

INTISARI

Teori Permainan untuk Cybersecurity: Permainan Non-Kooperatif Dinamis dalam Adopsi Sistem Pembayaran Digital

Oleh

Caslyne Liebermann

21/476826/PA/20608

Digitalisasi sistem pembayaran memberikan berbagai keuntungan seperti efisiensi, kecepatan transaksi, dan kemudahan akses. Namun, perluasan penggunaan pembayaran digital juga meningkatkan risiko keamanan siber yang dapat menurunkan kepercayaan pengguna. Dalam skripsi ini dikaji mengenai dinamika adopsi sistem pembayaran digital melalui pendekatan teori permainan dengan melibatkan tiga pemain, yaitu penyedia layanan, pengguna, dan pelaku kejahatan siber. Interaksi ketiga aktor diformulasikan sebagai permainan non-kooperatif dinamis berurutan (*dynamic sequential game*), di mana penyedia menentukan tingkat investasi keamanan dan insentif, pengguna menentukan keputusan adopsi dan investasi keamanan pribadi, sedangkan pelaku kejahatan memilih tingkat usaha serangan. Model matematis dikembangkan dengan mendefinisikan manfaat dan biaya yang dihadapi masing-masing pemain dan menurunkan strategi optimal melalui analisis *backward induction*. Penelitian ini memperoleh bentuk eksplisit dari usaha serangan optimal e^* , investasi keamanan optimal pengguna λ^* , serta batas minimum insentif ι_{\min} yang diperlukan agar pengguna bersedia mengadopsi sistem. Keseimbangan permainan dalam bentuk *Subgame Perfect Nash Equilibrium* (SPNE) diperoleh sebagai *quadruple* $(\alpha_f^*, \iota^*, \lambda^*, e^*)$ yang memaksimalkan manfaat dan biaya yang diterima setiap pemain pada setiap subgame. Hasil simulasi numerik menunjukkan bahwa peningkatan investasi keamanan penyedia dan pengguna dapat menurunkan probabilitas keberhasilan serangan, memperkecil upaya optimal pelaku kejahatan, dan meningkatkan tingkat adopsi. Sebaliknya, peningkatan kerugian potensial D atau rendahnya awareness pengguna mengakibatkan berkurangnya ukuran jaringan.

ABSTRACT

Game Theory for Cybersecurity: Dynamic Noncooperative Games in Digital Payment System Adoption

By

Caslyne Liebermann

21/476826/PA/20608

The digitalization of payment systems offers various advantages such as efficiency, faster transactions, and improved accessibility. However, the rapid expansion of digital payment usage also increases cybersecurity risks, which can undermine user trust. In this thesis, the dynamics of digital payment adoption are examined using a game-theoretic approach involving three players: the service provider, users, and cyber attackers. The interaction among these actors is formulated as a dynamic sequential non-cooperative game, in which the provider determines the level of security investment and user incentives, users decide whether to adopt the system and how much personal security to invest, while cyber attackers choose their optimal attack effort. A mathematical model is developed by defining the benefits and costs of each player and deriving their optimal strategies through backward induction. The analysis yields explicit expressions for the attacker's optimal effort e^* , the user's optimal security investment λ^* , and the minimum incentive ι_{\min} required for users to adopt the system. The equilibrium of the game, expressed as a Subgame Perfect Nash Equilibrium (SPNE), is obtained in the form of a quadruple $(\alpha_f^*, \iota^*, \lambda^*, e^*)$ that maximizes each player's benefits and costs in every subgame. Numerical simulations show that increasing the security investment of both providers and users reduces the probability of a successful attack, lowers the attacker's optimal effort, and increases the adoption rate. Conversely, higher potential loss D or low user awareness leads to a reduction in overall network size.