Workgroup: Internet Engineering Task Force
Internet-Draft:
draft-chen-atomized-security-functions-00
Published: 8 October 2022
Intended Status: Informational
Expires: 11 April 2023
Authors: Chen, Ed. China Mobile
L. Su China Mobile

the Description and Definition for Atomic Security Functions

Abstract

At present, many security products are deployed in the network, and the security functions of security products overlap. Atomized security function refers to the smallest representation unit of security function, which cannot be split again and can be implemented by independent code. Atomized security functions can quickly and effectively assemble security capabilities and provide security services. It no longer takes security products as the unit, but atomic security functions as the basic unit, by reorganize and define the security functions supported by existing network devices then provide guidance for secure routing, finally, each security function will be uniformly coded.

Status of This Memo

This Internet-Draft is submitted in full conformance with the provisions of BCP 78 and BCP 79.

Internet-Drafts are working documents of the Internet Engineering Task Force (IETF). Note that other groups may also distribute working documents as Internet-Drafts. The list of current Internet-Drafts is at https://datatracker.ietf.org/drafts/current/.

Internet-Drafts are draft documents valid for a maximum of six months and may be updated, replaced, or obsoleted by other documents at any time. It is inappropriate to use Internet-Drafts as reference material or to cite them other than as "work in progress."

This Internet-Draft will expire on 11 April 2023.

Copyright Notice

Table of Contents

1. Introduction
2. Security functions
  2.1. Identity
  2.2. Protect
  2.3. Detect
  2.4. Respond
  2.5. Recover
3. Yang Model for Atomic security functions
4. IANA Considerations
5. Security Considerations
Authors' Addresses

1. Introduction

At present, there are many security companies and products on the market, the most common include firewall, vulnerability scanning system, intrusion detection system, intrusion prevention system, WEB application firewall, VPN, anti DDoS equipment.

The equipment purchased by telecom operators takes security products as the basic unit to ensure the availability of the whole network; With the development of the network and the security transmission requirements of users, in addition to the availability of the network, it is also necessary to provide external security capabilities. The availability of the basic network has been in a stable state, but the ability to provide external security needs to be improved.

Atomic security functions: it refers to the smallest unit that independently provides security capability in code implementation. The definition and classification of atomization security capabilities are based on IPDRR, IPDRR is the network security framework of the National Institute of Standards and Technology. Identify, protect, detect, respond, and recover (IPDRR) are the 5 high level functions of the framework core, there are 23 categories that are spread across these 5 functions. When different from the 23 categories, the definition and classification of atomic security capabilities start from the actual security products and aim at providing external security capabilities.

2. Security functions

At present, we refer to the IPDRR model to classify the capabilities of existing security products into 23 security capability categories. Of course, the fine granularity of this classification is not yet atomicized. We will atomicize the 23 security capability classifications and reflect them in Yang's model.

2.1. Identity

Asset identification: through active detection and passive monitoring, identify the assets in the organization or network and their status changes, distinguish and classify their value and vulnerability in information security, and ensure the accuracy, real-time and consistency of assets. Typical products include asset management system, asset exploration platform, etc.

Identity identification: identify and verify the identity of visitors to networks, systems, applications, etc. to establish trust in their identity, and find unauthorized behaviors that do not conform to their identity. Typical products include identification.

Threat intelligence identification: identify the threat intelligence related to strategy, tactics and operations according to the rules or methods of threat intelligence identification. Typical products include advanced continuous threat detection products.

Vulnerability identification: use appropriate vulnerability scanning tools, or organize penetration testing or vulnerability evaluation, to scan and identify possible security vulnerabilities in equipment and software, classify vulnerabilities, and verify whether vulnerability repair is successful. Typical products include vulnerability scanning systems.

Configuration vulnerability detection: use configuration verification tools to scan and identify possible configuration vulnerabilities in equipment and software, so as to find and timely repair configuration problems. Typical security products include configuration verification system, configuration verification, etc

2.2. Protect

Access control: through information security level and information classification, restrict privileged access, complete the separation of access control functions (such as access request, access authorization, access management) and the management of authorization and authority of access request, and make it only access authorized networks, terminals and other resources to prevent unauthorized access. Typical products include firewalls, bastion computers, operation and maintenance security gateways, etc.

Security interface protection: set interface security call conditions, disable or restrict unnecessary functions and interfaces. Typical products include baseline configuration check products.

Encryption protection: provide password management, password operation and other password functions to provide confidentiality, tamper resistance, and non repudiation protection for files, communication links, etc. Typical products include cryptographic devices, commercial encryptors, encryption cards, and public key infrastructure.

Malware protection: use black and white list to prevent unauthorized software use. Typical products include anti-virus products.

Isolated exchange: by cutting off the network connection and stripping the network protocol, the data is ferried between different networks in the form of proprietary data blocks to achieve data exchange in a network isolated environment. Typical products include gateways, security isolation and information exchange systems.

Flow control: monitor network flow, limit bandwidth, filter messages and other operations, optimize the use of loan resources, and avoid network congestion. Typical products include Web application firewall, Web application security protection system, anti DDoS attack, etc

Data desensitization: based on desensitization rules such as data masking, data simulation, replacement of key parts, and random replacement of data, the sensitive data is transformed to achieve data hiding, deformation, and fuzziness. At the same time, the desensitized data can maintain the original semantics and association relationships, and ensure the validity of the data while preventing the leakage of model sensitive information. Typical products include data desensitization, etc

Active defense: hide real assets or lure attackers to attack virtual targets through simulation, dynamic or static permutation and combination, deformation, transformation or confusion to achieve the security protection of real assets. Typical products include honeypot, deception defense, pseudo security products, mobile target defense products, etc.

Security environment support: Follow specific security policies in the design, implementation and use phases to provide a trusted computing module, a secure operating system and other security environments or enhance environment security. Typical products

include secure operating systems, secure databases, trusted execution environments, etc

Residual information protection: Completely destroy the bearing data to be deleted on the storage media through overwriting, isolation, etc., to prevent the data leakage caused by unauthorized recovery of the deleted sensitive data, and to ensure that other data are not affected. Typical products include data clearing, etc

2.3. Detect

Security monitoring: Collect and gather information such as network traffic, terminal information, online behavior, email information, and network assets, and provide on-demand or continuous monitoring. Typical products include network activity monitoring, etc.

security analysis: analyze the network traffic, network behavior, terminal behavior, logs and other data with a reproducible and descriptive method, find out the abnormal and threatening behaviors, and determine the attack means and evaluate the attack loss. Typical products include public opinion analysis, security detection analysis, intrusion detection system, etc.

Security audit: identify, record, store and analyze information related to security activities, so that the organization can know whether its security activities meet the requirements of security compliance, and at the same time, it can help the organization fully understand and master the effectiveness, adequacy and suitability of its security activities. Typical security products include code audit, log audit, behavior audit, flow audit, comprehensive audit, etc.

system risk assessment: provide semi-automatic or automatic risk assessment for the system, with the purpose of improving system security. Typical security products include system risk assessment services.

2.4. Respond

Security orchestration: Integrate third-party tools across security and business ecosystems through scripts to achieve triage and coordination of security events and collaborative response to security events. Typical security products include security orchestration and automated response.

Attack mitigation: for viruses, trojans, worms, network attacks, data leaks, e-mail attacks and other events, use alarm, anti-virus, process termination and other means to block, limit or pull the attackers or leak sources, so as to mitigate the expansion of events, reduce and eliminate the impact.

Attack traceability: for general exceptions in the network system, security events without results, and security events with clear results (leakage, destruction) after serious damage, trace the source of infection, infection path, infection object and other information of tampering, destruction, latency and other attacks.

2.5. Recover

Backup and recovery: In order to cope with unexpected situations such as loss or damage of files and data, two or more sets of systems with the same functions can be established for files and data copies exported from the original system and stored separately. Health status monitoring and function switching can be performed between them. When one system stops working unexpectedly, it can be switched to another system to ensure that all functions and services of the system are normal. It can be divided into data backup and recovery, website backup and recovery, disaster recovery auxiliary support, configuration rollback, etc.

3. Yang Model for Atomic security functions

TBD

4. IANA Considerations

This memo includes no request to IANA.

5. Security Considerations

TBD

Authors' Addresses

Meiling Chen (editor)
China Mobile
BeiJing
China

Email: chenmeiling@chinamobile.com

Li Su
China Mobile
BeiJing
China

Email: suli@chinamobile.com