|  |
| --- |
| **Theory, Technology and Application of Cyberspace Active Defense** |
| Contact: WU Chunming | Email: wuchunming@zju.edu.cn |
| **Research background:** Due to the dangers in cyberspace, all countries in the world are suffering unprecedented threats to national security. Cyber security is thus upgraded to the strategic height of national security.The traditional cyberspace defense, which is passive defense based on the prior experience, cannot effectively resist the attacks in bugs and backdoors, or deal with infiltrative network invasion which becomes more complicated and intelligent. From the perspective of engineering, there is a dilemma that "the bugs are unavoidable, so are the backdoors”.Bugs and backdoors of existing cyberspace system, which are results from its steady state, similarity, and deterministic, make it easy to be attacked or controlled.We attempt to take active defense approach. Our researchesfocus on creating a dynamic cyber environment by active reconstruction or migration of networks, platforms, systems, software and data, which varies in a way that defenders can control. This approach can break the attack chain relying on the certainty and persistent of execution environment, and thus stop the attack, increase the difficulty and cost of attack behavior and reduce the risks in security system.  |
| **Main research topics and progress:** 1. Research on basic theory in active defense: a. ADSATF (Active Defense System Architecture and Technology Framework), whichsupports virtualization, dynamization, self-healing and customization of security rules. b. Goals and requirements of dynamic changes and migration of interconnection topology, network protocols, devices, services and data, which are based on the attack chain model.c. Technical principles, classification support techniques and corresponding change strategies and linkage mechanisms of dynamic changes on all levels. d. Decision model, mechanism and technology of dynamic system. e. Hierarchical awareness and comprehensive evaluation techniques, dynamic change decision strategies and algorithms, system change execution techniques against system security threat.2. Research onarchitecture and key technologies of active defense: a. BSAMD (Basic Security Architecture of Mimic Defense) in the aspect of webs, platforms, runtimes, software, data, and application scenarios, which can solve the relationship between mimic defense mechanism and different technical levels and different security objectives in cyberspace, provide guidance and reference for applying and implementing mimic defense technology in actual scenesb. Specific mimic security defense architecture by combining BSAMD with different application scenarios in cyberspace. c. Key common technologies of active defense, principle model for technical verification, which can evaluate the environmental adaptability and achievability.3. Research on key technology in active defense of web security gateway and system development: a. Architecture of the prototype of web secure gateway in active defense, key technologies such as script isomerization and diversity compilation. b. Heterogeneous redundant execution resource pool, control and voting unit and storage unit related software and hardware system. c. Isomerization technology in all levels, dynamic Isomerization Combinations, the evaluation mechanism of heterogeneous differences and dynamic isomerization scheduling. 4. Research and application of active defense technology in industrial control systems: In order to establish a core technology system which is safe in function, information and operation, and can guarantee the safety, reliability, real-time and usefulness of industrial control system as well, we innovate the dynamic reconfiguration of industrial control system and work on trusted promotion technology, integrating with characteristics of information physical system, and realizeactive defense in the endogenous security of industrial control system. 5. Research and application of industrial internet active defense technology: a. Active security protection system in the open integrated industrial Internet environment. b. Situational awareness and decision technology based on swarm intelligence. c. Pseudo active protection against the uncertainty threat. d. Cloud computing and the large data platform security protection. e. Industrial internet key control system security protection.  |
| **Members and colleges:** College of Computer Science and TechnologyResearch Center of Cyberspace SecurityCollege of Control Science and EngineeringCollege of Information Science and Electronic EngineeringChina National Digital Switching System Engineering & Technological R&D CenterInstitute of System Architecture and Network SecurityInstitute of Information Engineering,Chinese Academy of SciencesZTE CorporationNational Research Center for the development of industrial information securityZhejiang province company in State powerNetwork Security Corps, Zhejiang Provincial Public Security BureauCollege of computer science, Zhejiang University of Technology College of computer science, Hangzhou Dianzi UniversityJiaxing Vocational and Technical College |
| **Representative achievements:** * Journal articles

[1] Evolving Defense Mechanism for Future Network Security, IEEE Communications Magazine, 2015, 53(4): 45-51.[2] SDN-LIRU: A Lossless and Seamless Method for SDN Inter-Domain Route Updates, IEEE/ACM Transactions on Networking, 2017, 25(4): 2473-2483.[3] Elevate Abstraction Level for Network Functions, IEEE/ACM Transactions on Networking,2018, 26(1):189-202.[4] On the design of green reconfigurable router toward energy efficient internet, IEEE Communications Magazine, 2011, 49(6): 83-87.[5] Engineering traffic uncertainty in the OpenFlow data planeIEEE INFOCOM, 2016:1-9, San Francisco, USA, 2016.4.10-4.15.[6] Programming Network via Distributed Control in Software-Defined Networks, IEEE ICC, 2014, 3051-3057, Sydney, Australia, 2014.06.10-14.[7] HSTS Measurement and A New Stripping Attack Against HTTPS，Securecomm,2017.[8] H2DoS: An Application Layer DoS Attack towards HTTP/2 protocol，Securecomm,2017.[9] [Adaptive IP Mutation: A Proactive Approach for Defending against Worm Propagation](http://ieeexplore.ieee.org/abstract/document/7600155/), IEEE 35th Symposium on Reliable Distributed Systems Workshops (SRDSW)2016.[10] Improving QoS in SDN with Lossless Multi-domain Reconfigurations，IEEE/ACM IWQoS 2016.* Patents

(1)Trojan detection method based on network data flow(2)An active defense method against Trojan based on virtual environment(3)A Channel Allocation Method for Active Defense(4) A malicious program detection method based on internal honeypot technology(5) An SDN controller-based DoS/DDoS attack defense module and method(6) An SDN-based trusted routing source management method(7) A mimic method in cloud database to randomized sensitive information (8) A website structure mimicry method to protect web application security(9) A decoy method for securing web applications* Prototype system

1. Anomaly detection platform based on mimic defense. 2. Situational awareness data analysis platform. 3. China’s first industrial control system of active defense gateway. 4. China’s first active web servers with the ability to tamper. 5. China’s first active defense web gateway.  |