

Question 4/17 – Cybersecurity and countering spam

(Continuation of Question 4/17)

1 Motivation

The telecommunications landscape is constantly changing, and with it, requirements for associated telecommunication/ICT security. In this cyber environment, threats and attacks to telecommunication/ICT are constantly evolving to be more sophisticated and more targeted and cause a complex range of problems to users, service providers, operators and networks. There is a strong need for developing cybersecurity frameworks and requirements – a set of recommendations including best practices to assist organizations in managing cybersecurity risks.

Cybersecurity frameworks and requirements against threats and attacks consist of a set of components, which should consist of identifying, protecting, detecting, responding, and recovering. Countering cyber-attacks by technical means needs holistic requirements for: mitigating risks, detecting and responding early to incidents, and recovering from their affects; sharing cybersecurity information using methods such as Cybersecurity Information Exchange techniques (CYBEX) and Structured Threat Information Expression (STIE) and securing protocols, infrastructures and applications which are used as an integral part of our daily communications.

Artificial intelligence and machine learning are being applied more broadly across industries and applications than ever before. Technical means enabled by artificial intelligence and machine learning should improve the quality and efficiency of the technical activities against threats and attacks. There are two aspects of managed security services: technical, managerial.

The rise of new AI-driven applications and technologies has the potential to have great impacts on cybersecurity, in terms of new threats and new defence strategies. For instance, generative AI models that mime human language can be potential tools for massive attacks using social engineering techniques, as well as possible screenings of vulnerabilities through analysis of code and detection of bugs. On the other hand, AI can be used, e.g., to assist in tasks and decrease risks of breaches caused by human errors or to create or improve product design with cybersecurity focus.

Cybersecurity technologies involve technical supports for managed security services, endpoint detection and response, intrusion prevention/detection, and identification of the source of attackers in order to protect services and personal information including personally identifiable information (PII), and to provide information assurance (IA) among interacting entities.

By prioritizing supply chain security including software, and addressing the security issues around AI (AI for security, security for AI) including consequence of a generative AI, organizations can strengthen their defences and build a resilient security posture.

In addition, the aggressive pace of cyber threats evolution requires a review of technical aspects to support cybersecurity procedures, technical policies and frameworks. There is a challenge to achieve a minimum level of harmonization since cybersecurity requires collaboration among all stakeholders.

In the area of cybersecurity challenges, spam has also become a widespread problem causing potential loss of revenue to Internet service providers, telecommunication operators, mobile telecommunication operators and business users around the globe. Furthermore, spam creates problems of information and telecommunication network security while being used as a vehicle for phishing and spreading viruses, worms, spyware and other forms of malware, etc. Therefore, WTSA Resolution 52 instructs the relevant study groups to continue to support ongoing work, in particular in Study Group 17, related to countering spam and accelerate their work on spam in order to address existing and future threats within the remit and expertise of the ITU-T, as appropriate. In addition, it instructs to continue collaboration with relevant organizations, in order to continue developing, as a matter of urgency, technical Recommendations with a view to exchanging best practices and disseminating information through joint workshops and training sessions, etc., and

further instructs Study Group 17 to report regularly to the Telecommunication Standardization Advisory Group on the progress of this resolution.

With the rapid expansion of mobile internet and the convergence of ICT technologies, spam threats become more challenging with new features. The main ingredients of spam have significantly evolved from traditional advertisements and fraud to convergent malicious software such as ransom and targeted attacks. The new generation of spam is also unsolicited and harasses ICT service consumers, but they do even more serious damage than traditional ones. With the evolution of artificial intelligence / machine learning (AI/ML) technology, some communications can be initiated by machines but not humans, such as robocalls, robot chat, automatic text messages and so on. AI/ML algorithms can also make use of personal information more accurately to find target recipients to make large-scale commercial marketing spam or even fraud spam.

With the wide deployment of IMT-2020, emerging IMT-2030, Internet of Things and other telecommunication/ICT technologies, spam has also gradually begun to affect the industrial systems.

Countering spam has been recognized as a global problem that requires a multifaceted, comprehensive approach. Study Group 17, as the lead study group on telecommunication security and in supporting the activities of WTSA Resolutions 52, is well-positioned to study the range of potential technical measures to counter spam as it relates to the stability and robustness of the telecommunication network. In addition, technical structure for existing and potential Recommendations on countering spam by technical means has been established to facilitate Recommendation production. Furthermore, new Recommendations should be published to counter new forms of spam.

Recommendations, Supplements and Technical Reports under responsibility of this Question as of 12 September 2024: X.1205, X.1206, X.1207, X.1208, X.1209, X.1210, X.1211, X.1212, X.1213, X.1214, X.1215, X.1216, X.1217, X.1218, X.1219, X.1220, X.1231, X.1232, X.1233, X.1234, X.1235, X.1236, X.1237, X.1240, X.1241, X.1242, X.1243, X.1244, X.1245, X.1246, X.1247, X.1248, X.1249, X.1303, X.1303bis, X.1500, X.1500.1, X.1520, X.1521, X.1524, X.1525, X.1526, X.1528, X.1528.1, X.1528.2, X.1528.3, X.1528.4, X.1541, X.1542, X.1544, X.1546, X.1550, X.1570, X.1580, X.1581, X.1582, Supplements 6, 8, 9, 10, 11, 12, 14, 18, 20, 25, 29, 33, 37 to the X-series Recommendations, and Technical Report TR.usm.

Texts under development as of 12 September 2024: X.stie, X.taeii, X.gpmr, X.nspam, X.sf-dtea, X.sgc_rcs, X.st-ssc, and Technical Report TR.verm.

2 Question

Study items to be considered include, but are not limited to:

- How should telecommunication/ICT providers secure their infrastructure, maintain secure operations and use security assurance mechanisms?
- What are the security requirements that software, telecommunications protocols, communications systems designers and manufacturers need to consider in the design, development and sharing of best practices in the cyber environment?
- How should information on vulnerability, weakness and attack measures be shared efficiently to aid in vulnerability life-cycle processes?
- What requirements and solutions are needed for telecommunication/ICT assurance of composable systems' resilience, security and integrity?
- What requirements and solutions are needed for telecommunication/ICT accountability, incident response, managed security services, cyber-attack attribution, and threat monitoring and risk communication?

- How can artificial intelligence and machine learning be used to quickly identify and analyse new threats and vulnerabilities? How can AI-driven technologies enhance cybersecurity strategies?
- What threats can be developed by AI-driven technologies? How AI-generated attacks can be avoided or mitigated?
- How should telecommunication/ICT providers utilize the threat intelligence to enhance their security activities?
- What are the set of components of cybersecurity framework that an organization can use to address risks?
- What are the necessary security guidelines and best practices for identifying, mitigating and reducing impact of cyber threats, including malware, distributed denial of service and social engineering?
- How to understand and identify spam?
- What are new forms of spam in existing and future networks?
- What are the serious effects of spam?
- What are technical factors which contribute to difficulties in identifying the sources of spam?
- How can new technologies, services and applications, such as instant messaging, social networking, mobile application, Voice Over Long-Term Evolution (VoLTE), and Rich Communication Services (RCS), etc., lead to opportunities to create and spread spam?
- How can routes, sources and volumes of spam be identified and the amount of investment in facilities and other technical means be estimated to counter and combat such spam?
- How can the messaging security be implemented?
- How can the distribution of malicious software and malware through email be prevented?
- How can AI/ML communication form of spam be identified and prevented?
- How to protect personal information with the adoption of AI/ML technology to avoid spam message spread?
- What technical work is already being undertaken within the IETF, 3GPP, GSMA, M3AAWG, in other fora, and by private sector entities to address the problem of spam?
- What telecommunication network standardization work, if any, is needed to effectively counter spam as it relates to the stability and robustness of the telecommunication network?
- What are the effective and efficient solutions for countering spam?
- How are generic and specific requirements developed for information sharing on countering spam?

3 Tasks

Tasks include, but are not limited to:

- Work on frameworks and Recommendations to address how telecommunication/ICT providers may secure their infrastructure and maintain secure operations and exchange cybersecurity information.
- Produce a set of Recommendations for providing security solutions for telecommunication/ICT accountability, assurance and incident response and recovery, including technical aspects of managed security services.
- Study and specify the security techniques and capabilities for service providers to coordinate and exchange information regarding vulnerabilities, platforms, and cyber-attacks.

- Study and specify cybersecurity framework consisting of a set of components that should consist of identify, protect, detect, respond, and recover.
- Specify how to use artificial intelligence and machine learning, and address the security issues around AI including consequence of a generative AI, to quickly identify and analyse new threats and vulnerabilities.
- Specify how to apply accountability, assurance, and incident response mechanisms in telecommunication/ICT networks.
- Develop guidelines and techniques to protect personal information and also to protect personally identifiable information (PII) using cybersecurity information sharing techniques such as CYBEX, STIE and TAEII and related security tools.
- Develop best practices and guidelines for the sharing of vulnerability information and remedies to aid in vulnerability life-cycle processes.
- Collaborate with other standards developing organizations.
- Work on Recommendations and Technical reports on how to address cybersecurity challenges including software supply chain security.
- Act as the lead group in ITU-T on technical means for countering spam, as spam is described by Study Group 2.
- Identify and examine telecommunication network security risks (at the edges and in the core network) introduced by the constantly changing nature of spam.
- Identify routes, sources and volumes of spam and estimate the amount of investment in facilities and other technical means to counter and combat such spam.
- Develop a comprehensive and up-to-date resource list of the existing technical measures for countering spam in telecommunication networks that are in use or under development.
- Develop new Recommendations for countering existing and emerging forms of spam.
- Develop a set of technical measures to support messaging security.
- Develop new Recommendations for preventing malicious software and malware distributed through e-mail.
- Develop a set of solutions to prevent targeted attacks using spear phishing through e-mail.
- Develop new Recommendations for preventing ransomware distributed through e-mail.
- Develop generic and specific requirements for information sharing on countering spam.
- Determine whether new Recommendations or enhancements to existing Recommendations, including methods to combat delivery of unsolicited email, malware, and other malicious contents, and combat compromised network equipment, such as Botnets, would benefit efforts to effectively counter spam as it relates to the stability and robustness of telecommunication network.
- Develop a set of solutions or new Recommendations for counting AI/ML communication form spams and preventing AI-generated telecom fraud including fake messages, voice, images, and videos.
- Provide regular updates to the Telecommunication Standardization Advisory Group and to the Director of the Telecommunication Standardization Bureau to include in the annual report to Council.

An up-to-date status of work under this Question is contained in the SG17 work programme at https://www.itu.int/ITU-T/workprog/wp_search.aspx?sp=18&q=4/17.

4 Relationships

Recommendations:

- X-series and others related to security

Questions:

- All ITU-T SG17 Questions

Study groups:

- ITU-T SG 2
- ITU-T SG 11
- ITU-T SG 13
- ITU-T SG 20
- ITU-T SG 21
- ITU-D SGs 1 and 2

Standardization bodies:

- European Telecommunications Standards Institute (ETSI)
- Institute of Electrical and Electronics Engineers (IEEE)
- Internet Engineering Task Force (IETF)
- IEC TC 57, IEC TC 292, IEC TC 65/WG10
- ISO/IEC JTC 1/SC 27
- National Institute of Standards and Technology (NIST)
- Organization for the Advancement of Structured Information Standards (OASIS)
- Open Mobile Alliance (OMA)
- Open Group
- Object Management Group (OMG)
- Third Generation Partnership Project (3GPP)
- Trusted Computing Group (TCG)

Other bodies:

- Anti-Phishing Working Group (APWG)
- CERT/CC
- CIRTs
- European Network and Information Security Agency (ENISA)
- GSM Association (GSMA)
- Messaging, Malware and Mobile Anti-Abuse Working Group (M³AAWG)
- Forum for Incident Response and Security Teams (FIRST)
- National Institute of Standards and Technology (NIST)
- Organization for Economic Cooperation and Development (OECD)

WSIS Action Lines:

- C5

Sustainable Development Goals:

- 8, 9