HUAWEI TECHNOLOGIES CO., LTD.
Huawei Industrial Base
Bantian Longgang
Shenzhen 518129, P.R. China
Tel: +86-755-28780808
www.huawei.com

Trademark Notice

General Disclaimer

The information in this document may contain predictive statements including, without limitation, statements regarding the future financial and operating results, future product portfolio, new technology, etc. There are a number of factors that could cause actual results and developments to differ materially from those expressed or implied in the predictive statements. Therefore, such information is provided for reference purpose only and constitutes neither an offer nor an acceptance. Huawei may change the information at any time without notice.

Huawei Product Security Baseline

Huawei Practices for Managing Cyber Security

Contents

1. Foreword 01

2. Executive Summary 02

3. Product Security Is Critical to Cyber Security 03

4. Security, a Fundamental Capability Built into Products 04

5. Baseline Application in Huawei Business Processes 04

6. Principles for Baseline Development and Update 08

· Result-based 08

· Universal 08

· Apply to all 08

· Continuously optimized 08

7. Baseline Overview 09

Protecting users' communication content 10

Protecting user privacy 10

Backdoor prevention 10

Prevention of malware and malicious behavior 10

Access channel control 10

System hardening 10

Application security 11

Encryption 11

Sensitive data protection 11

Management and maintenance security 11

Secure boot and integrity protection 11

Security documentation 11

Secure coding 12

Secure compilation 12

Lifecycle management 12

8. Summary 12

1. Foreword

In 2020, the COVID-19 pandemic changed the way we live and how organizations operate. Many activities have gone online, and telecommuting, video conferencing, distance education, and telemedicine have become the new normal. In this context, digital technology has played an irreplaceable role in keeping our lives on track and our businesses open. At the same time, as digital transformation picks up speed, we see growing challenges relating to cyber security and privacy protection. We have witnessed a record number and scale of security vulnerabilities and cyber attacks around the world, with persistent occurrences of ransomware and data breaches. In a digital, intelligent world empowered by 5G, cloud, and AI, a secure and stable cyberspace is critical to securing people's livelihoods and protecting the vital public and economic functions of any society. It is clear that cyber security and privacy protection are becoming the inherent requirements and basic core capabilities in a digital world.

Cyber security is an opportunity for us to promote security and digitization through enhanced cooperation. All stakeholders in the digital space — including governments and regulators, industry and standards organizations, communication service and technology providers, and digital service providers — share a joint responsibility to address cyberspace challenges and improve the level of cyber security. In the case of a cyber attack, every product and service in the cyberspace is exposed to the attack, independent of the supplier. Only by strengthening cyber security protection for the end-to-end supply chain can we more effectively reduce the security risks across the entire network.

As a leading global provider of ICT infrastructure and smart devices, we offer a broad array of products and solutions that apply to diverse scenarios. Effectively managing the security of these products is a huge but surmountable challenge. In order to do so, Huawei has incorporated cyber security management requirements into all its business processes, especially the Integrated Product Development (IPD) process. By integrating product cyber security requirements throughout the planning, design, development, verification, launch, and lifecycle management of the entire IPD process, Huawei is able to ensure that every product and version it releases delivers the expected level of quality in terms of cyber security. The applied management requirements and engineering and technical specifications include the Huawei Product Security Baseline ("the Baseline"), which contains mandatory requirements that Huawei products must meet. Drawing on our extensive experience over the past more than 10 years in product security quality, we continuously update and optimize the Baseline and share its value in ensuring the end-to-end security of the supply chain with our partners, suppliers, and others. Practices show that the Baseline applies not only to Huawei products but also to its entire supply chain. Our security practices over the past more than 10 years also demonstrate that the Baseline is an effective way to manage the quality of product security. The Baseline has ensured a stellar security record of Huawei products on customer networks.

NOTE: The Huawei Product Security Baseline describes the requirements that must be met in order to ensure Huawei products deliver the expected security capabilities. The requirements in the Baseline are a subset of all product security requirements.

Over the past more than 10 years, Huawei has been continuously updating the Baseline in order to address existing and emerging threats. Each update applies only to products developed after the update is released, unless otherwise specified.

2. Executive Summary

We believe that:

• Improving product security is key to mitigating risks of the cyber security incidents that occur frequently worldwide.

• Embedding security management into the product development process and making cyber security a fundamental capability of products is a fundamental approach to resolving cyber security issues.

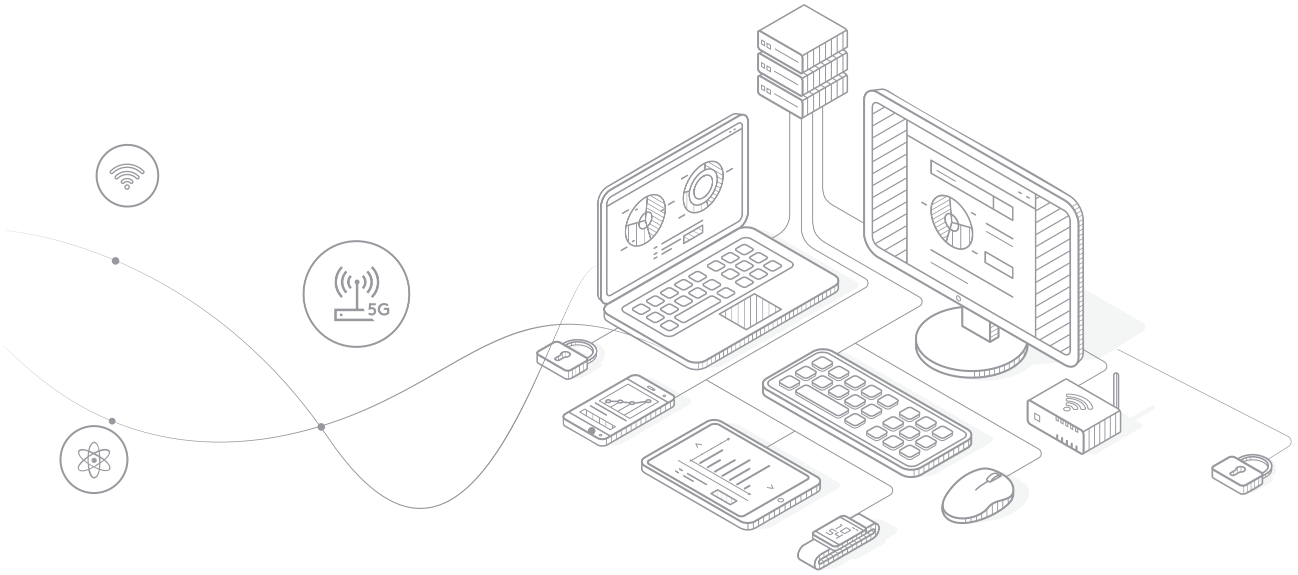
• Developing and implementing a Baseline of common product security requirements ensures that all products meet the same fundamental requirements in terms of the security quality, and the security quality continuously improves as the Baseline is updated.

• Huawei's end-to-end cyber security framework integrates the Baseline into the product development process as a fundamental security requirement. The Baseline and various quality assurance activities are strictly implemented in order to ensure product security quality and prevent security incidents.

Huawei Product Security Baseline:

• Huawei has developed the result-based, universal, applicable-to-all, and continuously optimized Baseline, which is effective, implementable, and verifiable, and continuously improves the security quality of Huawei products.

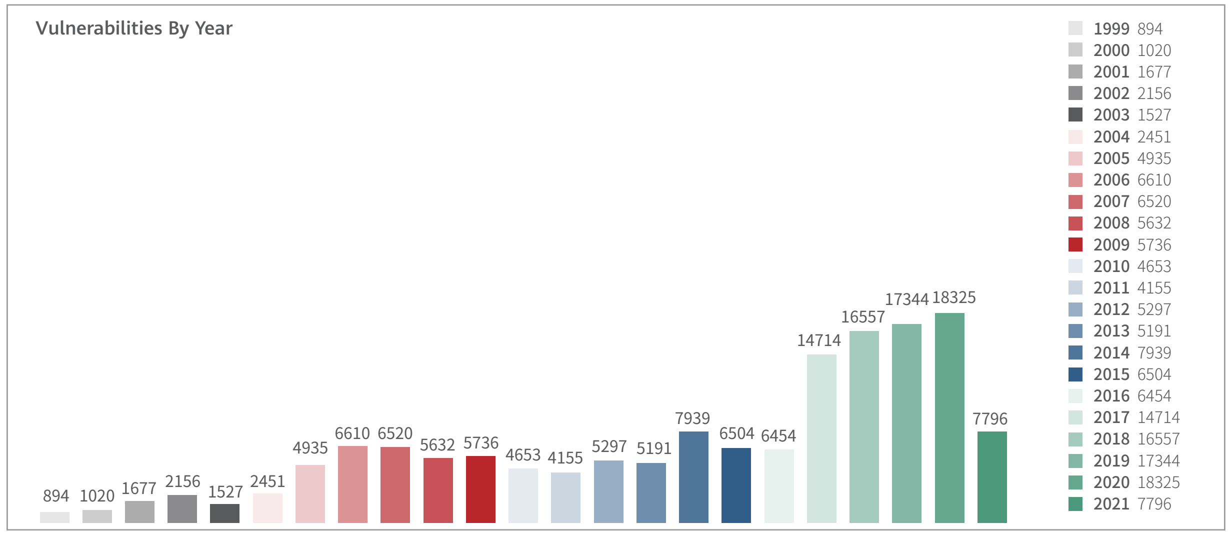
• Huawei has developed the Baseline based on common and critical security requirements identified through its study of applicable laws and regulations as well as its deep understanding of legal and regulatory requirements, customers' business requirements, industry best practices, known issues, and more. The Baseline consists of 54 requirements under 15 categories and 112 entries for implementation guidance and interpretation.



3. Product Security Is Critical to Cyber Security

5G, alongside digitization, not only facilitates the deployment of autonomous driving, smart cities, and smart factories, but also serves as the foundation for human-to-human, machine-to-machine, and human-to-machine connections. While digitalization promotes economic development and fundamentally changes our lives, it also blurs the physical boundaries of traditional networks. As a result, there are more network risks and threats, and the consequences of vulnerabilities and attacks are more serious.

Cyber security incidents occur frequently worldwide, and poor product security is a major cause. Cyber security incidents never cease; for example, the Greek wiretapping incident in 2006, Stuxnet worm in 2010, Heartbleed in 2014, WannaCry in 2017, and Meltdown and Spectre vulnerabilities of processors in 2018.



Sources: CVE Details (https://www.cvedetails.com/browse-by-date.php)

According to the Common Vulnerabilities and Exposures (CVE) statistics[1] shown in the preceding figure, since 2017, the number of security vulnerabilities has exceeded 14,000 each year and is increasing year on year. As systems become more complex, new software frameworks and technologies continue to emerge and develop, and companies use more open-source and third-party components, an increasing number of more complex factors affect product security, posing increasing risks. As a result, the industry is attaching greater importance to product security.

[1] Statistics by June 2, 2021: https://www.cvedetails.com/browse-by-date.php

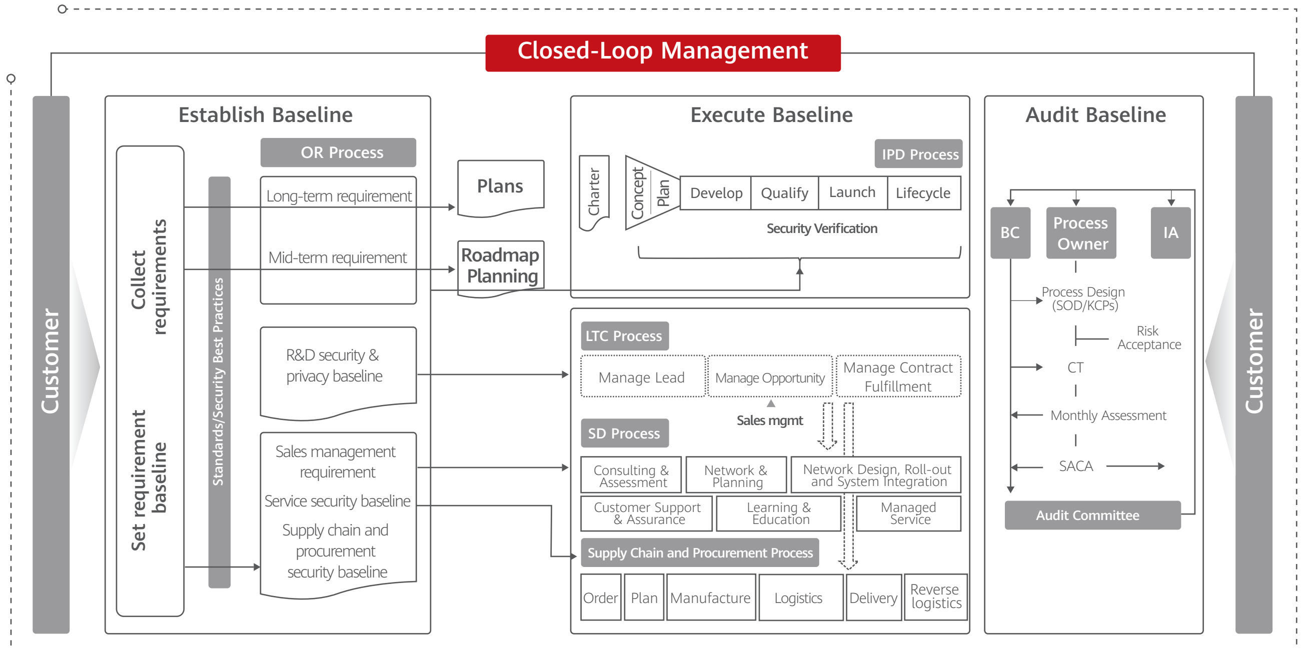
4. Security, a Fundamental Capability Built into Products

Traditional border defense that relies on security products, such as firewalls, security software, and intrusion detection systems, is no longer effective in today's complex security environments. Nor is sufficient to simply fix vulnerabilities promptly, as this cannot effectively address current cyber security challenges given that products have poor security quality and are highly vulnerable.

Today, the industry has agreed that we should implement security by design, and that security should be built into products rather than being only an add-on. To ensure security, in addition to identifying risks and fixing vulnerabilities, it is more important to systematically consider and plan security in the early design phase, and implement security by design throughout the entire development and product lifecycle. Security must be built into products as a fundamental capability in order to resolve security issues in a cost-effective manner.

5. Baseline Application in Huawei Business Processes

We are committed to providing secure, reliable, and high-quality ICT infrastructure and place cyber security as our top priority. Huawei has established an end-to-end cyber security framework (see the following figure) to manage product security based on the Baseline.

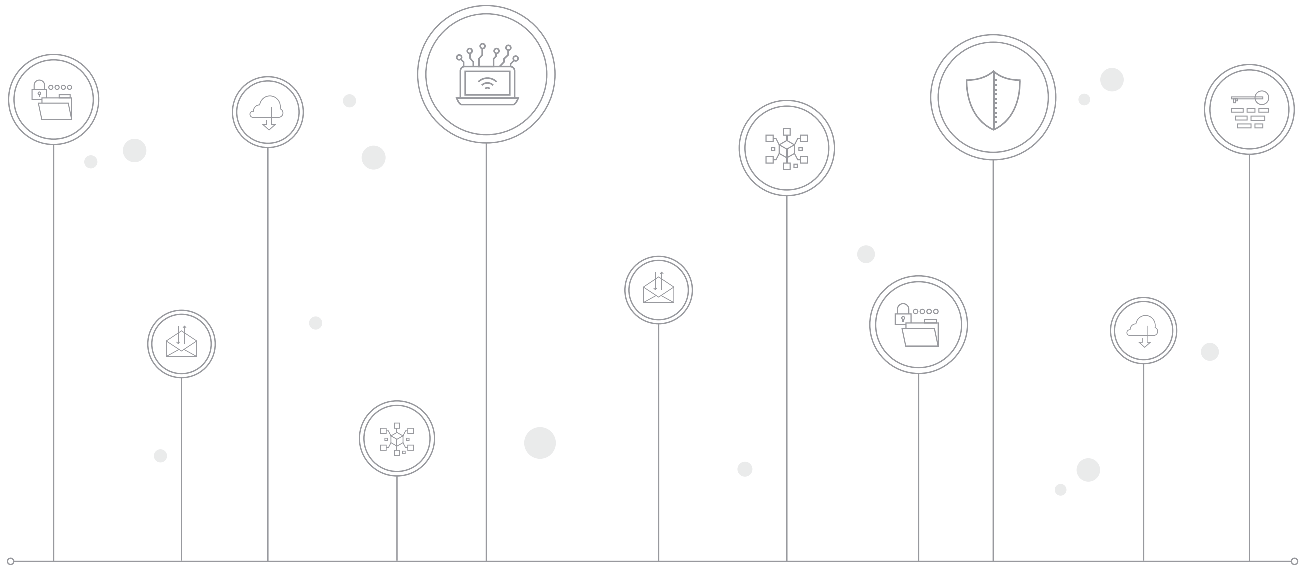


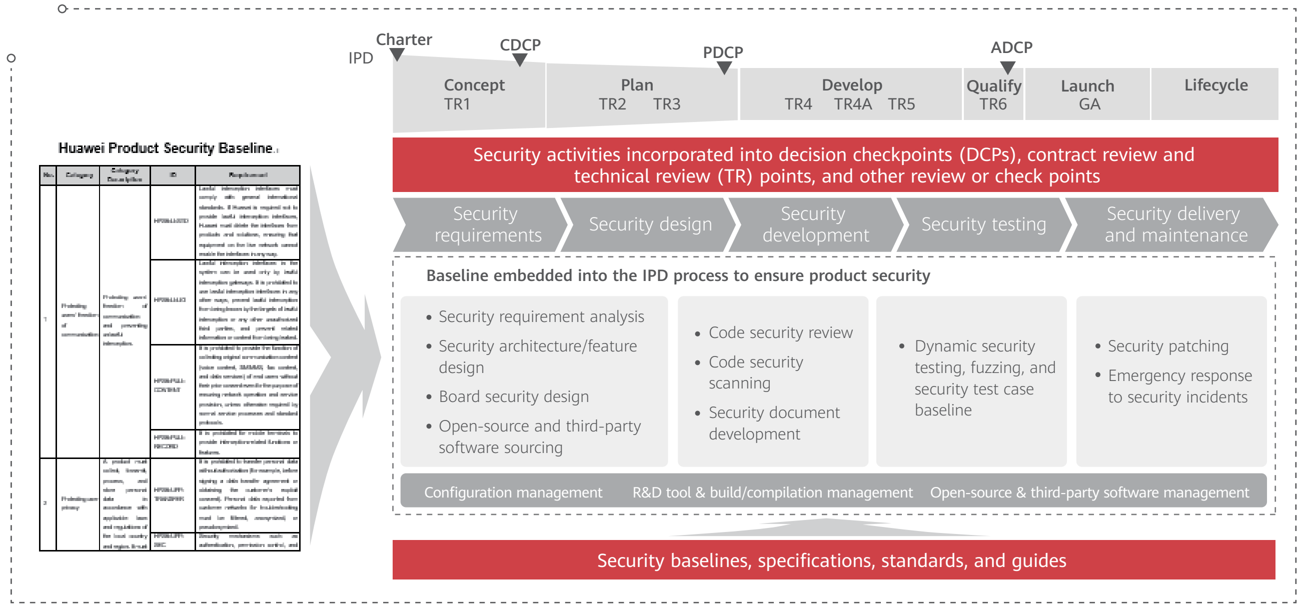
OR: Offering Requirement
IPD: Integrated Product Development

LTC: Lead to Cash
SD: Service Delivery
BC: Business Controller

IA: Internal Audit
CT: Compliance Test
SACA: Semi-annual Control Assessment

We have identified common and the most critical security requirements, developed the Baseline accordingly, and implemented the Baseline across all Huawei products. In this way, we can ensure that all our products meet a consistent set of security quality requirements, and the security quality of our products continuously improves as we update the Baseline. As an integral part of Huawei's end-to-end cyber security assurance framework, the Baseline comprises 54 requirements under 15 categories. It is developed based on a wide range of laws, regulatory requirements, and technical standards, while also conforming to Huawei's product development practices. It ensures that all products and versions we deliver to customers meet stakeholders' fundamental security quality requirements.



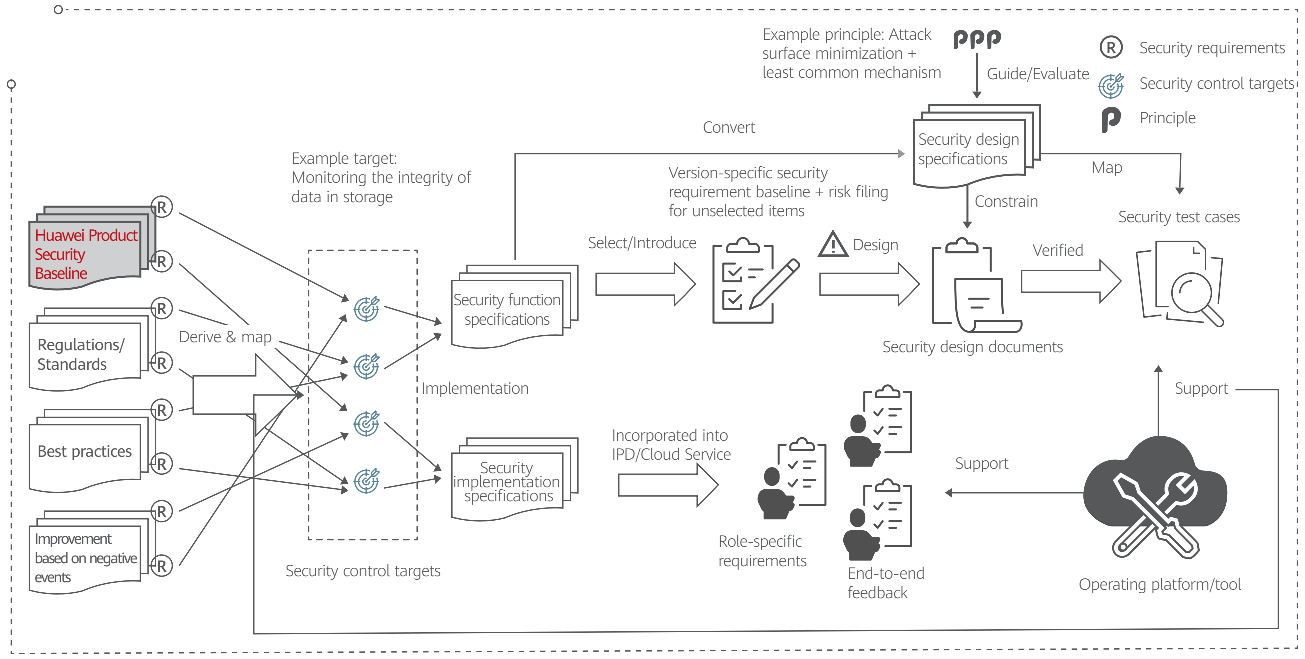

IPD
Charter
CDCP
PDCP
ADCP
Concept
TR1
Plan
TR2 TR3
Develop
TR4 TR4A TR5
Qualify
TR6
Launch
GA
Lifecycle
Huawei Product Security Baseline
Security activities incorporated into decision checkpoints (DCPs), contract review and technical review (TR) points, and other review or check points
Security requirements
Security design
Security development
Security testing
Security delivery and maintenance
Baseline embedded into the IPD process to ensure product security
• Security requirement analysis
• Security architecture/feature design
• Board security design
• Open-source and third-party software sourcing
• Code security review
• Code security scanning
• Security document development
• Dynamic security testing, fuzzing, and security test case baseline
• Security patching
• Emergency response to security incidents
Configuration management
R&D tool & build/compilation management
Open-source & third-party software management
Security baselines, specifications, standards, and guides

As shown in the preceding figure, Huawei has embedded the Baseline into its Integrated Product Development (IPD) process as a fundamental security requirement. In this way, the Baseline is executed repeatedly rather than randomly. All roles and organizations involved in the IPD process must strictly comply with the Baseline throughout the product lifecycle.

1. The GSPO/GSPO Office is responsible for developing, releasing, and continuously optimizing the Baseline. They analyze laws, industry standards, industry best practices, customer requirements, industry cases, and the latest developments in security technologies to identify the most critical requirements and continuously update the Baseline accordingly.

2. Each domain updates related policies, processes, and procedures to keep consistency with the updated Baseline.

3. As one of the inputs, the Baseline is used by the R&D to develop and update the technical standards, specifications, templates, and guides. We provide appropriate training and awareness education when needed, in order to standardize and guide product design and development.


Example principle: Attack surface minimization + least common mechanism
Guide/Evaluate
Security requirements
Security control targets
Principle
Convert
Security design specifications
Map
Constrain
Security test cases
Example target: Monitoring the integrity of data in storage
Version-specific security requirement baseline + risk filing for unselected items
Select/Introduce
Design
Verified
Huawei Product Security Baseline
Regulations/ Standards
Derive & map
Security function specifications
Security design documents
Implementation
Support
Best practices
Incorporated into IPD/Cloud Service
Security implementation specifications
Support
Improvement based on negative events
Role-specific requirements
End-to-end feedback
Operating platform/tool
Security control targets

As shown in the preceding figure, we regard the Baseline as external requirements. Based on the Baseline, external regulations and standards, as well as internal and external best practices, we have developed our own specifications that the products must abide by during R&D, thereby developing product security capabilities in an efficient and standardized manner.

4. Each business department implements the Baseline; reviews, makes decisions on, executes, and monitors it in the business and decision-making systems; and backtracks Baseline violations and holds related personnel accountable.

5. Before a product version is released, Huawei's Independent Cyber Security Lab (ICSL) verifies whether it meets the Baseline requirements from the customers' perspective. If it does not, the GSPO has the right to veto its release.

6. Huawei manages the identified issues from start to finish, thus cyclically improving the Baseline and corresponding management mechanism.

6. Principles for Baseline Development and Update

To ensure that the Baseline is effective, implementable, and verifiable, and that it continuously improves the security quality of products, we comply with the following principles to develop and manage it:

Result-based

Only result-based requirements are objective and verifiable. Result-based product security requirements ensure that products achieve expected objectives, and help customers compare and select required products based on the objective results.

Universal

Requirements specified in the Baseline must be common and applicable to all or most Huawei products. This ensures that all Huawei products meet a consistent set of fundamental security quality requirements.

Apply to all

Today's supply chain spans the entire globe. To ensure the security of all systems and infrastructure, we must apply the same set of fundamental security standards equally to all suppliers (regardless of when and where the product is produced) and product components (regardless of the physical location, network, or network position of the deployment).

Continuously optimized

Cyber security is a dynamic process. Therefore, the Baseline must be continuously and regularly updated to adapt to the ever-changing cyber security environment.

7. Baseline Overview

Based on the analysis and summary of laws, regulations, standards, specifications, and security practices, Huawei developed the Huawei Product Security Baseline and dynamically updates it with the development of cyber security and Huawei's practices. The latest version is the Huawei Product Security Baseline V3.0 released in 2020.

Huawei Product Security Baseline	
1. Protecting users' communication content	4
2. Protecting user privacy	7
3. Backdoor prevention	5
4. Prevention of malware and malicious behavior	2
5. Access channel control	5
6. System hardening	4
7. Application security	3
8. Encryption	5
9. Sensitive data protection	4
10. Management and maintenance security	5
11. Secure boot and integrity protection	2
12. Security documentation	3
13. Secure coding	2
14. Secure compilation	1
15. Lifecycle management	2

The Baseline consists of 54 requirements under 15 categories. To facilitate the accurate understanding and implementation of the Baseline in different Huawei products and scenarios, we have developed 112 entries for implementation guidance and interpretation.

Protecting users' communication content

In many countries, users' communication content is protected by law. Huawei strictly complies with industry-wide security standards in product design to ensure communication data security.

Protecting user privacy

Huawei has analyzed the European General Data Protection Regulation (GDPR) and other privacy laws and regulations of different countries, such as Germany, France, the UK, Canada, and China. Based on the analysis and industry practices, such as the GSMA's Privacy Design Guidelines, Huawei has summarized seven basic privacy protection principles to guide product design and development: lawfulness, fairness and transparency; purpose limitation; data minimization; accuracy; storage limitation; integrity and confidentiality; and accountability.

Backdoor prevention

Huawei will never implant or allow others to implant backdoors in its equipment.

Prevention of malware and malicious behavior

Huawei does not allow products to contain malicious software such as viruses and Trojan horses, or malicious behavior such as malvertising, fee-absorbing, and malicious traffic consumption.

Access channel control

Huawei uses several ways to control access channels, such as isolation and authentication, to effectively reduce the attack surface and secure product access.

System hardening

Security hardening is performed on products by configuring security features and functions, installing patches, and removing or disabling unnecessary services, to improve product security and anti-attack capabilities.

Application security

Various applications, such as web and mobile applications, are vulnerable to attacks by hackers and malware, resulting in unauthorized access and modification. Authentication and authorization are basic security protection mechanisms for applications.

Encryption

Cryptographic algorithms are the basis of security and using them correctly is critical to product security. Only public, professionally reviewed, verified, and secure cryptographic algorithms, as well as correct algorithm parameters and options, can be used.

Sensitive data protection

During product design, sensitive data in the product must be identified based on possible applications. Typical sensitive data includes authentication credentials (such as passwords, private keys, and dynamic tokens), encryption keys, and sensitive personal data (such as bank accounts and users' communication content). Security mechanisms, such as authentication, authorization, and encryption, must be used to secure data in storage, transmission, and processing.

Management and maintenance security

Various security mechanisms, including strict account password verification, secure access protocols, and complete log auditing, are used to ensure product operation and maintenance security.

Secure boot and integrity protection

Software package integrity is verified during product installation and upgrade to prevent tampering. For products that are expected to deliver high security, secure boot verification must also be considered during product startup.

Security documentation

Product documentation must include security documentation, such as a communication matrix, list of accounts, and security hardening and configuration documents, in order to help customers deploy, use, and maintain products in the most secure way.

Secure coding

Generally, a large number of security vulnerabilities are caused by code quality defects, such as non-standard coding, improper understanding of programming language features, and improper interface invocation. These defects can be identified through routine static code security and quality scanning, and by minimizing unsafe functions. This can improve the quality of code and reduce potential security vulnerabilities.

Secure compilation

The compiler provides a variety of security options to harden software security. Enabling compiler security options in software hardens the security of code quality. It also makes it more difficult for attackers to launch an attack, thus reducing the risk of code quality defects becoming exploitable vulnerabilities.

Lifecycle management

Product software shall use open-source and third-party components that have a good security record and are within their lifecycle. Any vulnerability shall be promptly fixed through patching or upgrading, in order to control the security of the product software throughout the software lifecycle.

8. Summary

Today, cyber security is an opportunity for us to promote security and digitization through enhanced cooperation. All stakeholders in the digital space — including governments and regulators, industry and standards organizations, communication service and technology providers, and digital service providers — share a joint responsibility to address cyberspace challenges and improve the level of cyber security.

Huawei's experience demonstrates that the Baseline is an effective way to manage cyber security, and it has helped us ensure a stellar security record of Huawei products on customer networks. We are happy to communicate and discuss the Baseline with all stakeholders — including operators, enterprises, upstream and downstream supply chain partners, and government regulators — on details of security management, engineering and technical specifications, and testing and verification solutions. In this way, we can continuously optimize our Baseline and promote cyber security of the end-to-end supply chain.

Cyber security is a never-ending journey. As we continue to emphasize: "Security, We Do More."