# Built-in Object Security

Martín Abadi

Computer Science Department
University of California, Santa Cruz
abadi@cs.ucsc.edu

Modern programming languages and systems provide much support for security. Through strong typing, they can substantially reduce the opportunities for low-level coding errors that could result in buffer overflows and other vulnerabilities. They also allow protection by encapsulation and the treatment of objects as unforgeable capabilities. In addition, they sometimes include rich security infrastructures, for example libraries for authentication and authorization.

Although common programming languages are not primarily concerned with security, language definitions can be the basis for security guarantees. A language specification may imply, for instance, that object references are unguessable. An implementation may resort to cryptography in order to enforce this property and others built into the language.

Conversely, for better or for worse, security machinery can have a significant effect on language semantics and implementations, even when it is regarded as an add-on. For instance, access-control techniques that depend on the contents of the execution stack give an observable role to the stack, affecting program equivalences. A language perspective can help in understanding such security mechanisms and sometimes in developing new ones.

## References

1. Martín Abadi. Protection in programming-language translations. In *Proceedings of the 25th International Colloquium on Automata, Languages and Programming*, volume 1443 of *Lecture Notes in Computer Science*, pages 868–883. Springer-Verlag, July 1998.
2. Martín Abadi and Cédric Fournet. Access control based on execution history. In *Proceedings of the 10th Annual Network and Distributed System Security Symposium*, pages 107–121, February 2003.
3. Martín Abadi, Cédric Fournet, and Georges Gonthier. Secure implementation of channel abstractions. *Information and Computation*, 174(1):37–83, April 2002.
4. Leendert van Doorn, Martín Abadi, Mike Burrows, and Edward Wobber. Secure network objects. In *Proceedings of the 1996 IEEE Symposium on Security and Privacy*, pages 211–221, May 1996.