5G－7

公開鍵ベースケルベロス認証サービスにおける サービスチケット失効リストの分散管理法の提案

水野伸太郎 山下高生 小野諭
日本電信電話株式会社 ソフトウェア研究所

1.はじめに

電子メールやNet News等、インターネット上でのコミュニケーションが広く利用されつつある。しかし、一方で嫌がらせメールや執拗な広告メール等、望ましくないコミュニケーションも増加している。このような事を防ぐ方法として、認証の枠組みの利用が考えられる。認証の枠組みにはX.509認証[1]、Kerberos[2]等が知られているが、公開鍵インフラ（PKI: Public Key Infrastructure）を利用したKerberos認証方式[3][4]が、各アプリケーションに依存した有効期限や利用条件などの、ユーザ情報を含んだサービス独自のサービスチケットを利用できることからコミュニケーションの制御での利用に適していると考えられる。サービスチケットを利用したコミュニケーションの制御は、チケットの発行と失効により実現することができる。失効の枠組みはX.509において議論されている[6][7][8]が、コミュニケーションの制御を行うためのチケットの失効では、（A）チケットにより提供されるサービスの部分的失効、（B）失効リスト参照者とリストによる受益者との不一致性 という二つの異なった特性を持っている。しかし、既存技術では、全てのノードが同一の失効リストを参照するため、これらの特性から(A)に関しては、失効する必要の無い場所でも失効されるという問題が生じる。また、(B)に関しては、全てのノードで参照する事により、リストによる受益者と参照者が一致する点で必ず失効されるが、複数地点で同一のリストの参照による負荷の増大という問題が生じる。そこで本研究では、この(A),(B)の要求を実現できるような失効の枠組みを、コミュニケーションの制御に用いるチケットの、失効リスト参照者の予測可能性という特徴を利用し、効果的な方法を提案する。

2.コミュニケーションの制御における失効の要件

前節で述べたコミュニケーションの制御に必要なチケットの失効の要件について詳しく述べる。

(A)チケットにより提供されるサービスの部分的失効

コミュニケーションの制御を考える場合、1対1のコミュニケーションのみならず、メーリングリストやチャット等の場合のような、グループ通信も考える必要がある。ここで、グループ通信におけるチケットの使い方を考えると、個人へのチケットを複数利用する方法と、グループへのチケットを利用する方法が考えられるが、動的なメンバーの変更が可能であるという点で、グループへのチケットの利用が適していると考えられる。グループ通信を考えた場合、グループの一部のメンバーへの失効ができることが必要となる。グループへのチケットを用いる場合、チケットで提供されるサービスは全てのメンバーへのコミュニケーションを表す。よって一部のメンバーへの失効は、サービスの部分的失効を表す事になる。しかし、既存の失効の枠組みでは全ての参照者が同一の失効リストを参照するため、失効されるべきでないものも失効されるという問題が生じる。

(B)失効リスト参照者とリストによる受益者との不一致性

コミュニケーションのチケットを考えた場合、失効リストは複数の主体から様々な目的で発行される。そのため、失効リスト参照者にとって不利益となるリストも存在する可能性がある。リスト参照者は自分にとって都合の悪いリストは実行しないと考えられるため、すべての失効リストを確実に実行させるためには、失効リストを確実に実行する主体、すなわちリストによる受益者に参照させる必要がある。既存の技術を用いた場合、同一のリストを、全てのノードで参照する事により、リストによる受益者と参照者が一致する点で必ず失効されるが、複数地点で同一のリストを参照しなければならないため、検索による負荷の増大という問題が生じる。

3.各要件を満たす失効の枠組みの提案

3.1. 要件(A)の実現

グループへのチケットは、グループのメンバーから失効を受けた場合、そのメンバーに対しては無効であるが、その他のメンバーに対しては有効でなくてはならない。グループへのコミュニケーションでは、メッセージがFig.1のように発信者を根とし、受信者を葉とするツリー

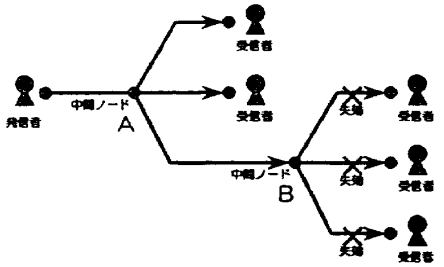

Fig. 1 グループへのチケットの失効

上を分岐しながら流れる。そのため、中間のノードでチケットの失効を行った場合、そのノードの子孫に含まれる受信者へのコミュニケーションはすべて失効される。これを防いで部分的失効を実現するためには、

(1) 参照位置非依存型失効リスト
(2) 参照位置依存型失効リスト

を用いる方法が考えられる。

(1)を用いた場合、次のように部分的失効を実現する。

- 各主体を識別する情報を用いて、全ての失効リストにどの主体からどの主体へのメッセージを失効するのかを記述し、このリストを全てのノードが参照することにより失効リストを実行する。

この場合、リストが増大する事と、執行しないリストまでも全てのノードで参照しなくてはならないことから、参照によるネットワーク負荷と、検索による計算機負荷を増大させる。

(2)を用いた場合、さらに次の2つの方法が考えられる。

(2)-1 リストの配置のみを利用する方法
(2)-2 リストの配置と付加情報を利用する方法

(2)-1の方法では次の様にして部分的失効を実現する。

Shintaro MIZUNO, Takao YAMASHITA, Satoshi ONO
NTT Software Laboratories

- 各参照者がそれぞれの失効リストを自分の近くに持ち、末端でメッセージの失効を行う
- 中間ノードBのように子孫に含まれる受信者がすべて失効されるような時は中間ノードで失効する

(2)-2の方法では次の様にして部分的失効を実現する

- Fig.1の中間ノードAのように、子孫の一部で失効される場合、失効される子孫の情報をリストの付加情報として持ち、メッセージを選択的に流す

この方法は、(2)-1に加え、リスト以外の付加的な情報を用い、できるだけ先祖で失効する方法で、無駄なトラフィックを減らす事ができる。しかし、付加情報を加える範囲を広げすぎると(1)を用いた方法と同様になってしまうため、付加情報をどの程度利用するかを、中間ノードでの処理の負荷などを考慮して決める必要がある。

3.2. 要件(B)の実現

コミュニケーションにおいて失効リストを発行する主体には、

- 受信者
- サービス提供者
- その他の第3者

が考えられる。失効リストを参照／執行するのは、

- 受信者
- サービスを構成するノード

である。

次にリストを発行する主体と参照／執行する主体との関係から生じる、執行の確実性と、ネットワーク資源、計算機資源の効率について考察する。

(1) 受信者の発行する失効リスト

受信者が参照／執行

- 自身の失効リストであるため、確実に執行される
- ツリーの葉にあたり、無駄なトラフィックが流れるが、処理が分散されるため、計算機負荷は少ない

サービスを提供するノードが参照／執行

- サービス提供者の都合によりリストが執行されない可能性がある
- 先祖ノードで処理するほど無駄なトラフィックは減るが、ノードでの計算機負荷は受信者による場合と比較して増大する

(2) サービス提供者の発行するリスト

受信者が参照／執行

- 受信者にとって不利益となるリストは執行されない

サービスを提供するノードが参照／執行

- 自身の発行したリストであるため確実に執行される

ネットワーク資源、計算機資源の効率は(1)と同様である。

(3) 第3者の発行するリスト

受信者が参照／執行

- 受信者にとって不利益となるリストは執行されない

サービスを提供するノードが参照／執行

- サービス提供者の都合によりリストが執行されない可能性がある

ネットワーク資源、計算機資源の効率は(1)と同様である。

以上から、リストを確実に執行させるためにはリストの発行者自身が参照／失効することが必須であることが分かる。しかし、これだけでは無駄なトラフィックや、計算機負荷の増大が起こり得るため、これを回避できる他の方法との併用を考える必要がある。

第3者のリストの場合、目的によってどちらの参照／執行者の場合も確実に執行されるとは限らない。そのため、どの主体がリストの受益者であるかを発行者自身が判断し、確実に執行されるように管理されなくてはならない。失効リストには、サービスの提供ポリシー的、社会的に失効されるべきものと失効されるべきでないものがあると考えられるが、失効されるべきものに関しては、サービス提供者が中立的立場に立って失効を行う機能を持つべきであると考えられる。

4.今後の課題

本稿では、コミュニケーションの制御におけるグループ通信のための、チケットの失効リスト管理法について考え、失効を行うのに必要な2つの要件に関して、これらを実現する方法を述べた。今回は失効リストが確実に実行され、ネットワーク及び計算機資源を有効活用するような方法を提案したが、今後は本方法の詳細化および最適化を行うと共に、DSA(Denial Service Attack)に対する対策や、ユーザが頻繁にネットワーク上を移動する場合でも失効リストが有効に動作する方法などを考えていく。

謝辞

研究をご支援くださる市川晴久広域コンピューティング研究部長に感謝致します。

参考文献

[1] R. Housley, W. Ford, W. Polk, D Solo, "Internet Public Key Infrastructure X.509 Certificate and CRL Profile", IETF PKIX WG Internet Draft 1998

[2] J. Kohl, C. Neuman, "The Kerberos Network Authentication Service (V5)", IETF RFC 1510, 1993

[3] B. Tung, C. Neuman, J. Wray, A. Medvinsky, M. Hur, J. Trostle, "Public Key Cryptography for Initial Authentication in Kerberos", IETF CAT WG Internet Draft 1998

[4] M. A. Sirbu, J. C. Chuang, "Distributed Authentication in Kerberos Using Public Key Cryptography", Proc. of IEEE Symposium on Network and Distributed System Security, pp.134-140, 1997

[5] A. Medvinsky, M. Hur, C. Neuman, "Public Key Utilizing Tickets for Application Servers (PKTAPP)", IETF CAT WG Internet Draft 1998

[6] S. G. Stubblebine, "Recent-Secure Authentication: Enforcing Revocation in Distributed Systems", Proc. of IEEE Symposium on Security and Privacy, pp.224-234, 1995

[7] Perlman et al., "Certificate Revocation Performance Optimization", United States Patent #5687235, 1997

[8] Van Oorschot et al., "Method for Efficient Management of Certificate Revocation Lists and Update Information", United States Patent #5699431, 1997