Resume of Marlena Erdos

marlena@acknowledgesoftware.com
(617) 216-6563

SUMMARY

What I do: Solve "intractable" IT identity, security, and privacy problems using superior listening, analysis and (re)design skills; Work from the abstract conceptual level through to fine deployment details; Produce and present reports to explain complex issues to diverse audiences; Collaborate effectively with C-level executives, marketers, engineers, technical writers, and customers.

Career Highlights:

- Architected Internet2's Consent-informed Attribute Release (CAR) system, 2016
- Co-created the SAML & Shibboleth Federated Identity Management standards, 2001
- Published "RFID & Authenticity of Goods" in *RFID: Applications, Security, and Privacy*, 2005
- Hacked two "highly secure" commercial systems by finding design flaws, and then provided ways to secure the systems (1992 and 2005)

Expertise In: Distributed computing, security, privacy, identity management, federated systems, authentication and authorization, policy language for access control and privacy, OAUTH/OIDC, SAML, PKI (digital signatures and certificates), communications protocols, RFID, and the Common Criteria (a set of US government security standards).

Facility With: REST APIs, Swagger, JSON, XML, LDAP, SQL, crypto systems, GDPR, medical privacy (HIPAA), low-level networking tools, servlets, HTTPD, provisioning, software implementation and deployment.

PROFESSIONAL and CONSULTING EXPERIENCE

Acknowledge Software, Inc. – business entity for my consulting work **October 1995 – Present**
Consult in security and privacy. Analyze and architect secure distributed systems. Provide advice to my clients on external vendors, products, and industry standards. Create papers and presentations for a variety of audiences related to security and privacy. Dive deep into code as needed for analysis and design (and software development!).

Evolv Technology – makers of innovative weapons detections systems (evolvtechnology.com) **December 2019 – February 2020**

- Provided recommendations for enhancing overall system security.
- Created adversary model and threat model approach.
- Created analysis of select sensitive system flows.

Internet2/InCommon – a consortium of US universities and colleges (internet2.edu) **March 2016 – September 2017**
Architected a system ("CAR") for consent-informed release of user info. CAR integrates institutional policies with user policies, and provides for fine-grained policy control over specific attributes. Handles GDPR requirements on user info release. CAR is currently being developed at a major research university, with deployment set for 2020.

- Created the system architecture of three interacting services.
- Created the policy language at each of three services (with input from the implementation lead), including how to resolve policy conflicts. Created formal grammar for these languages (needed for the API).
- Created the REST API for the services using Swagger.
- Worked closely with implementation lead and UI designers.
- Worked closely with product marketing, providing significant input on and review of marketing materials.
- Contributed significantly to Internet2's "Reference Architecture," providing a "C-Level" diagram, a "one-pager" about the reference architecture, and other materials.

Harvard University IT (HUIT), Identity & Access Management team **2012 – 2016**
Hired to worked on a variety of projects, especially those that were known to be difficult or lacking traction. Key projects and outcomes included:

- Architected a new set of services for enhanced person-finding and identifier assignment, providing architecture diagrams, extensive text discussions, and sequence diagrams. A variant of this system was deployed in 2016.
- Designed new tool to de-duplicate identifiers in six weeks using input from SMEs.
- Deciphered an "undecipherable" body of PowerShell code, MS SQL Server stored procedures and database tables that formed the identity management system for Harvard Medical School.
- Deployed Harvard's first Shibboleth/SAML IdP and wrote secure code that integrated the IdP with Harvard's legacy authentication system.

- Created and presented talks on identity federation, authentication in the web, and communications protocols to various groups within Harvard IT, including a play on sessions and cookies.

Ozmott **Summer 2011**

Consulted to CTO of company creating a mobile phone app with a social networking component:

- Clarified the model of users, accounts, and phones.
- Provided design and implementation recommendations to protect both client and server resources. Recommendations covered authentication, authorization, crypto keys, and life-cycle management of users and keys.

Resilient Networks **Winter 2010**

Provided security consulting to C-level executives and senior staff at this innovative healthcare startup. Topics included identity management, network architecture, and PKI.

Harvard Medical School (HMS) **Autumn 2009**

HMS researchers needed to give scientists from other institutions (limited) access to HMS resources for collaboration and to meet grant requirements. Existing process was staff-intensive and slow.

- Created automated provisioning of new foreign users and authentication and authorization of these users, employing the Shibboleth/SAML federation standard in a novel way.

IBM/DataPower **2005 – 2008**

Worked with senior technical staff members to successfully meet the requirements of an EAL4 Common Criteria (CC) evaluation of Datapower's XML security gateways (XS40 and XI50). Performed technical analyses of the products, did deep code examination (C++) in support of the analyses, provided advice on security-related design and implementation decisions, created low-level protocol validation tests, served as point person for CC rule interpretation, and created/modified the CC-specified documents that serve as the basis for the evaluation.

Identity Associates **Autumn 2005**

Analyzed use cases for an LDAP "adapter" that was part of a certificate management system. Systematized use case factors. Analyzed error conditions. Provided initial architecture and operational considerations for the adapter service. Found, and provided a solution for, a major security hole in the client's current product.

Bank of America/Axis Technology **Winter 2004**

Technical lead on Entitlements & Authorization project in the Information Delivery and Services group within the Wealth and Investment Management group.

- Created initial security and privacy requirements surrounding a key cross-department information delivery initiative.
- Helped Bank personnel begin to model the distributing computing flows for this initiative.
- Analyzed an existing Bank of America privacy project for applicability to needs of wealthy clients.
- Performed data analysis/reduction, reducing 20 pages of individual access control rules into two single page access trees.

IBM **1998 – 2004**

Consultant working as a member of IBM's security architecture team:

- Designed a solution for the security "bootstrapping" problem for turn-key RFID readers installed in retail stores.
- Analyzed RFID-based loss prevention schemes.
- Contributed to the SAML federation standard. SAML is now used worldwide by Google and Microsoft.
- Initiated and co-authored the Shibboleth architecture document.
- Analyzed and reviewed designs for a next-generation privacy system.
- Reviewed/critiqued next-generation privacy policy language (EPAL).

Blackwatch/Tandem **1996 – 1997**

- Provided architectural guidance related to extensions to an X.509-compliant PKI system.
- Enhanced code base (in C++), providing for directory-independent cross-certification and handling of foreign users.

JavaSoft **Autumn 1996**

Consultant to Development Team: performed a security analysis of the Java Virtual Machine (JVM) and Java Development Kit (JDK). Co-wrote ***The Java Security Reference Model,*** a plain-language discussion of security in Java.

Banyan Systems (a networking company) **1993 – 1995**
Served as Banyan's security lead across the product line. Provided expertise on other enterprise computing issues (X.500, RPC, communications, licensing). Found security holes in Banyan's "best in class" security via design analysis, and provided solutions.

Fidelity Investments **Winter 1992**
Consultant to Technical Architecture team. Advised team developing enterprise-wide computing strategy for Fidelity. Topics included security (Kerberos), transaction systems, naming, and interoperability.

HP/Apollo **1985 – 1992**
- Designed/implemented object activation and message handling (in C++) for a client-server system.
- Co-designed a distributed object (discretionary) security system.
- Coded thread-safe database access layer (in C).
- Designed and implemented GUI-based configuration editor for an LU6.2 client-server protocol.

Intermetrics **1983 – 1985**
Team Member on Defense Data Network IVV project. Evaluated BBN's test plans for network monitoring and control center; analyzed and reported on Internet gateway issues (e.g. congestion).

PUBLICATIONS

- Author "RFID & Authenticity of Goods" in *RFID: Applications, Security, and Privacy* (ed. Simson, Rosenberg) 2005.
- Contributor *SAML "Core" Specification* 2003 (https://www.oasis-open.org/committees/download.php/3406/oasis-sstc-saml-core-1.1.pdf)
- Co-author *Shibboleth Architecture Document* 2002 (now at https://www.switch.ch/fr/aai/docs/shibboleth/internet2/draft-internet2-shibboleth-arch-v05.pdf)
- Co-author *Java Security Reference Model* 1996 (now at https://dl.packetstormsecurity.net/papers/java/SRM.html)
- Co-author *Enhancing the DCE Authorization Model to Support Practical Delegation.* Proceedings of the Privacy and Security Research Group Workshop 1993.

LANGUAGES: C++, C, PowerShell, assembler, SQL, Perl, Java, etc.
PATENTS: *Object-Oriented Distributed Computing System (*co-holder) Patent # 5475817, 12/12/95.
AWARDS: Best Speaker for "RBAC: Supplement or Slim-Fast?" Network Applications Consortium Spring 2002
EDUCATION: Sc.B. (BS) in Electrical Engineering, Brown University
HOBBIES: Songwriting, juggling, improv acting, playwriting

SELECTED PAPERS, PRESENTATIONS, AND DIAGRAMS

o Diagrams for multiple projects along with project descriptions: https://acknowledgesoftware.com/diagrams.html

o CAR (consent) system architecture: The architecture I created for Internet2 to provide "consent" in federated identity systems. The CAR system is being developed at a major research university with an intent to deploy it university-wide in 2020.
https://docs.google.com/document/d/1rgzVa3hNv1e6yW_Wqds0t_3EswFYLv9-WaIbkeMnMoU/edit?usp=sharing

o "Stupid Security Decisions By Smart People": Bare bones slides for a rich talk on "systems thinking in security." I gave this talk at a Boston security conference in 2015, orienting the presentation to a mixed-level audience. The slides (here as a PDF) include simple but very useful sequence diagrams—and info on how to create them to aid in IT security analyses.
https://drive.google.com/file/d/1Y05v7Uinds_bNLaM6ETq7bouGrXqvcI7/view?usp=sharing

o Shibboleth Short play: An explication of the Shibboleth (aka SAML) identity federation protocol via an analogy with a museum visit. This fun and yet deep piece also explains HTTP redirects, cookies and other aspects of the HTTP protocol. I gave this talk to library IT personnel at Harvard who had little knowledge of these topics.
https://docs.google.com/document/d/1ijA1o7MSsyVbaWJtvUvrMH5IDkKmU3sX_0JUTVvMt9c/edit?usp=sharing

o RFID & Authenticity of Goods (book chapter): I wrote this paper for persons interested in RFID who potentially had no background in security. Because of that, I included a short but cogent tutorial on authentication. Overall, I employed a somewhat formal style in the writing as per book editor wish. (Note: I'm the copyright holder.)
https://drive.google.com/file/d/1vaeyo3LnPsPNeMVp8MFd9xJCoAKEznQc/view?usp=sharing