

Arcot User & Technology Conference 2007

Presentations and Case Study Summaries

Thursday, April 19, 2007
Morning Sessions

Strategy and Vision

The Authentication Landscape

Ram Varadarajan

Arcot Systems
President and CEO

Ram discussed that Arcot was founded on the principle of solving the identity problem in a new way - without the expense and inconvenience of hardware deployments. The authentication landscape has expanded beyond authentication to include value added applications such as statement delivery, and digital signing applications. Ram enumerated the virtues of an ideal solution and concluded that Arcot is truly a "one-of-one" company combining software technology and ubiquitous distribution on the desktop via Adobe Acrobat and Reader and the ArcotID Flash Client. He also discussed Arcot's strategic relationships with Microsoft, IBM, and Oracle.

Fraud Trends and Solutions

Avivah Litan

Gartner
VP and Distinguished Analyst

As the keynote speaker, Avivah covered common fraud attack vectors along with the key issues and trends in consumer identity fraud with potential solutions to these problems. She commented about the loosely organized criminal rings that are the source of the majority of attacks. High income users are targeted more, respond less, but lose more in value. This used to be absorbed by the banks, but recent surveys show that the losses are shifting to consumers.

Avivah recommended a multi-pronged, multi-layered security approach as the best way to solve the problem. Banks need a bifurcated authentication strategy – one piece for consumer confidence, one for fraud prevention. She concludes that a software solution provides the right balance of cost, convenience and security.

Identity Management: The Big Picture

Kamal Bherwani

New York City Department of Health & Mental Hygiene
Associate Commissioner & CIO

In this talk Kamal discussed his vision for providing online services to the citizens of NYC and the benefits of Identity Management. The NYC DOHMH has 6,500 staff in 50 locations with a budget of \$1.5 Billion. They provide services including vital statistics, inspections of restaurants, day care, emergency response, health clinics, and laboratory analysis just to name a few. They are innovators with many nationwide firsts.

The IT goals are to save lives, save money, increase customer service and increase productivity in the vast network of services provided by the DOHMH. Identity management is a necessity to help achieve those goals. Kamal outlined 4 themes: simplified IT landscape, IT governance ("doing the right thing, then doing the thing right"), impenetrable security, and business intelligence. He also talked about how they will use different types of authentication technologies, including the Arcot solutions.

A Consumer Risk Management Approach to Authentication

Stan Szwalbenest

JPMorgan Chase
Remote Channel Risk Director

Stan remarked on how trends in remote channels have changed consumer behavior over the last 3-5 years. Data aggregation by criminal groups has become a critical challenge to the banks operating model. The ramifications of data abuse include criminals stockpiling unprecedented quantities of transaction account data, phishing and weak authentication methods. Authentication at channel, product, and line of business silos should move to a customer centric view. The cornerstones of customer centric authentication are enrollment, aberrant transaction monitoring, and confirmation processes - which cross lines of business and channels. The biggest challenge in this model is customer acceptance with enrollment being the key to a successful authentication strategy. Stan closed with a summary of how they are using Arcot technology and a discussion around the long term strategy option of using a single credential for online banking, POS, signed message delivery and transaction signing.

Thursday, April 19, 2007
Afternoon Sessions

Technology & Consumer Authentication

Mad About Identity

Jim Reno

Arcot Systems
CTO

Jim asked the question "who am I?" and discussed what identity means in today's world. He proposed that identity can be defined by a series of "links". He showed the progression of a person's identity from birth and tracked the identity links as you age. For instance, your birth certificate links to your SSN, which in turn links to your mailing address, cell phone, driver's license, bank account and credit card, etc. And, all of these are in turn linked to each other. So what's the big deal? The links are prime targets for identity attacks. Once a link is captured, it can be used to compromise other links, making the spread of an "identity virus" more sinister. Because you also have links to other people, the virus can spread to them. This obviates the need for a strong authentication solution that can be scaled to reach and protect everyone.

Arcot User & Technology Conference 2007 Presentations and Case Study Summaries

Adobe's Identity and Security Solutions for the Desktop

John Landwehr

Adobe
Director of Security Solutions

John reviewed the business benefits of moving paper transactions online. He discussed Adobe's Information Assurance Offerings and their support of digital signatures. He provided a definition for security which translates into a focus of confidentiality, authorization, and accountability for information rights management solutions and authenticity and integrity with digital signatures. Adobe's end-goal is to support regulation, IP protection, customer privacy, and generally make electronic transactions more secure than paper. An example of this strategy is embedding Arcot authentication and signing solutions into Adobe Acrobat and Adobe Reader to make it easier for consumers to authenticate and sign using roaming IDs. He demonstrated how digital signing can be as familiar and easy as signing a form with a wet signature while providing additional non-repudiation benefits and cost savings.

User-Centric Digital Identity

Mike Jones

Microsoft
Director of Identity Partnerships

Mike provided information on User-Centric Digital Identity, Information Cards, and Windows CardSpace and how they enable people to use strong digital cryptography in their online lives as easily and naturally as they use the cards in their wallet in the physical world today. He discussed the laws of identity which can be found on www.identityblog.com. He emphasized that focusing on human integration is required for success. Those past implementations that only looked at the technical aspects of identity fell short. People require a consistent experience across contexts online. Windows CardSpace uses familiar credit card symbols to make the digital identity experience easy for consumers. He gave a demo and showed Windows CardSpace working with the ArcotID and commented that Arcot was the first vendor to demonstrate Windows CardSpace integration. The audience was glad to hear that Windows CardSpace uses open protocols and integrates with other platforms.

Is your desktop ready to be an identity agent?

Panel Debate

Moderator:
Avivah Litan, Gartner

Panelists:
Mike Jones, Microsoft
John Landwehr, Adobe
Stan Szwalbenest, JPMorgan Chase
Jim Reno, Arcot Systems

Avivah asked very pointed questions of the panel and a lively discussion ensued around identity and authentication for consumers. The questions included: What is being done to facilitate authentication and user identity at the desktop? How can FIs provide strong authentication while ensuring minimal disruption to consumers. What role does the desktop play? Will mobile banking become a reality? What are the desktop vendors doing to solve the problem? What does the banking community require to ensure a successful implementation? Will the consumer accept it? What consumer trends will translate to the enterprise environment?

Verified by Visa Program Update

Gerry Sweeney

Visa USA
Senior Vice President, Cross Platform Products

Gerry outlined Visa's security and authentication strategy – Secure the payment environment; Monitor, identify and prevent fraud; Manage the impact of fraud; Maintain trust in Visa payments; and Build Industry-wide partnerships. He reviewed the Verified by Visa statistics and talked about the need for a more dynamic environment especially with respect to enrollment.

MasterCard SecureCode Update

Carl Stefanelli

MasterCard
Vice President e-Business & Emerging
Technologies Global Development

Carl shared the opportunities available for members of the MasterCard SecureCode program. He reviewed the impact of online fraud from the merchant perspective and highlighted lost sales opportunities. He discussed the Chip Authentication Program (CAP) integration with SecureCode and how it also applies to Card Not Present and Mail Order/Telephone Order transactions. He closed with a discussion of consumer security concerns, and ecommerce trends worldwide.

Reducing Fraud in 3-D Secure Programs with Arcot Risk-Based Authentication

Sanjay Vyas

Arcot Systems
VP Worldwide Services

Sanjay educated the audience on how the 3-D Secure program and protocol works. He pointed out areas that are subject to a high risk of fraud, in particular, activation during shopping (ADS) and identified the fraud characteristics involved. Sanjay showed how Arcot's RiskFort solution prevents these identified areas of fraudulent behavior including unauthenticated and authenticated transaction fraud, self-enrollment fraud and unauthorized administrator access. He showed a case study where fraud was significantly reduced using RiskFort while not impacting valid customer shopping.

Arcot User & Technology Conference 2007

Presentations and Case Study Summaries

Friday, April 20, 2007

Customer Case Studies & Identity Management Solutions

The Arcot Product Vision and Roadmap

Doc Vaidhyanathan

Arcot Systems
VP Product Management

In this session, Doc revealed Arcot's product strategy and vision for authentication. Arcot solved the first problem in authentication which is to provide a good alternative to hardware and that now we have solved the second obstacle to strong consumer authentication which is how to get it to the consumer's desktop. He reviewed Arcot's "single client" vision of embedding Arcot technology into software that is ubiquitous at the client. He showed 2 ways that Arcot has already solved the client problem with a flash client and embedding the Arcot authentication and signing technology into Adobe Acrobat and Adobe Reader making it invisible to the consumer. He also discussed Arcot authentication as part of the identity management stack integrated with IBM, Oracle, and CA.

Identity Federation For Real -- What's Making It Happen

Jim Gross

Wells Fargo Bank
Sr. Vice President, WellsSecure

Jim started his presentation by asking the audience how assurance of identity is determined. How do you verify someone's identity in the real world? Looks can be deceiving. He contrasted this with digital identities and defined the Wells Fargo WellsSecure Identity Assurance Services in terms of Trust, Simplicity and Reasonable price. Jim discussed the meaning of "Federated Identity" and the value drivers that are converging to make it a reality. He talked about generation II of federated identity and gave a live example of how the GSA Federal Acquisition Service uses the WellsSecure Identity Assurance Service.

Enterprise PKI: The Identity Factor

Mike Lavoie

Pfizer Inc.
Manager, Digital Certificate Services

Mike described the Identity Services at Pfizer. He talked about implementing PKI and the related cost and complexity. However, the potential savings in paper, processes and cost are enormous. Getting a typical drug to market involves 1-2 tractor loads of paper at a staggering cost of \$25-\$135 per sheet! Using Pfizer medium assurance certificates and SAFE medium assurance certificates, Pfizer implemented digital signatures in their workflow processes for both internal employees and external contractors and third parties. He reviewed how Arcot customized its RegFort product to Pfizer specifications and he showed the flow of enrolling and using the Pfizer Certificate Management System.

Securing Business for Today and Tomorrow

Rohit Gupta

Oracle Corporation
Director, Director, Identity Management and Security Products

Rohit covered the evolution of fraud from amateur hackers to organized crime and the current state of security in the enterprise. He outlined the ways that Identity Management can solve enterprise security problems by 1) Establishing the Enterprise Identity, 2) Enforcing strong and granular security policies, 3) Automating security related processes, and 4) Defining an audit and control framework. Oracle's Identity and Access Management Solutions provide this identity management framework for the enterprise. He also discussed Oracle's partner EcoSystem and Arcot's multi-factor authentication integration with Oracle Access Manager.

IBM Integrated Identity Management Solution

Venkat Raghavan

IBM Tivoli Software
Director Information, Storage and Security Market Management

Venkat described the context for identity management in the enterprise in terms of people, information, application and services. What can users access? Who can access and modify data? How can I securely connect my partners and suppliers? Who made changes? He stated that Identity Management must automate the process of creating value and addressing IT governance & compliance through effectively and efficiently managing users (and entities) and their access to IT resources and being able to prove what they're doing with that access. He discussed the logical elements of an identity management system and showed how IBM Tivoli Solutions provide integrated identity management in the enterprise.

Identity management is the drawbridge to your corporate secrets. How do you keep the trolls at bay?

Panel Debate

Moderator:
Keith Goldstein

Panelists:

Jim Gross , Wells Fargo
Rohit Gupta, Oracle
Venkat Raghavan, IBM Tivoli Software
Doc Vaidhyanathan, Arcot Systems

Keith challenged the panel to discuss how enterprise organizations deploy multi-layered identity management solutions now while anticipating the evolving fraud environment. The panel discussed the drivers behind identity management and took questions from the audience on their implementations and recommendations. The also debated what vendors are doing to help companies deploy identity management and strong authentication solutions? What are the long-term benefits? The panel ended on a more strategic discussion around the ultimate vision for identity management.