[Document Name] DESCRIPTION

[Title of Invention] ANALYSIS SYSTEM, ANALYSIS METHOD, AND STORAGE MEDIUM

[Technical Field]

[0001]

The present invention relates to a technology of analyzing cryptographic communication executed by an information communication apparatus and the like.

[Background Art]

[0002]

There is a demand for a technology of analyzing communication processing executed by an information processing apparatus (such as a computer) that is connected to a communication network (hereinafter simply referred to as an "information communication apparatus"), in recent years.

[0003]

For example, such analysis of communication processing is used for analysis of behavior of an information communication apparatus during development and operation stages, or analysis of behavior of a communication processing program executed on an information communication apparatus.

[0004]

There is a particular demand in recent years for a technology for analyzing a content of improper communication processing caused by an improper computer program (a computer program includes various types of software programs, and may be hereinafter simply referred to as a "program"), such as a virus, that is executed on an information communication apparatus.

CLAIMS:

1. An analysis system comprising:

memory acquisition means for acquiring at least part of data stored in a memory unit in an information communication apparatus including a computing unit and the memory unit;

communication processing means for instructing the memory acquisition means to acquire data stored in the memory unit when determining, based on communication data transmitted and received in accordance with a cryptographic communication protocol between the information communication apparatus and a communication network, that key data including an encryption key used for encryption processing in the cryptographic communication protocol are stored in the memory unit; and

cryptanalysis means for,

extracting, based on data indicating a feature of the key data, one or more key data candidates that are candidates of the key data, from the data acquired by the memory acquisition means, the data being stored in the memory unit, and

extracting, from one or more of the key data candidates, correct key data that enables to decrypt correctly the encrypted communication data, based on a result of decrypting the encrypted communication data transmitted and received between the information communication apparatus and the communication network, by use of the extracted key data candidate, wherein

the communication processing means executes specific processing according to the communication data decrypted by the cryptanalysis means.

2. The analysis system according to Claim 1, further comprising

communication data modification means for modifying at least part of the communication data when determining, based on a result of analyzing the communication data being decrypted by the cryptanalysis means, to modify the communication data,

wherein,

the communication processing means transmits, as the specific processing, the communication data modified by the communication data modification means to at least one of the information communication apparatus and the communication network.

3. The analysis system according to Claim 2, wherein

the communication processing means

suspends communication between the information communication apparatus and the communication network when determining that key data including an encryption key used for encryption processing regarding to the communication data stored in a memory space in the information communication apparatus, and,

resumes the suspended communication processing when transmitting, as the specific processing, the communication data modified by the communication data modification means to at least one of the information communication apparatus and the communication network.

4. The analysis system according to Claim 3, wherein

the communication processing means

suspends communication between the information communication apparatus and the communication network when determining that key data including an encryption key used for encryption processing related to the communication data stored in a memory space in the information communication apparatus.

resumes communication between the information communication apparatus and the communication network when the memory acquisition means completes processing of acquiring data stored in the memory unit,

in the resumed communication, suspends again communication between the information communication apparatus and the communication network at a liming when the first encrypted communication data are transmitted and received between the information communication apparatus and the communication network, and.

resumes again the suspended communication processing when transmitting, as the specific processing, the communication data modified by the communication data modification means to at least one of the information communication apparatus and the communication network.

5. The analysis system according to any one of Claims 2 to 4 wherein

the communication data modification means

includes a communication data modification policy storing, a modification determination criterion that represents information that enables to determine whether the communication data need to be modified or not. and modification information that enables to specify a part to be modified in the communication data can be specified, in association with each other, and

modifies the to be modified in the communication data, based on the communication data modification policy.

6. The analysis system according to Claim 5, wherein

the modification determination criterion represents information that enables to distinguish a type of communication processing of transmitting and receiving the communication data , and

the communication data modification means

distinguishes a type of communication processing of transmitting and receiving the communication data, based on the modification determination criterion, and

determines whether the communication data need to be modified, based on the distinguished type of communication processing.

7. The analysis system according to Claim 6, wherein

the modification determination criterion represents information that enables to distinguish the type of communication processing of transmitting and receiving the communication, based on at least one of, a value of at least part of the communication data decrypted by the cryptanalysis means, and an attribute of the part of the communication data.

8. The analysis system according to Claim 2, wherein

the communication data modification means encrypts the modified communication data by use of the extracted correct key data, and

the communication processing means transmits the communication data encrypted by the communication data modification means to at least one of the information communication apparatus and the communication network.

9. An analysis method comprising, by an information processing apparatus:

acquiring at least part of data stored in a memory unit when determining, based on communication data transmitted and received in accordance with a cryptographic communication protocol between an information communication apparatus including a computing unit and the memory unit and a communication network, that key data including an encryption key used for encryption processing in the cryptographic communication protocol stored in the memory unit;

extracting, based on data indicating a feature of the key data, one or more key data candidates that are candidates of the key data, from the acquired data stored in the memory unit;

extracting, from the one or more key data candidates, correct key data by which the encrypted communication data can be correctly decrypted, based on a result of decrypting, by use of the extracted key data candidate, the encrypted communication data transmitted and received between the information communication apparatus and the communication

network; and

executing specific processing, based on the decrypted communication data.

10. A non-transitory computer-readable storage medium storing a computer program allowing a computer to execute:

processing of acquiring at least part of data stored in a memory unit when determining, based on communication data transmitted and received in accordance with a cryptographic communication protocol between an information communication apparatus including a computing unit and the memory unit, and a communication network, that key data including an encryption key used for encryption processing in the cryptographic communication protocol exist in the memory unit;

processing of extracting, based on data indicating a feature of the key data, one or more key data candidates that are candidates of the key data, from the acquired data stored in the memory unit;

processing of extracting, from the one or more key data candidates, correct key data by which the encrypted communication data can be correctly decrypted, based on a result of decrypting, by use of the extracted key data candidate, the encrypted communication data transmitted and received between the information communication apparatus and the communication network; and

processing of executing specific processing, based on the decrypted communication data.