

Policies and Mechanisms for Safe Information Release

Andrei Sabelfeld

Department of Computer Science
Chalmers University of Technology
412 96 Göteborg, Sweden

Much work on security-typed languages lacks a satisfactory account of intentional information release (or leakage). In the context of confidentiality, a typical security guarantee provided by security type systems is noninterference, which allows no information flow from secret inputs to public outputs. However, many intuitively secure programs do allow some release, or declassification, of secret information (e.g., password checking, information purchase, and spreadsheet computation). Noninterference fails to recognize such programs as secure. In this respect, many security type systems enforcing noninterference are impractical.

On the other side of the spectrum are type systems designed to accommodate some information leakage. However, there is often little or no guarantee about what is actually being leaked. As a consequence, such type systems are vulnerable to laundering attacks, which exploit declassification mechanisms to reveal more secret data than intended.

We discuss two policies to bridge this gap, *delimited release* [SM04] and *robust declassification* [ZM01,MSZ04], capturing *what* information is released and *who* controls information release, respectively. These security policies provide two kinds of end-to-end guarantees that declassification cannot be exploited by laundering attacks. We present security type systems that straightforwardly and provably enforce delimited release and robust declassification.

In addition, we explore avenues for comparing and combining policies for information release with the intention of preventing hazardous situations where policies provide only partial assurance that information release mechanisms cannot be compromised.

Based on pieces of published joint work with Andrew C. Myers and Steve Zdancewic, and unpublished joint work with David Sands.

References

- [MSZ04] A. C. Myers, A. Sabelfeld, and S. Zdancewic. Enforcing robust declassification. In *Proc. IEEE Computer Security Foundations Workshop*, June 2004.
- [SM04] A. Sabelfeld and A. C. Myers. A model for delimited information release. In *Proc. International Symp. on Software Security (ISSS'03)*, LNCS. Springer-Verlag, 2004. To appear.
- [ZM01] S. Zdancewic and A. C. Myers. Robust declassification. In *Proc. IEEE Computer Security Foundations Workshop*, pages 15–23, June 2001.