Marlena Erdos

marlena@acknowledgesoftware.com
(857) 308-6986

Key Strengths: Deep enterprise computing expertise; superior design, analysis, and problem-solving skills from abstract conceptualization down to fine technical details; excellent presentation and written communication skills; ability to explain complex technical concepts and issues to laypersons; ability to work well with people having diverse concerns (C-level executives, engineers, customers, marketeers, technical writers). Good coding skills too.

Areas of Expertise: Security and Privacy; Enterprise Identity Management; Federated Systems; Authorization systems; Policy languages for access control and privacy; RFID (radio-frequency identification); RBAC (role-based access control); PKI (digital signatures and certificates), software development, and the Common Criteria (a set of US government security standards).

Areas of Familiarity: REST APIs, Swagger, JSON, XML; LDAP and other naming/directory systems; crypto systems; communications systems; medical privacy (HIPAA); low-level networking tools, SQL databases.

Career Highlights: Co-creating the SAML & Shibboleth Federated Identity Management standards; publishing "RFID & Authenticity of Goods" in *RFID: Applications, Security, and Privacy* (ed. Simson, Rosenberg) 07/2005; co-authoring The Java Security Reference Model; breaking two "highly secure" commercial systems by finding design flaws—and then providing ways to secure the systems; co-creating Internet2's Consent-informed Attribute Release (CAR) system

Work Experience:

Internet2/InCommon/TIER – a consortium of US universities and colleges (March 2016 – present)

I architected a system for consent-informed release of user information. This system (called "CAR") integrates institutional policies with user policies, and provides for fine-grained control over even values of specific attributes. The system handles OAUTH-based resources as well as directory attributes.

- Created the system architecture of three interacting services
- Co-created the policy language at each of three services (with input from two co-creators)
- Created the REST API for the services using the Swagger tool
- Worked closely with the implementation lead and with product marketing
    - Provided significant input on and review of marketing materials

I also 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) (April 2012 – March 2016)

Working in HUIT's Identity & Access Management team:

- architected a new set of services for enhance person-finding and identifier assignment. A variant of this system is now deployed. I produced architecture diagrams, extensive text discussions, and sequence diagrams.
- designed a new tool for de-duplication system for identifiers, using input from SMEs (i.e. the admins who did the duplication using two old not-very-good tools).
- de-tangled an "undecipherable" body of code, database tables and stored procedures for Harvard Medical School.
- served as Federation Manager for Harvard to Internet2, a consortium of US universities and colleges.
- deployed Harvard's first Shibboleth Identity Provider (IdP) and Service Provider
- wrote secure code that integrated the IdP with Harvard's legacy authentication system

- wrote code to ensure compliance with vendor rules on authorization
- provided input on Internet2 standards for person schema.
- created and presented a number of talks on identity federation, authentication in the web, and communications protocols to various groups within Harvard IT, including a play on sessions and cookies.
- investigated HUIT's authentication systems and related infrastructure. As part of this effort, I
  - uncovered a number of security vulnerabilities and came up with initial ideas on how to address them.
  - communicated effectively to IT leadership on both the vulnerabilities that I discovered and that others have raised.
  - improved the decision procedure (i.e. "go forward or rollback") used during upgrade of an aging infrastructure component.
  - worked with others to improve the documentation of the end to end flow of information in authentication transactions. My background in communications systems as well as "security" allows me to help with network-level flows and issues (e.g. ip address translation and routing) as well as application-level flows.

Ozmott (Summer 2011)
Ozmott is creating a mobile phone app with a social networking component. Consulting to their CTO, I did the following:

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

Resilient Networks Winter (Winter 2010)
Provided short-term 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) (Fall 2009)
HMS researchers need to give scientists from other institutions access (albeit limited access) to HMS resources. Such collaboration is not only scientifically useful, it's also required by certain grants. The process of provisioning foreign users was staff-intensive and slow. Additionally, the process of on-going authentication of foreign users had some "issues." Working with the HMS IT team, I created a solution for automated provisioning of new foreign users and on-going authentication and authorization of these users. My solution employs the Shibboleth/SAML federation standard in a novel way.

IBM/DataPower (Feb 2005—Oct 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 the focal point for CC rule interpretation, and created/modified the CC-specified documents that serve as the basis for the evaluation.

Identity Associates (Fall 2005 & Spring 2006)
Fall 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. Also, found (and provided a solution for) a major security hole in the client's current product.

Spring 2006: Compared/contrasted/analyzed existing web service federation standards (Liberty and a sub-set of the WS documents) for an internal project.

Bank of America/Axis Technology LLC (Nov 2004—Jan 2005)
Technical lead on Entitlements & Authorization project in the Information Delivery and Services group within the Wealth and Investment Management group.

- Created a requirements document laying out the 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 high net worth bankers and their clients.
- Performed data analysis/reduction transforming twenty 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 within both IBM and its Tivoli subsidiary.

RFID: Served as one of two experts on privacy and security from Tivoli, consulting to the rest of IBM.
- Designed a solution for the security "bootstrapping" problem for turn-key RFID readers installed in retail stores.
- Analyzed RFID-based loss prevention schemes.
- Instigated and furthered a change to IBM's privacy stance on RFID deployment.

Federation: Seminal contributor to Federation standards.
- Contributor to the initial SAML specification.
- Creator of the privacy architecture for Internet2's Shibboleth system.
- Co-designer of Shibboleth's federated computing architecture.
- Initiator and co-author of the Shibboleth architecture document.

Enterprise Identity Management: Co-creator of secure identity mapping system for heterogeneous enterprises.

Privacy: Served as the liaison from the security architecture team to IBM's Privacy Manager team.
- Analyzed and reviewed designs for a next-generation privacy system.
- Reviewed/critiqued next-generation privacy policy language (EPAL).
- Created and gave presentations on privacy both internally and externally.

Miscellaneous:
- Analyzed a variety of third-party security systems (for IBM) e.g. CoreStreet and ConnecTerra's CDAP.
- Voted Best Speaker for my presentation "RBAC: Supplement or Slim-Fast" at the Network Applications Consortium Spring 2002 meeting.

Tandem (4/96—8/97)
Consultant to team developing an electronic commerce application.
- Provided architectural guidance related to extensions to an X.509-compliant public key infrastructure system.
- Enhanced code base (in C++), providing for directory-independent cross-certification and handling of foreign users.

JavaSoft (Sun Microsystems) (8/96—10/96)
Consultant to JavaSoft Development Team. I performed a security analysis of the Java Virtual Machine (JVM) and Java Development Kit (JDK). I co-wrote ***The Java Security Reference Model,*** a plain-language discussion of security in Java.

Shiva Corporation (4/96—8/96)
Worked with management, marketing, and developers on Shiva's on-going security plans.

Banyan Systems (11/93—12/95)
Security Lead. I served as Banyan's security expert for all internal and external issues concerning authentication, authorization, digital signature, C2/B1, etc. I provided expertise on other enterprise computing issues (X.500, RPC, communications, licensing).

- Proposed/Architected Public-key based authentication system.
- Enhanced Banyan's directory and security system software (in C).
- Created/delivered presentations to customers and analysts.
- Solved hot customer and third-party system software problems (in C and assembler).
- Advised management on directory, security, and interoperability strategies.
- Evaluated third-party products and contracts for marketing and management.

Fidelity Investments (12/92—2/93)
Consultant to Technical Architecture team. Adviser to team developing enterprise-wide computing strategy for Fidelity. Topics included security (Kerberos), transaction systems, naming, and interoperability.

HP/Apollo (3/85—11/92)
Senior Team Member on Distributed NewWave (DNW) (1/90 - 11/92). DNW was an RPC-based platform for writing distributed object-based applications. DNW was HP's basis for OMG Object Request Broker (CORBA) compliance. I co-designed a distributed object (discretionary) security system. I designed/implemented object activation and message handling (in C++).

Team member on Passwd Etc (4/88 - 1/90). Passwd Etc was a distributed user account system. It consisted of replicated, multi-threaded servers containing user account information (e.g. encrypted passwords, home directories) and client software. Passwd Etc was part of OSF's distributed computing environment (DCE). I wrote thread-safe database access layer (in C). I coded an enhanced update propagation scheme using the thread-safe access routines.

Team Member on LU6.2 (6/86 - 4/88). LU6.2 is an IBM client-server communications protocol. I implemented remote invocation of LU6.2 application programs. I designed and implemented UIMS-based configuration editor.

Intermetrics Inc. (8/83—2/85)
Team Member on Defense Data Network IVV project. I evaluated BBN's test plans for network monitoring and control center; Analyzed and reported on Internet gateway issues (e.g. congestion).

Languages: C++, C, assembler, Pascal. Some knowledge of Java, SQL, Python, Perl, HTML, CSS
Publications:
- author "RFID & Authenticity of Goods" in *RFID: Applications, Security, and Privacy* (ed. Simson, Rosenberg) 07/2005.
- contributor *SAML "Core" Specification* xml.coverpages.org/SSTC-SAMLCoreV20Draft17-7750.pdf
- co-author *Shibboleth Architecture Document* shibboleth.internet2.edu/docs/ draft-internet2-shibboleth-arch-v05.pdf 05/2003.
- co-author *Java Security Reference Model* http://java.sun.com/security/SRM.html 11/1996.
- co-author *Enhancing the DCE Authorization Model to Support Practical Delegation.* Proceedings of the Privacy and Security Research Group Workshop, 2/1993.

Patents: *Object-Oriented Distributed Computing System (*co-holder) Patent # 5475817, 12/12/95.
Education: Sc.B. (BS) in Electrical Engineering, Brown University 6/83.