Types in access control and privacy

Silvia Ghilezan

University of Novi Sad

NII Shonan Meeting 069
LOGIC AND VERIFICATION METHODS IN SECURITY AND PRIVACY
October 26-29, 2015

Type systems

- Types have gained an important role in the analysis of formal systems.
- A type system splits elements of the language, called terms, into sets, called types, and proves absence of certain undesired behaviours on the basis of the types that are thus assigned.
- Undesired behaviours - run-time type errors.
- Deadlocks, race conditions, arity mismatch, communication errors, security flaws,...

Outline

Types:

1. Role Based Access Control
2. Linked Data
3. Communication-centered Calculi

1. Dynamic Web Data

Process-like calculi

π-calculus $D\pi$ $XD\pi$

Models of reconfigurable concurrent systems

- processes and their parallel composition
- communication between processes
- channel transmission and creation of fresh channels
- nondeterminism
- replication of processes
- locations (M. Hennessy)
- Data (P. Gardner, S. Maffeis)

Role-Based Access Control of Dynamic Web Data

Joint work: M. Dezani-Ciancaglini, J. Patnović,
D. Varacca, S. Jakšić, 2006-2010.

- RBAC, standard of NIST, is an access control method that relies on the notions of users, roles and permissions.
- Role-based access control calculus for modelling dynamic web data in $XD\pi$.
  - A network is a parallel composition of locations, where each location contains processes with roles and a data tree whose edges are associated with roles.

$$N ::= l[D^r \mid P^r] \quad | \quad N|N$$

  - Processes can communicate, migrate from a location to another, use the data, change the data and the roles in the local tree.

Role-Based Access Control of Dynamic Web Data

Types to control:

- the communication of values,
- the migration of processes
- the access of processes to data
- update of roles.

M. Dezani-Ciancaglini, S. G., S. Jakšić, and Jovanka Pantović.
Types for Role-Based Access Control of Dynamic Web Data.
In Proceedings of WFLP'10, LNCS, Vol. 6559, pages 1–29, Springer, 2011.

M.Dezani-Ciancaglini, S. G., J. Pantovic, D. Varacca:
Security types for dynamic web data,
Theoretical Computer Science 402: 156-171 (2008).

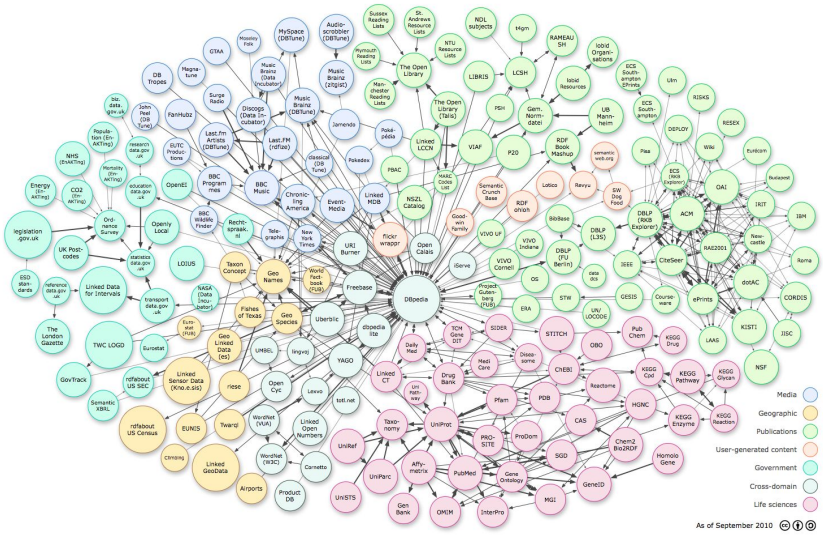
M.Dezani-Ciancaglini, S. G., J. Pantovic, D. Varacca:
Security types for dynamic web data,
TGC'06 - Trustworthy Global Computing, LNCS 4661: 263-280 (2006).

2. Privacy for Linked Data

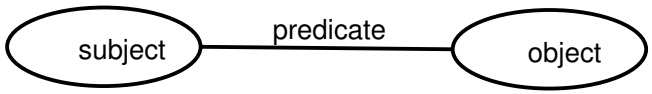
Joint work: J. Pantović, S. Jakšić.

- Web of Linked Data vs Web of Documents
- Technologies: URIs (Uniform Resource Identifiers), RDF (Resource Description Framework), SPARQL,...
- W3C project: Semantic Web
  `http://www.w3.org/standards/semanticweb/`
- Published Data: media, publications, life sciences, geographic data, DBpedia, e-government, user-generated content (including profiles from social networks and blogs),...

Linked Data Cloud



RDF/XML and the calculus



RDF as an XML document

$$(\texttt{subject}, \texttt{predicate}, \texttt{object})$$

$$D ::= \emptyset \quad | \quad (a, a, a)^U \quad | \quad D \parallel D$$

$$N ::= a[D \mid P] \quad | \quad N|N$$

Bizer, C. and Heath, T. and Berners-Lee, T. (2009)
Linked Data - the Story So Far
International Journal on Semantic Web and Information Systems, 5 (3):1 - 22.

Access Control and Privacy

- Access Control is a mechanism through which permissions are granted to entities to perform operations on Linked Data resources
- "Privacy is the ability to control who has access to information and to whom that information is communicated" - A. Westin (Privacy and Freedom, 1967).
- Privacy may not include just private status of some data but also significance or no significance of data for some group and the ability of readers to understand the data properly.

Privacy for Linked Data

Our goal:

to create a formal (typed) model of Linked Data that can statically detect run-time errors due to privacy violation.

S. Jakšić, J. Pantović and S. G.
Linked Data Privacy.
Mathematical Structures in Computer Science, online (2015).

3. Communication-centered Calculi

- Distributed systems rely on communication that run over open networks.
- They can be targeted by malicious parties trying to threaten their functionality or to seize or compromise sensitive data.
- Need for rigorous (and scalable) techniques to ensure the reliability and security of these systems.
- In programming languages, type systems represent a well-established technique to ensure program properties.

Behavioural types and reliability analysis

$$a!2 \mid a?x.x!5 \rightarrow 2!5$$

$$a!b \mid a?(x,y) \not\rightarrow$$

$$a?x.b!x \mid b?y.a!y \not\rightarrow$$

$$c!a \mid *c?x.c!x \mid a!7 \equiv c!a \mid c?x.c!x \mid *c?x.c!x \mid a!7 \rightarrow c!a \mid *c?x.c!x \mid a!7$$

Behavioural types and security analysis

- Behavioural types for communication-centered systems ensure that the type system obeys the prescribed security policies (e.g., access control or secure information flow).
- Session types allow interactions to be structured into basic units, called sessions.
- The expressiveness of session types has enabled their application in diverse contexts, targeting
  - different programming models (functional and object-oriented programming)
  - operating system design
  - middleware communication protocols.

Behavioural types and security analysis

BETTY - Behavioural Types for Reliable Large-Scale Software Systems, COST IC1201 (2012-2016)

WG2: Security - integrating behavioural types with techniques for security analysis

M. Bartoletti, I. Castellani, P.-M. Denielou, M. Dezani-Ciancaglini, S. Ghilezan, J. Pantovic, J. A. Perez, P. Thiemann, B. Toninho, H. Torres Vieira:
Combining behavioural types with security analysis,
Journal of Logical and Algebraic Methods in Programming 84 (2015) 763 - 780.

S. G., S. Jakšić , J. Pantović, J. A. Pérez and H. Torres Vieira:
Dynamic Role Authorization in Multiparty Conversations.
BEAT 2014. EPTCS 162: 1-9 (2014).
Formal Aspects of Computing

Conclusion

- BETTY - Behavioural Types for Reliable Large-Scale Software Systems, COST IC1201 (2012-2016)
  - WG2: Security - integrating behavioural types with techniques for security analysis
- Behavioural types - tools development (N. Yoshida)
- Types for Linked Data - different approaches (V. Sassone, M. Dezani, G. Ciobanu, R. Horne)
- Privacy Preference Ontology (O. Sacco and A. Passant).

TYPES 2016, May 23-27, 2016, Novi Sad

- **TYPES 2016** - 22nd International Workshop on **Types for Proofs and Programs**
- Affiliated events
- **Novi Sad, Serbia**
- **May 23- 27, 2016**