The IoT Value Chain



Hinweis: Appears in DLBINGEIT01

|  |  |
| --- | --- |
| Hardware  |  |
| Connectivity  |  |
| Platform  |  |
| Application |  |

IoT Clusters

Hinweis: Remove bold and follow text written out below.

|  |  |
| --- | --- |
| Applications: Similar solutions and software. |  |
| Use cases: Served by the same platform and need similar data processing capabilities. |  |
| Verticals: Specific industry segment with unique regulatory bodies, supports and standards. |  |

Core IoT Functional Stack



Hinweis: Appears in DLBINGEIT01.

|  |  |
| --- | --- |
| Application |  |
| Software backend |  |
| Connectivity  |  |
| Hardware |  |

IoT Access Technologies



Hinweis: Follow capitalization below.

|  |  |
| --- | --- |
| IoT Technologies |  |
| Wired IoT Technologies |  |
| Wireless IoT Technologies |  |
| Ethernet |  |
| PLC |  |
| Short-range |  |
| Long-range |  |
| Bluetooth |  |
| ZigBee |  |
| Thread |  |
| Wi-Fi |  |
| Unlicensed spectrum |  |
| Licensed spectrum |  |
| LoRaWAN |  |
| Sigfox |  |
| LTE-M |  |
| NB-IoT |  |

Traditional IT Versus IoT Security

Hinweis: Follow text as written out below.

|  |  |
| --- | --- |
| IoT security |  |
| IT security |  |
| Built-in security |  |
| Add-on security |  |
| Devices are usually in open environments |  |
| Devices are located in closed environments |  |
| Lightweight algorithms for resource-constrained devices  |  |
| Complex algorithms |  |

**Vulnerability Versus Threat Versus Risk**

Hinweis: Follow text as written out below.

|  |  |
| --- | --- |
| Vulnerability |  |
| Weakness in IoT devices, software, or procedures. |  |
| Threat |  |
| Process to steal or damage data, disrupt business, or create harm in general |  |
| Risk |  |
| Potential for damage or destruction of assets or data when a threat exploits a vulnerability. |  |

Top IoT Vulnerabilities

Hinweis: Follow text as written out below.

|  |  |
| --- | --- |
| Weak passwords |  |
| Insecure network services |  |
| Insecure ecosystem interfaces |  |
| Lack of secure update mechanism  |  |
| Use of insecure or outdated components |  |
| Insufficient privacy protection |  |
| Insecure data transfer and storage |  |
| Lack of device management |  |
| Insecure default settings |  |
| Lack of physical hardening  |  |

**IoT Attacks and Countermeasures**



|  |  |
| --- | --- |
| Application layer |  |
| Cloud services layer |  |
| Network layer |  |
| Device layer |  |
| Attacks |  |
| Malicious script |  |
| Viruses and trojans |  |
| Cryptanalysis attack  |  |
| Man-in-the-middle attack |  |
| Side channel attack |  |
| Denial of service |  |
| Third party relationship |  |
| Malicious insider |  |
| Traffic analysis attack |  |
| RFID spoofing |  |
| RFID cloning |  |
| Sinkhole attack |  |
| Malicious code injection |  |
| Sybil attack |  |
| Node tampering |  |
| Social engineering |  |
| Physical damage |  |
| Jamming in WSN |  |
| Malicious node injection |  |
| Sleep deprivation attack |  |
| Countermeasures |  |
| Data security |  |
| Access control list |  |
| Risk assessment |  |
| Anti-viruses |  |
| Anti-spyware |  |
| Firewalls |  |
| Intrusion detection |  |
| Web application scanner |  |
| Routing security |  |
| Routing protocol |  |
| Authentication |  |
| Hello flood detection |  |
| Data privacy |  |
| Identity validation  |  |
| Data privacy |  |
| Data integrity |  |
| Secure booting |  |
| Secure physical design |  |
| Device authentication |  |
| Risk assessment |  |

**Man-in-the-Middle Attack**



|  |  |
| --- | --- |
| User |  |
| Original connection |  |
| Application |  |
| New connection |  |
| Perpetrator  |  |

**Software Development Life Cycle (SDLC)**

|  |  |
| --- | --- |
| Requirement & analysis |  |
| Project Planning |  |
| Design |  |
| Coding & implementation |  |
| Testing |  |
| Deployment |  |
| Maintenance |  |

Static Application Security Testing

|  |  |
| --- | --- |
| Gather information |  |
| Prepare and compile |  |
| Scan source code vulnerability |  |
| Analyze and verify |  |
| Report |  |

**DevSecOps Software Lifecycle**



|  |  |
| --- | --- |
| Dev |  |
| Sec |  |
| Ops |  |
| Code Review |  |
| SAST |  |
| Composition Analysis |  |
| DAST  |  |
| Pen test |  |
| Code  |  |
| Build |  |
| Test |  |
| Plan  |  |
| Release |  |
| Compliance Validation |  |
| Deliver |  |
| Feedback |  |
| Deploy |  |
| Operate |  |
| Monitor |  |
| Security Config |  |
| Patch |  |
| Security Monitoring  |  |

**DevSecOps Pillars**

|  |  |
| --- | --- |
| DevSecOps |  |
| People |  |
| Process |  |
| Technology |  |

DevOps Versus DevSecOps

|  |  |
| --- | --- |
| Dev SecOps |  |
| DevOps |  |
| Development |  |
| IT operations |  |
| Application delivery |  |
| Security |  |

Security Risks Threatening IoT Devices



Hinweis: Copyright unclear.

|  |  |
| --- | --- |
| IoT security risks |  |
| Confidentiality |  |
| Data integrity |  |
| Theft of service |  |
| Availability  |  |

Categories of Device Security Attacks

|  |  |
| --- | --- |
| Security attacks |  |
| Expensive invasive attacks |  |
| Lower cost attacks |  |
| Reverse engineering |  |
| Chip microprobing |  |
| Passive software attacks |  |
| Communication attacks |  |
| Exploiting code vulnerabilities |  |
| Exploiting weaknesses in the internet protocols |  |
| Crypto or key handling |  |

Cost and Effort to Attack Versus Secure



Hinweis: Copyright unclear.

|  |  |
| --- | --- |
| Effort/Cost to attack |  |
| Effort/Cost to secure |  |
| Communication attacks |  |
| Software attacks |  |
| Non-invasive HW attack |  |
| Invasive HW attack |  |
| Code vulnerabilities |  |
| Man-in-the-middle |  |
| Weak RNG |  |
| Malware |  |
| Social engineering |  |
| Side channels |  |
| Physical access to device ports |  |
| Well resourced and funded |  |
| Unlimited time, money, equipment |  |
| Value for the attacker |  |

Cryptography



Hinweis: Copyright unclear.

|  |  |
| --- | --- |
| Plain text |  |
| Encryption key |  |
| Encryption algorithm |  |
| Ciphertext |  |

Message Relay



|  |  |
| --- | --- |
| Plain text |  |
| Encryption key |  |
| Encryption Algorithm |  |
| Cipher Data packet |  |
| Sniffs and intercepts data packets |  |
| Replays data packets |  |

Message Authentication Code



|  |  |
| --- | --- |
| Message |  |
| Secret key |  |
| MAC algorithm |  |
| MAC |  |
| Equal? |  |
| Sender |  |
| Receiver |  |

Cloud, Fog, and Edge Computing



|  |  |
| --- | --- |
| Data |  |
| Commands |  |
| Cloud |  |
| Fog |  |
| Edge |  |
| Thousands of data centers |  |
| Millions of nodes |  |
| Billions of devices |  |

Fog Computing Layer Model

|  |  |
| --- | --- |
| Transport layer |  |
| Security layer |  |
| Temporary Storage Layer |  |
| Pre-processing layer |  |
| Monitoring layer |  |
| Physical virtualization layer |  |
| Uploading pre-processed and secured data to the cloud |  |
| Encryption/decryption, privacy, and integrity measures |  |
| Data distribution, replication, and de-duplication |  |
| Storage space virtualization and storage devices |  |
| Data analysis, data filtering, reconstruction, and trimming |  |
| Activities, power, and resource monitoring |  |
| Virtual sensor networks |  |
| Things and wireless sensor networks |  |

Types of IAM

|  |  |
| --- | --- |
| Identity-based |  |
| Resource-based |  |
| Alice can read resource x |  |
| Bob can modify resources X and Y |  |
| Resource X |  |
| Alice can read |  |
| Bob can read and write |  |
| Resource Y |  |
| Alice is denied access |  |
| Bob can modify |  |

Multi-Factor Authentication



Big Data 5Vs

|  |  |
| --- | --- |
| Volume |  |
| Velocity |  |
| Variety |  |
| Value |  |
| Veracity |  |

Supervised Learning Operation



Hinweis: Follow text as written out below.

|  |  |
| --- | --- |
| Labeled data |  |
| Labels |  |
| Rabbit  |  |
| Cow |  |
| Dog |  |
| Model training |  |
| Prediction |  |
| Test data |  |

Types of Supervised Learning Algorithms

Hinweis: Follow text as written out below.

|  |  |
| --- | --- |
| Supervised learning |  |
| Regression |  |
| Classification |  |
| Linear regression |  |
| Regression trees |  |
| Non-Linear regression |  |
| Bayesian Linear Regression |  |
| Polynomial Regression |  |
| Random Forest |  |
| Decision Trees |  |
| Logistic Regression |  |
| Support vector Machines |  |

Regression Versus Classification



|  |  |
| --- | --- |
| Classficiation |  |
| Regression |  |

Linear Regression Versus Polynomial Regression



Hinweis: Follow text as written out below.

|  |  |
| --- | --- |
| Linear regression |  |
| y = a0 + a1x |  |
| Polynomial regression |  |
| y = a0 + a1x + a2x2 |  |

Decision Trees



Hinweis: Follow text as written out below.

|  |  |
| --- | --- |
| Root Node |  |
| Decision Node |  |
| Leaf Node |  |

SVM Algorithm



Hinweis: Copyright unclear. Hinweis: Follow text as written out below.

|  |  |
| --- | --- |
| Support Vectors |  |
| Negative Hyperplane |  |
| Positive Hyperplane |  |
| Maximum Margin Hyperplane |  |

Unsupervised Learning



Hinweis: Follow text as written out below.

|  |  |
| --- | --- |
| Unlabeled data |  |
| Interpreter |  |
| Algorithm |  |
| Processor |  |
| Cows |  |
| Rabbits |  |
| Dogs |  |