논문 2010-47TC-2-14

확장 화이트리스트 기법을 이용한 SPIT 대응 프레임워크

(SPIT Prevention Framework using Expanded White List)

배 광 용*, 채 강 석**, 김 영 범***

(Kwang-Yong Bae, Kang-suk Chae, and Young-Beom Kim)

요 약

본 논문에서는 실시간 동작 환경인 VoIP에 적용 가능한 SPIT 대응 기법으로서 확장 화이트리스트 기법과 이를 적용한 SPIT 대응 프레임워크를 제안한다. SPIT을 차단하기 위한 연구가 다양하게 진행되고 있지만, SPIT 대응을 위한 기존 기법들은 스패머가 자신의 ID를 바꿔가면서 지속적으로 SPIT을 전송하는 공격에 취약하다. 또한 기존 SPIT 대응 프레임워크들은 프레임워크를 구성하고 있는 모든 SPIT 대응 기법들이 실시간으로 수행되어야 하기 때문에 콜 세션 설립 시간에 지연이 발생한다. 제안 기법은 화이트리스트를 이용한 사회망을 형성하여 화이트리스트의 범위를 확장하지만, 전체 데이터베이스를 검색하지 않고 빠르게 그 통과 여부를 결정하는 방법이다. 제안하는 SPIT 대응 프레임워크는 3 단계 구성과 Fast Scoring 시스템을 이용하여 사용자의 직접적인 개입으로 인한 사용자의 불편성과 세션 설립 시간 지연을 최소화한다. 따라서 제안 기법 및 프레임워크는 실시간 동작을 요구하는 VoIP 환경에서 SPIT에 효과적으로 대응할 수 있다.

Abstract

This paper proposes a SPIT(Spam over IP Telephony) prevention framework which is using expanded white-list in real-time VoIP environment. The existing schemes are vulnerable to attack from spammers since they can continue to transfer SPIT upon changing their ID. And existing frameworks have experienced the time delay and overload as session initiates due to real-time operation. To solve these problems, the proposed scheme expands the scope of white lists by forming social networks using the white list, but it is to decide quickly whether pass a caller ID without searching the entire database. The proposed framework takes the three-stage architecture and the fast scoring system. The proposed framework minimize user's inconvenience and time delay for initiation of session, therefore, it is proper for real-time VoIP environment.

Keywords: VoIP, Spam, SPIT, White List

I. 서 론

최근 VoIP 기술의 발전으로 이에 대한 서비스가 상용화되어 활발히 상품화되면서 VoIP 스팸 문제가 중요한 이슈가 되고 있다. 특히 SIP[1] 기반의 VoIP 환경에서 SIP는 텍스트 기반의 프로토콜로써 기존 이메일 시스템과 비슷한 스팸 공격이 가능하며, 인터넷 기반의 VoIP 환경은 PSTN 환경보다 비용이 저렴하기 때문에 쉽게 스팸 공격이 가능하다.

SPIT 대응을 위한 기법으로는 크게 이메일 스팸 대응 기법을 활용하는 방법, VoIP 및 SIP의 고유한 특성을 이용한 방법으로 나뉜다. 이메일 스팸 대응 기법을 활용한 방법으로는 화이트/블랙리스트와 같은 리스트 기법들과 평판도 시스템 및 Payment at risk 기법[2], Turing 테스트 기법[3~4] 등이 있다. 그러나 리스트 기법 중 블랙리스트는 스패머가 자신의 ID를 바꿔가면서 SPIT을 전송할 경우 블랙리스트를 회피할 수 있는 단점이 있다. 또한 평판도 시스템 및 Payment at risk 기법, Turing 테스트 기법 등은 사용자의 개입이 요구되는 불편성이 있다. SPIT 대응을 위한 다른 방법으로

* 정회원, KT 기술개발실 (KT)
** 학생회원, 숭실대학교 정보통신전자공학부 (Soongsil University)
*** 정회원, 건국대학교 전자공학부 (Kunkuk University)
접수일자: 2009년10월22일, 수정완료일: 2010년2월17일

VoIP 및 SIP의 고유한 특징을 이용한 Simultaneous calls, Call rate, Number of error messages associated with the caller, Progressive Multi Gray-Leveling (PMG) 등과 같이 사용자의 행동 패턴을 분석하는 SPIT 대응 기법들이 있다[5~7].

화이트리스트 기법은 스패머가 자신의 ID를 바꿔가며 SPIT을 전송하는 것에 영향을 받지 않으며, 화이트리스트 기법을 통과할 경우 다른 SPIT 대응 기법을 사용하지 않고 빠르게 콜 연결 요청을 수락할 수 있는 장점이 있다. 이러한 이유로 사회망 (Social Network)을 이용한 화이트리스트 이메일 필터링 기법이 제안되었다[8]. 이 기법은 VoIP 환경에 적용이 가능하지만, 사회망 전체의 데이터베이스를 검색하는데 소요되는 시간 때문에 실시간 동작을 요구하는 VoIP 환경에 그대로 적용하기에는 무리가 있다. 또한 사회망 이메일 필터링 기법에서는 신뢰도를 계산하는 적절한 방법이 제시하고 있지 않다.

SPIT 대응을 위한 프레임워크로는 화이트리스트에 중점을 두고 구성하는 방법[9], 사용자의 개입 여부를 고려한 단계적 구성 방법[5], SPIT 검출 및 반응 시스템으로 구성하는 방법 등이 있다[6].

본 논문의 구성은 다음과 같다. Ⅱ장에서 SPIT 대응을 위한 관련 연구들을 살펴보고, Ⅲ장에서 SPIT 대응을 위한 확장 화이트리스트 기법과 이를 적용한 SPIT 대응 프레임워크를 제안한다. Ⅳ장에서 제안 기법을 분석한 후, 마지막으로 Ⅴ장에서 연구에 대한 결론을 맺는다.

Ⅱ. 관련 연구

VoIP 환경에서 발생할 수 있는 스팸에는 텍스트 기반의 인스턴트 메시징 스팸과 프리젠스 스팸, 그리고 콜 스팸 형태의 SPIT으로 나뉜다[9]. 이러한 SPIT 대응 기법들은 어느 하나의 기법만으로 모든 SPIT에 대하여 완벽하게 대응하기 어렵기 때문에 다양한 기법들을 적절하게 배치하는 SPIT 대응 프레임워크 연구도 필요하다.

1. SPIT 대응 기법

SPIT 대응 프레임워크에 적용 가능한 기법으로는 이메일 환경에서의 사용하는 스팸 대응 방법과 VoIP 및 SIP의 고유한 특성을 이용한 SPIT 대응 방법으로 구분하여 볼 수 있다.

이메일 환경에서 스팸 대응을 위한 대표적인 기술로 블랙/화이트 리스트 기법이 있다. 블랙리스트 기법은 스패머로 식별된 사용자 혹은 수신자의 수신거부 피드백을 받은 사용자를 데이터베이스로 구축한 블랙리스트 내의 사용자의 연결을 거부하는 방법이다. 화이트리스트는 블랙리스트와 반대 개념의 리스트로, 연결을 허용할 사용자를 데이터베이스로 구축한 것이다.

이메일 스팸 대응 기법을 VoIP 환경에 맞게 응용하는 방법으로는 평판도 시스템, Payment at risk 방법, Turing 테스트 기법을 이용한 기법들이 있다[2~4]. 그러나 이러한 SPIT 대응 기법들은 사용자의 직접적인 개입으로 사용자의 불편성이 있거나 세션 설립시 지연이 발생하는 문제점이 있다.

VoIP 및 SIP의 고유한 특성을 이용한 SPIT 대응 기법은 Simultaneous calls, Call rate, Number of error messages associated with the caller와 같은 모니터링을 통한 방법들이 있다[5~6]. Shin 등은 앞에서 살펴본 모니터링 기법들과 같이 하나의 주기만 가지고 있을 경우 세션 설립 주기의 조절을 통한 지속적인 SPIT 공격이 가능한 문제가 있기 때문에 두 개의 모니터링 주기를 두고 Leveling하는 Progressive Multi Gray-Leveling (PMG) 기법을 제안하였다[7]. 이러한 모니터링을 이용한 기법들은 발신자의 과거 행동 분석을 통한 SPIT 여부를 판단하는 기법이기 때문에 스패머가 자신의 ID를 바꿔가면서 SPIT 전송을 할 경우 대응하기 힘든 단점이 있다.

이메일 스팸 대응 기법으로 화이트리스트의 구성원간의 연결성을 이용하여 사회망을 형성하고, 스팸을 차단하는 사회망 필터링 기법이 Reeves에 의해 제안되었다[8]. 사회망 필터링 기법은 사회망 전체 데이터베이스를 검색해야 하는 시간지연의 문제를 가지고 있어서 실시간 동작을 요구하는 VoIP 환경에 그대로 적용하기는 어렵다. 또한 이 기법에서는 사회망을 이용한 신뢰도를 계산하는 방법을 구체적으로 제시하지 못하고 있다.

2. SPIT 대응 프레임워크

IETF RFC 5039 표준에서는 화이트리스트에 중점을 둔 프레임워크를 구성하는 방법을 제시하고 있다[9]. 이 표준에서는 SPIT 대응 프레임워크를 구성하기 위한 권장사항으로 강한 사용자 인증, 화이트리스트, 화이트리스트로의 사용자 추가 문제의 3가지 사항을 제시해주고

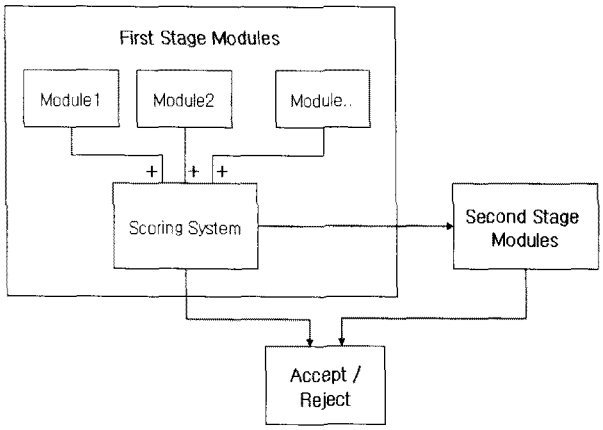

그림 1. 두 단계 구조를 갖는 SPIT 대응 프레임워크[5]
Fig. 1. SPIT prevention framework with two-step architectures[5].

있다. Schlegel 등은 SPIT 대응을 위한 프레임워크로 사용자의 개입 여부를 이용한 두 단계의 구조를 가지고 동작하는 프레임워크를 제안하였다[5]. 첫 번째 단계에서는 사용자의 개입 없이 SPIT을 판단하는 여러 기법들을 병렬로 배치하고, 각 기법의 결과를 합산하여 상향 임계값보다 크면 SPIT으로 판단한다. 각 기법의 결과 값은 SPIT으로 판단되면 1의 값을 가지고, 그렇지 않은 경우에는 -1의 값을 가진다. 이러한 각 기법 결과 값의 합이 상향 임계값보다 크면 SPIT으로 판단하여 세션 연결 요청을 거절하고, 하향 임계값보다 작으면 SPIT이 아님으로 판단하여 세션 연결 요청을 허락한다. 두 번째 단계에서는 사용자의 직접적인 개입이 필요한 Turing 테스트 같은 기법으로 SPIT 여부를 판단한다. 이 프레임워크는 사용자에 대한 강한 인증은 대부분의 SPIT 대응 기법에서도 필요하기 때문에 이를 제외한 프레임워크는 그 성능이 떨어진다.

Mathieu 등은 그림 2와 같이 사용자 구분 시스템, SPIT 검출 시스템, SPIT에 대한 반응 시스템을 주요 구성 요소로 가지는 SDRS (Spam Detection and Reaction System)을 제안하였다[6]. 사용자 구분 시스템은 사용자들의 피드백을 받아 사용자들의 행동 패턴을 수집하는 일종의 데이터베이스 시스템이다. SDRS의 두 번째 구성 요소인 SPIT 검출 시스템은 다양한 스팸 대응 기법들의 점수를 통한 SPIT 레벨을 계산하는 시스템이다. 마지막으로 세 번째 구성 요소인 SPIT에 대한 반응 시스템은 사용자 구분 시스템의 결과와 SPIT 검출 시스템의 SPIT 레벨에 따라서 어떻게 정책을 적용하여 반응할 것인지 결정하는 시스템이다. 이 프레임워크는 모든 SPIT 대응 기법들의 결과가 필요하기 때문에 실시간 동작이 요구되는 VoIP 환경에 적용성이 떨어지는 단점을 가지고 있다.

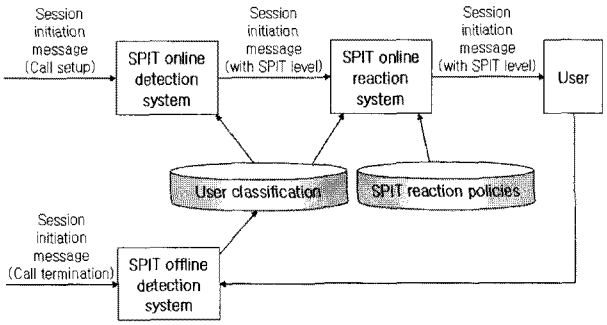

그림 2. SPIT Detection and Reaction System (SDRS)[6]
Fig. 2. SPIT Detection and Reaction System (SDRS)[6].

III. 제안 기법 및 프레임워크

1. 확장 화이트리스트

본 논문에서는 Reeves가 제안한 사회망 필터링 기법을 VoIP 환경에 맞게 적용하기 위한 방법으로 전체 데이터베이스를 검색하지 않고 적절한 수준 범위만을 검색하여 발신자의 신뢰 여부를 결정할 수 있는 확장 화이트리스트 기법을 제안한다. 확장 화이트리스트의 적용 개념은 그림 3과 같다. 사용자 A는 자신의 화이트리스트 내에 있는 사용자 B를 신뢰하고, 사용자 B는 자신의 화이트리스트 내에 있는 사용자 C를 신뢰한다. 사용자 A는 자신이 신뢰하는 B가 신뢰하는 사용자 C를 신뢰할 수 있다.

본 논문에서는 수신자 화이트리스트 내의 사용자를 0 수준 범위 사용자, 0 수준 범위 사용자들의 화이트리스트에 포함된 모든 사용자를 1 수준 범위 사용자와 같이 이전 수준 사용자들의 화이트리스트에 포함된 사용자를

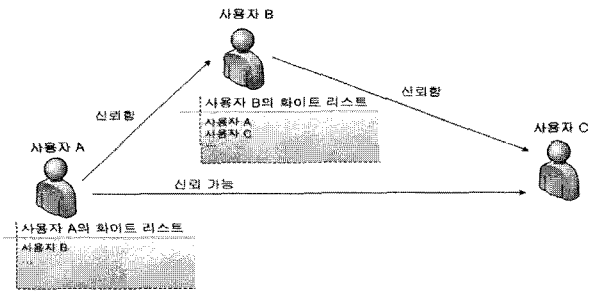

그림 3. 확장 화이트리스트의 적용 개념
Fig. 3. Concept of Expanded White List.

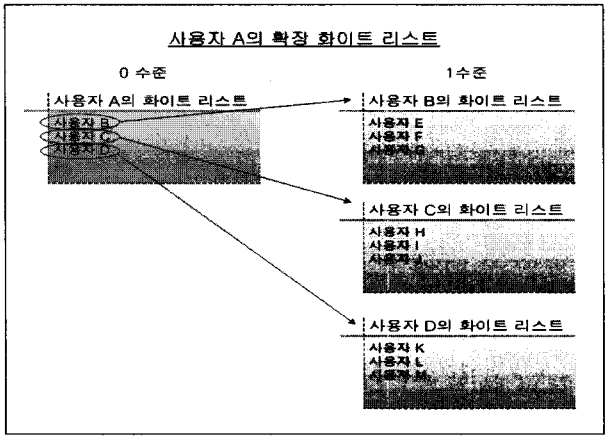

그림 4. 확장 화이트리스트 예
Fig. 4. Example of Expanded White List.

다음 수준 범위 사용자로 하는 각 수준의 범위를 정의한다. 만약 확장 화이트리스트의 범위를 1수준까지로 정의할 경우 그림 4와 같다.

각 i 수준에서의 사용자에 대한 신뢰도는 R_i로 정의한다. 확장 화이트리스트에서 0 수준 사용자들의 신뢰도는 1이고, 1 수준 이상 수준에서의 신뢰도 R_i는 1보다 작은 값을 가지지만 각 수준 범위에 해당 사용자가 많이 검색될수록 해당 수준에서의 신뢰도는 1에 가까워진다. i 수준의 화이트리스트에 해당 사용자가 검색되는 횟수를 n_i라고 할 때 신뢰도 R_i를 구하는 식은 다음과 같다.

$$\begin{cases} R_0 = R_1 \text{ or } 1 & ,i=0 \\ R_i = \dfrac{n_i + R_{i+1}}{w + n_i + R_{i+1}} & ,i>0 \end{cases} \quad (1)$$

$$(0 \le R_i < 1,\ 0 < w \le 1)$$

식 (1)에서의 w는 각 수준 간 획득 신뢰도 차이를 위한 가중치로서 다음 수준의 사용자가 가질 수 있는 최소한의 신뢰도를 결정하는 값이다. 다음 수준의 범위에 포함된 사용자에 대한 신뢰도는 적어도 이전 수준의 신뢰도 1의 절반인 0.5 이상이 되도록 하고, 이를 위해서는 w 값이 1이하가 되어야 한다. 따라서 식 (1)과 같은 w의 범위를 정의한다. 신뢰도 계산식은 이후 수준의 신뢰도가 아무리 높더라도 이전 수준에서의 한명에 대한 신뢰도보다 낮은 값을 갖는 기준을 두고 설계하였다. 예를 들면, 사용자는 본인의 화이트리스트 내의 사용자를 1 수준 이상의 화이트리스트에 포함된 임의의 다른 사용자보다 신뢰할 수 있다. 즉, 임의의 다른 사용자가 해당 수준에서 화이트리스트에서 검색된 횟수가 다수가 되더라도 이전 수준의 한명에 대한 신뢰도보다 높지 않다. 0 수준을 제외한 각 수준의 신뢰도는 $0 \le R_i < 1$ 이고, 식 (2)와 같은 조건을 갖게 된다. (이하 계산식은 0 수준을 제외한 1 수준 이상으로 적용)

$$\frac{n_i}{w+n_i} \le \frac{n_i + R_{i+1}}{w + n_i + R_{i+1}} < \frac{n_i + 1}{w + n_i + 1} \quad (2)$$

확장 화이트리스트의 i 수준의 신뢰도 임계값을 T_i라고 할 때, 최종 임계값 T는 확장 화이트리스트 통과를 위한 신뢰도의 임계값이며 $T = T_1$이다. 임계값 T_i를 확실히 넘을 수 있는 최소의 정수 n_i를 $n_{pass(i)}$라고 하고 임계값을 확실히 넘지 못하는 최대의 정수 n_i를 $n_{fail(i)}$라고 할 때, 임계값 이상의 값을 갖는 신뢰도에 대한 조건을 식 (3)과 같이 나타낼 수 있으며, 임계값 T_i 이상의 값을 갖는 신뢰도 R_i를 만족하는 최소의 정수인 $n_{pass(i)}$를 구할 수 있다.

$$\begin{aligned} & T_i \le \frac{n_{pass(i)}}{w + n_{pass(i)}} \le R_i \\ & \Rightarrow \frac{w T_i}{1 - T_i} \le n_{pass(i)} \end{aligned} \quad (3)$$

임계값 미만의 값을 갖는 신뢰도에 대한 조건은 식 (4)와 같이 나타낼 수 있으며, 이를 정리하면 $n_{fail(i)}$를 구할 수 있다.

$$\begin{aligned} & R_i < \frac{n_{fail(i)} + 1}{w + n_{fail(i)} + 1} \le T_i \\ & \Rightarrow n_{fail(i)} \le \frac{w T_i}{1 - T_i} - 1 \end{aligned} \quad (4)$$

만약 $n_{pass(i)}$와 $n_{fail(i)}$ 사이의 n_i가 존재하고, 사용자 검색 횟수가 n_i일 때 다음 수준의 신뢰도에 따라서 확장 화이트리스트 통과 여부가 결정된다. 이와 같이 다음 수준의 검색이 필요한 경우의 n_i를 $n_{continue(i)}$로 정의하고, 식 (5) 과정으로 유도된 식에 대입하여 다음 수준의 임계값 T_{i+1}을 구한다. 이후 그 다음 수준의 통과 여부를 식 (3), (4) 과정을 반복하여 결정한다.

$$\begin{aligned} & T_i \le R_i = \frac{n_{continue(i)} + R_{i+1}}{w + n_{continue(i)} + R_{i+1}} \\ & \Rightarrow w T_i + n_{continue(i)} T_i + R_{i+1} T_i \le n_{continue(i)} + R_{i+1} \\ & \Rightarrow w T_i - (1 - T_i) n_{continue(i)} \le (1 - T_i) R_{i+1} \\ & \Rightarrow T_{i+1} = \frac{w T_i}{1 - T_i} - n_{continue(i)} \le R_{i+1} \end{aligned} \quad (5)$$

본 논문에서 제안한 확장 화이트리스트 신뢰도 계산식은 이후 수준의 신뢰도를 포함하고 있기 때문에 전체 화이트리스트 사회망의 신뢰도를 고려한다고 볼 수 있다.

2. SPIT 대응 프레임워크

본 논문에서 제안하는 SPIT 대응 프레임워크는 Schlegel 등이 제안한 프레임워크[5]를 개선하는 방향으로 구성한다. 본 논문에서 제안하는 SPIT 차단 프레임워크는 다음과 같은 기준 조건을 바탕으로 구성하였다.

- 효과적인 SPIT 대응을 위한 강한 사용자 인증
- VoIP의 실시간 동작 환경을 고려한 구성
- SPIT 대응 기법으로 인한 사용자 불편성 최소화

그림 5는 앞의 조건을 만족하는 제안 SPIT 대응 프레임워크의 구성을 보여준다. 크게 3 단계의 구성을 가지는 제안 프레임워크는 각 단계별로 다음과 같은 특징을 갖는다.

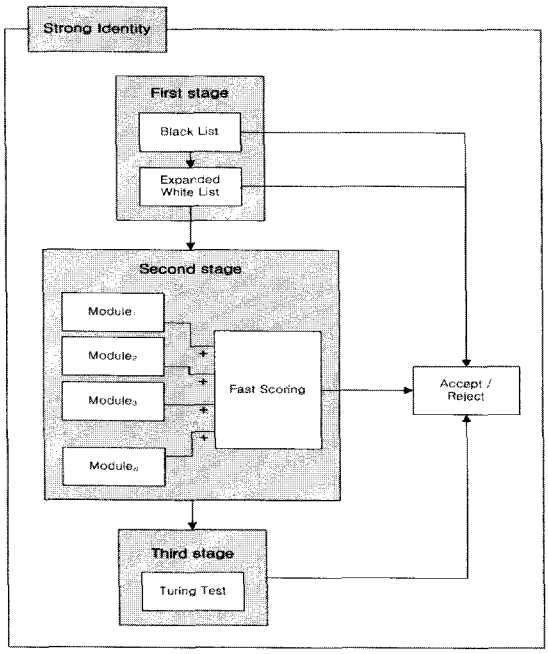

그림 5. 제안 SPIT 대응 프레임워크
Fig. 5. Proposed SPIT prevention framework.

• 단계 1(First stage)

단계 1은 수신자의 사전 피드백 정보를 담고 있는 리스트 기법을 활용한 단계로 블랙리스트와 제안 기법인 확장 화이트리스트를 포함한다. 발신자가 확장 화이트리스트 기법을 통과할 경우 바로 연결 요청을 수락한다. 따라서 확장 화이트리스트 기법을 단계 1에 적용함으로써 SPIT 판단을 위한 다음 단계를 수행하지 않는 정상 사용자의 범위를 증가시켜 사용자 불편성 및 세션 설립 시간 지연을 감소시키는 효과를 가질 수 있다. 만약 프레임워크 단계 1에서 발신자에 대한 SPIT 여부를 판단할 수 없으면 단계 2를 수행한다.

• 단계 2(Second stage)

단계 2는 사용자의 직접적인 개입이 필요하지 않는 SPIT 대응 기법들로 구성된다. 단계 2를 구성하는 SPIT 대응 기법은 병렬로 배치되고, SPIT 판단을 위한 결과 값으로 0과 1 사이의 값을 갖는다. 각 기법은 발신자에 대하여 스패머로 판단될 경우 0의 결과를 가지며, 정상적인 사용자로 판단될 경우 1의 결과를 가진다. 신뢰 레벨은 각 기법의 결과에 가중치를 적용하여 합산한 값이다. 두 번째 단계에서 n개의 기법으로 구성되어 있고, 각 기법의 결과 값이 R_i, 각 기법의 가중치가 w_i일 때 신뢰 레벨 L은 식 (6)과 같이 구할 수 있다.

$$L = \sum_{i=1}^{n} w_i R_i \tag{6}$$

$$L_{\max} = \sum_{i=1}^{n} w_i \tag{7}$$

최대 획득 가능한 신뢰 레벨 L_{max}는 모든 기법의 결과 값이 1인 경우로 식 (7)과 같이 구할 수 있으며, L_{max}를 기준으로 SPIT 판단을 위한 임의의 상향 임계값과 하향 임계값을 결정한다. 발신자에 대한 신뢰 레벨 L이 상향 임계값 이상이 되면 연결 요청을 수락하고, 하향 임계값 이하가 되면 연결 요청을 거절한다. 각 기법에서 발신자가 정상 사용자로 판단될 경우의 결과 값을 1로 결정하였기 때문에 모든 기법의 결과 값이 나오지 않았을 경우라도 계산된 신뢰 레벨이 상향 임계값 이상이 되면, 이후의 처리 속도가 느린 기법의 결과를 기다리지 않고 빠르게 연결 요청을 수락할 수 있다 (Fast Scoring 시스템). 신뢰 레벨이 상향 임계값과 하향 임계값 사이일 경우 단계 3을 수행하여 발신자에 대한 SPIT 판단을 한다.

• 단계 3(Third stage)

제안 SPIT 대응 프레임워크의 최종단계인 단계 3은 사용자의 개입으로 확실하게 SPIT 여부를 판단한다.

표 1. 가중치와 임계값에 따른 확장 화이트리스트 동작
Table 1. Operation of the Expanded White List according to threshold and weight values.

가중치 w	1 수준			2 수준			3 수준			비고
	임계값 T_1	$n_{pass(1)}$	$n_{fail(1)}$	$T_2(n_{continue(1)})$	$n_{pass(2)}$	$n_{fail(2)}$	$T_3(n_{continue(2)})$	$n_{pass(3)}$	$n_{fail(3)}$	
0.5	0.5	1	×	0.5(0)	1	×	0.5(0)	1	×	4수준 이상 검색
	0.6	1	×	0.75(0)	2	0	0.5(1)	1	×	4수준 이상 검색
	0.7	2	0	0.16(1)	1	×	0.1(0)	1	×	4수준 이상 검색
	0.8	2	1	×	×	×	×	×	×	1수준만 검색
	0.9	5	3	0.5(4)	1	×	0.5(0)	1	×	4수준 이상 검색
1	0.5	1	0	×	×	×	×	×	×	1수준만 검색
	0.6	2	0	0.5(1)	1	0	×	×	×	2수준만 검색
	0.7	3	1	0.33(2)	1	×	0.5(0)	1	0	3수준만 검색
	0.8	4	3	×	×	×	×	×	×	1수준만 검색
	0.9	9	8	×	×	×	×	×	×	1수준만 검색

자동 SPIT 발송 여부 판단을 위한 challenge를 발신자에게 전송하고 응답을 확인하는 Turing 테스트와 같은 사용자 개입이 필요한 기술이 이 단계에 포함된다. 만약 자동화 도구를 이용한 SPIT 발신자라면 Turing 테스트를 통과하지 못하고 이 연결 요청은 거절된다.

IV. 제안 기법 분석

1. 확장 화이트리스트 기법의 효율성 분석

본 논문에서는 화이트리스트의 효과적인 적용을 위하여 화이트리스트의 적용 범위를 넓히기 위한 방법을 제안하였다. 확장 화이트리스트 기법은 화이트리스트보다 적용 범위가 넓지만, 적용 범위를 모두 검색하지 않고 각 범위에 따른 기준으로 통과 여부를 결정할 수 있어서 효율적이다.

본 논문에서는 확장 화이트리스트를 통과하기 위한 기준이 되는 신뢰도 계산식을 제안하였으며, 이 계산식은 확장 화이트리스트의 모든 범위를 고려하고 있으나 전체 데이터베이스를 검색할 필요가 없이 각 수준 범위에서 발신자가 검색되는 횟수를 이용하여 확장 화이트리스트의 통과 여부를 빠르게 결정할 수 있다.

확장 화이트리스트의 동작을 임의의 임계값과 가중치를 적용하여 살펴보면 표 1과 같다. 확장 화이트리스트의 0 수준에 발신자가 없을 경우 1 수준부터 발신자가 있는지 검색을 시작한다. 이 때 확장 화이트리스트 통과를 위한 신뢰도의 임계값은 T_1과 같다. 표 1에서 임계값에 따른 $n_{pass(i)}$는 확장 화이트리스트를 통과할 수 있는 i 수준에서 발신자 검색 횟수의 최소값, $n_{fail(i)}$는 확장 화이트리스트를 통과할 수 없는 i 수준에서 발신자의 검색 횟수의 최대값이고, $n_{continue(i)}$는 $n_{pass(i)}$와 $n_{fail(i)}$ 사이의 값으로 다음 수준의 검색이 필요하다고 판단되는 i 수준에서 발신자의 검색 횟수를 나타낸다. T_i는 i 수준에서 확장 화이트리스트 통과를 위한 해당 수준의 평판도에 대한 임계값으로 $n_{continue(i-1)}$과 T_{i-1}의 값에 따라 결정된다 (단, $T=T_0=T_1$, $n_{continue(0)}=0$).

표 1과 같이 해당 수준의 범위에서 발신자가 검색되는 횟수에 따라서 확장 화이트리스트의 통과 여부 또는 다음 수준의 검색 여부를 빠르게 결정할 수 있다. 또한 가중치와 임계값의 설정에 따라서 일정 수준 범위 내에서 확장 화이트리스트의 통과 여부가 결정되기도 한다. 가중치 w가 0.5이고 임계값 T_i가 0.8일 때 1수준에서 확장 화이트리스트를 통과할 수 있는 발신자의 검색 횟수가 2이고, 통과할 수 없는 발신자의 검색 횟수가 1인 것과 같이 1수준 내에서 확장 화이트리스트 통과 여부가 결정된다. 그러나 가중치 w가 0.5이고 임계값 T_1이 0.5일 경우에는 다음 수준의 검색이 필요한 패턴이 무한히 반복된다. 이와 비슷하게 특정한 값의 가중치와 임계값에 따라서 4 수준 이상의 검색이 필요한 패턴이 발생하는 것을 표 1의 예를 통해 확인할 수 있다. 따라서 실시간 VoIP 환경을 고려하여 일정 수준의 범위 내에서 확장 화이트리스트의 통과 여부가 결정되기 위한 적절한 가중치와 임계값의 설정이 필요하다. 각 수준 범위 내에서 확장 화이트리스트의 통과 여부가 결정되기 위한 가중치와 임계값의 조건은 식 (8)의 n이 자연수가 되는 것이다. 자연수가 되는 n의 의미는 확장 화이트리스트를 통과할 수 있는 i 수준 범위 내 사용자의 검색횟수

$n_{pass(i)}$이다.

$$\frac{w T_i}{1-T_i}=n \quad (8)$$

$$(0.5 \le T_i < 1,\ 0 < w \le 1,\ n \in N)$$

실시간 VoIP 환경에서 확장 화이트리스트가 효과적으로 동작하기 위하여 그 범위를 1 수준으로 정의하고, 이때의 가중치와 임계값을 식 (8)을 이용하여 결정할 수 있다. 그림 6은 임계값 및 가중치에 따른 식 (8)의 결과를 나타내는 그래프이다. 그림 6에서 임계값 T에 따른 조건식의 결과 n이 자연수가 되는 경우의 w가 확장 화이트리스의 범위를 1 수준이 되게 하는 가중치이다. 확장 화이트리스트 범위를 1 수준이 되게 하는 임계값에 따른 순환소수를 제외한 유리수로 구해지는 가중치는 표 2와 같다. 이때 임계값에 따른 가중치 및 확장 화이트리스트 통과를 위한 사용자 검색 횟수의 쌍은 6개임을 확인할 수 있다. 이와 같은 방법으로 확장 화이트리스트의 적절한 범위를 갖는 임계값과 가중치를

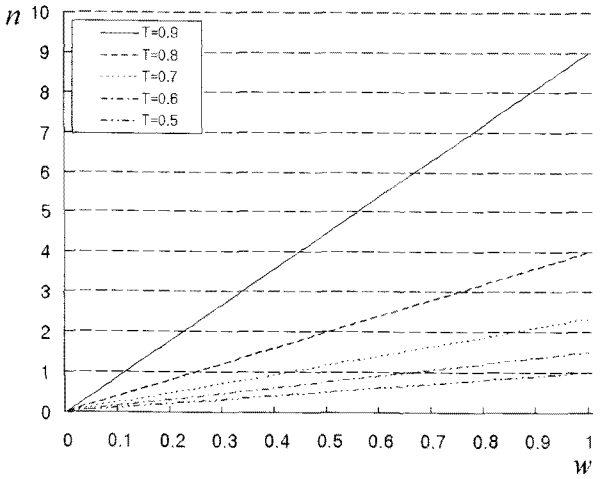

그림 6. 임계값 및 가중치에 따른 조건식 결과
Fig. 6. The result of a conditional expression according to threshold and weight values.

표 2. 확장 화이트리스트 범위를 1 수준으로 갖기 위한 임계값에 따른 가중치 및 확장 화이트리스트 통과를 위한 사용자 검색 횟수 (w, $n_{pass}(1)$)
Table 2. The (w, $n_{pass}(1)$) to pass the Expanded White List according to thresholds on 1 level.

임계값 T	(w, $n_{pass(1)}$)
0.5	(1, 1)
0.6	없음
0.7	없음
0.8	(0.25, 1), (0.5, 2), (0.75, 3), (1, 4)
0.9	(1, 9)

결정하여 실시간 VoIP 환경에 적용이 가능하다.

2. 제안 프레임워크의 효과 및 요구사항 분석

본 논문에서 제안한 SPIT 대응 프레임워크는 단계적으로 동작을 하며, 각 단계별로 SPIT 여부를 판단하여 연결 요청에 대한 수락 및 거절 여부를 결정한다. 제안한 SPIT 대응 프레임워크는 리스트 기법을 별도의 단계로 구분하고 직접적인 사용자 개입 여부로 다시 단계를 구분한 3 단계 구조를 가짐으로써 실시간 동작성과 사용자 불편성 감소와 같은 장점을 모두 가진다. 특히 단계 1의 확장 화이트리스트 기법은 정상 사용자에 대한 범위를 넓혀주고, 단계 2의 Fast Scoring 시스템은 각 기법의 결과로 SPIT 레벨을 계산하지 않고 신뢰 레벨을 계산함으로 정상적인 사용자를 더욱 빠르게 판단하는 효과를 가진다.

그러나 제안 SPIT 대응 프레임워크는 사용자에 대한 강한 인증을 구성 조건으로 하고 있기 때문에 만약 모든 서비스 제공자가 이와 같은 강한 사용자 인증을 지원하지 않는다면 그 성능은 떨어진다. 따라서 근본적인 SPIT 대응 효율을 높이기 위해서는 SIP 사용자 인증을 위한 HTTP 다이제스트 인증[10], 홉간 보안을 위한 TLS[11], 양 단간 인증을 위한 S/MIME[12], 또는 개선된 인증 기법[13] 등과 같은 사용자 인증 기법이 VoIP 환경에 적용되어야 한다.

V. 결 론

본 논문에서는 실시간 동작 환경인 VoIP에서 적용 가능한 SPIT 대응 방법으로써 확장 화이트리스트 기법을 이용한 프레임워크를 제안하였다. 제안 프레임워크에서의 확장 화이트리스트 기법은 전체 데이터베이스를 검색하지 않고 빠르게 확장 화이트리스트의 통과 여부를 결정하는 방법이다. 또한 제안 프레임워크는 단계적 구성과 Fast Scoring 시스템을 이용하여 정상 사용자일 경우 세션 설립을 위한 시간 지연을 최소화한다. 따라서 제안 프레임워크는 사용자의 불편성을 최소화하고 있으며, 실시간 동작을 요구하는 VoIP 환경에서 효과적으로 SPIT에 대응할 수 있다.

참 고 문 헌

[1] J. Rosenberg, H. Schulzrinne, G. Camarillo, A.

Johnston, J. Peterson, R. Sparks, M. Handley, and E. Schooler, SIP: Session Initiation Protocol, IETF RFC 3261, June 2002.
[2] Y. Rebahi, D. Sisalem and T. Magedanz, "SIP Spam Detection," in Proc. of IEEE ICDT '06, June 2006.
[3] J. Quittek, S. Niccolini, S. Tartarelli, and R. Schlegel, "Prevention of Spam over IP Telephony," *NEC Technical Journal*, vol. 1, no. 2, pp. 114-119, February 2006.
[4] J. Quittek, S. Niccolini, S. Tartarelli, M. Stiemerling, M. Brunner, and T. Ewald, "Detecting SPIT Calls by Checking Human Communication Patterns," proc. of ICC '07, June 2007.
[5] R. Schlegel, S. Niccolini, S. Tartarelli, M. Brunner, "SPam over Internet Telephony (SPIT) Prevention Framework," in Proc. of IEEE GLOBECOM '06, November 2006.
[6] B. Mathieu, S. Niccolini, and D. Sisalem, "SDRS: A Voice-over-IP Spam Detection and Reaction System," IEEE Security and Privacy, vol. 6, no. 6, pp. 52-59, November/December 2008.
[7] D. Shin, J. Ahn, C. Shim, "Progressive Multi Gray-Leveling: A Voice Spam Protection Algorithm," IEEE Network, vol. 20, no. 5, pp. 18-24, September/October 2006.
[8] L. C. Reeves, "Social Network Email Filtering," European Patent Application, November 2005.
[9] J. Rosenberg, and C. Jennings, The Session Initiation Protocol (SIP) and Spam, IETF RFC 5039, January 2008.
[10] J. Franks, P. Hallam-Baker, J. Hostetler, S. Lawrence, P. Leach, A. Luotonen, and L. Stewart, HTTP Authentication Basic and Digest Access Authentication, IETF RFC 2617, June 1999.
[11] T. Dierks and C. Allen, The TLS Protocol Version 1.0, IETF RFC 2246, January 1999.
[12] B. Ransdell, S/MIME Version 3 Message Specification, IETF RFC 2633, June 1999.
[13] 최재덕, 정수환, "효율적이고 안전한 SIP 사용자 인증 및 키 교환," 정보보호학회논문지, 제 19권, 제 3호, pp. 73-82, 2009년 6월.

저 자 소 개

채 강 석(학생회원)
2008년 숭실대학교 정보통신전자공학부 학사
2008년~현재 숭실대학교 전자공학과 석사과정
<주관심분야 : 이동 네트워크 보안, VoIP 보안, 차량 네트워크 보안>

김 영 범(정회원)
건국대학교 전자공학부 교수
대한전자공학회 논문지
제 35권 S편 제4호 참조

배 광 용(정회원)
1990년 숭실대학교 전자공학과 학사 및 석사 졸업
2004년 건국대학교 전자정보통신공학과 박사 수료
1990년 KT 연구개발본부 전임연구원
2002년~현재 KT SD부문 기술개발실 부장
<주관심분야 : USN 보안, VoIP 보안, M2M통신>