ZTE

Vision of Intrinsic Cybersecurity Beyond 2030

June 2021

ZTE

CAICT 中国信息通信研究院

中国移动 China Mobile

中国电信 CHINA TELECOM

China unicom 中国联通

奇安信

Joint Publishers (listed in no particular order):

ZTE Corporation

China Academy of Information and Communications Technology

China Mobile Communications Group Co., Ltd.

China Telecommunications (Group) Co., Ltd.

China Unicom Network Communications Co., Ltd.

QI-ANXIN Technology Group Inc.

Authors and Editors (listed in no particular order):

Lu Ping | Wang Jigang | Wang Qing | Ge Linna | Yang Hongmei | Feng Zebing

Jiao Yang | Zhang Feng | Qiu Qin | Yu Le | Zhang Hongyang | Xu Lei

Ma Zheng | Zhang Manjun | Wang Shanshan | Liu Yatian | Xu Hao | Hu Bowen

He Guofeng | Jin Huamin | Wang Jinhua | Huang Chengbin | Qiao Siyuan | Luo Hailong

Li Na | Su Zhu | Wang Fei | Yan Xincheng | Hao Zhenwu, et al

Contents

01 Preface

02 Driving Force

03 Definition

04 Vision

05 Requirements

06 Evolution

07 Conclusion

08 References

Preface

2020 has been a unique year for mankind. With the coronavirus outbreak, great changes have taken place in people's life, including surging demands for telecommuting and online education. The increasing reliance on science and technology, especially mobile communications networks, has made cyberspace the fifth space for human activities, besides space, air, sea, and ground. Networks have become indispensable in today's society.

Against such a backdrop, new infrastructure and digital transformation have been on the march. 5G is rapidly empowering thousands of vertical industries and DOICT convergence is accelerating, making networks more important and valuable. Value increase always requires more reliable security. Therefore, cybersecurity has been in the spotlight of all industries, becoming a basic requirement that determines whether a network can give full play to its potential. Currently, human beings have entered a new era of security.
From 1G to 5G, each generation of mobile communications network has its unique characteristics. Before 4G, due to the closed network architecture, network security can be guaranteed by fulfilling the requirements specified in related standards. When it comes to 5G, the Service-Based Architecture (SBA) and new technologies such as NFV, network slicing, and edge computing have greatly enhanced network service capability and enabled 5G networks to support eMBB, mMTC, and uRLLC. Besides, more business and applications have been migrated to the cloud and the Internet of Everything (IoE) is in full swing. All these changes greatly accelerate the development of mobile communications technologies, making them applied in more fields. The open architecture, introduction of new technologies, cloud-network convergence, and scenario-based applications in various industries expose networks to more complicated security risks. In view of market demands, especially those generated from vertical industries and during network construction, there is still a long way ahead in cybersecurity despite the improvements that have been made in 5G standards.

At the same time, the research on 6G has started across the globe. The space-air-ground-sea network convergence and the soaring development of technologies such as communications technologies, supercomputing, AI, and perception will definitely generate higher requirements for network trust models, security access, data storage, and emergency handling. However, the traditional distributed, plug-in, or patched security defense models in the IT field cannot meet the increasing demands. Cybersecurity requirements and standards need to be changed and innovated, and should be fully considered at the beginning of network building.
In July 2020, ZTE officially proposed a new intrinsic cybersecurity concept for 5G and future networks at GSMA Thrive. In light of the working principle of the human immune system, secure networks that ZTE delivers have a self-protection mechanism of basic immunity and self-learning adaptation. At GSMA Thrive, ZTE also called on the industry to jointly conduct research and exchange ideas, which arouses great attention in the industry.

Building intrinsic cybersecurity needs long-term research, exploration, practices, and verification. This white paper outlines the network architecture beyond 2030, elaborates on the vision of intrinsic cybersecurity for future networks, defines intrinsic cybersecurity, describes relevant requirements, and proposes three phases of evolution, to provoke discussions and new thoughts in the industry.

At present, the construction of 5G is in full swing, while research on 6G is still in the initial stage. In the future, ZTE will continue to work with the industry to promote the building of intrinsic cybersecurity systems and research on potential technologies, and make contributions to the sustainable development and evolution of networks.

Driving Forces

Social Development

Sustainable development is the common aspiration of mankind. The mobile communications network has redefined the operation of society and way of life. For example, the network helps people face up to the COVID-19 in 2020:

- Online education could be provided to children.
- Doctors could diagnose diseases online and even carry out operations on patients.
- Cloud applications and remote automated production ensured the normal operation of the industry.
- People could work from home and shop online through e-commerce platforms.

In the future, the network will be deeply integrated with the industry, economy, education, and other aspects of our life, and security is the foundation for such integration.

Technology Evolution

Driven by the rapid development of society, various networks are converging, including the existing Internet, mobile communications network, Internet of Things (IoT), and Industrial Internet, with the convergence of space-air-ground-sea networks becoming inevitable. The future network gains great computing power and intelligence from technologies, including the mobile technology, cloud technology, big data, and artificial intelligence. Security technologies and new concepts including Zero Trust, Software-Defined Security (SDS), Cloud Native, and Secure Access Service Edge (SASE) continue to emerge. The traditional patch defense is not systematic and far from bringing into full play the potential of a single technology, nor can it promote the healthy development of new technologies. Therefore, we are in urgent need of establishing an "always in response" security system based on top-level design.

Business Model

Immunity is the main force to resist diseases. The immune system can help the body heal itself with the support of medical treatment. The importance of immunity has been proved by thousands of years of experience, indicating that if we only deal with existing problems and ignore their causes, we will be unable to cure and prevent diseases. Only by carrying out in-depth studies on the operation, immune system, and capacities of human bodies can we cure diseases efficiently. This kind of wisdom is also applicable to the network. The only difference is that an infant's immune system starts to form in its mother's womb, but the immune system of the network needs to be built by intelligent network experts. In the future, based on the network immune system, the cybersecurity industry chain and services will develop in the same way as the medical system, and the business models of cybersecurity will develop and evolve in a healthy, positive, and sustainable manner.

Definition

The term "intrinsic security" has already been created in the biological field years ago to describe the feature of the biological immune system, and used in the technology, IT field, and CT fields. However, no consensus has been reached on its standard definition. Intrinsic security can serve as a new security concept and even a new model for the network and inspire us to recognize and view cybersecurity issues once again from the new perspective of "focusing on problems within the system.", that is, "turning inward and thinking inward."

Inspired by human biology and based on the research of predecessors from other fields, a clear definition of "intrinsic cybersecurity" is given in this White Paper: Intrinsic cybersecurity is a comprehensive capability of the network, consisting of a series of security capabilities that work together to form a self-perceptive, self-adaptive, and self-evolving network immune system. The intrinsic cybersecurity system should be built during network construction, and can adapt to network changes, and evolve dynamically, thus ensuring the security of the network, services, and data.

According to the definition, intrinsic cybersecurity has two basic features: congenital construction and postnatal growth. Congenital construction means that the intrinsic cybersecurity system should be designed and built during network construction, similar to a baby that already has a basic immunity system at birth. Although it might not be strong enough, it can provide a basic mechanism and environment for the subsequent development of immunity. Postnatal growth mainly refers to the improvement of security capability and its adaptation to the network. Immunity constantly improves and adapts to the environment during evolution, which is also similar to the immunity of a baby.

According to the definition, intrinsic cybersecurity has two key functions: convergence and immunity. Convergence refers to the comprehensive convergence of cybersecurity and the functional network in all aspects at all phases, including standard formulation, top-level design, construction, and operation and maintenance. Immunity refers to the complete closed-loop processing of feedback and response to malicious attacks and active information, thus protecting network data from leakage, tampering with, and repudiation throughout its lifecycle.

The design of the architecture of the future network is a prerequisite for depicting the vision of intrinsic cybersecurity. As the fifth space for human activities, the architecture of the future network will completely evolve into a new convergent network. This convergence is reflected in multiple dimensions: the complete convergence of DOICT, of the cloud, network, edge, and terminal, and of space-air-ground-sea networks. In the future, the concept of network will also change. It will become a virtual social space composed of terminals, networks, and management, which can be called a universal network. The current traditional network will become a part of the connection in the universal network. The future network will adopt a flat, layered, and decoupled architecture. We should perceive and find the nature of the future network for a deeper understanding and outlook from a new perspective.

In the future, intrinsic cybersecurity will exist as the basic capability of the universal network. Similar to the human immune system, a network with intrinsic cybersecurity consists of functional networks, management, and security. Security is not only deeply integrated with the network, but also becomes a complete and independent security plane. Integrated identification and trust system will be the cornerstone of the future network and intrinsic cybersecurity. Through the cooperation of the three lines of defense, namely boundary, network function, and the whole network, as well as the self-evolving, self-adaptive, and self-evolving functions, a convergent and intrinsic cybersecurity system can be realized.

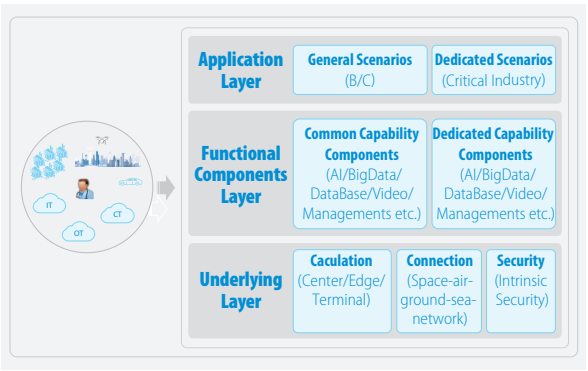

Figure 1 Architecture of Future Network

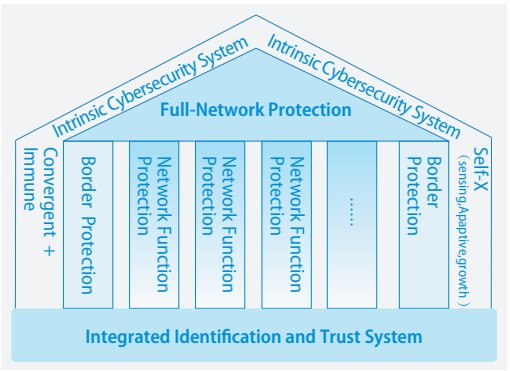

Figure 2 Intrinsic Cybersecurity System

Requirements

From the perspective of its functions, intrinsic cybersecurity should support the development of both networks and vertical industries. In addition, security itself needs to be secure. Therefore, requirements for intrinsic cybersecurity can be divided into three categories: security of business, services of security, and security of cybersecurity.

Security of business means that the intrinsic cybersecurity should guarantee the security of the underlying layer (network and computing power), capability component layer, and application layer, covering such capability components as software and hardware, transmission, operation, big data, and AI, as well as various industry scenarios (such as autonomous driving).

Services of security means that the intrinsic cybersecurity should provide security services related to security capabilities and security management for the application layer, for example, adaptive security for the stop of services and automatic orchestration of security capabilities for the launch of new services.

Security of cybersecurity means that intrinsic cybersecurity should guarantee its own security. The more exposed surfaces a system has, the greater security risks are likely to occur. Therefore, complying with the rule of simplicity, intrinsic security should be deeply integrated into the network with simplified and higher-performance devices, including software, hardware, and ports.

From the perspective of the construction and evolution of intrinsic cybersecurity, the congenital system should keep pace with the development of the network system, including standards formulation, top-level design, solution design, and product design.

Moreover, there should be reasonable and measurable classification and measurement standards for intrinsic cybersecurity.

Evolution

Currently, the existing network features the rapid convergence of multiple heterogeneous networks, and cloud-network convergence is accelerating in the 5G era. Against this background, the intrinsic cybersecurity is predicted to experience three phases of evolution.

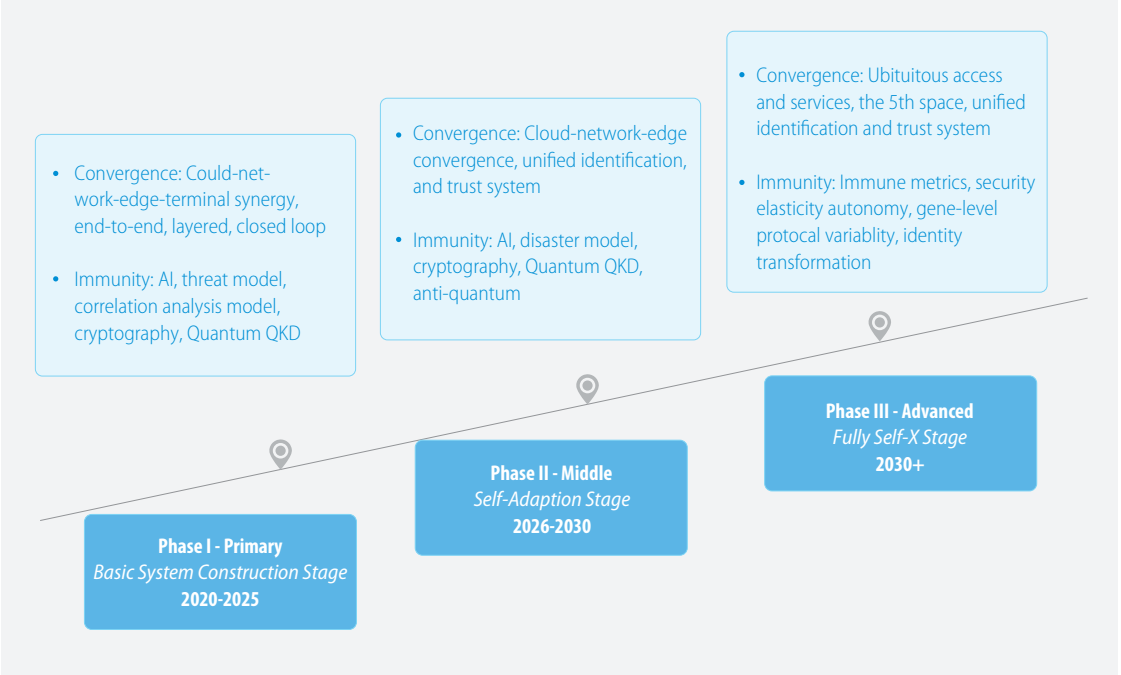

Figure 3 Evolution Phases of Intrinsic Cybersecurity

Phase I (2020-2025): This is the primary stage of intrinsic cybersecurity. In view of the current situation of existing networks, this phase aims to construct a basic end-to-end, layered, and closed-loop intrinsic security system under an architecture featuring cloud-network-edge-terminal synergy. Specifically, current security capabilities will be re-constructed in the following aspects:

- Develop edge security capabilities through such technologies as SDS and zero trust;
- Realize network functions with underlying security capabilities based on SDS, NFV, and cloud technologies;
- Build data security capability through cryptography and QKD technologies;
- Construct the whole cybersecurity linkage based on SIEM, correlation analysis, and APT technologies;
- Develop immunity based on AI, threat model, and correlation analysis model.

In this stage, cybersecurity will evolve from external divergent and uncontrollable construction to convergent and planned construction.

Phase II (2026-2030): This is the middle stage of intrinsic cybersecurity. Based on the congenital system constructed in Phase I, this phase will focus on the construction and development of the acquired adaptability, which in turn promotes the perfection and maturity of the congenital system. With an architecture characterized by cloud-network-edge-terminal convergence, the intrinsic cybersecurity system will develop its mature adaptability. Based on unified identification, the trust system using distributed technology can be constructed to further promote the convergence. On the basis of the construction in Phase I, the security capabilities of edge and network function will be deepened towards intelligence and collaboration. Furthermore, network immunity will be improved based on AI and cyberspace disaster model. In the self-adaption stage, manual intervention is needed while cybersecurity construction is gradually being convergent and under control.

Phase III (after 2030): This is the advanced stage of intrinsic cybersecurity. After Phase I and Phase II, a sound and convergent congenital system of intrinsic cybersecurity will be developed with a high degree of immunity. In Phase III, intrinsic cybersecurity will in turn promote the evolution of network architecture. With a terminal-network-management model, the convergent system of the fifth space is finally built based on a unified identification system. Cybersecurity skills such as supporting protocol-level changes and identity changes will be used to adapt to security demands. Network immunity can also be quantified. Resilient and autonomous security will be realized without manual intervention in most cases, which means that cybersecurity will be completely and systematically convergent.

Conclusion

As the purposes and means of cyber-attacks are changing constantly, security risks are also diversifying. Unlike the traditional security system, which develops only for responding to cyber-attacks or risks, the intrinsic cybersecurity system endows the network with security capabilities similar to human immunity. Therefore, intrinsic cybersecurity is regarded as a revolutionary concept or even a network security model.

Looking back on history, the major scientific and technological changes in human society are driven by various factors such as society, economy, philosophy, humanity, and technology. Likewise, technology cannot alone promote the future development of networks and cybersecurity. It is necessary for us to think in a broader perspective and long term. Human's immune system has undergone thousands of years of development and is still improving. To develop the intrinsic cybersecurity system, we still have a long way to go. Together with CAICT, China Mobile, China Telecom, China Unicom, QI-ANXIN Technology Group Inc., and all of our partners, ZTE will continuously explore and practice intrinsic cybersecurity to promote the sustainable development of networks and make great progress for a better world.

References

1. Cyberspace Endogenous Safety and Security, Jiangxing Wu
2. An artificial immune system architecture for computer security applications. [J]. Paul K. Harmer, Paul D. Williams, Gregg H. Gunsch, Gary B. Lamont. IEEE Trans. Evolutionary Computation. 2002 (3)
3. New Global Digital Economy Landscape (2020) -- New Dynamic Function of Sustainable Development Under the Great Changes, CAICT, October 2020
4. 5G Security Report, CAICT, February 2020
5. Vision and Requirement Report of 2030, China Mobile CRMI
6. White Paper of 2030 Cloud & Network Convergence Technical Report, China Telecom
7. White Paper of CUBE-Net3.0 Network Innovation System, R&D Institute of China Unicom
8. The New Generation of Enterprise Network Security Framework, QI-ANXIN Technology Group Inc., Xiangdong Qi, Siyuan Qiao
9. 5G Intrinsic Security: Where to Go? Research, Construction, and Thinking about Intrinsic Cybersecurity of 5G and Future Networks (Part I), ZTE, Linna Ge, Jigang Wang, Qing Wang
10. Network Immune System: Starting from the Design Closing to the Network Essence. Research, Construction, and Thinking about Intrinsic Cybersecurity of 5G and Future Networks (Part II), ZTE, Linna Ge, Jigang Wang, Qing Wang
11. Intrinsic Security of Could-network in 5G Era, ZTE, Jigang Wang, Linna Ge
12. Intrinsic Cybersecurity of 5G and Future Network, ZTE, Linna Ge, Jigang Wang
13. 6G Conference-Intrinsic Security Classification and Key Technologies, Xincheng Yan

ZTE ZTE CORPORATION

NO.55, Hi-tech Road South, ShenZhen,P.R. China Postcode:518057
Website:www.zte.com.cn Tel:+86-755-26770000 Fax:+86-755-26771999