IoT Security

Made by: Sri Chakradhar

CEO, Entersoft Security

Penetration Testing & Ethical Hacking

Corporates traditionally have depended on scanners to test product security

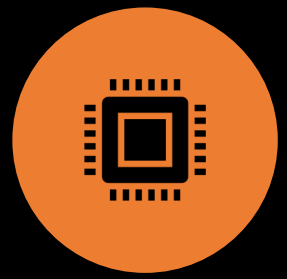
Scanners check for behavior and signature of code ignoring business use cases resulting in False Positives and False Negatives

Entersoft relies on a mixture of scanning tools and experienced white hat hackers.

White Hats understand business use cases and use their experience & tools to give you complete all round security

- The next couple of slides detail possible security compromise scenarios in IoT systems

Use Case 1 (Between App & Cloud)



DATA FROM SENSORS IS RELAYED THROUGH TO THE MASTER

MASTER CRUNCHES THE DATA AND SENDS IT TO CLOUD

DATA IS CRUNCHED ON CLOUD AND SENT TO MOBILE APP TO GIVE RECOMMENDATIONS TO CUSTOMER

IMPROPER SECURITY WHILE APP COMMUNICATES WITH THE CLOUD MAY PUT ALL USER DATA INCLUDING LOCATION HISTORY AND DRIVING PATTERNS IN HANDS OF MALICIOUS ENTITIES

Use Case 2 (Between sensors and Master)

The communication between Master and sensors plays key roles in many functionalities.

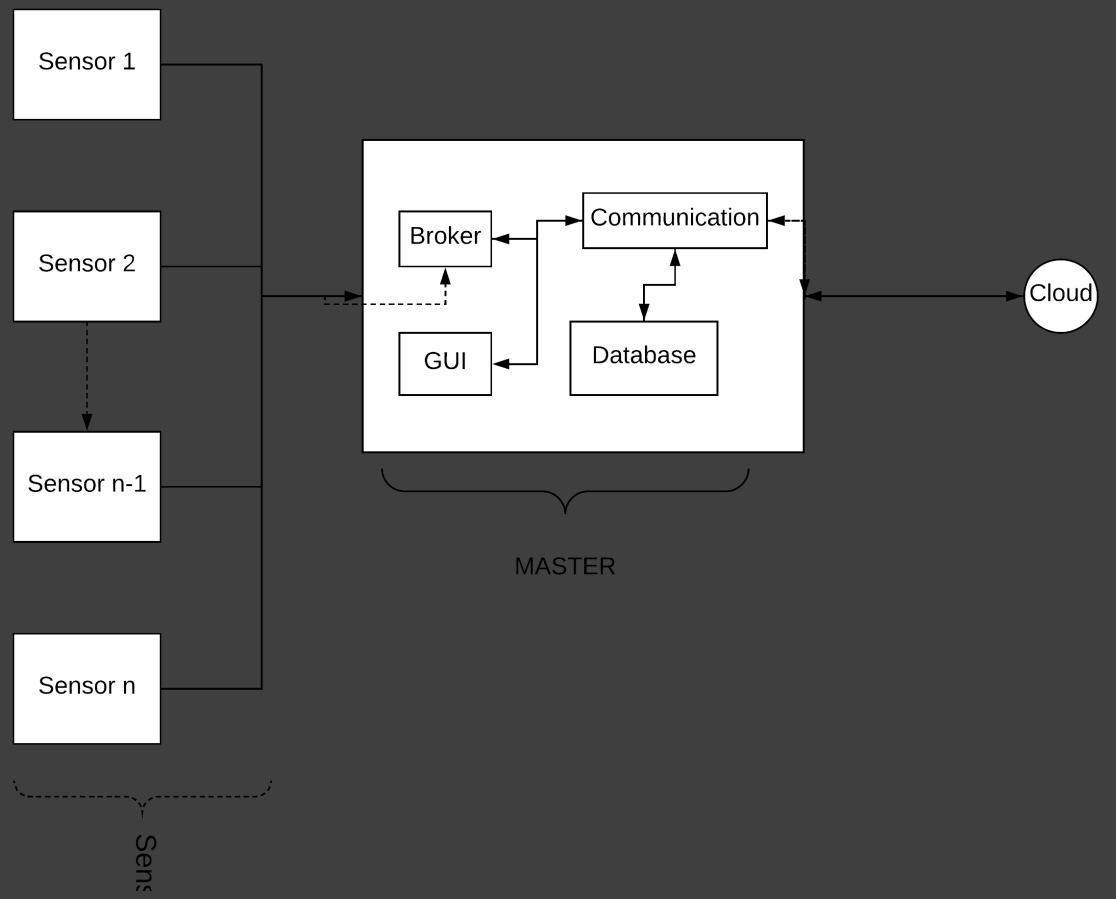
Improper authentication on the Master from sensors may result in third parties getting access to the Master

A keyless entry is possible if sensor tampering is not properly handled on the master

Third party hardware installed on the system might be the weak link allowing hackers to enter into your system. (e.g. OBD Dongles)

Basic IoT System

- The simplest of diagrams depicting IoT systems can be quite complex.
- Multiple components in the eco system like sensors, master, gateway, cloud and User Apps have further subsystems if delved into.
- The following 2 slides will illustrate two security risks possible at a high level
- The remaining slides shall focus on comprehensively covering the IoT ecosystem



Device related testing

Device Memory	Cleartext usernames
	Cleartext passwords
	Third-party credentials
	Encryption keys
Device Physical Interfaces	Firmware extraction
	User CLI
	Admin CLI
	Privilege escalation
	Reset to insecure state
	Removal of storage media
Device Web Interface	SQL injection
	Cross-site scripting
	Cross-site Request Forgery
	Username enumeration
	Weak passwords
	Account lockout
	Known default credentials

Device related testing (cont.)

Device Firmware	Hardcoded credentials
	Sensitive information disclosure
	Sensitive URL disclosure
	Encryption keys
	Firmware version display and/or last update date
Device Network Services	Information disclosure
	User CLI
	Administrative CLI
	Injection
	Denial of Service
	Unencrypted Services
	Poorly implemented encryption
	Test/Development Services
	Buffer Overflow
	UPnP
	Vulnerable UDP Services

IoT Ecosystem related Testing

Ecosystem Communication	Health checks Heartbeats Ecosystem commands Deprovisioning Pushing updates
Ecosystem Access Control	Implicit trust between components Enrolment security Decommissioning system Lost access procedures

Interface Related Testing

Administrative Interface	SQL injection
	Cross-site scripting
	Cross-site Request Forgery
	Username enumeration
	Weak passwords
	Account lockout
	Known default credentials
	Security/encryption options
	Logging options
	Two-factor authentication
	Inability to wipe device
Cloud Web Interface	SQL injection
	Cross-site scripting
	Cross-site Request Forgery
	Username enumeration
	Weak passwords
	Account lockout
	Known default credentials
	Transport encryption
	Insecure password recovery mechanism
	Two-factor authentication

API Related Testing

Third-party Back-end APIs	Unencrypted PII(Personally Identifiable Information) sent
	Encrypted PII sent
	Device information leaked
	Location leaked
Vendor Backend APIs	Inherent trust of cloud or mobile application
	Weak authentication
	Weak access controls
	Injection attacks

Communication related testing

Wireless (Bluetooth, Zigbee, Wi-Fi)	De-Authentication
	Sniffing
	Spoofing
	Replay Attacks
	Denial of Service
Network Traffic	LAN
	LAN to Internet
	Short range
	Non-standard

Mobile App related testing

Update Mechanism	Update sent without encryption
	Updates not signed
	Update location writable
	Update verification
	Malicious update
	Missing update mechanism
	No manual update mechanism
Mobile Application	Implicitly trusted by device or cloud
	Username enumeration
	Account lockout
	Known default credentials
	Weak passwords
	Insecure data storage
	Transport encryption
	Insecure password recovery mechanism
	Two-factor authentication

Thank you

Please contact gdp@entersoft.com for any queries.