# Analysis and Proof of Unidirectional Network Security Devices (Postprint)

**Authors:** Wang Xuejian, Zhao Guolei, CHANG Chaowen, Wang Ruiyun

**Date:** 2018-05-02T00:00:00+00:00

## Abstract

Unidirectional network security devices serve as the primary security equipment for network information transmission between networks of different classification levels. To ensure the security of both the internal components of these devices and the communication system, this paper analyzes the security requirements of unidirectional network security devices, proposes formal modeling using a non-interference model, and employs mathematical induction to prove the consistency between the security requirements of unidirectional network security devices and formal policy specifications. Furthermore, it analyzes and discusses the security vulnerabilities present in unidirectional network security devices, summarizes more comprehensive security policies, and ensures information security. This provides valuable reference for the security design of unidirectional network security devices.

## Full Text

## Preamble

**Title**: Analysis and Proof of One-Way Network Safety Equipment

**Authors**: Wang Xuejian, Zhao Guolei, Chang Chaowen, Wang Ruiyun (PLA Information Engineering University, Zhengzhou 450001, China)

**Abstract**: One-way network safety equipment serves as the primary security device for information transmission between networks of different classification levels. To ensure the security of both the internal components of one-way network safety equipment and the overall communication system, this paper analyzes the security requirements of one-way network safety equipment and proposes a formal modeling approach using noninterference models. Mathematical induction is employed to prove the consistency between the security requirements of one-way network safety equipment and formal policy specifications. The paper also analyzes and discusses potential security vulnerabilities in one-way network

safety equipment, summarizing more comprehensive security policies to ensure information security. This work provides valuable insights for the security design of one-way network safety equipment.

**Keywords**: one-way network safety equipment; formalization; noninterference model; security policies; mathematical induction

## 0 Introduction

In recent years, as network traffic volumes have increased and the risk of computer attacks continues to grow, traditional security measures (such as firewalls and intrusion detection systems) have become increasingly inadequate for handling corresponding attacks. To counter these new security threats and reduce system vulnerabilities, new security devices must be added or network architectures redesigned to provide enhanced security functions. Bidirectional information exchange between networks of different security levels further increases the complexity of information interaction within the internal communication systems of security devices, necessitating the introduction of one-way network safety equipment to ensure secure information flow from low-security-level networks to high-security-level networks.

Numerous security analysis and proof methods for one-way network safety equipment exist today, but most lack a solid theoretical foundation. The security requirements of one-way network safety equipment are determined by their internal security policies, and the formal analysis, design, and verification of security policy models represent a hot research topic in formal methods. Classic formal information security policy models include information flow models, the BLP model, and noninterference security models. Since the information flow hidden behind read and write operations is not as explicit as it appears, many restrictions must be added to eliminate covert channels. However, noninterference security models can not only verify security properties but also guide designers in judging information flows (achieving security during information transmission through a more inclusive notion of "read" and "write" operations). Therefore, this paper selects the noninterference security model to analyze the security policies of one-way network safety equipment and proves the consistency between functional specifications and security model policies.

The communication system composed of a sending end, one-way network safety equipment, and receiving end operates as follows: the sending end only transmits information to the one-way network safety equipment without receiving any data, ensuring unidirectional, secure, and rapid data transmission from computers or storage devices in low-security-level domains to those in high-security-level domains. Even if high-security-level computers are illegally controlled, file data cannot be transmitted to low-security-level storage devices. Common one-way network safety equipment includes one-way network gates and unidirectional security gateways.

This paper first introduces one-way network safety equipment and establishes

its abstract model. It then reviews relevant research on noninterference and formally transforms the abstract model based on the Goguen and Meseguer noninterference model, proposing corresponding security policies. Mathematical induction is used to verify that the formalized model satisfies the consistency between its requirements and specifications under these security policies. The paper discusses the existence of covert channels and proposes corresponding policy adjustments to ensure the security of the overall communication system. Finally, conclusions and future research directions are presented.

## 1 Abstract Model of One-Way Network Safety Equipment

One-way network safety equipment is commonly deployed at the boundary between classified and unclassified networks or between high-security and low-security-level networks, ensuring the confidentiality and integrity of high-level network data during information exchange between different security domains, as shown in [Figure 1: see original paper]. The equipment controls input information from low-security-level networks and contains a series of communication modules that analyze and transmit this information, enabling subjects/objects in low-security-level network domains (such as branch offices in the figure) to transmit information through the one-way network safety equipment to high-security-level networks (such as headquarters in the figure). However, whether this information transmission process is truly secure requires further investigation and analysis, which motivates the introduction of security models.

A security model aims to precisely describe system security requirements and possesses the following characteristics: it is precise and unambiguous; simple and abstract; general, addressing only security properties without overly restricting system functionality and implementation; and provides a clear expression of security policies.

The communication system studied in this paper, composed of a low-security-level network domain $D_L$ and a high-security-level network domain $D_H$, is a deterministic synchronous system. Its abstract logical structure is shown in [Figure 2: see original paper], representing the scenario where information flows from low-security-level network domain $D_L$ to high-security-level network domain $D_H$. Information entering from $D_L$ is processed by internal communication modules of the one-way network safety equipment before entering $D_H$.

### 1.1 Related Research on Noninterference

The concept of noninterference for information flow was initially proposed by Goguen and Meseguer, with various noninterference security models emerging subsequently. In 1992, Rushby improved upon the Goguen and Meseguer noninterference model, correcting several errors to make it more reasonable and understandable, thus maturing the noninterference model.

The noninterference model proposes a new perspective for analyzing security based on "interference." Essentially, if subjects in different groups within a

system do not interfere with each other, the system is secure. This approach is more inclusive than traditional write operations and can express policies and models more simply. Goguen and Meseguer used this to define security policy models.

### 1.2 Noninterference Policy Model

**Basic Definitions of Noninterference Policy Model**: A system $X$ is viewed as a state machine containing a set of subjects $S = \{s_1, s_2, ...\}$, a set of states $Q = \{\delta_0, \delta_1, ...\}$, a set of state commands $C = \{c_1, c_2, ...\}$, and an output set $O = \{o_1, o_2, ...\}$. (In practice, the security level of the subject executing a command affects the actual command executed, so a command set $Z = \{z_1, z_2, ...\}$ is used here.)

**Definition 1**: The state transition function $tra : C \times Q \to Q$ describes the effect of executing command $c$ in state $\delta$. The output function $out : C \times Q \to O$ describes the machine' s output when executing command $c$ in state $\delta$.

**Definition 2**: Let $s_i$ be a subject in system $X$ and $c^*$ a state transition sequence (a command sequence where $n$ is a positive integer), with $out^*(s_i, c^*)$ being the corresponding output. Then $out'(s_i, s, c^*)$ is a set of outputs representing the set of outputs that subject $s_i$ is authorized to see and that maintain the same order as in $out^*(s_i, c^*)$ (where $n$ is a natural number). That is: the function $\pi$ removes from the output all outputs not authorized for $s_i$ to obtain the resulting output sequence.

This definition expresses that due to security policy restrictions, $s_i$ may not see all outputs. However, $s_i$ may also not have knowledge of all commands, requiring the following definition.

**Definition 3**: Let $G$ be a set of subjects and $A$ a set of commands. The purge function $\pi$ deletes from $c^*$ all elements belonging to $A$ to obtain a subsequence. Define $c^* \setminus A$ as the subsequence obtained by deleting from $c^*$ all elements belonging to $A$. Define $c^* \setminus G$ as the subsequence obtained by deleting from $c^*$ all elements belonging to $G$. Define $c^* \setminus (G, A)$ as the subsequence obtained by deleting from $c^*$ all elements belonging to both $G$ and $A$.

Intuitively, a system is secure if any user' s visible output set is related to that user' s visible input set. The following definition formalizes this as "noninterference."

**Noninterference Theorem**: Let $G$ and $A$ be two different subject sets, and $C$ a command set. Users in $G$ running commands in $A$ do not interfere with users in $Z$ (denoted as $G, A \nrightarrow Z$) if and only if for all sequences $c^*$ composed of elements from $C$ and all states $\delta$:

$$out'(Z, \delta, c^*) = out'(Z, \delta, c^* \setminus A)$$

### 1.3 Formal Description of Noninterference

Based on the noninterference model in Section 1.2, we now formally describe the one-way network safety equipment model and its policies.

Consider the model in [Figure 3: see original paper] as a system $X = (S, Q, O, Z)$: - $S = \{l_1, l_2, ..., l_n\}$: a set of subjects (where $n$ is a positive integer) - $Q = \{\delta_0, \delta_1, ...\}$: a set of states, where $\delta_0$ is the initial system state and $\delta_0 = \{(l_1, \delta_0), (l_2, \delta_0), ..., (l_n, \delta_0)\}$ - $C = \{(l_i, c_i), (l_i, c_j), ...\}$: a set of state transition commands, where the command domain for subject $l_i$ is defined as $dom(c_i) = \{l_i\}$ - $O = \{o_1, o_2, ...\}$: an output set - $Z = \{z_1, z_2, ...\}$: a set of commands

The state transition function is defined as $tra : C \times Q \to Q$, and the output function as $out : C \times Q \to O$ (representing machine output at this state with the number of subjects/objects).

The purge function is consistent with Definition 3. $out'(s_i, s, c^*)$ represents the output sequence obtained by deleting from the output all outputs not authorized for $s_i$ to see.

[Figure 4: see original paper] shows the formal representation of internal modules, where: - $L$ represents the external network communication module, with any subject/object state in the module denoted as $l$ - $F_1, F_2$ represent two filter modules, with any subject/object states denoted as $f_1, f_2$ - $E$ represents the encryption/decryption module, with any subject/object state denoted as $e$ - $H$ represents the internal network communication module, with any subject/object state denoted as $h$

The information transfer state transitions involved in [Figure 4: see original paper] are shown in [Figure 5: see original paper].

To ensure information filtering by the one-way network safety equipment, the model must satisfy two security requirements: a) **Filterability**: Information transmitted to other network domains through the one-way network safety equipment must be filtered by the equipment' s internal communication modules. b) **Unidirectionality**: Information transfer between any communication modules within the one-way network safety equipment must be unidirectional.

Based on these requirements, the following functional specification is made for the simple serial transmission of information within the one-way network safety equipment ([Figure 3: see original paper]): For any module, when a high-level subject executes commands in that module, it satisfies noninterference with respect to low-level subjects.

## 2 Consistency Proof Between Requirements and Formal Policy Specification

This section uses formal methods and mathematical tools to prove that the policies of the one-way network safety equipment satisfy noninterference. Due to the inherent limitations of the noninterference model, we consider scenarios of information transfer between different security levels (information at the same level is discussed in Section 4).

Let $l_1$ and $l_2$ be two different subjects/objects with $level(l_1) < level(l_2)$. The state transitions are shown in [Figure 6: see original paper].

**Example**: Since subjects/objects $l_1$ in module $L$ can only observe states in $dom(c_1)$, we only need to consider the case where $c_1 \in dom(c_1)$. Without loss of generality, let the number of $\delta_0$ observed by subject $l_1$ within its authority at the initial system state be $m$ (where $m$ is a natural number), with $c_0$ being the empty command. Similarly, for subject $l_2$ we have $out'(l_2, \delta_0, c_0) = m$.

When the system executes command sequence $sc$ in module $L$, then $out'(l_1, \delta_0, sc) = m - 1$, and clearly $out'(l_2, \delta_0, sc) = m - 1$. Therefore:

$$out'(l_1, \delta_0, sc) = out'(l_1, \delta_0, sc \setminus dom(c_2))$$

Thus, module $L$ is internally noninterference-secure. Similarly, each individual module within the one-way network safety equipment satisfies noninterference.

For the serial composition of modules within the entire gateway, consider modules $L$ and $F_1$ as an example, as shown in [Figure 7: see original paper].

By the Noninterference Theorem, if $l_1$ and $l_2$ are two different subjects/objects with $level(l_1) < level(l_2)$, let $Z_1$ be the set of all subjects/objects at the same level as $l_1$, and $Z_2$ be the set of all subjects/objects at the same level as $l_2$. Let $C$ be a command set. For all sequences $sc$ composed of elements from $C$ and all states $\delta$, we need to prove that users in $Z_1$ running commands in $C$ do not interfere with users in $Z_2$ (denoted as $Z_1, C \nrightarrow Z_2$).

We use mathematical induction, letting $n$ be the number of commands in $sc$.

**(1) Base case**: When $n = 0$, the proposition clearly holds. When $n = 1$, i.e., $sc = c_1$, the proposition holds. For $sc = (c_j, s_i)$ where $j$ is a positive integer and $s_i \in Z_1$, the proposition holds. For $sc = (c_k, s_i)$ where $k$ is a positive integer and $s_i \in Z_2$, the proposition also holds.

**(2) Inductive hypothesis**: Assume the proposition holds for $||sc|| \leq n$.

**(3) Inductive step**: - When $i = 1$, for $sc = (c_j, s_i)$ where $j$ is a positive integer and $s_i \in Z_1$, we have $out'(Z_2, \delta_0, sc) = out'(Z_2, \delta_0, sc \setminus Z_1)$ by the inductive hypothesis. - When $i \neq 1$, for $sc = (c_j, s_i)$ where $j$ is a positive integer and $s_i \in Z_1$, we have $out'(Z_2, \delta_0, sc) = out'(Z_2, \delta_0, sc \setminus Z_1)$ by the inductive hypothesis.

Thus, the original proposition holds: users in $Z_1$ running commands in $C$ do not interfere with users in $Z_2$ (denoted as $Z_1, C \nrightarrow Z_2$). Similarly, if the internal modules of the one-way network safety equipment are serially connected, the internal system is noninterference-secure when information at different levels is transmitted.

## 3 Covert Channel Problems and Improvements

When information at the same security level passes through the one-way equipment, system security is obvious for single-module information transfer. We now consider only module composition scenarios, where analysis reveals information leakage behavior (covert channels). A covert channel is a communication channel not intended by system designers for communication, allowing processes to bypass mandatory security mechanisms and transmit information in violation of system security policies, thereby threatening system security.

### 3.1 Internal Covert Channels

Typically, one-way network safety equipment contains composition of modules at the same level, and buffer regions exist during actual information transfer. Without loss of generality, consider message transfer between the external network communication module $L$ and filter module $F_1$.

In [Figure 8: see original paper], buffer $B$ connects external network communication module $L$ with data filter module $F_1$. Any user can read this buffer. $B_f$ is the composite output buffer receiving input for module $F_1$. $B_1$ is the buffer for subject $l_1$' s information from module $L$ to module $F_1$, and $B_2$ is the buffer for subject $l_2$' s information from module $L$ to module $F_1$. Subjects $l_1$ and $l_2$ can write to their corresponding buffers, while $F_1$ can read information from these buffers. Both subjects $l_1$ and $l_2$ can write to buffer $B$, and $F_1$ can read this buffer. [Figure 8: see original paper] depicts this composition.

**Specific Analysis**: When module $L$ transfers messages to module $F_1$, subjects $l_1$ and $l_2$ each execute the first step of their respective algorithms. If module $F_1$ reads a value from $B_1$, subject $l_1$ completes the subsequent steps of its algorithm, and information is written to buffer $B_f$, while buffer $B_1$ is also written with a value. Similarly, if module $F_1$ reads a value from $B_2$, subject $l_2$ completes the subsequent steps of its algorithm, and buffer $B_2$ is also written with a value. Because $B_1$ and $B_2$ are isolated, subject $l_1$ cannot read buffers $B_2$ and $B_f$, making the system secure at this point.

However, when the sub-information packet size exactly matches the corresponding buffer size, during message transfer from module $L$ to module $F_1$, information packet $p_1$ executes the first step of algorithm $A_1$, and information packet $p_2$ executes the first step of algorithm $A_2$. If module $F_1$ reads a value from $B_1$, subject $l_1$ completes the subsequent steps of its algorithm, and information is written to buffer $B_f$, while buffer $B_1$ is also written with a value. Similarly, if module $F_1$ reads a value from $B_2$, subject $l_2$ completes the subsequent steps of

its algorithm, and buffer $B_2$ is also written with a value. The information read by module $F_1$ is copied one-to-one into buffer $B_f$, allowing high-level module information to flow into low-level modules through a covert channel (shown as dashed lines in the figure), making the internal system of the one-way network safety equipment insecure at this point.

In the above example, finite-length buffers using blocking send and receive operations serve as leaking covert channels. To prevent this information leakage, we propose the following improvement scheme (policy completeness), shown in [Figure 9: see original paper]:

Each information packet composed of subjects at the same level passes through only one buffer between adjacent modules. As shown in [Figure 9: see original paper], information packets $p_1$ and $p_2$ have $level(p_1) < level(p_2)$, so the output buffers for the two information packets are $B_f$. Without loss of generality, treat $P$ as an information packet set. If $P = \{p_1, p_2, ..., p_n\}$, then let information packet $p_1$' s subset cyclically execute algorithm $A_1$, and information packet $p_2$' s subset cyclically execute algorithm $A_2$.

**Conclusion**: When each module within the one-way network safety equipment uses serial connections, and each information packet of subjects/objects at the same level within each module has only one corresponding buffer, the internal system of the one-way network safety equipment is secure.

### 3.2 Communication System Security

We now consider the security of the entire system composed of the sending end, one-way network safety equipment, and receiving end. Without loss of generality, we can assume several transmission paths for users with different security levels in the system, as shown in [Figure 10: see original paper].

Let $P_{CL1}$, $P_{CL2}$, $P_{CL3}$ be users in the low-security-level network end $D_L$ accepting information from $D_L$, and $P_{CH1}$, $P_{CH2}$ be users in the high-security-level network end $D_H$ accepting information from $D_H$. Let $CR_A$, $CR_B$, $CR_C$, $CR_D$, $CR_F$ be sets of communication modules composed of serially connected communication modules (referred to as communication serial sets), with $CR_A \cap CR_B \cap CR_C \cap CR_D \cap CR_F = \emptyset$.

From the analysis conclusion in Section 3.1, we know that certain information flow protocols in [Figure 10: see original paper] would place the entire communication system in an insecure state. Therefore, the following policy improvements must be made to enable the one-way network safety equipment to achieve the desired security effect, as shown in [Figure 11: see original paper]:

The internal structure of the one-way network safety equipment contains only one communication serial set, or users at the same security level within the same security-level network end are processed by only one specific communication serial set. Information transfer in this structure ensures the security of the overall communication system.

## 4 Conclusion

Traditionally, people often rely on experience to design one-way network safety equipment, making it difficult to articulate their inherent security properties. This paper uses noninterference models to formally analyze and discuss the security of one-way network safety equipment, and through rigorous mathematical proof, determines its complete security policies. The conclusions are as follows:

a) Within the one-way network safety equipment, when communication modules use serial connections and each information packet of subjects/objects at the same level has only one corresponding buffer, the one-way network safety equipment is secure.

b) If the entire communication system composed of the sending end, one-way network safety equipment, and receiving end is to be secure, then the one-way network safety equipment must contain only one communication serial set, or users at the same level within the sending end must be processed by only one specific communication module serial set.

This design has obvious drawbacks: for users at the same level, waiting for processing by the same communication module is time-consuming. Therefore, consideration should be given to making the processing capability of internal communication modules in the one-way network safety equipment far greater than their reading capability.

Future work will further refine and classify the composite transfer of information within each module of the one-way network safety equipment, using formal analysis methods and mathematical tools to further prove the consistency between the behavior of each module and its code, thereby obtaining a one-way network safety equipment with rigorous and complete proof.

## References

[1] Chapman D B. Building Internet firewalls [M]. Beijing: Tsinghua University Press, 1999.

[2] Phifer L. Simplifying secure remote access: SSL VPNs [C]// Proc of Business Communications Review. 2003.

[3] Comer D E. Internetworking with TCP/IP [C]// Proc of IEEE Symposium on Computers and Communications. IEEE Computer Society, 1995.

[4] Ye S, Gao H, Zhang G. VPN implementation mechanisms and system evaluation [J]. Small Microcomputer Systems, 2002, 23(9): 1053-1058.

[5] Xiong W, Liu Y. Research progress on communication network reliability [J]. Journal of Communications, 1990(4): 43-49.

[6] Tolstrup T K, Nielson F, Hansen R R. Locality-based security policies [C]// Lecture Notes in Computer Science. 2007: 185-201.

[7] Zhou Q, Xiao D, Tang Y. Design and implementation of VPN security gateway based on Linux and IPSec [J]. Computer Application Research, 2005, 22(9): 229-231, 234.

[8] Matt Bishop. Computer security: art and science [M]. Beijing: Publishing House of Electronics Industry, 2005.

[9] Denning D E. A lattice model of secure information flow [J]. Communications of the ACM, 1976, 16(5): 236-243.

[10] Bell D E, Lapadula L J. Secure computer systems: mathematical foundations [C]// Proc of Computer Security Foundations Workshop. 1973.

[11] Goguen J A, Meseguer J. Security policies and security models [C]// Proc of IEEE Symposium on Security & Privacy. 1982: 11-20.

[12] Rossum P V, Rossum P V, Smith G. Computing the leakage of information-hiding systems [C]// Proc of International Conference on TOOLS and Algorithms for the Construction and Analysis of Systems. Springer-Verlag, 2010: 373-389.

[13] Askaro A, Chong S, Mantel H. Hybrid monitors for concurrent noninterference [C]// Proc of IEEE Computer Security Foundations Symposium. 2015: 137-151.

[14] Alvim M S, Chatzikokolakis K, Palamidessi C, et al. Measuring information leakage using generalized gain functions [C]// Proc of IEEE Computer Security Foundations Symposium. 2012: 265-279.

[15] Goguen J A, Meseguer J. Unwinding and inference control [C]// Proc of IEEE Symposium on Security and Privacy. 1984: 75-75.

[16] Mclean J. Proving noninterference and functional correctness using traces [J]. Journal of Computer Security, 1992, 1: 37-58.

[17] Forster R. Non-interference properties for nondeterministic processes [D]. University of Oxford, 1999.

[18] Rafnsson W, Jia L, Bauer L. Timing-sensitive noninterference through composition [C]// Proc of International Conference on the Principles of Security and Trust. 2017.

[19] Barthe G, Kopf B. Information-theoretic bounds for differentially private mechanisms [C]// Proc of IEEE Computer Security Foundations Symposium. 2014: 191-204.

[20] Biondi F, Kawamoto Y, Legay A, et al. HyLeak: hybrid analysis tool for information leakage [C]// Proc of International Symposium on Automated Technology for Verification and Analysis. Cham: Springer, 2017: 156-163.

[21] Yasuoka H, Terauchi T. Quantitative information flow-verification hardness and possibilities [C]// Proc of IEEE Computer Security Foundations Symposium. IEEE Computer Society, 2010: 15-27.

[22] Chothia T, Kawamoto Y. Statistical estimation of min-entropy leakage [Z]. 2017.

[23] Focardi R, Gorrieri R, Martinelli F. Non interference for the analysis of cryptographic protocols [C]// Proc of International Colloquium on Automata, Languages and Programming. Springer-Verlag, 2000: 354-372.

[24] Mccullough D. Noninterference and the composability of security properties [C]// Proc of IEEE Symposium on Security and Privacy. 1988: 177-186.

[25] Bevier W R, Young W D. A state-based approach to noninterference [C]// Proc of IEEE Computer Security Foundations Workshop. 1994: 11-21.

[26] Johnson D M, Thayer F J. Security and the composition of machines [C]// Proc of the 1st IEEE Computer Security Foundations Workshop. 1988: 72-73.

*Note: Figure translations are in progress. See original paper for figures.*