Dagstuhl Seminar 07091 on Mobility, Ubiquity and Security

Executive summary

Gilles Barthe Heiko Mantel Peter Müller Andrew C. Myers Andrei Sabelfeld

Increasing code mobility and ubiquity raises serious concerns about the security of modern computing infrastructures. The focus of this seminar was on securing computing systems by design and construction.

The seminar covered a wide span of application areas, including:

- telecommunications
- automotive industry
- web browsers
- electronic voting
- web services
- distributed systems
- media distribution
- data mining

The need for security in these applications is critical. The seminar structure reflected the general categories of security properties that are required in scenarios as above. Each category served as a theme for presentations on each of the first four days of the seminar. Each of these days was kicked off by a tutorial talk. These categories were:

Confidentiality David Sands' tutorial showed that (partial) equivalence relations were ubiquitous in security modeling. The tutorial was followed by these talks:
Anindya Banerjee: Information flow, modularity and declassification
Alejandro Russo: Closing internal timing channels by transformation
Gregor Snelting: Information flow control for Java based on path conditions in dependency graphs
Peeter Laud: Dependency-graph-based protocol analysis
Henning Sudbrock: A probabilistic justification of the combining calculus
Mads Dam: A complete logic of knowledge and one-way computable terms
Alexander Reinhard: Controlling the what and where in language-based security
David Pichardie: A certified lightweight non-interference java bytecode verifier
Richard Bubel: Integration of a security type system into a program logic

Integrity Joshua Guttman's tutorial illuminated the interaction between two aspects of integrity: invariants vs. causality. The tutorial was followed by these talks:
Steve Zdancewic: Combining access control and information flow in DCC
Cédric Fournet: Secure implementations for typed session abstractions
Fausto Spoto: Optimality and condensing of information flow through linear refinement
Brendan Eich: JavaScript: Mobility and ubiquity—two out of three ain't bad
Peter Ryan: Trustworthy elections
Flemming Nielson: Static analysis for DRM
Amy Felty: Program verification, noninterference, and declassification applied to privacy in data mining
Dieter Hutter: Preserving privacy in service composition using information flow control
Brigitte Pientka: Contextual modal logic

Availability Thomas Jensen's tutorial emphasized that even simple availability were hard to enforce. The tutorial was followed by these talks:
Pierpaolo Degano: A static approach to secure service composition
Andrew Myers: Ensuring confidentiality, integrity, and availability by construction

Foundations of cryptography Cédric Fournet's tutorial demonstrated that computational and semantic views of security can be reconciled, although more progress is needed. The tutorial was followed by these talks:
Tamara Rezk: Computational noninterference
Hanne Riis Nielson: Flow sensitive analysis of security properties
Aslan Askarov: Gradual release: unifying declassification, encryption, and key release policies
Santiago Zanella Béguelin: Towards code-based cryptographic proofs
Daniel Hedin: A framework for parameterizing type systems with relational information
Ian Stark: Resource type checking in database queries
Joshua Guttman: Programming cryptographic protocols

The seminar was concluded with the following talks:
Peter Müller: Generic universe types
Arnd Poetzsch-Heffter: A behavioral semantics of object-oriented components
Gilles Barthe: Certificate translation
Marieke Huisman: BML
Fabio Martinelli: Modeling and enforcing security & trust management policies (on JVM)

Thanks to Dagstuhl's stimulating environment, many insightful discussions, planned and unplanned, took place. There were two large organized discussion, where all participants were involved: a panel on electronic voting (e-voting) and a general discussion.

Panel on e-voting A panel on e-voting was moderated by Peter Ryan and featured Jorge Cuellar, Joe Kiniry, and Carsten Schürman. This panel generated a lively discussion on the role of formal methods in e-voting. E-voting includes both supervised and remote scenarios where the results are processed electronically. While several concerns were raised about trust involved in various e-voting schemes much evidence was brought up for benefits of e-voting and the need for formal methods for its support.

General discussion The general discussion reiterated the need for building the security in. It arrived at the following important directions for future research:

- There is potential in combining advanced static analyses, program logics, type systems, and program transformation for security.
- Integrated approaches to enforcing multiple security properties are much desired.
- The web page is the new operating system. Language-based techniques may help securing it.
- Formal methods are needed for e-voting protocol design and implementation.

With a top-of-the-line collection of invitees placed in Dagstuhl's productive environment, it may seem that little could have gone wrong with the seminar. Still, the we are fully satisfied that our efforts on organizing the meeting have been rewarded by a seminar with a clear focus; good balance between talks, panels, and discussions; and rich cross-fertilization that have already resulted in new collaborations.