Deteksi Email Spoofing Dengan Menggunakan Metode Header Analysis

Ery Defriyanto S[1], Niken Dwi Wahyu Cahyani, ST., M.Kom., Ph.D[2]

[1,2]Fakultas Informatika, Universitas Telkom, Bandung
[1]erydss@students.telkomuniversity.ac.id, [2]nikencahyani@telkomuniversity.ac.id,

Abstrak

Email spoofing **merupakan salah satu kejahatan** ***cyber*** **yang dilakukan dengan menipu atau menyebar berita bohong dengan menyamarkan nama pengirim** ***email*** **menjadi** ***email*** **tertentu. Karena itu sebuah metode untuk melakukan deteksi diperlukan untuk melihat apakah sebuah email terindikasikan sebagai** ***spoof*** **atau tidak. Pada penelitian ini dilakukan sebuah percobaan membuat sebuah sistem untuk mengetahui** ***email*** **yang** ***spoof*** **dan tidak. Metode yang digunakan pada forensik email ini adalah menganalisa header email (*header analysis*) dan mengimplementasikan algoritma deteksi** ***email spoofing*** **yang telah didapatkan dari penelitian terdahulu. Teknik ini bekerja dengan memeriksa beberapa nilai yang terdapat pada** ***header email*** **yang ditetapkan sebagai parameter deteksi** ***email spoofing*****. Metode** ***header analysis*** **pada penelitian ini mengimplementasikan dua metode** ***header analysis*****. Metode pertama menganalisa** ***field 'From', 'Message-ID', 'Date',*** **dan** ***'Received'*****. Jika value yang terdapat pada header tersebut identik, maka** ***email*** **tersebut dikategorikan sebagai** ***email legitimate*****, jika tidak maka** ***email*** **tersebut dikategorikan sebagai** ***email spoofing*****. Metode kedua menganalisa nilai pada standar autentikasi kebijakan email yaitu SPF, DKIM, DMARC, DKIM-signature, dan SPF-Value. Pada penelitian ini ada perubahan algoritma pada metode kedua, karena algoritma yang digunakan pada penelitian terdahulu terdapat kekurangan yang membuat akurasi deteksi** ***email spooing*****nya menurun. Hasil dari penelitian ini adalah metode pertama dapat diterapkan pada email yang berasal dari seseorang atau individu, namun metode ini tidak dapat mendeteksi** ***email legitimate*** **yang pengiriman emailnya dijadwalkan dan** ***email legitimate*** **yang berasal dari sebuah organisasi atau perusahaan. Kemudian metode kedua dapat digunakan untuk mendeteksi** ***email spoofing*** **pada semua jenis** ***email*****. Hasil selanjutnya adalah mengetahui keefektifan kedua metode setelah diadaptasi dari penelitian sebelumnya dengan membandingkan akurasi algoritmanya dalam mendetkasi** ***email spoofing*****. Ditemukan bahwa metode pertama memiliki akurasi 60% dan metode kedua memiliki akurasi 100% dalam mendeteksi** ***email spoofing*****.**

Kata kunci : Forensik email, header analysis, email spoof, email legitimate