MERIMETSO

IoT Penetration Testing

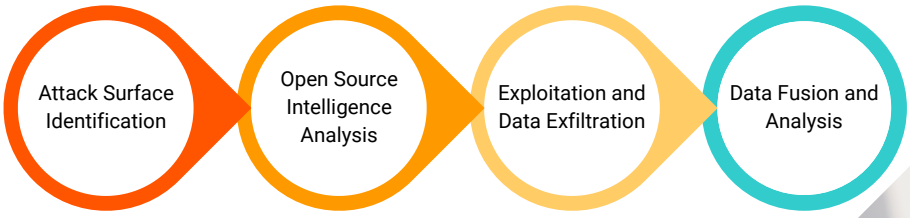
Service Description Introduction

IoT systems are used in a wide variety of environments to provide a board set of services. These can range from Medical, Transport, Manufacturing and Infrastructure Management to name just a few. During an IoT penetration test, the consultant will perform a series of structured activities the goal of which is to identify and validate the security vulnerabilities contained within the IoT device or system. IoT penetration test can be used to demonstrate regulator compliance.

Purposes for an IoT penetration test can include

1. Validation that regulatory requirements have been adhered.
2. Verification that intellectual property is being protected.
3. Validate that the system can bot be accessed/modified in an unauthorised manner.

Our Approach



@merimetsocyber
@merimetso
contact@merimetso.net www.merimetso.net

Engagement Structure

An IoT penetration test, examines all routes through which a device can be accessed and data modified or extracted. This involves the construction of a detailed attack surface and the execution of a set of attack principles that cover all access points to the system. To ensure complete coverage of the attack surface, closed and open-source intelligence analysis is performed. This is fused with the attack surface to provide a detailed set of attack scenarios through which data can be extracted and analysed.

Methodology

Attack Surface Identification

A holistic analysis of the IoT device, covering everything from the device's human machine interface to the printed circuit boards (PCB). This element focuses upon component identification.
Key access points focused upon include:

- USB, UART, I2C, SPI and JTAG
- WIFI, Bluetooth, Zigbee, RFID and CAT5/CAT6
- Controller Area Network Bus and MODBUS
- PCB Test Point identification and PCB X-Ray

Open Source Intelligence Analysis

Open source intelligence analysis makes use of a variety of data sources to validate the findings of the Attack Surface Identification phase and augment it. This augmentation will take the form of:

- Identification of Flash and CPU components that can contain data/firmware and may have hidden access points.
- Validation of identified access points and protocols used for data sharing.
- Identification of the host operating system and/or firmware being executed by the device

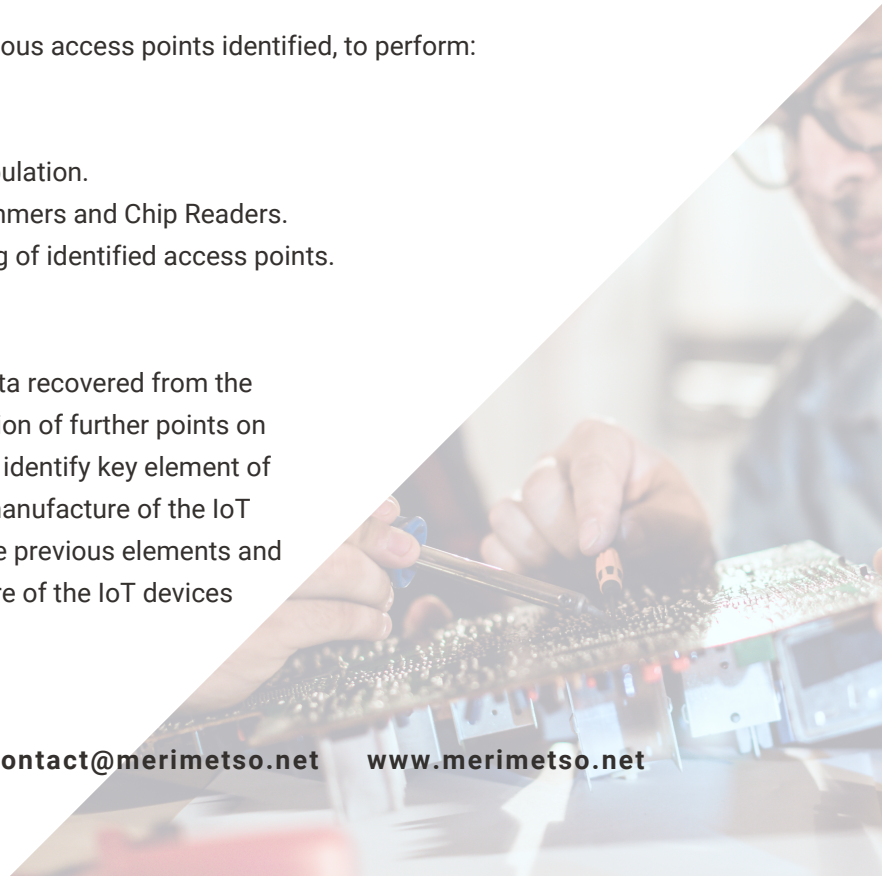
Exploitation and Data Exfiltration

This element will include:

- Execution of the attack surface via the various access points identified, to perform:
  - data extraction and data recovery, and
  - data modification of data fabrication.
- Direct hardware access for memory manipulation.
- Chip-off and direct attack via Chip programmers and Chip Readers.
- Protocol/network attacks and brute forcing of identified access points.

Data Fusion and Analysis

This involves the analysis and fusion of the data recovered from the device with a view to identification and validation of further points on the attack surface. This element also seeks to identify key element of intellectual property that are propriety of the manufacture of the IoT device. This element also draws upon all of the previous elements and fuses the data together to give a holistic picture of the IoT devices security vulnerabilities.



Deliverables

In-depth report, broken down into 3 main parts:

1. Management Summary
2. Technical Overview
3. Detailed Technical Findings

Highlighting the vulnerabilities:

1. Type of RISK
2. The EFFECT of that RISK
3. Recommendations on how to address and mitigate vulnerabilities
4. Estimate of effort required to remediate any vulnerabilities identified

Project Management

Project Management resource will be assigned throughout the engagement but will not be allocated full time.
Key roles and responsibilities:

- Run engagement kick off workshop.
- Run engagement closure.
- Maintain and communicate engagement risks and issues log.
- Weekly status meetings and engagement tracker.

Prerequisites

The following pre-requisites are required from the client:

- Physical access to the device or exported configuration files
- Make and Model of the Firewalls
- Written permission from the client to test
- Login credentials and digital certificates (if applicable)
- Point of Contact details

Deliverable Acceptance Criteria

Merimetso may present interim deliverables to the customer for review throughout the engagement. Should Merimetso present an interim deliverable, the customer will review, and either accept, or document specific corrective items in writing within three (3) business days. In the absence of any comments, deliverables produced by Merimetso will be deemed accepted after three (3) business days.

Limitations & Exclusions

- This engagement covers only the activities detailed in this document. Additional Merimetso offerings may be purchased as add-ons, otherwise additional consulting work not contained in this engagement is deemed out of scope.
- Working time is defined as Monday to Friday (excluding local bank/statutory holidays), 9am-5pm, with a 60-minute break for lunch.
- Merimetso is not responsible for the installation, configuration, or validation of any third-party software, tools, or utilities.
- Only third-party software and infrastructure identified during the pre-sales phase will be in scope for the engagement. There will be no change of scope where third-party software or infrastructure has been changed by the customer during the course of the engagement, or this will incur additional cost.

Customer Responsibilities

1. The customer must provide appropriate resources during the engagement from commencement date.
2. The customer must provide Merimetso representatives with information and resources to ensure Merimetso is able to successfully execute the engagement. This can include, without limitation, providing access and credentials to systems, completing installation prerequisites, providing resources, and attendance in planning, execution, or training meetings.
3. Customer will ensure resources are available in a timely manner to undertake tasks such as change control and documentation review.
4. Customer must ensure it has the necessary escalation and communication channels to resolve any blockers in a timely manner, including dependencies on third parties customer vendors, suppliers, and consultants.
5. If the consultant should travel to a customer location for the delivery of this engagement, there will be additional travel and expense costs. These travel and expense costs can be paid for prior to the engagement, or at actuals, at engagement completion.
6. The customer shall provide at least seventy-two (72) hours' notice for the cancellation or postponement of any work already scheduled as part of the engagement. In such scenario of a cancellation or postponement Merimetso reserves the right at its sole discretion to charge the customer for additional resources at Merimetso's then current daily rate for the delay period.
7. Customer must have a right to use the software and licenses. This requires that the customer must have purchased, or have converted, the appropriate license rights to the target environment.
8. Hardware requirements are the responsibility of the customer, and it is the customer's responsibility to ensure the hardware requirements are met prior to the engagement.

Merimetso may subcontract all or a portion of the services and/or have the services performed by one of its affiliates.
Note: The services described in this Service Description are subject to the terms and conditions by Merimetso Terms

Our Senior Testing Team

Dr Andrew Blyth - Founder and Director of R&D

Dr Blyth received his PhD in Computer Science in 1995 from Newcastle University, UK. Dr Blyth held the position of Professor of Computer Forensics at the University of South Wales, UK, throughout his illustrious career. Co-authored a textbook on Information Assurance, supervised 15 successful PhD candidates, created several BSc and MSc Computer Forensics and Cybersecurity Programmes. He was instrumental in the University of South Wales being the first University in the UK to behave an MSc in Computer Forensics accredited by the UK Government's National Technical Authority (GCHQ/NCSC).

He was the Cybersecurity Technical Lead at the UK Ministry of Defence's (MOD), Defence Science and Technology Laboratory (DSTL). During that time, he created and ran the Computer Network Defence Technical Demonstrator programme and defined various other research programmes within DSTL. He has over 50 peer-review publications and managed millions of dollars of research funding.

Campbell Murray - Founder and COO

Campbell is an established global leader in the field of information security. With over 25 years of experience ranging from offensive security assessments and security engineering in a vast range of environments providing Campbell with rare detail and insight into the field of cybersecurity. Campbell established himself as a penetration testing consultant in 2000. A firm believer in knowledge transfer, Campbell was a founding director of the TigerScheme in 2007 and the Cyber Scheme in 2013.

The Cyber Scheme is the recognised course used by NCSC to affirm CHECK status on any penetration tester who wishes to work on Government infrastructure in the UK. Campbell is now the chair of the technical panel for the Cyber Scheme and is one of only a handful of GCHQ appointed CHECK Team Leader assessors.

David Mound - Founder and CTO

David is a highly experienced Cyber Security Researcher with a demonstrated history of working in the Computer & Network Security industry and threat intelligence. Skilled in Penetration Testing, Reverse Engineering, Computer Forensics, Red Teaming and Threat Intelligence, he has worked with numerous global agencies within the 5 Eyes community, including GCHQ and the NSA delivering, advising on Red Team methods and engagements to assess Blue Team capabilities.

David's current speciality and focus are cloud-based technologies, and he holds multiple cloud certifications such as AWS Certified Security Specialist. David is an ex-Naval officer and is currently a member of the Army Reserves, where he coordinates threat hunting and assists network defence within the UK MOD and Gov estates. David brings his extensive technical capability to design the innovation to the Merimetso Cyber Technical Training platform.