IBM’s statements regarding its plans, directions, and intent are subject to change or withdrawal without notice at IBM’s sole discretion.

Information regarding potential future products is intended to outline our general product direction and it should not be relied on in making a purchasing decision.

The information mentioned regarding potential future products is not a commitment, promise, or legal obligation to deliver any material, code or functionality. Information about potential future products may not be incorporated into any contract.

The development, release, and timing of any future features or functionality described for our products remains at our sole discretion.

Performance is based on measurements and projections using standard IBM benchmarks in a controlled environment. The actual throughput or performance that any user will experience will vary depending upon many factors, including considerations such as the amount of multiprogramming in the user’s job stream, the I/O configuration, the storage configuration, and the workload processed. Therefore, no assurance can be given that an individual user will achieve results similar to those stated here.
Abstract

We all want devices to be smarter. The benefits of IoT across industries, such as healthcare, manufacturing, oil and gas, and others, are gaining greater appreciation, but the security implications of all these connected things are also becoming better understood.

How long can we continue to place trust in the everyday devices we rely on? In an age of growing connectedness for everything from manufacturing robots to toothbrushes, the Internet of Things has the potential to morph from a helpful productivity enhancer into a cover for malicious infiltration of your home and office.

Learn how makers can build secure "things" and the security controls operators can implement. We'll present a simple model for assessing threats to the IoT ecosystem relevant to your industry and products. Security practitioners will learn how to be effective early adopters, without being victims of "things".

Key Takeaways:

• About the credible threats and real risks of the IoT and wearables to organizational security
• How makers can build secure "things"
• How operators can implement effective security controls and avoid being victims of "things"
• How to avoid the political and policy pitfalls when the physical world collides with digital technology
Agenda

1. Overview of IoT and security threats
2. Security requirements
3. IoT security facts
4. Anatomy of trusted and secure solutions
5. IoT security maturity journey & continuous lifecycle
6. Cognitive IoT security
Introduction to IoT

By 2020 over

30 Billion*

Connected devices 285% increase

$: The economic impact of the Internet of Things will be measured in $trillions.

$\Sigma$: The number of connected devices will be measured in billions.

$\infty$: The resultant benefits of a connected society are significant, disruptive and transformational.

IoT is Driving Digital Disruption Into the Physical World

Accelerating Advancements in Technology... Are transforming every part of business...

- Advanced Analytics
- Product Lifecycle Management
- Cloud Computing
- Pervasive Connectivity
- Embedded Sensors

- Boosting operational performance and lowering costs
- Driving engagement and customer experience
- Creating new products and business models
# Extracting Business Value from IoT solutions

<table>
<thead>
<tr>
<th>Touch Point</th>
<th>Prevent failure and fix in a timely manner</th>
<th>Optimise maintenance</th>
</tr>
</thead>
<tbody>
<tr>
<td>Direct contact with the owner / user of the thing</td>
<td>Connectivity CRM</td>
<td>Asset management Predictive Analytics</td>
</tr>
<tr>
<td>Predict and Prevent</td>
<td>Learn from usage and optimise future designs</td>
<td>Improve efficiency of activities with data from things</td>
</tr>
<tr>
<td>Optimize</td>
<td>Interact with the thing in new ways</td>
<td>Mobile</td>
</tr>
<tr>
<td>Extend and Interact</td>
<td>Other departments, companies and users can benefit from the data</td>
<td></td>
</tr>
<tr>
<td>Value to a wider ecosystem</td>
<td>Move to a pay per use / as a service model</td>
<td>Change design to optimize return on investment</td>
</tr>
<tr>
<td>Business transformation</td>
<td></td>
<td>Billing</td>
</tr>
</tbody>
</table>
IoT security threats are real and becoming more publicised
Brand reputation and customer trust are at risk from targeted IoT attacks

Forbes
The Dyn DDOS Attack And The Changing Balance Of Online Cyber Power

WIRED
Hackers Remotely Kill A Jeep On The Highway—with Me In It

The New York Times
EUROPE
Hackers Use New Tactic at Austrian Hotel: Locking the Doors
A selection from the IoT hackers tool box

**Credential Compromise**

- **Brute force attacks** on device side hardcoded credentials, default credentials (anywhere) and deployment of default secure configurations.
- **Dictionary attacks** on devices, cloud services & applications using non-trivial passwords – particularly embedded and automated logic services where interactive human intelligence can not be used to distinguish between errors and attacks.
- **Rainbow Table attacks** on Devices, could services & applications relying on encrypted credential repositories.

Mitigation options: credential salting/hashing, transport encryption & PKI authentication.

**Social Compromise :**

- **Phishing** and spear-phishing by requesting sensitive information through misrepresentation to gain device or system access for control purposes.

Mitigation options: cyclical access revocation

**Network/Communications Compromise: Snooping & Scanning:**

- Searching networks for open end points and devices as a system access point to manipulate resources and behaviors
- Intercepting network protocol exchanges to manipulate control variables, misdirect commands or passive subversion of information for later use (e.g. Man in the Middle)
- Deploying botnets to gain control of access, control of system behavior (e.g. Stuxnet) or malicious misdirection of compute resources (e.g. Miria DDoS)

Mitigation options: physical and network endpoint protection

**Ransomware** – holding business or individuals hostage to misfortune in system controlled home, business or industrial environments.

**Backdoor attacks** - deployed or designed in “debug code” that opens system access to the designer or collaborators.
Where IoT Hackers attack:
Chip to Cloud Application Vulnerabilities

Silicon Attacks
- Tampering
- Take over
- Repurposing
- Destruction
- Invalidation

Device Attacks
- Identity
- Secure tokens & passwords
- Client-side Certs. & Keys
- Take over
- Redirection/snooping

Local Network Attacks
- Snooping
- Man-in-the-Middle
- Take over
- Spoofing/Simulation
- Redirection
- Command Injection

Gateway Attacks
- Gateway Identity
- Secure tokens & passwords
- Gateway Certs & Keys
- Protocol repurposing
- Data manipulation

Global Network Attacks
- Transport Corruption
- Transport Disruption
- Snooping

Cloud Service Attacks
- Denial of Service
- Snooping/Probing
- Man-in-the-Middle
- Take over
- Spoofing/Simulation

Cloud Application Attacks
- Data manipulation
- Resources Access
- Resource abuse
- Take Over
- Repurposing
- Identity

Silicon
IoT Devices
Gateways
Networks
Cloud
Solution & Applications

Destroy valuable assets
Cause unexpected device behaviour
Disrupt solution behaviour
Create malicious behaviour
Gather Information for use elsewhere

Deny Service
Gather Info.

Deny Service
Cause unexpected behaviour
Disrupt solution behaviour
Create malicious behaviour
Gather/Manipulate Data

Watson IoT
Risks and security threats in IoT environments

Information Technology (IT)
Attacks on data-center hosted data and services

- Exposure to IT networks from OT networks
- Human error or sabotage of operations systems
- Unprotected (or under protected) components in network
- DDoS or mis-information attack
- Attack from mobile-based remote maintenance apps
- Technical malfunctions of components

Operational Technology (OT)
Damage to plant, equipment, quality and output

- Loss of production
- Loss of intellectual property
- Capital Loss
- Triggering safety procedures or interfering with safety systems
- Deterioration of product quality
IoT Security Requirements – from Chip to Cloud Application

**End-end IoT security**

- **Silicon**
  - Partnerships with manufacturers and designers:
    - leverage in silicon security & trusted modules

- **IoT Devices**
  - Mutual identity validation device-cloud:
    - Secure tokens or client-side certificates

- **Gateways**
  - Edge security:
    - Trusted gateways
    - Auto device registration

- **Networks**
  - Secure communications:
    - TLS v1.2, HTTPS
    - Encrypted data

- **Cloud**
  - Authentication
  - Authorization
  - Access Control
  - Data encryption
  - Firewalled
  - Secure operations
  - ISO27k compliance
  - Security dashboard

- **Solution & Applications**
  - Application access control & user management
  - Visibility of threats:
    - security dashboard
  - Incident response:
    - policies
  - Solution or industry specific security
IoT IAM Example Use Cases

**IDoT—Identity of things**
- Device identity
- Gateway identity
- User Identity

**Device association**
- Dynamic relationships
- Multi to Multi

**Lifecycle Management**
- Transfer of ownership—Adding and removing users to devices
- Manufacturer vs user access
- Certificate creation, distribution
IoT Security Facts – for Device and Solution Creators

Devices will operate in hostile environments

Software security will degrade over time

Shared secrets do not remain secret

Weak configurations will persist

As data accumulates, exposure issues will increase

Listen to Podcasts on these topics:
https://soundcloud.com/securityintelligence/sets/5-indisputable-facts-about-iot
Anatomy of trusted and secure IoT solutions

Secure by design: Multi-layer Security Strategy
- Physical and Operational Security
- Network Security
- System, Application and Data Security
- Standards e.g. ISO27001 Compliance

Basic & Advanced Security Controls
- Authentication (identity & credentials)
- Authorization (privileges)
- Access Control (application resource access & data isolation)
- Role Based Authorization (Pre-defined roles)
- Data Security (encryption at rest & in flight)
- Visualize critical risks and drive mitigation actions

IoT and Security Expertise
- Define and update IoT Security Strategy
- Assessment and training of personnel
- Streamline processes e.g. vulnerability disclosure and incident response
- Penetration testing of devices and solutions
IBM Thought Leadership

*IoT Security is different and requires a new perspective*

The IBM point of view: IoT Security

- The connectivity of “things” presents an exciting environment for innovation and opportunity, but also a broad set of security challenges and threats
- Including new risks since IoT devices are different
  - Environment: “out in the wild”
  - Consequences: actuators have a physical effect
  - Variety: no standard footprint
  - Volume: billions
  - Organization: maintained by plant operators rather than IT staff

Read the paper: [ibm.co/IoTSecurity](http://ibm.co/IoTSecurity)

IoT Security maturity journey & continuous lifecycle

- Start by providing protection capabilities
- Generate intelligence to enhance protection
- Use intelligence to see threats
- Feed intelligence into a cognitive solution to be able to predict issues before they occur
- Never stand still: evolve as threats evolve
Cognitive IoT Security

Cognitive IoT opens new capabilities and threats
- Active and passive attacks
- Safety, Security, and Privacy
- Attacks against the cognitive computation (dis-information)

Device Lifecycle for Scale and Security
- Research using blockchain for managing device identity
- Additional crypto-backed device authentication

Attention to Privacy
- Research on tokenization and privacy-protecting authentication

Cognitive IoT used for Security
- Machine-learning and use of cognitive functions to
  - Monitor and distill
  - Correlate and predict
  - Adapt and pre-empt

Design and manufacture securely
- Design for security
- Design for privacy
- Test for security
- Continuous delivery model
- Ensure integrity in manufacturing and delivery

Operate securely
- Harden the device (check for device resiliency)
- Secure the communications channel
- Audit and analyze usage patterns
- Maintain an up-to-date security environment

https://ibm.co/iotsecurity-POV2
IBM is a Leader in The Forrester Wave™: IoT Software Platforms, Q4 2016

“The Watson IoT Platform can serve a broad range of advanced IoT use cases. The tech giant doubled down on IoT in 2015 with an investment of $3 billion dollars to create a new IoT business unit. The new org includes more than 1,000 researchers, developers, and designers dedicated specifically to developing the Watson IoT Platform. Since then, IBM has added significant capabilities to the platform, including augmented reality, cognitive capabilities, blockchain, edge analytics, analytics tooling, and natural language processing (to name a few). With a strong commitment to open source standards and a robust global partner ecosystem, IBM is well positioned for market leadership. However, according to some customers, Watson is not well integrated with analytics engines, and IBM’s product portfolio terminology is confusing and hard to decipher.”

SECURITY FIRST APPROACH
...designed in at the start
FIT FOR PURPOSE
...right sized for the application
RESILIENCE
...through operating life

https://iotsecurityfoundation.org/

• Framework and Best practice guides:
  • IoT Security Compliance Framework
  • Connected Consumer Products
  • Vulnerability Disclosure
  • Best Practice User Mark

https://iotsecurityfoundation.org/best-practice-guidelines
Key Takeaways

• IBM is a thought leader in IoT Security. Our Security Point of View paper [https://ibm.co/iotsecurity-POV2](https://ibm.co/iotsecurity-POV2)

• IBM has new IoT Security Professional Services Offerings to help customers on their IoT journey and adoption. [https://ibm.com/iot/security](https://ibm.com/iot/security)

• IBM is innovating in IoT Security. Try all the features of the Watson IoT Platform today. Explore IBM Watson IoT [Play Try Buy](https://ibm.com) for free*

*according to terms and conditions of Watson IoT Platform lite plan on the [bluemix catalog](https://ibm.com/bluemix)
Notices and disclaimers

Copyright © 2017 by International Business Machines Corporation (IBM). No part of this document may be reproduced or transmitted in any form without written permission from IBM.

U.S. Government Users Restricted Rights — use, duplication or disclosure restricted by GSA ADP Schedule Contract with IBM.

Information in these presentations (including information relating to products that have not yet been announced by IBM) has been reviewed for accuracy as of the date of initial publication and could include unintentional technical or typographical errors. IBM shall have no responsibility to update this information. This document is distributed “as is” without any warranty, either express or implied. In no event shall IBM be liable for any damage arising from the use of this information, including but not limited to, loss of data, business interruption, loss of profit or loss of opportunity. IBM products and services are warranted according to the terms and conditions of the agreements under which they are provided.

IBM products are manufactured from new parts or new and used parts. In some cases, a product may not be new and may have been previously installed. Regardless, our warranty terms apply.”

Any statements regarding IBM’s future direction, intent or product plans are subject to change or withdrawal without notice.

Performance data contained herein was generally obtained in a controlled, isolated environments. Customer examples are presented as illustrations of how those customers have used IBM products and the results they may have achieved. Actual performance, cost, savings or other results in other operating environments may vary.

References in this document to IBM products, programs, or services does not imply that IBM intends to make such products, programs or services available in all countries in which IBM operates or does business.

Workshops, sessions and associated materials may have been prepared by independent session speakers, and do not necessarily reflect the views of IBM. All materials and discussions are provided for informational purposes only, and are neither intended to, nor shall constitute legal or other guidance or advice to any individual participant or their specific situation.

It is the customer’s responsibility to insure its own compliance with legal requirements and to obtain advice of competent legal counsel as to the identification and interpretation of any relevant laws and regulatory requirements that may affect the customer’s business and any actions the customer may need to take to comply with such laws. IBM does not provide legal advice or represent or warrant that its services or products will ensure that the customer is in compliance with any law.
Notices and disclaimers continued

Information concerning non-IBM products was obtained from the suppliers of those products, their published announcements or other publicly available sources. IBM has not tested those products in connection with this publication and cannot confirm the accuracy of performance, compatibility or any other claims related to non-IBM products. Questions on the capabilities of non-IBM products should be addressed to the suppliers of those products. IBM does not warrant the quality of any third-party products, or the ability of any such third-party products to interoperate with IBM’s products. IBM expressly disclaims all warranties, expressed or implied, including but not limited to, the implied warranties of merchantability and fitness for a particular, purpose.

The provision of the information contained herein is not intended to, and does not, grant any right or license under any IBM patents, copyrights, trademarks or other intellectual property right.

IBM, the IBM logo, ibm.com, Aspera®, Bluemix, Blueworks Live, CICS, Clearcase, Cognos®, DOORS®, Emptoris®, Enterprise Document Management System™, FASP®, FileNet®, Global Business Services®, Global Technology Services®, IBM ExperienceOne™, IBM SmartCloud®, IBM Social Business®, Information on Demand, ILOG, Maximo®, MQIntegrator®, MQSeries®, Netcool®, OMEGAMON, OpenPower, PureAnalytics™, PureApplication®, pureCluster™, PureCoverage®, PureData®, PureExperience®, PureFlex®, pureQuery®, pureScale®, PureSystems®, QRadar®, Rational®, Rhapsody®, Smarter Commerce®, SoDA, SPSS, Sterling Commerce®, StoredIQ, Tealeaf®, Tivoli® Trusteer®, Unica®, urban{code}®, Watson, WebSphere®, Worklight®, X-Force® and System z® Z/OS, are trademarks of International Business Machines Corporation, registered in many jurisdictions worldwide. Other product and service names might be trademarks of IBM or other companies. A current list of IBM trademarks is available on the Web at "Copyright and trademark information" at: