Hagai Bar-El

Information Security Architect

5 Aaron Ciechanover St., Rehovot 7608632, Israel

hagai@hbarel.com www.hbarel.com

Field of Activity

System security: architecture and vision. Expertise and experience in the architecture of secure systems, information-security evaluation, and management of security research and analysis teams, as a C-level executive. Experience also covers evaluation of emerging technologies and research plans (e.g., for FP7 and H2020), problem solving, standardization activities, and management of innovation processes and intellectual property.

Work Experience

Senior Director of Security, IoT Business Unit, *ARM*, 2015 to present

Responsible for information security design and engineering, and head of the *Security Group* of the IoT Business Unit of ARM. This position consists mainly of:

- Professional and organizational management of the *Security Group* of the IoT Business Unit (formerly, the *CTO Office* of *Discretix Technologies*).
- Responsibility for the Secure Development Lifecycle (SDL) of *ARM mbed*®, and the security of its operation.
- Participation in the design and evaluation of information security technologies across ARM.
- Participation in the definition of Security Strategy in ARM; assuring coherence between security roadmaps of different divisions of the company.
- Conducting security review processes for ARM products — within the IoT Business Unit and otherwise.

Chief Technology Officer, *Discretix Technologies*, 2012–2015

Full CTO capacity, in addition to being the Chief Information Security Architect and to managing the CTO Office, as specified below. This position was held until Discretix Technologies (a.k.a. *Sansa Security*) was acquired by ARM and ceased to exist as an independent company, on August 2015.

Senior Security Architect, *Discretix Technologies*, 2000–2015

Head of the CTO Office (Technology Group), and Chief Information Security Architect, since the establishment of the company. The position consisted mainly of:

- Being a member of the company management, as of September 2011.
- Management of the *CTO Office* (formerly referred to as the "Technology Group"). The CTO Office was chartered at defining new technologies for future products (2–5 year span), defining security requirements, security analysis, and at forming the focal point for security knowledge in the company.
- Management of innovation processes at the company: evaluating new ideas for products and security enhancements, defining and enforcing the patent filing strategy, drafting patent applications and defining patent claims, seeing the intellectual property throughout the patent prosecution process, managing the analysis of prior art, and interacting with IP service providers.

- Definition of security requirements and of the security schemes and protocols that are implemented into products. This includes the security mechanisms that are at the core of the CryptoCell® CryptoFlash®, Sansa Provisioning®, and other product lines. Such mechanisms include: secure storage, secure boot, code integrity, content protection, automotive firewall, key provisioning, etc.
- Porting information security knowledge into the company: constant review of publications and standards, and through participation in, and moderation of, discussion forums. This activity was extremely important, because Discretix was a security company that is trusted by its customers to possess the most up to date knowledge in this domain.
- Interaction with evaluation labs that attest for the robustness of the products, such as in the context FIPS 140 and EMV certification.
- Representation of the company and its technologies in standardization bodies such as the GlobalPlatform, MeT (Mobile Electronic Transactions), OMTP (Open Mobile Terminal Platform), OTAFF (Over The Air Flash Forum), OMA (Open Mobile Alliance), and IIC (Industrial Internet Consortium).

Information Security Architect, *hbarel.com*, 1995 to present

Self-employed (as sole proprietorship) architect in the field of information security. Services provided consist mainly of:

- Design of secure systems, such as for an industrial firewall, IP TV, and more.
- Evaluation of research proposals, for the 7^{th} Framework Program of the European Commission, in several calls addressing all areas related to security, as well as in its continuation program, H2020.
- Periodic review of an ongoing security research project, for the 7^{th} Framework Program of the European Commission.
- Evaluation of information security products, from both functional and robustness perspectives.
- Evaluation of new and emerging technologies, e.g., for Venture Capital customers.

Customers along the years included major corporate players in the fields of telecommunication, banking, venture capital, defense, and technology, both in the public and in the private sectors.

Education

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

1996–2013 Attended several seminars, academic courses, and conferences, on information security, cyber 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 Institute, Israel.

Publications

Publicly available papers are listed at: `https://www.hbarel.com`, under "Recent Publications". Select publications are:

- Intra-Vehicle Information Security Framework *(presented at the ESCAR 2009 Conference, Düsseldorf, Germany, November 2009)*
- DRM on Open Platforms *(presented at the 2^{nd} 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

A professional blog is maintained at: `https://www.hbarel.com`

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:

United States Patent 8,687,813 *Methods, Circuits, Devices and Systems of Provisioning of Cryptographic Data to One or More Electronic Devices*, a system, method, circuit and device for lightweight key provisioning that supports delegation between provisioning entities.

United States Patent 8,201,260 *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.

UK Patent 2,434,673 *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.

Application 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.

Application 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.

Application 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.

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

US Patent 9,231,758 *System, Device, and Method Of Provisioning Cryptographic Data To Electronic Devices*, Secure provisioning of assets while supporting complex trust models between stakeholders.

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$^{\text{th}}$, 2008.

US Patent 7,934,049 *Methods Used in a Secure Yet Flexible System Architecture for Secure Devices with Flash Mass Storage Memory*

US Patent 8,369,526 *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.

US Patent 8,321,686 *Secure Memory Card with Life Cycle Phases*, Enables different levels of system functionality according to the life cycle state of a device.

European Patent 2,189,922 *Memory System with Versatile Content Control*, Flash card based corporate secure storage.

US Patent 9,344,275 *System, Device, and Method of Secure Entry and Handling of Passwords*, allowing secure password and PIN entry.

Application 20060242429 *Memory System with In-stream Data Encryption/Decryption*, Secure Flash card architecture including on-the-fly encryption/decryption.

Application 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.

Application 20130301830 *Device, System, and Method of Secure Entry and Handling of Passwords*

Application 20130305041 *Method, Device, and System of Secure Entry and Handling of Passwords*

Co-inventor of 3 other *granted* patents in China, Japan, and Korea, as well as of one other non-published patent applications in the US.