10 POINTS OF DATA VULNERABILITY IN IoT

Trust is the backbone of the Internet of Things.
Continually sharing data is what makes IoT valuable, but it's also what makes it vulnerable. It's essential to understand where those vulnerabilities lie and what you should be doing to secure them.

AT THE EDGE

#1 PHYSICAL SECURITY

Compromising the physical device is a common and effective tactic for gaining access to IoT data.

- Minimize external ports
- Ensure the device OS is protected
- Limit administrative capabilities

#2 SOFTWARE/ FIRMWARE

Security updates on edge devices are the first line of active defense for IoT systems.

- Sign updates
- Verify updates before install
- Secure update servers

#3 SECURITY SETTINGS

Allowing admins to configure permissions and settings empowers them to better protect the IoT system.

- Make security logging available
- Allow selection of encryption options
- Enable security alerts for admins

DATA TRANSMISSION

#4 TRANSPORT ENCRYPTION

Secure sensitive data via encryption to minimize risk of compromise, even if intercepted.

- Encrypt communication between components
- Maintain SSL/TLS implementations
- Avoid proprietary encryption solutions

#5 NETWORK SERVICES

As IoT components share data on a network, they can be left exposed, putting the system at risk.

- Minimize open network ports
- Avoid using risky protocols
- Review network services for vulnerabilities

THE KEY TO IT ALL:
PARTNERSHIP

IoT security doesn't happen in a bubble. It's the collaboration between OEMs, platform developers, system integrators, network providers, and customers—down to the individual end user—that keeps data secure. Communication, feedback, and working together to enforce security standards are all essential.

T-Mobile is bringing together a winning roster of IoT innovators to collaborate and solve problems at all levels, like making IoT more secure.

IN THE CLOUD

#6 CLOUD INTERFACE

Preventing the wrong people from accessing the hub for your IoT data—and entire IoT system—is critical.

- Perform assessment of all cloud interfaces/APIs
- Follow industry best practices for secure cloud development
- Implement strong perimeter defenses

WITH THE USER

#7 PRIVACY CONCERNS

The first step to keeping a user's personal data safe is being careful about what you collect.

- Minimize collection
- Make data anonymous
- Leverage opt-in to give users control of their data

#8 AUTHENTICATION /AUTHORIZATION

If a person with bad intentions gains access they shouldn't have, all other protections become ineffective.

- Require strong, complex passwords
- Verify that password recovery mechanisms are secure
- Implement two-factor authentication

#9 WEB INTERFACE

Web-based IoT device interfaces provide an easy route to compromise your system if they aren't properly secured.

- Require default user names, passwords to be changed
- Follow industry best practices for secure web development (e.g. OWASP)
- Conduct assessments of web applications

#10 MOBILE INTERFACES

Accessing data on mobile devices makes IoT more powerful but also can increase exposure to risk.

- Lock out accounts after failed log-in attempts
- Enable customer friendly strong authentication mechanisms (e.g. biometrics)

A HOLISTIC APPROACH TO IoT SECURITY

T-Mobile is working to make IoT safer with an end-to-end perspective on security.
We work hand in hand with standards bodies, OEMs, application providers, and at all layers of IoT to set high standards and to actively test security measures. We are committed to giving you the confidence to make the most of your IoT solutions.

To learn more about securing your IoT system on the T-Mobile network, visit T-Mobile.com/business/iot.

T-MOBILE FOR BUSINESS

T-Mobile and the magenta color are registered trademarks of Deutsche Telekom AG. ©2020 T-Mobile USA, Inc.