

Report on ITU Workshop on "Zero Trust and Software Supply Chain Security"

28 August 2023

Heung Youl YOUM, ITU-T SG17 Chairman

Presentation Summary – Session 1: Need, security issues, threats and controls for zero trust

- **Moderator:** Zhiyuan Hu, WP2 Vice-Chair and Q2 Co-Rapporteur, ITU-T Study Group 17, Security | Director, Security Research, vivo Mobile Communication Co. Ltd.
- **Presentations**
 - Martin Goldberg, 5G Cybersecurity Standards Lead, U.S. National Security Agency: “The Need for Zero Trust in 5G”
 - Sokjoon Lee, Professor, Department of Computer Engineering (Smart Security), Gachon University, Korea (Rep. of): “Zero trust, how to understand the paradigm”
 - Junzhi Yan, Co-rapporteur of ITU-T SG17 Q6 I Senior Researcher & Project Manager, China Mobile Research Institute | Editor of TR.zt-acp: " Zero Trust and Practice in Telecommunication Networks"
 - Francesco Chiarini, Chairman, ISSA.org Cyber Resilience Special Interest Group: " High Value Targets: Adversarial Viewpoint on Software Misuse"
 - Manoj Sharma, Global Head, Security Strategy Symantec Enterprise Division, Broadcom: “Zero Trust - A customer and Vendor Perspective”
 - Sounil Yu, Author, Cyber Defense Matrix: “Understanding Zero Trust through the Cyber Defense Matrix”
 - Ilia Gerasimov, Researcher, Cryptography Lab, JSRPC “Kryptonite”: "Anonymous authentication for mitigation extended attack surface in zero trust systems"

Session 1: Takeaways and suggestions (1/3)

Takeaways and conclusions

- NIST released SP 800-207 Zero Trust Architecture (ZTA), which includes 7 tenets of zero trust. It's suggested that the guidance in SP 800-207 needs to be adjusted for 5G System.
- The concept of Zero Trust, common understanding for Zero Trust, misconceptions and how to understand the paradigm are elaborated.
- With the evolution of telecom networks, security boundary is becoming vague, and traditional passive static security defense methods are no longer sufficient. Zero trust is a good approach to improve identity management for O&M System in telecom networks and to secure service access between multiple clouds.

Suggestions to ITU-T SG17

- SG17 is developing TR.zt-acp, *Guidelines for zero trust based access control platform in telecommunication networks*, with introducing zero trust to telecom networks.
- More studies on zero trust in 5G system and telecom networks are welcome to SG17 in the future.

Session 1: Takeaways and suggestions (2/3)

Takeaways and conclusions

- High value targets and their categories & attributes are introduced. Threat scenarios to high value assets are also described. It's recommended to increase understanding of cyber terrain by applying with high value target methodology.
- Zero trust is accepted as a layered Security Framework with several approaches, such as, access centric ZT and data centric ZT. From the perspective of vendors, a vision of zero trust architecture is given. A use case, i.e., zero trust for software supply chain security to build trust with vendors, is also elaborated.

Suggestions to ITU-T SG17

- Zero trust for software supply chain security to build trust between customers and vendors is a potential topic for SG17.

Session 1: Takeaways and suggestions (3/3)

Takeaways and conclusions

- Cyber defense matrix serves as the foundation for CISA's Zero Trust Maturity Model. All types of requesting entities (e.g., devices, applications, networks, data, users) have an identity, which enables to determine the level of trustworthiness based on the strength of the identity attributes. It's suggested implementing "zero trust" access proxies that can consume the broader set of identity attributes for access decisions.
- Zero trust security model (e.g., OpenID, OAuth, FIDO UAF) has been applied to personal data protection. However, there may be message linkability for extending attack surface during personal data exchange zero trust systems. X-protocol is proposed to reduce such an attack surface.

Suggestions to ITU-T SG17

- It's suggested studying how to apply zero trust to network access and application access in SG17, with cooperation and coloration with CISA, which have defined Zero Trust Maturity Model.

Presentation Summary – Session 2: Need, security issues, threats and controls for software supply chain security

- **Moderator:** Jonghyun Kim, WP1 Vice-Chair and Q4 Co-Rapporteur, ITU-T Study Group 17, Security | Principal Researcher, Electronics and Telecommunications Research Institute (ETRI).
- **Presentations**
 - Zero Trust are key functions of Critical SW security measures and Secure Software Development Framework(SSDF).
 - Difficulty of generating the precise SBOM exists and the exploitability of vulnerability found is very hard to be determined in a systematic way
 - One of Essentials for SBOM Management is FOSSLight Open Source Project that provides an automation for SBOM generation and management.
 - SBOMs are key elements of the EU's policies for provision of cybersecure products and services to the market.
 - Framework of security inspection for supply chain and suggestion to ITU-T Standardization such as a new use case of attribute certificates were discussed.
 - SBOMs are part of the initiative to enforce transparency and explainability on products containing digital elements

Session 2: Takeaways and suggestions

Takeaways and conclusions

- Automation for SBOM generation and management is important
- It is difficult to determine the minimum unit of SBOM component.
- Implementing Zero Trust is necessary for better supply chain security
- Ensuring the security level of the entire supply chain and automating inspection with conformance validation
- Addressing the software supply chain must align and integrate with smart device supply chains
- Trust, visibility, and integrity needs to be conveyable across all supply chains

Suggestions to ITU-T SG17

- Consider to make a guideline for SBOM component unit such as the necessary for commercial software or self-developed software and so on
- Collaborate with other groups and organizations in order to overcome these technical challenges?
- Consider to make a new use case of X.509 Attribute Certificates for SBOM
- Consider to make automation guidelines to capture and convey assurance attestations across supply chains for smart devices and standalone software.

Presentation Summary – Session 3 Implementation of zero trust and software supply chain security

- **Session 3:** Implementation of zero trust and software supply chain security
- **Moderator:** Afnan AlRomi, Communications, Space & Technology Commission (CST), Saudi Arabia | Vice-chair, ITU-T Study Group 17
- **Presentations:**
 - **Sheeba Baskaran**, Advisory Researcher - Lenovo, Motorola Mobility | Rapporteur for the 3GPP SA3 ZT TR
 - **Tim Ashton**, Policy lead, U.K. National Cyber Security Centre (NCSC)
 - **Ray Sung Joon Ahn**, Director of Marketing, Sparrow Co., Ltd
 - **Chen Zhang**, R&D Director of Security, China Mobile Group Design Institute
 - **Youngrang Kim**, CEO/CTO, PRIBIT Technology
 - **Cassie Crossley**, VP, Supply Chain Security, Schneider Electric
 - **Dmitry Raidman**, CTO, Cybeats
 - **Jini SungJin Park**, Director/Embedded Solution Team/Solution Business Division, COONTEC

Session 3: Takeaways and suggestions (1/2)

Takeaways and Conclusions


- As a summary (what and why):
 - **Zero Trust:** Do not trust anything and validate everything → goal protecting network and resources.
 - **Software Supply Chain:** Do not trust code you did not build → goal protecting software.
- Implementing zero trust comes with great benefits, but take care not to open your network and systems to unintentional risks by removing traditional security measures before suitable controls are in place.
- Software supply chain comes with new challenges in computing force network (CFN):
 - Sparsely Distributed CFN resources & components
 - Heterogeneous platforms & Diverse hardware devices
 - Additional risks from service supply chain

Suggestions to ITU-T SG17

- Study the cybersecurity threats and risks related to Zero Trust and Software Supply Chains.
- Issue guidelines and models on Zero Trust Architectures, like Software Supply Chain Security Architecture based on Zero Trust.
- Consider developing guidelines and recommendations that help enable the implementation of zero trust and software supply chain security.

Session 3: Takeaways and suggestions (2/2)

Takeaways and Conclusions

- Most customers are not familiar with software standards and supply chain security standards, so they build their own assessment process. Therefore, better adoption of the current standards is needed through references in contracts. Some examples:
 - Software Standards: ISA/IEC 62443-4-1
 - Supply Chain Security Standards (ISO/IEC 20243:2018 Open Trusted Technology Provider Standard O-TTPS, SCS 9001 Supply Chain Security Standard, and ISO/IEC 27036 Information Security for Supplier Relationships).
- By 2025, 45% of organizations worldwide will have experienced attacks on their software supply chains, a three-fold increase from 2021.
- Key principles of Zero Trust and Software Supply Chain: 

Suggestions to ITU-T SG17

- Issue guidelines on minimum standards for developer verification for software.
- SG17 has some work on Zero Trust (ZT) and Supply Chain, so has SG13. Hence, a collaborative work could be achieved:
 - SG17: Guidelines for ZT based access control platform in telecom networks
 - SG13: Assessing trust evaluation models for telecom. Networks.

Zero Trust	SW Supply Chain
Least Privilege	Visibility
Micro-Segmentation	Risk Assessment
Continuous Monitoring	Control
Trust is earned	Monitoring
	Response

Presentation Summary – Session 4: Panel discussion – Future directions for Study Group 17

- **Moderator:** Yutaka Miyake, WP2/17 Chairman | Senior Manager, Technology Strategy Department, KDDI Corporation.
- **Panelists**
 - Arnaud Taddei, Vice-chairman, ITU-T Study Group 17, Security | Broadcom
 - Heung Youl Youm, Chairman, ITU-T Study Group 17, Security | Professor, Department of Information Security Engineering, Soonchunhyang University
 - Sheeba Baskaran, Advisory Researcher - Lenovo, Motorola Mobility | Rapporteur for the 3GPP SA3 ZT TR
 - Duncan Sparrell, Chief Cyber Curmudgeon, sFractal Consulting
 - Tony Rutkowski, CEO, Netmagic Associates

Session 4: Takeaways and suggestions(1/3)

Takeaways and conclusions

- SG17 remains the only global intergovernmental body devoted to cybersecurity standards – which gives it a unique status.
- Relationship between cybersecurity regulations and international standards should be considered. Because the role of international standards is changing, SG17 needs to take this situation into account.
- SG17 can serve as a counterpoise to unilateral cybersecurity developments occurring – some of which are not helpful.
- There are many organizations for collaboration on this matter, such as ETSI, NIST, CISA, TTA, TTC, CCSA, ITU-T SG13, ISO/IEC SC27/WG5, etc.
- SG17 need to invite experts from other groups to work actively on these areas.

Suggestions to ITU-T SG17

- SG17 needs to identify the position for these standardization works as global intergovernmental body, and to lead this activity by collaborating with other organizations.
- Consider the requirements from regional or national regulations.

Session 4: Takeaways and suggestions(2/3)

Takeaways and conclusions

- There are many activities on supply chain security and zero trust, so we need to survey and analyze documents published by other groups. We need to avoid duplication work and need to find good area to promote these technologies.
- Collaboration with other groups is very important, and SG17 needs to consider making standardize specifications which are developed by other groups, such as OASIS etc.
- In recent years, its ability to gather best of breed current developments occurring across today's cybersecurity international standards ecosystem of scores of diverse bodies and convey them as recommendations and reports is well done and a great benefit to its members – which is manifested in this workshop. Implementing and harmonizing Zero Trust Models will form a significant component of SG17 work.

Suggestions to ITU-T SG17

- SG17 needs understand activities of other groups on these topics to avoid duplication work and make effective Recommendations for the market.
- Making Recommendations based on published document by other groups are important work for SG17.
- Invite experts from national and regional organizations to SG17 work.

Session 4: Takeaways and suggestions(3/3)

Takeaways and conclusions

- Zero trust security (ZTS) principles can be applicable to a wide range of systems (e.g., for enterprise, IT infrastructure, communication network etc.). Especially next generation network will include diverse services and functionalities whose deployment may utilize virtualization and cloud native approaches. The defense in depth approach of ZTS principle if applied holistically to the e2e network can effectively deal with insider and external threats (i.e., even if any function/device is compromised inbuilt ZTS mechanism can prevent data breaches and limit lateral threat movement).
- 3GPP security work group has started discussions (e.g., TR 33.894) on how to adapt the applicable ZTS principles to the mobile network.
- ITU-T SG17 is apex of cybersecurity Recommendations.

Suggestions to ITU-T SG17

- SG17 can consider the use of zero trust technology to realize secure environment efficiently for various kinds of services and functions.
- Explore wholistic view/picture and study new concept/approach including security assurance, etc.
- Undertake and accelerate studying underlying technologies, such as general models and maturity models, including format of SBOM data.