Michał Domański

PLATFORMA ZARZĄDZANIA ZAUFANIEM

pod kierunkiem: prof. dr. inż Zbigniew Kotulski
dr. inż Igor Margasiński

PLAN

- wprowadzenie
- problematyka
- proponowane rozwiązanie
- przewidywane korzyści

PROBLEMY DZIŚ

- jak zagwarantować bezpieczeństwo i anonimowość jednocześnie ?
- jak zapewnić maksymalną możliwą odporność zabezpieczeń na ataki ?
- czy anonimowość to cena bezpieczeństwa ?

PROBLEMY JUTRO

- sieć usług inteligentnych, będących połączeniem usług podstawowych

- bez wymaganych gwarancji bezpieczeństwa

- ale w znaczącym stopniu zależne od zaufania do udostępnianych wzajemnie danych

CEL

Platforma pozwalająca korzystać z danych na temat zaufania dotyczącego danych węzłów, ocenianego względem ich faktycznych działań.

BEZPIECZEŃSTWO

hard security - oparte o typowe obecnie metody: szyfrowanie, certyfikaty, klucze kryptograficzne

soft security - zabezpieczenia nowej generacji, oparte o systemy generowania zaufania i zarządzanie ryzykiem

ZAUFANIE

Postrzegane w świecie komputerów podobnie jak wśród ludzi, jako zbiór doświadczeń, zbieranych w czasie interakcji z drugą stroną.

ANONIMOWOŚĆ A BEZPIECZEŃSTWO

- aktywność użytkownika nie powoduje ujawnienia informacji o jego tożsamości
- jego dane są bezpieczne
- jego tożsamość również musi być bezpieczna

GDZIE MA TO SENS ?

- systemy które wymagają wysokiego poziomu wzajemnej anonimowości
- systemy w których bezpieczeństwo można rozumieć jako adekwatność informacji

A WIĘC?

- sieci anonimizujące
- usługi dodatkowe
- oraz jako nadmiarowe zabezpieczenie dla usług podstawowych

ZAGROŻENIA WOBEC SIECI ANONIMIZUJĄCYCH

- topologia sieci jest znana
- ponieważ zasoby każdego węzła można sprawdzić, możliwe jest monitorowanie ruchu w sieci
- skoro możemy monitorować ruch, to możemy monitorować sieć

ZAGROŻENIA WOBEC USŁUG DODATKOWYCH

- ataki typu ‚man in the middle'
- spoofing na wszystkich poziomach architektury
- search engine poisoning

POWÓD ?

- demokracja - architektura protokołów rzadko projektowana jest z myślą o bezpieczeństwie, traktowanym bardziej jako osobna dziedzina

METRYKI ZAUFANIA

- dostępność
- udostępniane zasoby
- ilość pozytywnych transakcji
- ilość negatywnych transakcji

JAK TEGO UŻYĆ ?

- każdy węzeł zbiera i udostępnia dane o swoim otoczeniu
- chcąc przeprowadzić transakcję z nieznanym użytkownikiem, odpytujemy znane nam węzły o dane o jego zaufaniu
- jeśli nasi znajomi nie znają odpowiedzi, zapytanie propaguje się dalej

EFEKTY

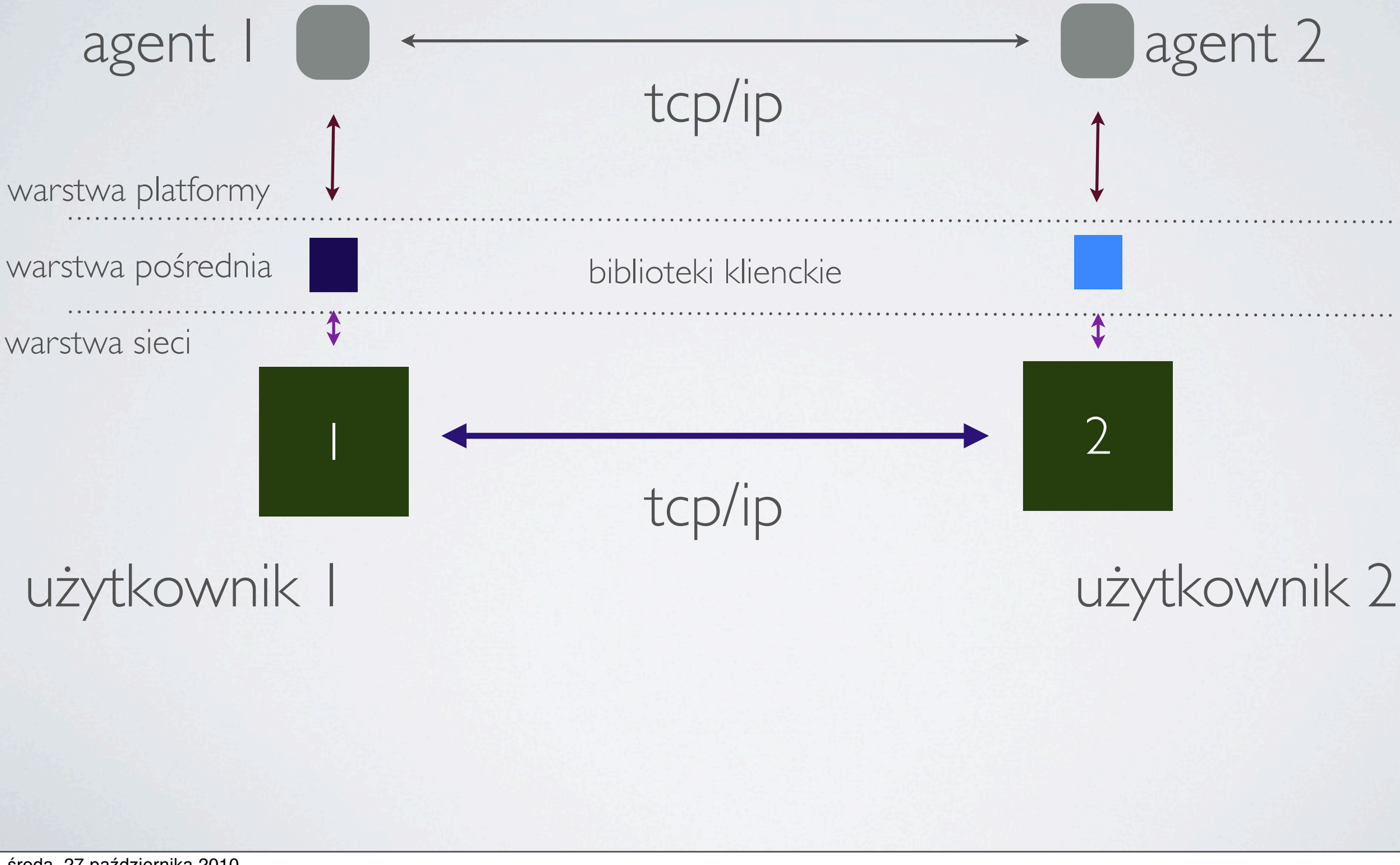
- topologia sieci zależna od tego jakim zaufaniem darzymy danego użytkownika

- nowi użytkownicy muszą zapracować na korzyści wynikające z dobrej reputacji

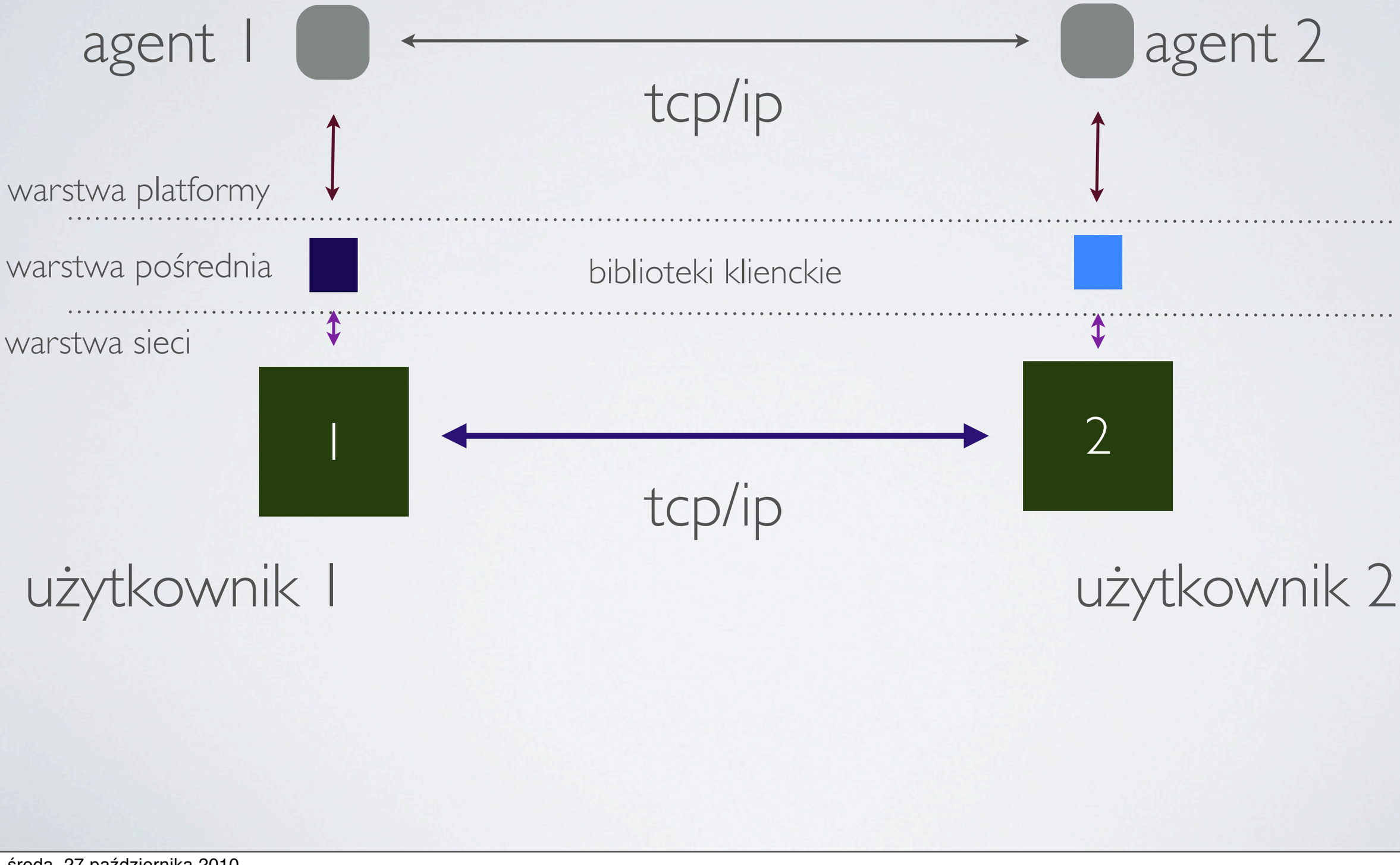
- wysoki poziom zaufania gwarantuje duże zyski, ale łatwo go stracić

WYKONANIE

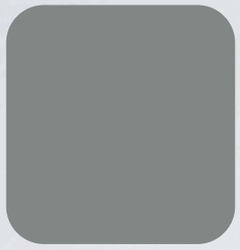
SCHEMATYCZNIE



SCHEMATYCZNIE

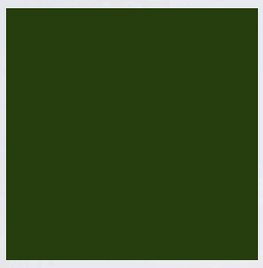


I OPISOWO



agent

1. gromadzi statystyki
2. pośredniczy w komunikacji z platformą



użytkownik

1. komunikacja za pomocą biblioteki
2. pobiera dane o innych użytkownikach i generuje nowe oceny

AKTUALNIE

- agent jako samodzielny serwer pracujący jako usługa na maszynie użytkownika
- dostęp do niego poprzez odpowiednią bibliotekę kliencką

BIBLIOGRAFIA

[1] „Low-resource routing attacks against anonymous systems” K.Bauer, D.McCoy, D.Grunwald, T.Kohno, D.Sicker
[2] “Decentralized trust managment” M.Blaze, J.Feigenbaum, J.Lacy
[3] „Trust managment and network layer security protocols” M. Blaze, J. Ioannidis, D. Keromytis
[4] „Trust managment for IPSec” M. Blaze, J.Ioannidis, D.Keromytis
[5] „Prospectives for online trust managment” A.Josung
[6] „Challenges for robust trust and reputation systems” A.Josung, J.Golbeck
[7] „Combining trust and reputation managment for web-based services” A.Josung, T.Bhuiyan, Y.Xu, C.Cox
[8] „The EigenTrust algorithm for reputation managment in p2p networks” S.D.Kamvar, M.T.Schloser, H. Garcia-Molina
[9] „Taxonomy of trust: categorizing p2p reputation systems” S.Marti, H.Garcia-Molina
[10] „Trust Strategies for the Semantic Web” Kieron O’Hara, Harith Alani, Yannis Kalfoglou, and Nigel Shadbolt
[11]] „Free-Riding and Whitewashing in Peer-to-Peer Systems” M. Feldman, C. Padimitriou, J. Chuang, I. Stoica
[12] „A social mechanism of reputation management in electronic communities” B. Yu, M. P. Singh 154–165.
[13] „Enhancing Reputation Mechanisms via Online Social Networks” T. Hogg, L. Adamic
[14] „SPROUT: P2P Routing with Social Networks” S. Marti, P. Ganesan, H. Garcia-Molina
[15] „The social cost of cheap pseudonyms” E. Friedman, P. Resnick,
[16] „The PageRank Citation Ranking: Bringing Order to the Web” L. Page, S. Brin, R. Motwani, and T. Winograd
[17] „The small world problem” S.Milgram
[18] „The Sybil attack” J.R. Douceur
[19] „The Graph API” http://developers.facebook.com/docs/api
[20] „Trust based knowledge outsourcing for semantic web agents” L. Ding, L. Zhou, T. Finin
[21] „Low-cost traffic analysis of Tor” S.J. Murdoch, G. Danezis
[22] „Provable unlinkability against traffic analysis” R. Berman, A. Fiat, A. Ta-Sharma
[23] “Privacy vulnerabilities in encrypted HTTP streams,” G. Bissias, M. Liberatore, D. Jensen, and B. Levine,
[24] M. Liberatore, B. N. Levine, “Inferring the source of encrypted HTTP connections ,”
[25] D. X. Song, D. Wagner, and X. Tian, “Timing analysis of keystrokes and SSH timing attacks,” in *USENIX Security Symposium*, 2001.
[26]Hiding Routing Information, D. M. Goldschlag, M. G. Reed, P. F. Syverson , 1996
[27]DINGLEDINE, R., MATHEWSON, N., AND SYVERSON, P. Tor: The second-generation onion router. In Proceedings of the 13th USENIX Security Symposium (August 2004)
[28]GOLDBERG, I. On the security of the tor authentication proto- col. In Proceedings of the Sixth Workshop on Privacy Enhancing Technologies (PET 2006) (Cambridge, UK, June 2006), Springer.
[29] „Anonymous routing in peer-to-peer overlays”, Nikita Borisov
[30] „Rumor riding: anonymizing unstructured peer-to-peer systems”, J. Hang, Y. Liu
[31] „Tor performance problems and how to solve them”, R.Dingledine
[32] „Covert channel vulnerabilities in anonymity systems” S. Murdoch
[33] „Performance improvements on Tor or, why Tor is slow and what we’re going to do about it”, R.Dingledine, S. Murdoch
[34] „Personal communication” P. Syverson
[35] „On the optimal path length for Tor”, K.Bauer, J. Juen, N. Borisov, D. Grunwald, D. Sicker, D. McCoy
[36] „Tor protocol specification”, R. Dingledon, N. Mathewson
[37] „The Traffic Analysis of Continuous-Time Mixes” G. Danezis

PYTANIA ?