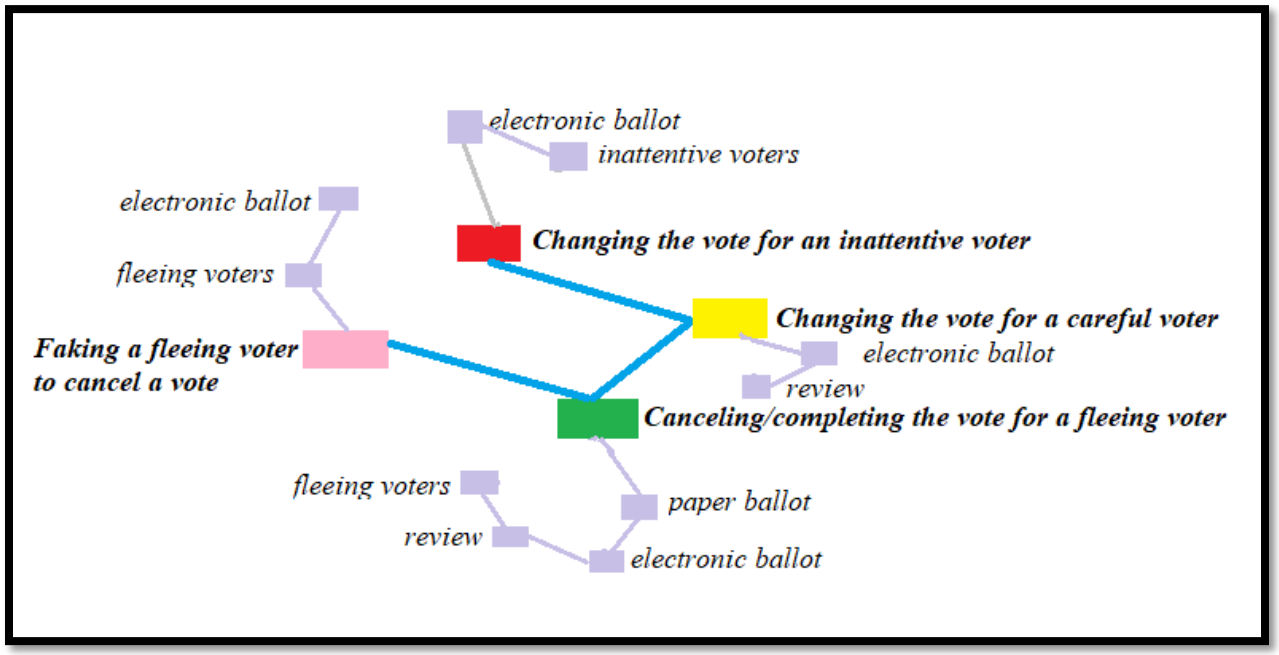
Serangan Sistem E-Voting Menggunakan Skenario Denial-Of-Service (Dos)

Gambar :



Scenario :
Beberapa skenario penggunaan Trojan telah dilaporkan oleh para peneliti di bidang e-voting. Weldemariam (Weldemariam, Kemmerer, & Villafiorita, 2009), antara lain, menjelaskan 4 (empat) skenario yang dapat digunakan untuk meng-ekspos sistem e-voting buatan ES&S, salah satu pabrikan sistem e-voting yang popular. Perlu diketahui bahwa ES&S menghadirkan fungsi verifikasi VVPAT (*Voter-Verified Paper Audit Trail*) dimana untuk setiap suara yang diberikan melalui sistem, akan dikeluarkan rekaman suara berupa kertas tercetak. Fungsi ini memberikan kesempatan kepada pemilih untuk memastikan suara yang tercatat dalam sistem adalah yang suara yang diberikan.

1.***Changing the vote for an inattentive voter***. Adakalanya pemilih tidak menyadari pentingnya fungsi verifikasi. Pemilih dengan karakteristik demikian biasanya melakukan proses pemberian suara secara normal dan setelah selesai tidak memeriksa apakah suara yang ia berikan telah terekam dengan baik dalam sistem. Trojan biasanya disimpan dalam sistem dan diaktivasi untuk: (1)memotong proses penyimpanan suara sesaat sebelum *review* suara ditampilkan dalam *electronic ballot*; (2)mengubah nilai suara yang telah diberikan menjadi nilai untuk kandidat lain. Skenario ini mengandalkan kecenderungan *inattentive voters* mengabaikan nilai suara akhir yang ditampilkan dalam *electronic ballot*, dan ketidaksesuaian suara pemilih dengan kertas rekaman suara tercetak. Skenario ini akan gagal jika pemilih menyadari ketidaksesuaian tersebut dan memutuskan untuk melakukan pemberian suara ulang. Jika hal ini terjadi, Trojan akan mendeteksi identitas pemilih dan menghentikan proses pengubahan nilai suara untuk sementara. Jika sebaliknya, maka nilai suara yang akan direkam adalah nilai yang telah diubah

oleh Trojan. Yang demikian akan sulit untuk dideteksi apabila telah sampai pada proses perhitungan suara hingga akan sangat merugikan sebagian kandidat.

2.***Changing the vote for a careful voter***. Dalam skenario ini, pemilih diasumsikan melakukan proses pemberian suara normal dan mereka cukup berhati-hati dengan juga memperhatikan *review* yang ditampilkan dalam *electronic ballot*. Kelemahan yang diserang disini adalah kekurangmengertian pemilih tentang informasi yang disampaikan dalam kertas rekaman suara tercetak. Untuk itu, pengubahan nilai suara tidak dilakukan sebelum *review* nilai suara dalam *electronic ballot* melainkan sesudahnya. Ketidaksesuaian terjadi antara nilai suara yang di-*review* dengan kertas rekaman suara tercetak. Sama dengan yang terjadi dalam skenario sebelumnya, jika tidak perubahan nilai suara tidak terdeteksi sejak dini, maka suara tersebutlah yang akan ditabulasikan.

3.***Canceling/completing the vote for a fleeing voter***. Harus diakui bahwa penggunaan *electronic ballot* dalam proses pemungutan suara dapat menyebabkan ketidaknyamanan bagi sebagian pemilih. Hal ini dapat terjadi salah satunya akibat dipengaruhi kebiasaan dalam menggunakan *paper ballot*. Proses pemberian suara menggunakan *electronic ballot* yang berbelit-belit, keharusan untuk menunggu *review* nilai suara yang diberikan; menyebabkan sebagian pemilih memilih untuk tidak menyelesaikan proses pemberian suara. Pemilih yang demikian disebut sebagai *fleeing voters*, dan skenario ini memanfaat tipe pemilih ini. Perlu diketahui bahwa ES&S memiliki fitur alarm untuk memberitahu petugas di TPS bila seorang pemilih tidak menyelesaikan proses pemberian suaranya. Trojan dapat melakukan 2 (dua) hal disini: (1)jika pemilih memilih kandidat yang tidak diinginkan, membiarkan alarm berbunyi agar petugas TPS mengetahui proses pemberiaan suara belum selesai dan membuang suara yang belum dikonfirmasi; atau (2)jika pemilih memilih kandidat yang diinginkan, menghentikan alarm dan menyelesaikan proses pemberian suara hingga suara terekam.

4.***Faking a fleeing voter to cancel a vote***. Jika di skenario sebelumnya, serangan dilakukan dengan memanfaatkan *fleeing voters*, dalam skenario ini Trojan "memalsukan" *fleeing voters*. Pemilih yang memilih kandidat yang tidak diinginkan dan telah melakukan pemberian suara normal akan disodorkan tampilan dalam *electronic ballot* yang menunjukkan bahwa seolah-olah suara mereka telah terekam. Sesungguhnya Trojan menahan suara pemilih tersebut hingga setelah pemilih meninggalkan TPS, Trojan akan mengaktivasi alarm. Petugas TPS akan menyangka bahwa pemilih tersebut adalah *fleeing voter*dan membuang suara yang belum dikonfirmasi tersebut.

Dampak :

Trojan bertujuan untuk mengambil alih kontrol atas sebuah mesin atau system, Trojan akan mampu melakukan bentuk serangan lain yang lebih merusak, seperti: mencuri password, mengubah data, menjalankan program tertentu, dan lain-lain.

Sumber :

https://www.kompasiana.com/evotingindonesia/skenario-hacking-sistem-e-voting-part-02-attacks-of-the-trojan_5500e6ffa33311376f5127e6