles receive firmware and software updates wirelessly. These OTA updates, while convenient, represent a significant and often overlooked attack vector, capable of delivering malware, backdoors, or malicious firmware that can compromise devices and exfiltrate sensitive data. Training Course on Over-the-Air (OTA) Update Forensics delves into the intricate mechanisms of OTA update processes across diverse platforms, enabling participants to intercept, analyze, and forensically examine update packages for signs of tampering or malicious intent.

The curriculum provides a deep dive into the technical intricacies of OTA update protocols, cryptographic signing mechanisms, file system patching, and rollback procedures. Through intensive hands-on labs and real-world case studies, participants will learn to identify compromised update servers, analyze firmware differences, detect supply chain attacks, and extract crucial digital evidence related to malicious updates. The course emphasizes both proactive threat intelligence gathering and reactive incident response, ensuring graduates are proficient in protecting systems from OTA-borne threats and meticulously investigating incidents where OTA updates have been weaponized, contributing vital expertise to the evolving landscape of supply chain security and advanced persistent threat (APT) analysis.

Course Duration

5 Days

Course Objectives

1. Understand the architecture and security models of Over-the-Air (OTA) update mechanisms across various device types (mobile, IoT, automotive).
2. Identify common OTA update protocols and their communication flows (e.g., HTTP/S, proprietary protocols).
3. Perform network traffic interception and analysis to capture OTA update packages in transit.
4. Decipher cryptographic signing and verification processes used in OTA updates to detect tampering.
5. Conduct firmware analysis and reverse engineering of OTA update packages for malicious code or unauthorized modifications.
6. Analyze file system patching techniques employed by OTA updates and their forensic implications.

7. Identify indicators of compromise (IOCs) related to malicious OTA updates, including altered update servers or corrupted packages.
8. Investigate supply chain attacks leveraging compromised OTA update infrastructure.
9. Reconstruct update timelines and identify specific versions of firmware installed on devices.
10. Develop custom tools and scripts (Python) for automated parsing and analysis of OTA update artifacts.
11. Understand rollback mechanisms and their forensic value in analyzing prior device states.
12. Generate comprehensive forensic reports detailing findings from OTA update investigations for legal admissibility.
13. Formulate proactive defense strategies against malicious OTA updates and enhance firmware security.

Organizational Benefits

1. Enhanced Supply Chain Security: Proactively identify and mitigate risks associated with compromised software and firmware updates.
2. Improved Incident Response: Quickly detect and analyze malicious OTA updates, minimizing their impact on systems and data.
3. Advanced Threat Detection: Develop internal capabilities to identify sophisticated, stealthy attacks leveraging OTA infrastructure.
4. Protection of Critical Assets: Safeguard devices, data, and intellectual property from compromise via malicious updates.
5. Reduced Financial & Reputational Risk: Prevent costly data breaches, system downtime, and reputational damage from OTA attacks.
6. Proactive Vulnerability Management: Gain insights into OTA update vulnerabilities to strengthen internal security practices.
7. Compliance Adherence: Ensure update mechanisms align with security best practices and regulatory requirements.
8. Actionable Threat Intelligence: Contribute to internal and external threat intelligence on emerging OTA attack methodologies.
9. Optimized Security Operations: Equip security teams with specialized skills to handle a modern attack vector.
10. Increased Investigative Success: Uncover elusive evidence of compromise from devices updated with malicious firmware.

Target Participants

- Digital Forensic Investigators
- Cybersecurity Incident Responders
- Firmware Reverse Engineers
- Application Security Analysts

- Security Architects
- Threat Intelligence Analysts
- Red Team / Penetration Testers
- Product Security Teams (Mobile, IoT, Automotive)
- Supply Chain Security Professionals
- Government Cyber Warfare Units

Course Outline

Module 1: Fundamentals of Over-the-Air (OTA) Updates (OTA Update Basics)

- Overview of OTA Update Ecosystems (Mobile, IoT, Automotive)
- Components of an OTA Update System (Update Server, Client, Package)
- Types of OTA Updates (Full, Differential, Firmware, Software)
- The Role of OTA in Device Lifecycle and Security
- **Case Study**: Tracing the typical OTA update process for a modern smartphone.

Module 2: OTA Update Protocols & Communication Analysis (OTA Protocol Forensics)

- Common Protocols Used for OTA Updates (HTTP/S, Custom Binary Protocols)
- Intercepting OTA Traffic: Proxying, Packet Sniffing, SSL/TLS Decryption
- Identifying OTA Update Requests and Responses in Network Traffic
- Analyzing Network Artifacts related to OTA Servers and Downloads
- **Case Study**: Capturing an OTA update package in transit using a network proxy.

Module 3: OTA Package Analysis & Reverse Engineering (OTA Package Forensics)

- Structure of OTA Update Packages (ZIP, proprietary formats)
- Dissecting Firmware Images and Software Components within the Package
- Analyzing Patch Files and Differential Updates
- Using Tools like Binwalk, Firmware Mod Kit (fmk) for Package Extraction
- **Case Study**: Extracting and examining the contents of an Android OTA update `.zip` file.

Module 4: Cryptography in OTA Updates & Integrity Verification (OTA Crypto Forensics)

- Understanding Digital Signatures and Hashes in OTA Updates
- Verification Processes: How Devices Authenticate Update Packages
- Detecting Tampered or Maliciously Signed OTA Updates
- Extracting Public Keys and Certificates from Firmware
- **Case Study**: Verifying the digital signature of a captured OTA update package.

Module 5: Firmware Forensics & Difference Analysis (Firmware Difference Analysis)

- Techniques for Extracting Firmware from Devices (Physical, Logical)
- Comparing Firmware Versions (Binary Diffing) to Identify Changes
- Analyzing Code Patches and Modified Binaries within Updates
- Detecting Malicious Code Injections or Backdoors in Firmware
- **Case Study**: Performing a binary diff between a legitimate and suspected malicious firmware update.

Module 6: OTA Update Incident Response & Threat Hunting (OTA Incident Response)

- Identifying Indicators of Compromise (IOCs) in OTA Update Attacks
- Investigating Compromised Update Servers and Supply Chain Vectors
- Forensic Triage of Devices Suspected of Receiving Malicious Updates
- Strategies for Containment, Eradication, and Recovery from OTA Attacks
- **Case Study**: Investigating a scenario where a device received a malicious OTA update from a compromised server.

Module 7: Automated Analysis & Proactive Defenses (Automated OTA Forensics)

- Developing Custom Scripts (Python) for Automated OTA Package Analysis
- Building Automated Systems for Monitoring OTA Updates
- Strategies for Proactive Firmware Security and Secure Update Mechanisms
- Implementing Reputation-Based and Behavioral Analysis for OTA Updates
- **Case Study**: Writing a Python script to extract key information from multiple OTA update packages.

Module 8: Legal, Ethical & Emerging Trends (OTA Legal & Trends)

- Legal Implications of Investigating OTA Update Infrastructure
- Ethical Considerations in Simulating or Intercepting OTA Traffic
- Emerging Threats: OTA Updates for IoT Botnets, Connected Cars, Industrial Systems
- Future Challenges: Quantum-Resistant Cryptography, AI in OTA Updates
- **Case Study**: Discussing the legal boundaries of intercepting OTA updates for forensic purposes in Kenya.

Training Methodology

This course employs a participatory and hands-on approach to ensure practical learning, including:

- Interactive lectures and presentations.
- Group discussions and brainstorming sessions.
- Hands-on exercises using real-world datasets.
- Role-playing and scenario-based simulations.
- Analysis of case studies to bridge theory and practice.
- Peer-to-peer learning and networking.
- Expert-led Q&A sessions.
- Continuous feedback and personalized guidance.

Register as a group from 3 participants for a Discount

Send us an email: info@fineskilltrainingcenter.org or call *+254769199797*

Certification

Upon successful completion of this training, participants will be issued with a globally- recognized certificate.

Tailor-Made Course

We also offer tailor-made courses based on your needs.

Key Notes

a. The participant must be conversant with English.

b. Upon completion of training the participant will be issued with an Authorized Training Certificate

c. Course duration is flexible and the contents can be modified to fit any number of days.

d. The course fee includes facilitation training materials, 2 coffee breaks, buffet lunch and A Certificate upon successful completion of Training.

e. One-year post-training support Consultation and Coaching provided after the course.

f. Payment should be done at least a week before commence of the training, to Fineskill Training Center account, as indicated in the invoice so as to enable us prepare better for you.

Upcoming Scheduled Sessions

Start Date	End Date	Location	Price
21 Sep 2026	25 Sep 2026	Online	$1,000
21 Sep 2026	25 Sep 2026	Physical	$1,500
21 Sep 2026	25 Sep 2026	Physical	$0
21 Sep 2026	25 Sep 2026	Physical	$0
21 Sep 2026	25 Sep 2026	Physical	$0
21 Sep 2026	25 Sep 2026	Physical	$0
21 Sep 2026	25 Sep 2026	Physical	$0
21 Sep 2026	25 Sep 2026	Physical	$0

Ready to enroll or request a customized program? Book online or contact us:

Register Online Now

Email: info@fineskilltrainingcenter.com | Website: www.fineskilltrainingcenter.com