

# Hagai Bar-El

Information Security Specialist

16 Mukasey St., Rehovot 76657, Israel

Tel./Fax (Israel): +972 (8) 935-4152 Tel. (US): (202) 657-4705

E-mail: [hagai@hbarel.com](mailto:hagai@hbarel.com) Web: [www.hbarel.com](http://www.hbarel.com) Skype: hbarel

## Field of Activity

**Active in the field of system security; practice and vision.** Primary expertise and experience is in the design of security systems, security evaluation of designs, and management of innovation groups. Experience also covers evaluation of new technologies and research plans (e.g., for FP7), designing solutions to given customers' problems, standardization activities, and management of invention and innovation processes, including the filing of several patent applications.

## Work Experience

### Senior Security Architect, *Discretix Technologies*, 2000 to present

**Head of the Technology Group, and a senior information security analyst**, since the establishment of the company. Job consists mainly of:

- Management of the *Technology Group*. The Technology Group is chartered at defining new technologies for future products (2-5 year span) for both business units, at defining security requirements, and at forming the focal point for security knowledge in the company.
- Management of innovation processes at the company: managing a team of inventors, evaluating new ideas, deciding on patent filing (as a member of the Patent Committee), drafting patent applications and defining patent claims, seeing the intellectual property throughout the patent prosecution process, managing the analysis of prior art, and managing and interacting with patent attorneys. I handled more than a dozen individual patent files, including all professional aspects of prior-art analysis, claim specification, office-action responses, etc. Licensing of this intellectual property forms a significant part of the company's revenues.
- Definition of security requirements and definition of the security schemes and protocols that are implemented into products. This includes the security mechanisms that are at the core of the primary (CryptoCell<sup>®</sup> and CryptoFlash<sup>®</sup>) product lines — secure storage, secure boot, code integrity, etc.
- Design of security mechanisms for solving real-world business needs of customers, such as in the fields of m-commerce, Digital Rights Management (DRM), and secure device management.
- Porting information security knowledge into the company; accomplished by constant review of publications and standards, and through participation in various discussion forums, as well as the moderation of one. This activity is extremely important as Discretix is a security company that is trusted by its customers to possess the most up to date knowledge.
- Interaction with evaluation labs that attest for the robustness of the products, as well as seeing through the certification of the products by FIPS 140.
- Representation of the company and its technologies in standardization bodies such as the MeT (Mobile Electronic Transactions), OMTP (Open Mobile Terminal Platform), OTAFF (Over The Air Flash Forum), and OMA (Open Mobile Alliance).
- Functioning as a conduit, linking between the business development and the engineering groups. Notable achievements include the introduction of security methods into Device Management and Mobile Broadcast specifications.

## Information Security Analyst, *hbarel.com*, 1995 to present

Self-employed (sole proprietorship) as a specialist in the field of information security. The types of services that are provided by the office (in brief) are:

1. Design of secure systems
2. Invention, and management of innovation expert groups
3. Evaluation of information security products
4. Evaluation of research proposals, e.g., for the 7<sup>th</sup> Framework Program of the European Commission
5. Evaluation of new and emerging technologies, e.g., for VCs
6. Research and management of research groups
7. Delivery of lectures on various aspects of information security
8. Testing network security
9. Consulting on various information security topics

Services that currently provided are listed in: <http://www.hbarel.com/Services.htm>.

Clients include major corporate players in the fields of telecommunication, banking, venture capital, defense, and technology, both in the public and the private sectors.

## Education

**1994–1997** B.A. cum laude in Computer Science, from the Academic College of Tel-Aviv Jaffa.

**1996–2008** Attended several seminars, academic courses, and conferences, on information security, cryptography and intellectual property. Included are trade shows in Israel and abroad, and a “practical cryptography” course at the Weizmann Institute of Science.

**2008** Attended a course on Intellectual Property Management, in Lahav Inst., Israel.

## Publications

Publicly available publications are available at: <http://www.hbarel.com/publications.htm>

Publications currently are:

- Intra-Vehicle Information Security Framework (*presented at the ESCAR 2009 Conference, Düsseldorf, Germany, November 2009*)
- DRM on Open Platforms (*presented at the 2<sup>nd</sup> IEE Secure Mobile Communications Forum, London, UK, September 2004*)
- The Sorcerer’s Apprentice Guide to Fault Attacks (*published in the Proceedings of the IEEE, Volume 94, Number 2*)
- Challenges in Designing Content Protection Solutions
- Challenges of Standardizing Renewable Broadcast Security
- On The Importance of Secure Coding
- Security Implications of Hardware vs. Software Cryptographic Modules
- Why We May Never Have DRM
- When To Use Biometrics
- Introduction to Side-Channel Attacks
- Known Attacks Against Smartcards

# Patents

DESCRIPTIONS ENCLOSED IN THIS SECTION MAY BE OF EXEMPLARY EMBODIMENTS OF CLAIMED INVENTIONS. THESE DESCRIPTIONS SHALL NOT BE TREATED AS DEFINING, LIMITING, OR SUGGESTING AT THE SCOPE AND/OR SUBJECT OF THE CLAIMED INVENTIONS.

Sole inventor of the following patents and pending patent applications:

- UK Patent 2434673** *Method, Device, and System of Securely Storing Data*, Hardware-based secure storage for keys and credentials with data confidentiality and integrity and with protection against rollback attacks.
- 20060232826** *Method, Device, and System of Selectively Accessing Data*, Corporate secure storage allowing server-based control of secure data stored as files on a client device, as well as user-level access control to files, implemented under the file-system layer.
- 20060294236** *System, Device, and Method of Selectively Operating a Host Connected to a Token*, SIM Lock (and other) mechanisms based on a secure embedded Flash device.
- 20090031133** *Method And System For Screening And Authorizing Content*, a system and method for utilizing fingerprinting technologies for content identification and blockage on mobile devices.
- 20090031427** *Device, System, And Method Of Digital Rights Management Utilizing Supplemental Content*, a system, method, and device for allowing the introduction of supplemental content, such as advertisements, into DRM systems.

Co-inventor of the following patents and pending patent applications:

- US Patent 7,467,304** *System, Device, and Method of Selectively Allowing a Host Processor to Access Host-executable Code*, Secure system boot based on a secure embedded Flash device. This patent was granted on December 16<sup>th</sup>, 2008.
- 20060242429** *Memory System with In-stream Data Encryption/Decryption*, Secure Flash card architecture including on-the-fly encryption/decryption.
- 20070061597** *Secure yet Flexible System Architecture for Secure Devices with Flash Mass Storage Memory*, Secure boot mechanism for a secure flash card with program code stored on flash memory.
- 20060176068** *Secure Memory Card with Life Cycle Phases*, Enables different levels of system functionality according to the life cycle state of a device.
- 20060242068** *Memory System with Versatile Content Control*, Flash card based corporate secure storage.
- 20090202078** *Device, System, and Method of Securely Executing Applications*, A secure execution environment utilizing hardware components to assure execution and data isolation between multiple mutually-distrusting applications.