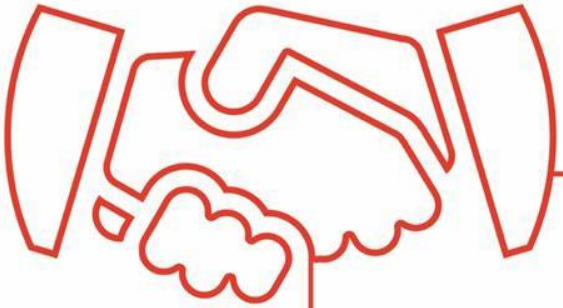
How Secure is Your Border?
An Attack and Penetration Audit



2019 Houston IIA Annual Conference

The Institute of Internal Auditors

Bill Jenkins
Manager, One Cyber

Phone: 720-810-0568
william.jenkins@pwc.com

Specialization
He organizes, leads, and delivers information protection and compliance projects across highly regulated industries addressing security and privacy controls in balance with operational imperatives.

Background

A proven Cyber Security professional providing insights and recommendations at the CISO/CSO level. Bill's skills and experiences make him a frequent selection for the enterprise engagements facing the challenges of establishing, maintaining and maturing a corporate cyber security program. Bill takes an integrated approach to satisfy customer, business, and regulatory concerns in response to evolving risks. He leverages his management, networking, and systems engineering background to be an organizational catalyst – connecting dots, and establishing relationships critical to effective performance.

Education and certifications

MS, The Johns Hopkins University, Computer Science

BS, Rice University Electrical Engineering

Certified Information System Security Professional (CISSP)

Certified Cloud Security Professional (CCSP)

Certified Information Systems Auditor (CISA)

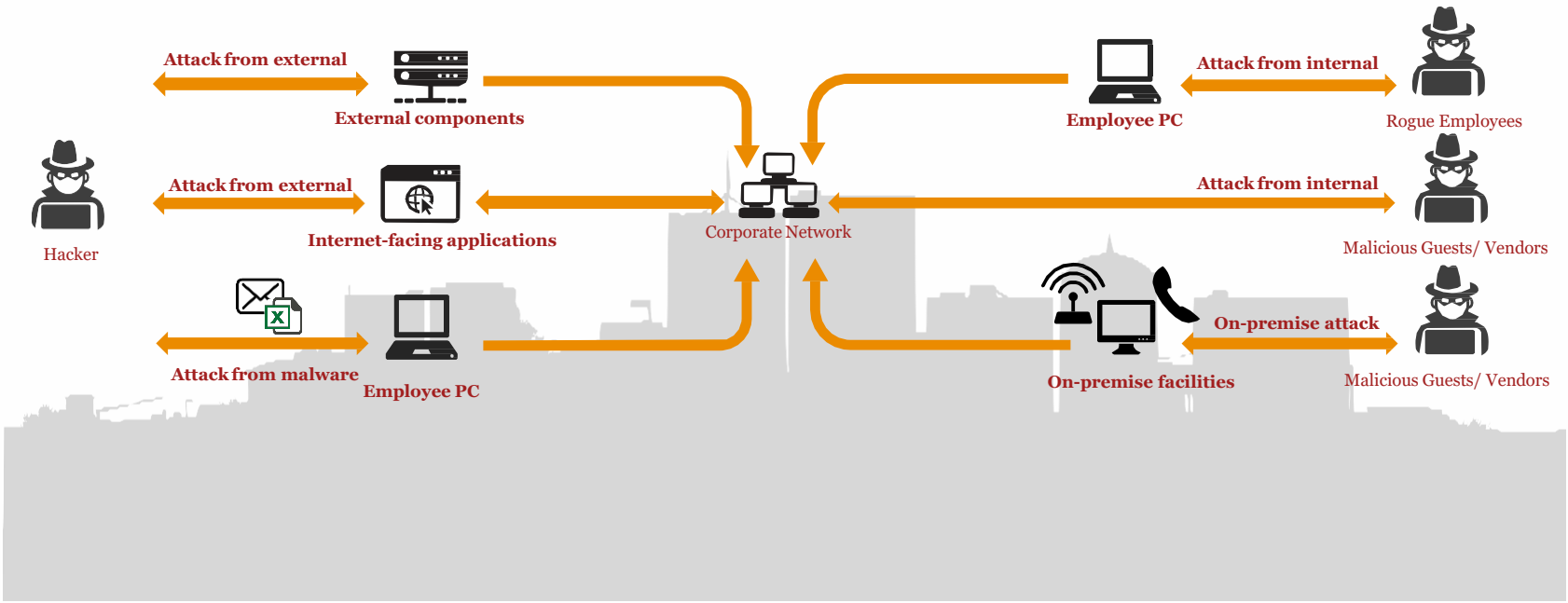
Motivations for a Penetration Test

Timing	Purpose
Pre- Audit	• Verify remediations are working • Discover blind spots
Audit	• Stress test • Operational and response validation
Periodic	• Operational readiness • Threat/Risk validation
Adhoc	• Someone thought of it • Hasn't been done in a while

Mindset

- Testing individual/specific controls?
- Assessing integration of controls and process?
- Validating overall security defense and response capabilities?
- Compliance requirement?
- A Board member asked?

So many threats to consider…



Scoping Checklist

- External Penetration Testing
- Social Engineering Exercise
- Internal Penetration Testing
- Wireless Network Penetration Testing
- Mobile Penetration Testing
- Web Application Security Assessment
- Red Teaming

External Penetration Testing Approach

Simulating a threat actor external to the organization trying to identify and leverage weaknesses in an attempt to gain access to internal systems and data; assess the effectiveness of detection and response capabilities, and highlight relevant risks.

Reconnaissance:

- Identify potentially vulnerable ports and services
- Analyze externally exposed services
- Generate usernames, passwords and password crack lists

Crack the perimeter:

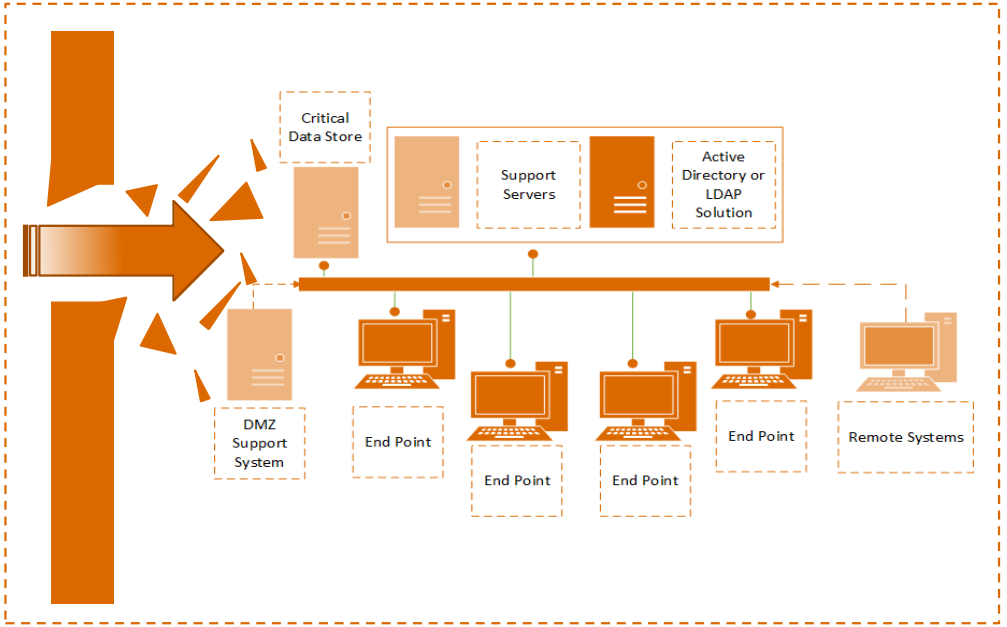
- Password sprays against exposed interfaces
- VPN pre-shared key interrogation
- Default configuration and credential manipulation
- Injection and execution attacks against exposed websites
- Non-standard port attacks
- Service interrogation (SNMP, TFTP, Finger, SMTP etc.)
- Remote Code Execution (RCE) attacks
- Manipulate old, outdated or no longer supported services

Lateral Movement:

- Pass-the-Hash (PtH)
- Native remote access solutions

Gain access to Crown Jewels

- Sensitive data exfiltration
- Establish persistence



Social Engineering

The methodology for engaging in phishing testing can be found broken down in the three steps listed below:

1. The first step in the phishing process involves performing open source intelligence gathering **using publicly available data sources and manual investigation** techniques to gather information on an organization's employees. Following this, a tester provides a list of discovered email addresses for validation. A tester will also propose scenarios that are likely to be successful based on the information discovered and work with any given organization to ensure the proposed campaign aligns with current threats seen in the industry.
2. At an agreed time by the client, a tester will execute a phishing campaign. Possible attack scenarios may include the sending of malicious attachments to employees or enticing users to visit a test website that would collect information which may include employee credentials, system configurations or other data that may allow an attacker to obtain access to sensitive information. This step is designed to **test the effectiveness of both security awareness training and technical security controls**.
3. Finally, the tester will **assess the impact and business risk of the phishing campaign**. The tester will provide detailed information including users who were successfully compromised and the date and time of our assessment activities to be compared to the business' internal system logs and alerts.

Internal Penetration Testing Approach

Simulate the threats faced from connected third parties, employees, or contractors who have direct internal network access. Perform manual testing and attempt to gain access to your resources from a standard network connection.

Internal fingerprinting:

- Identify potentially vulnerable ports and services
- Analyze internally exposed services and enterprise traffic

Gain a foothold:

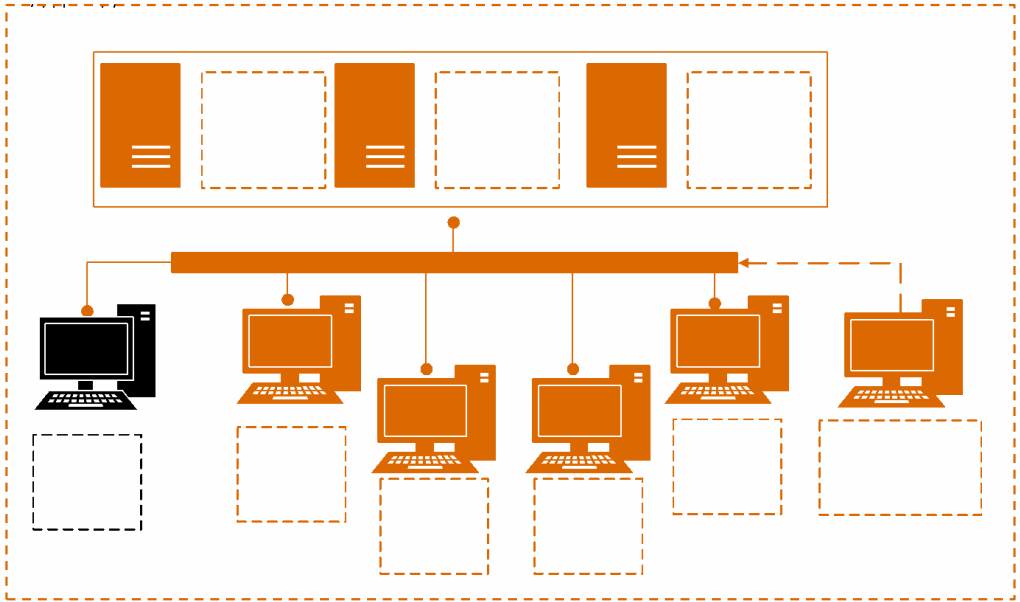
- Man-in-the-Middle (MitM) session attacks
- Web Proxy Auto-Detection (WPAD) poisoning
- Link-Local Multicast Name Resolution (LLMNR) poisoning
- NetBIOS Name Service (NB-NS) poisoning
- Manipulate old, outdated or no longer supported services
- Default configuration and credential manipulation

Lateral Movement:

- Pass-the-Hash (PtH)
- System pivoting
- Manipulation of whitelisted tools and services

Gain access to Crown Jewels:

- Attempt to gain privileged access
- Attempt to gain access to sensitive data



Wireless Network Assessment and Penetration Testing

Vulnerabilities in your wireless networks may provide access to data, workstations, and other internal systems that are connected to wireless networks.

Mobile Penetration Testing

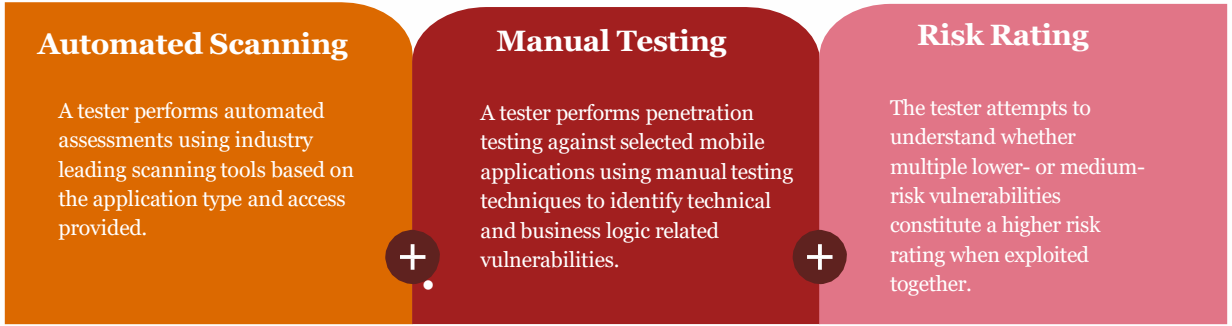
Reverse Engineering	Network Communications Analysis	Local Resource Handling Analysis	Run-time and Logic Manipulation
A tester attempts to reverse engineer the application content to **identify sensitive hard-coded values** that could be used to gain unauthorized access, or to identify potential logic and operational flaws pertaining in the execution of the application.	A tester eavesdrops on and manipulates network calls to the back end servers supporting the execution of the application. These tests are performed in an effort to **identify common input validation flaws** that could lead to sensitive information disclosure or unauthorized access.	A tester monitors and analyzes **local resource handling operations** as different tasks within the application are performed.	A tester performs various different techniques to manipulate the logic of the application as it is executed on the device, to attempt to **identify risks associated with misuse, data leakage, or unauthorized access.**

Physical Testing

Physical penetration tests are designed to assess an organization's physical security posture based on agreed upon objectives and agreed upon testing scenarios.

Web Application Security Assessment

PwC assesses each of web applications' susceptibility to a variety of attacks including Open Web Application Security Project (OWASP) top 10 security flaws:

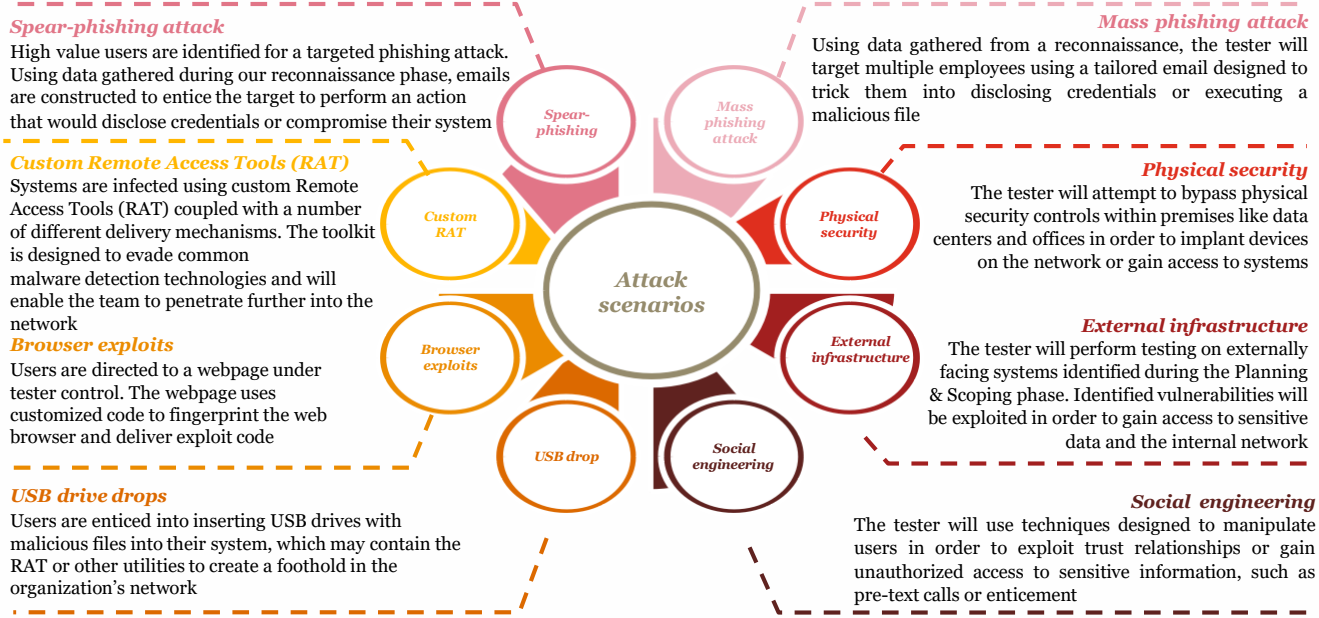


- Injection Flaws
- Weak Authentication and Session Management
- Cross-Site Scripting (XSS) Flaws
- Insecure Direct Object References
- Security Misconfigurations
- Sensitive Data Exposure
- Missing Functional-Level Access Control
- Cross-Site Request Forgery (CSRF) Flaws
- Using Components with Known Vulnerabilities
- Unvalidated Redirects and Forwards

Red Teaming

Testing

A range of techniques can be used to craft a customized attack scenario in line with client requirements. These techniques are designed to replicate the modus operandi of real-world attackers. Depending on the objective of the test, the tester will customize the assessment procedures, tools, techniques, and procedures, but at a high-level, some of these may include:



Spear-phishing attack

High value users are identified for a targeted phishing attack. Using data gathered during our reconnaissance phase, emails are constructed to entice the target to perform an action that would disclose credentials or compromise their system

Mass phishing attack

Using data gathered from a reconnaissance, the tester will target multiple employees using a tailored email designed to trick them into disclosing credentials or executing a malicious file

Custom Remote Access Tools (RAT)

Systems are infected using custom Remote Access Tools (RAT) coupled with a number of different delivery mechanisms. The toolkit is designed to evade common malware detection technologies and will enable the team to penetrate further into the network

Physical security

The tester will attempt to bypass physical security controls within premises like data centers and offices in order to implant devices on the network or gain access to systems

Browser exploits

Users are directed to a webpage under tester control. The webpage uses customized code to fingerprint the web browser and deliver exploit code

External infrastructure

The tester will perform testing on externally facing systems identified during the Planning & Scoping phase. Identified vulnerabilities will be exploited in order to gain access to sensitive data and the internal network

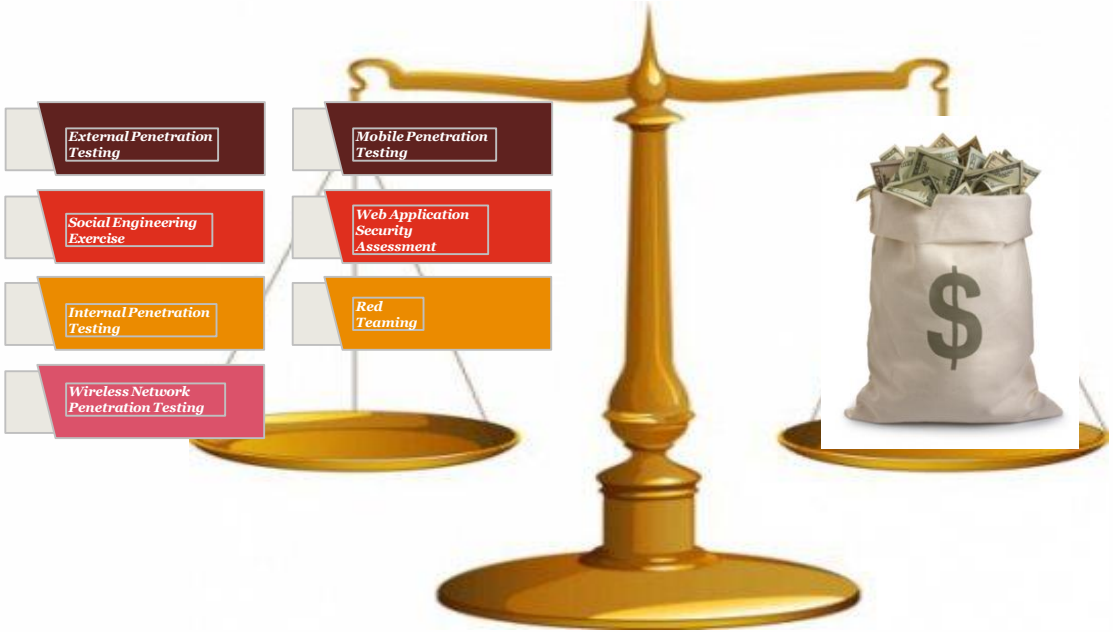
USB drive drops

Users are enticed into inserting USB drives with malicious files into their system, which may contain the RAT or other utilities to create a foothold in the organization's network

Social engineering

The tester will use techniques designed to manipulate users in order to exploit trust relationships or gain unauthorized access to sensitive information, such as pre-text calls or enticement

Recommendations

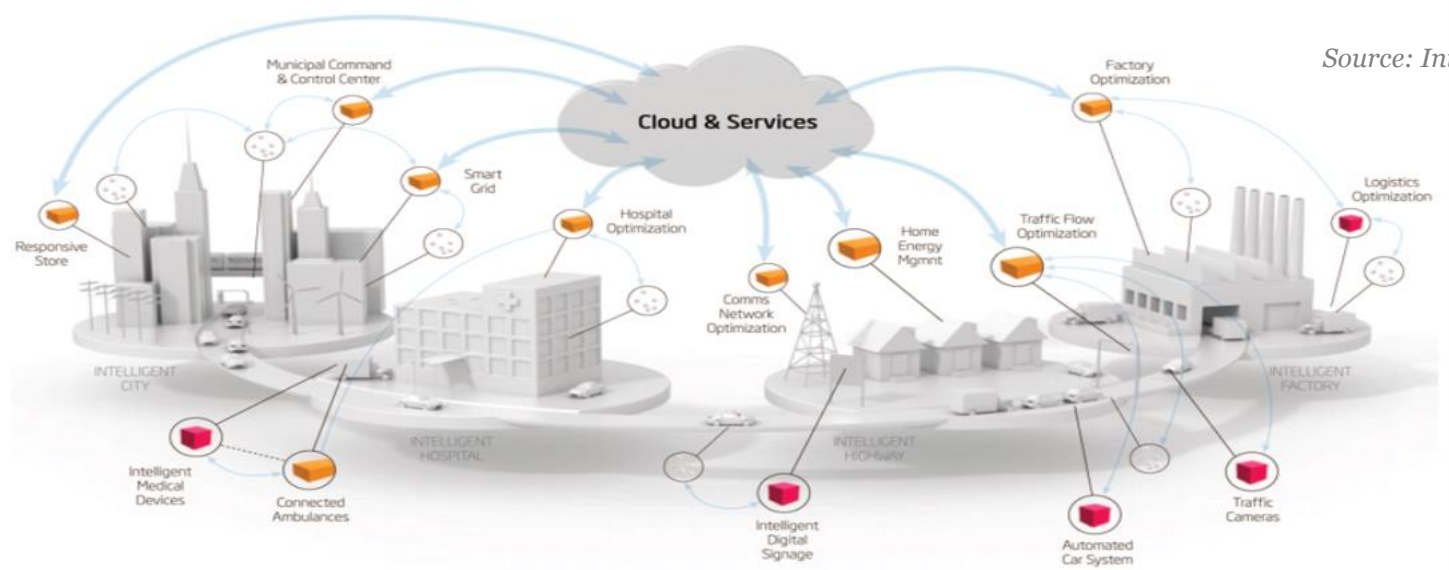


- *Targeted & Risk Aligned*
- *Objectives Documented*
- *Routinely Performed*
- *Methods Varied*

IoT - The Game Changes

What is the “Internet of Things”?

The “Internet of Things” (IoT) describes an ecosystem of sensors, embedded computers, and “smart” devices that communicate among themselves and with private/public cloud services in order to collect, analyze and present data about the physical world.

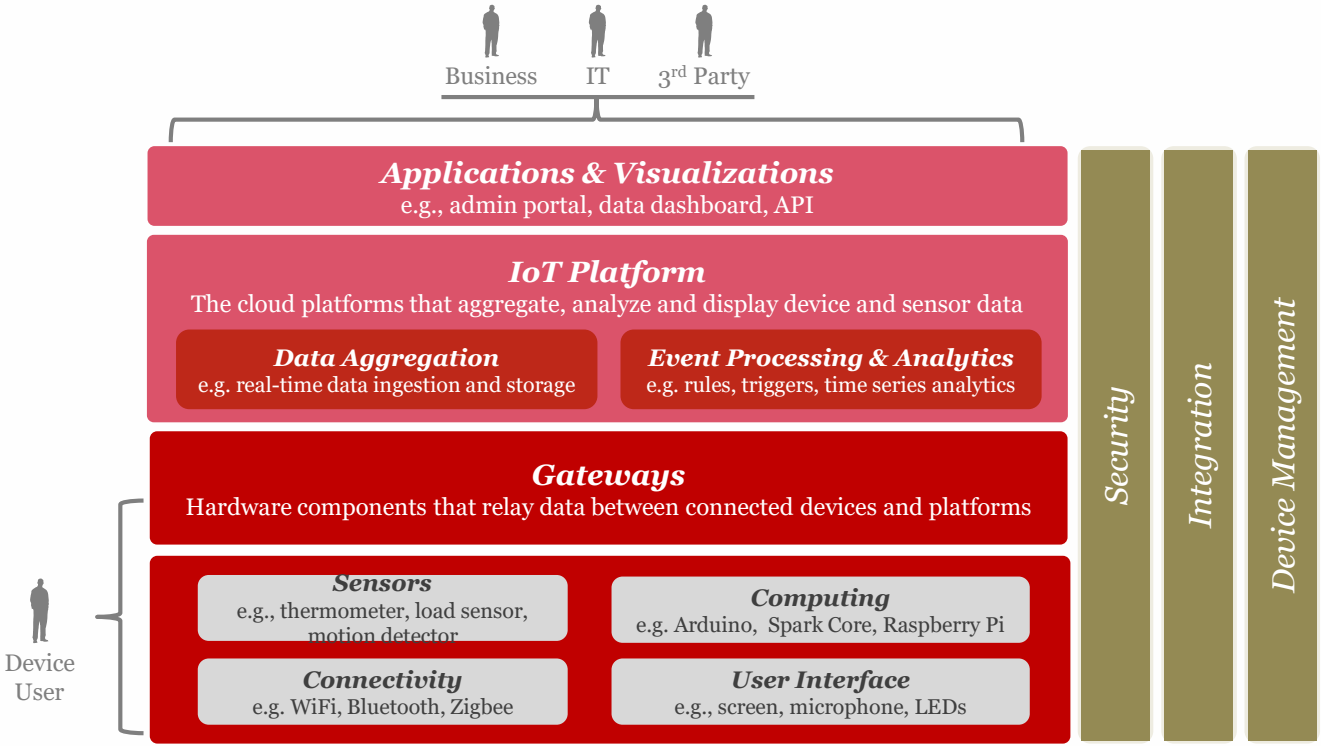


Source: Intel

Gartner expects 15-20% annual growth to 25 billion connected devices to be in use by 2020.

IoT Reference Architecture

An internet of things architecture is different from a traditional web application architectures due to the introduction of a fleet of connected devices and the data that they generate. This introduces a new set of challenges and considerations across the following areas.



Connected Devices

The term “connected device” is a catch-all that refers to a wide spectrum of devices but in its most fundamental form, a connected device must be able to capture, process and transmit some environmental data.

Example Connected Devices

Motion Sensor

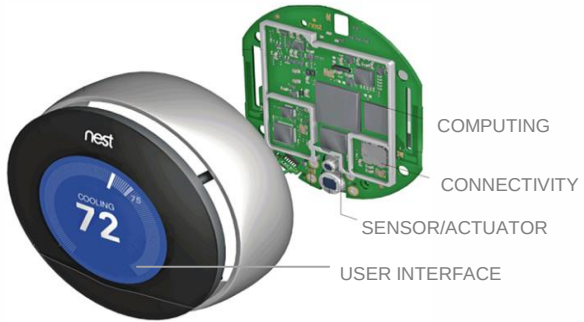
Connected Thermostat

Fitness Tracker

Smartphone

Connected Car

* All connected devices must also have a power source which is most often either a battery or a power outlet but can also include alternative sources such as solar or ambient electromagnetic power



Many “smart” consumer products may include a bundle of various sensors that work together as well as local data storage, local analytics and event triggering or a user interface to present the data.

Connected Device Components

User Interface *(Optional)*
The functionality through which a user interacts with the device
(e.g., screen, microphone, LED lights)

Connectivity
The transmitter that sends the data to another device or to a central platform for processing
(e.g., Wifi, Bluetooth, Zigbee)

Sensor/Actuator
The transmitter that sends the data to another device or to a central platform for processing
(e.g., temperature, humidity, speaker)

Computing
The processor that records, stores and analyzes the sensor output
(e.g., Arduino, Photon, ARM Chip)

New Questions Raised

Where is the boundary?

What are the roles, responsibilities and authority in Operational areas?

To what extent do we rely on attestation by 3rd parties and suppliers?

What are the risks to Operations in running a penetration test?

Do we have the knowledge?

Questions

Thank You