Design and implementation of a trusted third-party based cross-realm AAA system

Saber Zrelli(410067)

北陸先端科学技術大学院大学 情報科学研究科

2006 年 2 月 9 日

キーワード: Kerberos, AAA, cross-realm authentication.

IPv6 による次世代インターネットの普及により、IP ネットワークスタックをサポートできる十分なリソースを持つあらゆる電化製品が今後インターネットに接続されるであろう。基本的に、各デバイスはあるドメインに所属し、その所属するドメイン内部のサービスを利用する。しかし、様々な電化製品がインターネットに接続し、広い範囲を移動するようになると、他ドメインにより提供されるサービスも利用したいという要求も高まる。このような要求に答えるため、それぞれのドメイン間で協定および契約を行い、各デバイスは自身が所属するドメインと他のドメイン間の協定または契約に従って、他ドメインにおけるサービスを利用する。このような複数のドメインにまたがるサービスの相互利用には、認可と認証が不可欠である。一般的に AAA フレームワークで提供されているドメイン間をまたがるサービスの利用は、クライアントがサービスを利用するドメインからの証明書を得ることにより実現される。本論文では、まず AAA フレームワークの標準を調査した。特に Kerberos プロトコルに着目し、その長所および欠点について議論する。Kerberos に対するいくつかの改良はすでに提案されているが、ドメインをまたがる操作に関して、より良い性能および利便性のための更なる強化を行えることを示し、ドメイン間をまたがる操作を実現するため、新たなモデルを持つ XKDCP プロトコルを提案した。XKDCP プロトコルは、Kerberos の Key Distribution Centers(KDCs) 間でのメッセージ交換について定義しており、ドメインをまたがる操作が行われたときに利用される。我々の手法では、クライアントが他ドメインのサービスを利用するための手順が完全に透過的であるという利点がある。クライアントは、自身がどのドメインに接続しているのか、また利用したいサービスがどのドメインで提供されているかに関わらず、同一の操作によりそのサービスを利用できる。さらに、我々のアプローチでは、クライアント側の処理を簡素化し、非常に低い性能しかもたないデバイスでも、認証を用いて他ドメインで提供されているサービスを利用できる。