セキュアなDNSの実現に向けて

石原 知洋　東京大学

〔受賞論文〕
セキュリティを考慮した名前解決エージェントの設計と実装
石原知洋（慶應義塾大学），関谷勇司（東京大学），村井純（慶應義塾大学）
情報処理学会論文誌，Vol.50, No.3, pp.1012-1021 (2009)

このたび情報処理学会の論文賞をいただくことになり，誠に光栄に思うとともに非常に驚いている．本賞の受賞を励みに，今後も精力的に研究活動に邁進したいという思いである．

本研究で取り上げているDNS spoofingによる攻撃は，それ自体はインターネットの黎明期より知られていたが，実際に攻撃事例が多く報告され始めたのは2008年頃になってからである．本論文を投稿したのはちょうどその頃，DNS spoofingの問題点が再び大きく取り上げられていた時期であり，その点で本論文は注目いただいたのではと考えている．

受賞した論文は，DNS spoofingからクライアントを保護する方法について述べている．既存のDNS spoofingへの対抗策としてはDNSSECが以前より提案および実装されているが，運用コストの面から広く普及しているとは言いがたい状況である．そこで本研究ではDNS spoofingに見られるDNSの攻撃パケットの性質に着目した．それらの攻撃パケットを動的に判断し，名前解決を行うリゾルバエージェントを提案することで，DNSSECを利用できない環境でもDNS spoofingへの耐性を実現した．

本研究を行うにあたり欠かせなかった活動として2004年にWIDEプロジェクトの合宿において，JPRSの藤原和典氏および共著者である関谷勇司とともに行ったDNS攻撃実験が挙げられる．実験は，合宿に施設したネットワーク上で実際にDNS spoofingの攻撃を行うというものであった（参加者を巻き込んでこのような大胆な実験を行えるのはWIDEプロジェクトならではと言える）．その実験によりDNS spoofingによる問題点をまとめることができ，またその危険性を再確認できた．この実験が本研究の出発点と言える．

また，DNS実装であるBINDの開発をされている米Internet Systems Consortium社の神明達哉博士とお話した際に，「DNSSECを使ったとしても通常のリゾルバの仕組みでは応答が間違っていることしか判断できず，正しい答えを選択できない」という話題が出たことも，本研究で提案するリゾルバエージェントを提案するきっかけとなった．このように，本研究はWIDEプロジェクト，中でもDNS分科会の諸氏による活動や，ご意見・ご協力を得て行われている．この場を借りて感謝したいと思う．

DNSはインターネットに欠かせないインフラであり，悪意ある攻撃者にここを狙われるとインターネットの安全性を根底からゆるがしてしまうため，今後もDNSに関するセキュリティは重要だと考えている．今後も研究および普及に邁進したいと考えている．

最後になるが，本論文の初回投稿から査読結果受領までの間，2008年末にKaminsky博士による新たなDNS spoofing攻撃が発表された．そして，査読者の方から博士の発表した攻撃（博士の名を取ってKaminsky Attackと呼ばれる）を論文に盛り込めばより良い論文になるのではないか，との助言をいただき，Kaminsky Attackに対する本研究の有用性の評価を加筆した．この加筆により，本論文の新鮮さおよび有益さを向上させることができた．この場を借りて査読者に感謝の意を表したい．

（平成22年5月17日受付）

石原 知洋（正会員）　sho@c.u-tokyo.ac.jp
2001年日本大学理工学部物理学科卒．2003年慶應義塾大学政策・メディア研究科修士課程卒業．2009年慶應義塾大学政策・メディア研究科後期博士課程修了．同年より東京大学総合文化研究科特任助教に就任．2010年博士（政策・メディア）．ドメインネームシステムおよびインターネットの運用技術に関する研究・開発に従事．