Security, Privacy and Trust in the (Semantic)Web

Roman Špánek
Martin Řimnáč

Seminář projektu SemWeb
30.11. - 2. 12. 2008

Obsah

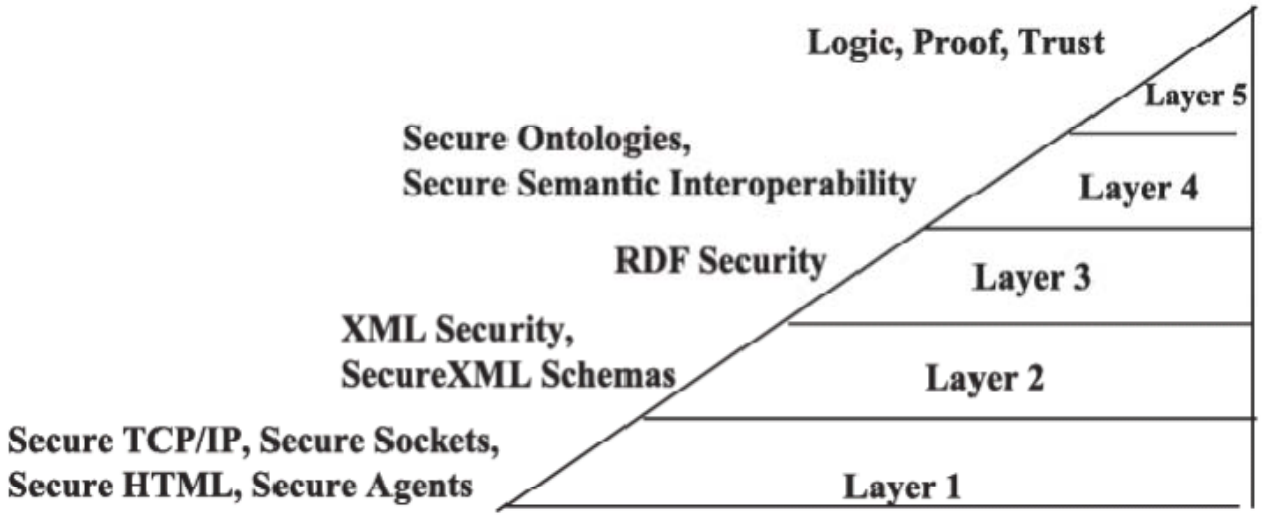
- Sémantický web a bezpečnost
- Shrnutí možných přístupů
- Naše výsledky v rámci projektu
- Závěr

Bezpečnost a budoucnost

- Slibná myšlenka Sémantického Webu
- Softwaroví agenti
- „Neomezená“ dostupnost „relevantních“ informací
- Jak řešit bezpečnost a zajistit soukromí uživatelům?

Jak řešit bezpečnost?

- Silné kryptografické algoritmy pro zabezpečení vlastní komunikace
  - na úrovni kanálů
  - zpráv
- Využít existujících řešení, např.
  - KERBEROS
  - PKI
  - PGP



Jak řešit bezpečnost? (pokr.)

- Bezpečnostní systém, který bude
  - Flexibilní
  - Sémanticky bohatý
  - Jednoduchý – automatizovatelný

- Systémy pro správu a budování důvěry
  - Policy based
  - Reputation based
  - Social Networks based

Policy based-existující mechanizmy

- Extensible Access Control Markup Language (XACML)
  - Jazyk pro popis politik
- The Platform for Privacy Preferences (P3P)
  - Definováno W3C pro popis zabezpečení (privacy) stránek, tak aby prohlížeče sami rozhodovali, zda zabezpečení koliduje s uživatelovými preferencemi
- …

Reputation based – existující mechanizmy

- Budovat důvěru mezi poskytovatelem dat, služeb a klientem na základě historických transakcí
- V současné době využívá řada webových portálů např. eBay, aukro.cz, …

Social-network based – existující mechanizmy

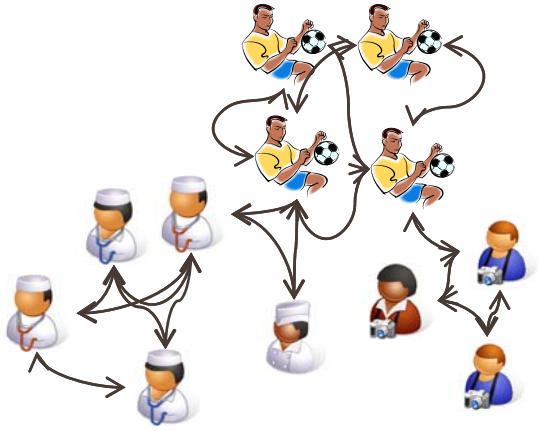
- Využití metod z oblasti sociálních sítí pro budování důvěry
- Virtuální organizace
- Virtuální komunity
- Nová sociální stránka internetu (Friendster, MySpace, LinkedIN,…)

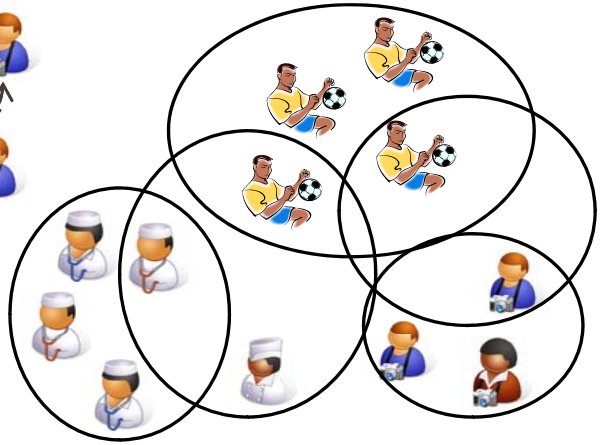
Naše výsledky

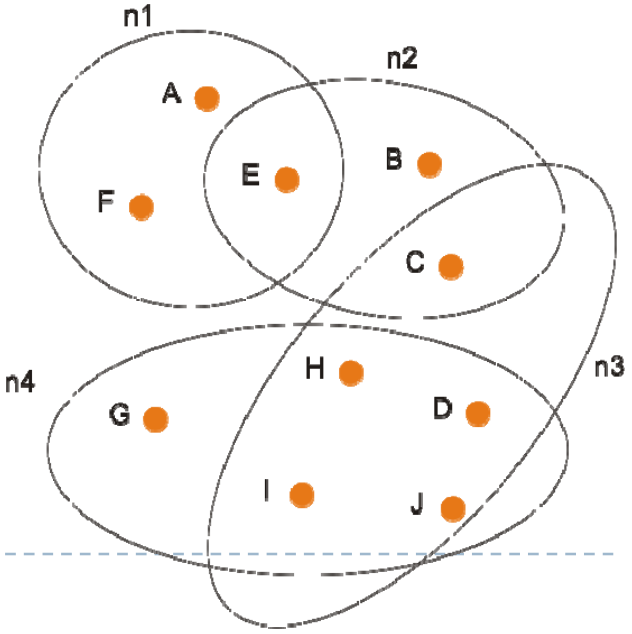
- **Systém SecGrid**
  - Disertační práce
    - R. Špánek, Self-organizing and Self-monitoring Security Model for Dynamic Distributed Environments
- **Reputační systém pro hodnocení kvality webových zdrojů**

SecGrid

- Model důvěry je založen výhradně na členství v určité skupině uživatelů
  - Hypergrafový model

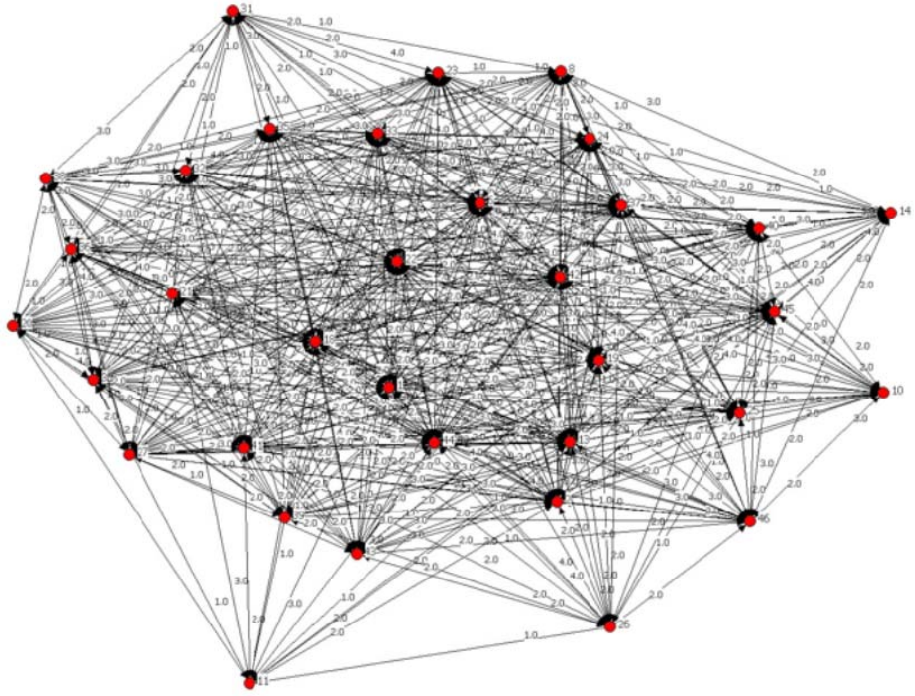


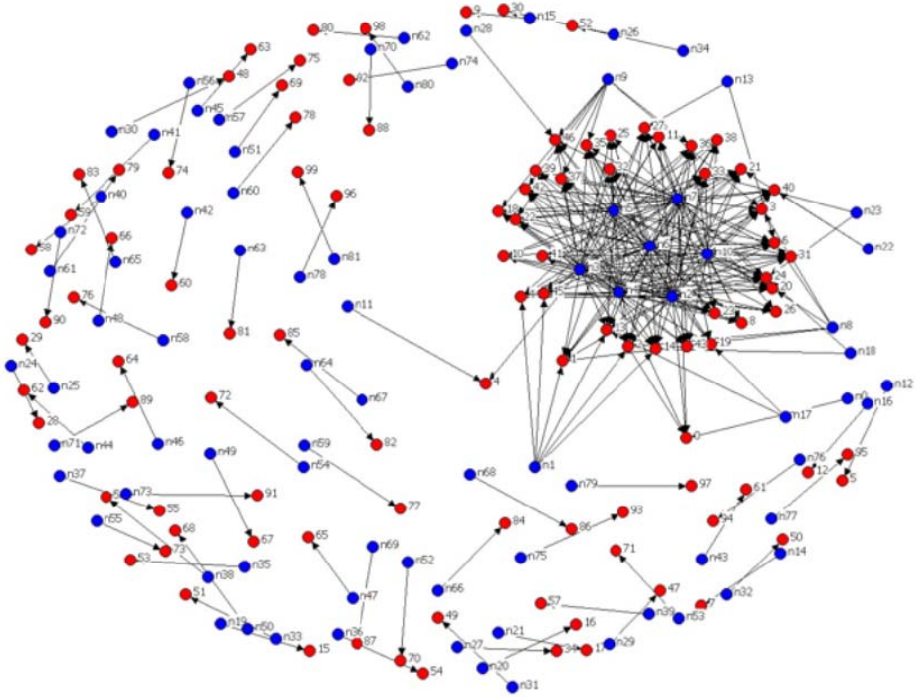




SecGrid

- Algoritmy pro transformaci obecného vstupu do hypergrafového modelu
  - G2H Algorithm (silně souvislé komponenty)
  - G2H Algorithm (triády)

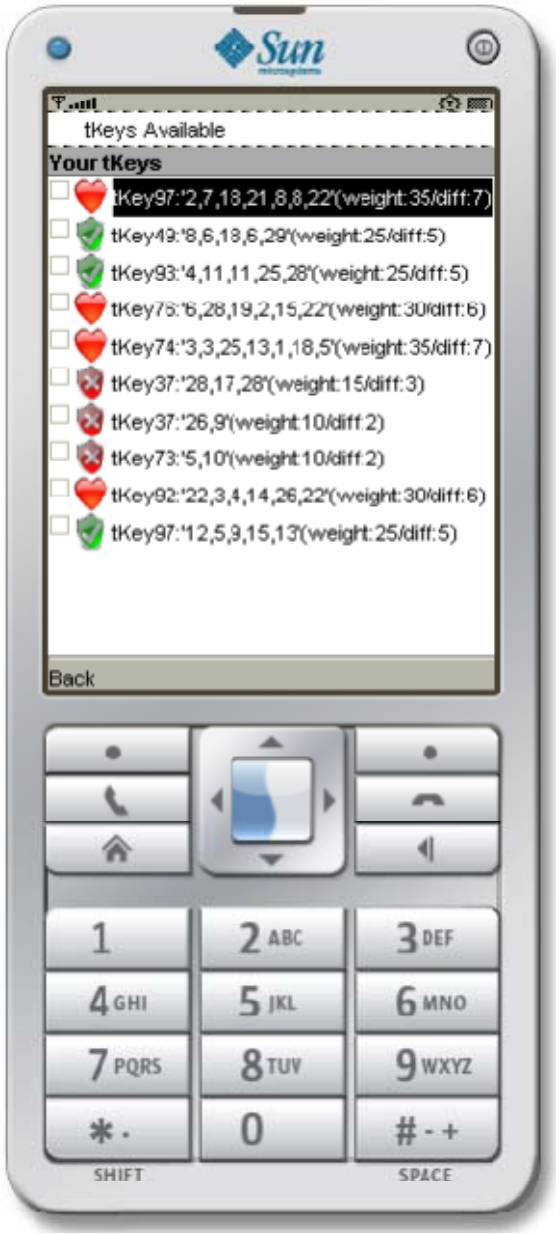




SecGrid

- *SD algoritmus* pro správu dynamiky systému skupin
- Bezpečnostní subsystém (*tKey*)
- Pilotní implementace pro mobilní telefony *MyKeys*

- Implementace v systému MediGRID

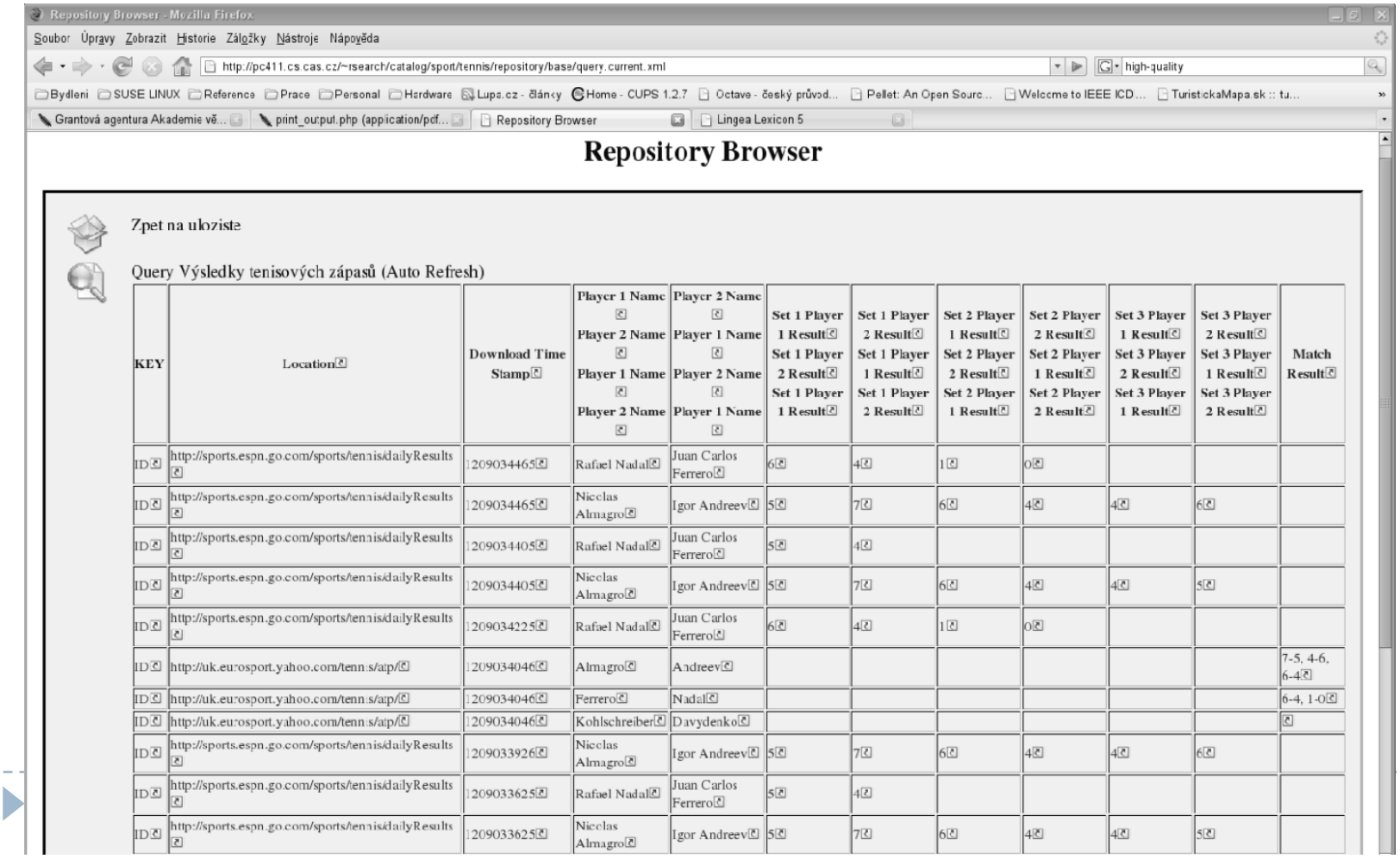


Reputační systém pro hodnocení kvality zdrojů

- Idea je vybudovat systém, který bude uživateli doporučovat data z důvěryhodnějšího zdroje
- Byl navržen systém pravidel a koeficientů, které se využívají pro výpočet reputace webového zdroje
- Využívá hypergrafový model
- Základní koeficienty zahrnují:
  - Koeficient pro potvrzená data
  - Koeficient pro zdroje poskytující nová data
  - Koeficient penalizující nekonzistence ve zdroji

Reputační systém pro hodnocení kvality zdrojů

- Experimentální implementace pro weby s „aktuálními“ informacemi o sportovních výsledcích



KEY	Location	Download Time Stamp	Player 1 Name / Player 2 Name / Player 1 Name / Player 2 Name	Player 2 Name / Player 1 Name / Player 2 Name / Player 1 Name	Set 1 Player 1 Result / Set 1 Player 2 Result / Set 1 Player 1 Result	Set 1 Player 2 Result / Set 1 Player 1 Result / Set 1 Player 2 Result	Set 2 Player 1 Result / Set 2 Player 2 Result / Set 2 Player 1 Result	Set 2 Player 2 Result / Set 2 Player 1 Result / Set 2 Player 2 Result	Set 3 Player 1 Result / Set 3 Player 2 Result / Set 3 Player 1 Result	Set 3 Player 2 Result / Set 3 Player 1 Result / Set 3 Player 2 Result	Match Result
ID	http://sports.espn.go.com/sports/tennis/dailyResults	1209034465	Rafael Nadal	Juan Carlos Ferrero	6	4	1	0			
ID	http://sports.espn.go.com/sports/tennis/dailyResults	1209034465	Nicolas Almagro	Igor Andreev	5	7	6	4	4	6	
ID	http://sports.espn.go.com/sports/tennis/dailyResults	1209034405	Rafael Nadal	Juan Carlos Ferrero	5	4					
ID	http://sports.espn.go.com/sports/tennis/dailyResults	1209034405	Nicolas Almagro	Igor Andreev	5	7	6	4	4	5	
ID	http://sports.espn.go.com/sports/tennis/dailyResults	1209034225	Rafael Nadal	Juan Carlos Ferrero	6	4	1	0			
ID	http://uk.eurosport.yahoo.com/tennis/atp/	1209034046	Almagro	Andreev							7-5, 4-6, 6-4
ID	http://uk.eurosport.yahoo.com/tennis/atp/	1209034046	Ferrero	Nadal							6-4, 1-0
ID	http://uk.eurosport.yahoo.com/tennis/atp/	1209034046	Kohlschreiber	Davydenko							
ID	http://sports.espn.go.com/sports/tennis/dailyResults	1209033926	Nicolas Almagro	Igor Andreev	5	7	6	4	4	6	
ID	http://sports.espn.go.com/sports/tennis/dailyResults	1209033625	Rafael Nadal	Juan Carlos Ferrero	5	4					
ID	http://sports.espn.go.com/sports/tennis/dailyResults	1209033625	Nicolas Almagro	Igor Andreev	5	7	6	4	4	5	

Závěr

- Důvěra je velmi cenná a také velmi křehká
- Systémy využívající důvěry jako klíče k řízení přístupu k datům či službám jsou využívány stále častěji a také ve stále větším množství scénářů a prostředí
- Systém SecGRID byl navržen tak, aby byl schopen budovat a spravovat důvěru ve velkých a dynamických prostředích
- Reputační systém pro webové zdroje se snaží uživatelům přinést způsob, jak se rozhodovat, kterému zdroji věřit

Děkuji za pozornost