G+D Mobile Security

G+D Comments

to the

National Institute of Standards and Technolo

(NIST)

G+D Mobile Security
Connectivity and Device Solutions

Version 1.0

March 13 2018

Table of Contents

G+D Mobile Security

G+D Mobile Security has pioneered security solutions to protect businesses, their machines, and data for years, and is at the forefront of providing the most up-to-date and robust cyber security solutions. Today's focus areas for G+D are Intelligent Automation, Cyber Security, and Digital Transformation.

G+D Mobile Security actively manages 3 billion SIM cards and 1 billion mobile devices, and we have issued billions of payment, authentication, and transit cards. In the few months since the commercial launches of the first eSIM enabled consumer devices (e.g. the Apple Watch, the Google Pixel phone, and tablets), G+D has activated and managed more than 2 million eSIM profiles on these kinds of consumer devices – and the number is growing exponentially.

G+D Mobile Security is part of the G+D Group with more than 11,300 employees worldwide. Our Mobile Security staff of 5,800 experts in more than 50 sales and partner offices is available to advise and support your investments. G+D's years of experience and comprehensive solutions empower you to meet the challenges of a connected society and capitalize on it.

About Scott Marquardt

Scott Marquardt joined G+D in September 2009 as President of the US operations and is now driving the IoT Identity Management Solutions for G+D on a global basis. For further background on Scott, see his LinkedIn profile: https://www.linkedin.com/in/scottmarquardt

G+D Mobile Security is a member of the Secure Technology Alliance (STA) which is contributing separately to this draft. Sridhar Ramachandran is the G+D representative on the STA IoT Security Standards and Best Practices Project.

Response to NIST

1.1 Lines 131-140

We would recommend highlighting a different set of IoT Technology Application Areas (somewhat in increasing order of security complexity - although Consumer is still a wild-card for reasons which are described in the document):

1. Track & Trace
2. Consumer
3. Smart Buildings
4. Critical Infrastructure and Remote Sensors
5. Smart Manufacturing
6. Connected Vehicles

The other area mentioned and described later in the document, Health IoT, is in such a nascent state as to possibly not be relevant here (further detailed below).

It may be that Critical Infrastructure is covered in another initiative by NIST. However, as IoT-type devices are increasingly used to capture real-time information from pipelines and grids and other devices that may be used as actuators, some mention should be made of Critical Infrastructure here if only to reference the other initiative.

With respect to Remote Sensors & Meters, these are deployed in large numbers today and are an important class of IoT Device today. Since many are deployed for utilities, they might best be included with Critical Infrastructure.

Track & Trace may be one of the most well-developed areas of the IoT – being used to track truck fleets and shipping containers (with the need for connections to land-based and satellite networks), battery power, and PII-type considerations. Similar systems are deployed to track buses, cars, bicycles, animals, etc.

1.2 Lines 150-153

We would add other relevant aspects of the IoT: battery-powered devices requiring very-low-power functions, often unreliable network connections.

1.3 Lines 251-282

We heartily endorse the perspectives shared here. Security for the IoT is a critical subject today, and solutions must be sought quickly.

1.4 Lines 291-301

We would suggest revisiting this section. There may be other concerns such as safety as well as cost and ease of implementation to consider.

1.5 Lines 329-334

We would re-order and rewrite the foundational concepts (we prefer devices):

1. IoT components (devices) have sensors and/or actuators that allow the components to interact with the physical world (or relay to other components which do). Some are simple (temperature sensor), and others are highly complex (automobile).

2. IoT components (devices) are connected – they can autonomously connect to networks of various types on a continuous or intermittent basis. They also can be “called” into connection.

1.6 Lines 338-380

The description given could be more specific:

Devices connect to gateways, hosts and/or the cloud. They may also connect to other devices, but this is normally only in a mesh network setting. Gateways may also do primary processing and deliver low-latency response when needed (Edge Computing).

The definitions of IoT Environment and System are confusing and the purpose is unclear – especially in the context of cloud-connect. Perhaps it would be more helpful to consider an IoT set-up in terms of the entity which is deploying it:

Enterprise/Agency —> IoT Framework —> Specific IoT Deployment (collection of devices, gateways and host/cloud accounts and data analysis/decision support, etc.)

Primary capabilities are: sensing, actuating, communicating, attaching to networks
Secondary capabilities are: storage, processing, UI and supporting

1.7 Lines 387-447 Primary Capabilities

See notes above as to which should be included and deleted as well as the below points.

Line 401 - We would prefer “communicating” to “networking”. This covers the transfer of data and not the specifics of the network characteristics which are described in lines 434-441.

Line 434 - We would add “authentication:” - Network Interface and Authentication. Network authentication is an essential part of cellular connectivity and should be for other network types. Other forms of authentication should be included in “Supporting” (line 442).

Line 442 - Supporting - We believe that authentication (beyond networks) is more easily implemented than described here, as well as protections for firmware and configuration downloads and updates. Other supporting functions would be Human UI, status-updates, clock synchronization, etc.

1.8 Section 5.1 (beginning line 461)

We would like to give feedback on this at a later date. We have considerable experience with connected cars, the manufacturers of telematics units, and the OEMs.

1.9 Lines 559-569

We fully support the statements here.

1.10 Section 5.3 Health IoT

We propose (as mentioned in the first section) that this area be the subject of a separate document as 1) much if what is described is not part of the Internet of Things, 2) the included aspects are nascent and not mainstream for IoT, and 3) there are specific multi-party considerations which may not exist for other IoT deployments.

1.11 Line 656

Actuating box in the table should include lights (as mentioned later) and perhaps the security alarm.

1.12 Section 5.5 Smart Manufacturing - line 690

Line 698 Diagram: Private M2M cloud may not always be Private. Some implementations are going directly to AWS and other Public cloud providers. IoT Gateway may also do some processing (as noted above).

1.13 Line 717

We fully support the notion of a assured/trusted identity for all IoT components

1.14 Line 728

There are considerable precedents to be found in Digital Rights Management for copyrighted materials which could be noted here.

1.15 Lines 744-5

It is perhaps more likely if the AR Shop Floor training/visual aid system were to be compromised, it would give incorrect instructions or hide necessary instructions rather than creating objects meant to look real.

1.16 Lines 769-780 - Five Pillars

We would suggest a sixth (or include in “Availability”): Controlled Access: The ability to limit access of any component/device without excluding it from the network altogether. This means that devices can be put in “quarantine” until they can be examined or updated. The means for examining/updating remotely must be preserved without the component being able to actuate or initiate communications beyond what is permitted.

1.17 Lines 806-812

In addition to “lightweight” cryptographic techniques, account must be made for the fact that IoT devices are often poorly connected (dropped packets, interrupted connections). This fact might also be inserted into lines 1055-1060.

1.18 Lines 1319-1325

Increasingly the concept of “digital twin” is being adopted (in the cloud) to provide a reference point for any device which loses functionality or connectivity.

1.19 Section 8 - Standards Landscape (beginning line 1675)

A recent development in IoT is the IoT Hub in the cloud services provided by Amazon Web Services, Microsoft Azure, Google Cloud, etc. This section might be reconsidered in light of the new developments.

About G+D Mobile Security

It's a long way to becoming a trusted identity service provider. Don't go it alone. G+D Mobile Security is part of the G+D Group with more than 11,000 employees worldwide. Our staff of 5,800 experts in over 50 sales and partner offices is eager to advise and support you with many years of experience and comprehensive solutions that let you meet the challenges of a connected automotive industry and capitalize on its opportunities.

Giesecke+Devrient Mobile Security America, Inc.
45925 Horseshoe Drive
Dulles, Virginia 20166

Phone: +1 (703) 480-2100
www.secyoure-identity-management.com
www.gi-de.com
info@gi-de.com