

IS THAT REALLY YOU?
PROVE IT!

Matt and Dan, Dan and Matt, Those Fookers!

Agenda

slide 2

- Who are we?
- Web Application Security Problems
- Business Drivers
- Solution Overview
- DEMO

Who are we?

slide 3

- Matt Topper, matt@matttopper.com
- Dan Norris, dannorris@dannorris.com

Web Application Vulnerabilities

slide 4

- The Classics
 - ▣ SQL Injection
 - ▣ Unvalidated Input
 - ▣ Broken Access Controls
 - ▣ Cross Site Scripting
 - ▣ Improper Error Handling
 - ▣ Denial of Service
- The Newbies (OK, not completely new)
 - ▣ Phishing
 - ▣ Key Logging
 - ▣ Pharming

Common Problems



A Few Headlines

slide 6

- “1 1.9 million Americans clicked on a phishing e-mail in 2005”
- “Gartner estimates that the total financial losses attributable to phishing will total \$2.8 bln in 2006”
- “Phishing and key-logging Trojans cost UK banks £1 2m”
- “Swedish bank hit by 'biggest ever' online heist”
“Swedish Bank loses \$1 Million through Russian hacker”

MillerSmiles.co.uk

slide 7

- rss feeds
- archives
- news
- submit scam
- articles
- f.a.q.
- forum
- about us
- contact us
- links

Ads by Google

Online Checking Account

Looking for Checking Account info? See our Bank Directory and Compare.
www.CheckingsAccount.c

Online Checking Account

Free Checks, online Bill Pay & more Bank Account Deals, Online Banking

home

298794 scams in our archive

Welcome to MillerSmiles.co.uk! We are one of the internet's leading anti-phishing sites, maintaining a massive archive of phishing and identity theft email scams.

We are currently storing all phishing scam reports with our HoneyTrap database which is now available for commercial license. This database currently holds 298794 reports.

Our 419 scams, lottery scams and growing spam email database is now also collecting scams from our HoneyTrap network.

We also run a news service (headlines below) which brings you all the latest headlines from the world of fraudulent emails and phishing.

Latest Phishing News Headlines:

- MillerSmiles cited in Vista book
- Yahoo phishing flaw revealed
- Anti-Phishing Browsers Not Working
- Keylogging Website Trend
- Facebook Phishing
- Phishing Trend Continues
- Tax Phishing Scams
- Christmas phishing threats loom
- Phishing - A Tougher Art
- Google fixes security flaw

Tuesday 9th October 2007

24 recent phishing scams

E*TRADE 9th October 2007
Please Read

Nationwide 9th October 2007
Unauthorized Transactions on your Internet Banking....

Wal-Mart 9th October 2007
Please confirm your information on our database

NatWest Bank 9th October 2007
Customer Mail: Your Account In Natwest OnLine Banking

Nationwide 9th October 2007
Important Banking Mail - Nationwide Building Society.

Egg Bank 9th October 2007
Egg Bank Online® : Important Security Information

Wachovia Bank 8th October 2007
Wachovia Bank Account : Update Request 29736AX

Natwest 8th October 2007
National Westminster Plc: Please Submit Your Banking Details

Nationwide 9th October 2007

Experiments at Indiana University

slide 8

- Reconstructed the social network by crawling sites like Facebook, MySpace, LinkedIn and Friendster
- Sent 921 Indiana University students a spoofed email that appeared to come from their friend
- Email redirected to a spoofed site inviting the user to enter his/her secure university credentials
 - ▣ Domain name clearly distinct from indiana.edu
- 72% of students entered their real credentials into the spoofed site
 - ▣ Males more likely to do this if email is from a female

Business Drivers for new kind of Authentication

slide 9

- 10,000,000 people - almost 5% of the US population - were victims of identity fraud in the last year * *[Not just theft, but actual fraud]*
- Total losses of \$53B * *[real \$ losses by both consumers and businesses]*
- Many consumers limit their use of internet-based transactions due to fear
- Organizations need to ...
 - ▣ Secure the site, transactions and sensitive information
 - ▣ Reduce the fraud risk of every transaction
 - ▣ Reduce the fear
 - ▣ Win customers away from competitors * US Federal Trade Commission

Challenges

slide 10

- ❑ IP and passwords are easy to steal or capture (keyboard logging)
- ❑ Can't demand that consumers change their passwords frequently – stay the same for years
- ❑ Tokens and smartcards for strong authentication are ...
 - ❑ Expensive to buy
 - ❑ Difficult to deploy to users
 - ❑ Easy to lose
 - ❑ Not flexible
 - ❑ Not feasible for consumer user populations that are large or have a lot of churn
 - ❑ Hated by doctors and other roaming users or kiosk users

Challenges (cont'd)

slide 11

- Biometrics have many of the same issues
- Typical IdM solutions do not help much with ...
 - ▣ Fraud after an identity theft happens
 - ▣ Spotting errant behavior of a user
 - ▣ Phishing and pharming
 - ▣ Giving peace of mind to an internet banking consumer

Bharosa

slide 12

- Hindi word for “trust”
- Founded 2003
- Created a new way to do “strong authentication” and to do real-time risk assessment of a user’s session
- Competed successfully with the traditional vendors of strong authentication like RSA and Entrust
- Proven in the marketplace, with 25,000,000 users

Bharosa - Acquisition

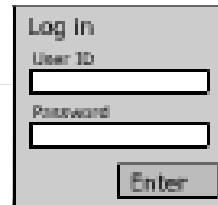
slide 13

- ❑ Acquisition announced July 2007
- ❑ Acquisition closed and product GA on Oct 1, 2007
- ❑ Product renamed “Oracle Adaptive Access Manager”
- ❑ Available as a normal Oracle product -- usual pricing structure, discounts, channels, etc.
- ❑ This will be a very popular addition to the IdM line:
 - ❑ Huge need
 - ❑ Unique approach
 - ❑ Short sales cycle
 - ❑ Easy to POC
 - ❑ Easy to deploy

Standard Access

Before:

Typical security



A simple login form with a grey background. It contains the following elements:

- The text "Log In" at the top.
- A label "User ID" above a text input field.
- A label "Password" above another text input field.
- An "Enter" button at the bottom right.

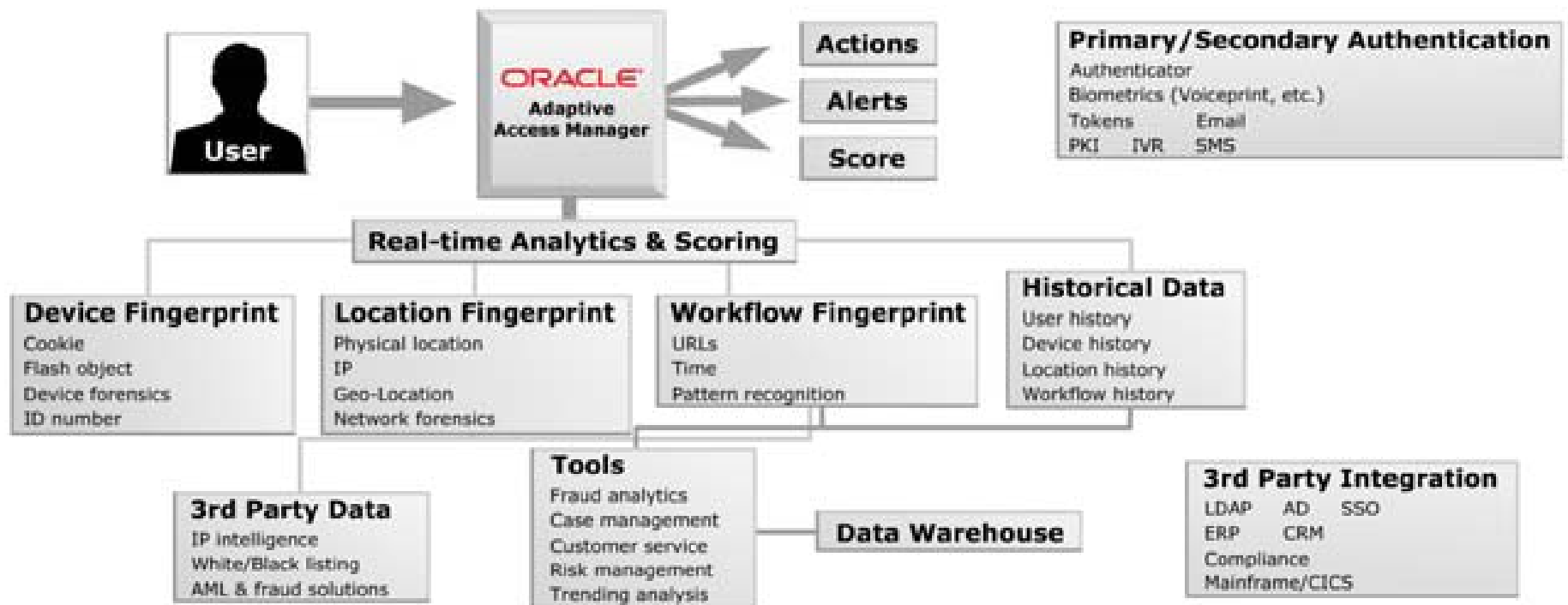
A horizontal line extends from the left side of the form across the slide.

Oracle Adaptive Access Manager

slide 15

After:

Advanced real-time risk assessment combines many factors:

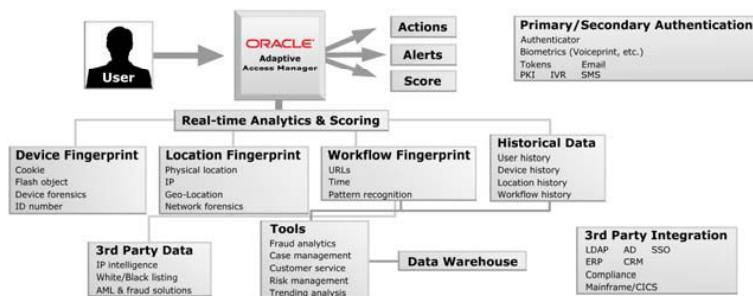


Oracle Adaptive Access Manager

“Adaptive Risk Manager”

slide 16

- This user usually connects either over a company LAN or his home DSL ... why is he now connecting from Russia?
- The CFO is trying to reach the financials app, but from a device never seen before.
- This user is coming from a known blacklist site.
- This customer has been doing some things that are atypical for her, and now wants to do a large transfer.



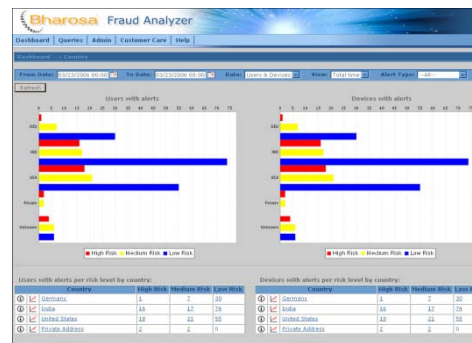
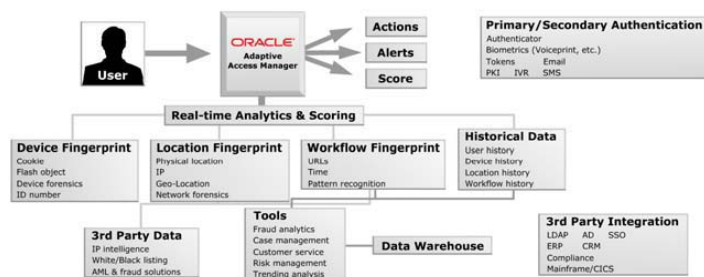
Compares “virtual fingerprints” and actions to known fraud models

Oracle Adaptive Access Manager

Real-Time Risk Assessment Capabilities

slide 17

- Learns a profile of each user's normal workflows
- Monitors the session in real time and continually scores the risk
- Evaluates “fingerprint” and workflow information against models and rules for “gated” security for each attempted transaction
- In case of red flags ...
 - can block access
 - can prompt the user with additional authentication steps
 - Can notify an administrator of potential fraudulent activity -- during the session – via powerful real-time event dashboards
- Audit data captured for offline forensic analysis



The screenshot shows the Bharosa Fraud Analyzer dashboard with a table of monitoring records. The table has columns for Session ID, Device ID, Login ID, Auth Status, Login Time, Device ID, Session ID, IP Address, Client Type, and Alerts. The table is filtered to show records for the date 11/11/2010.

Session ID	Device ID	Login ID	Auth Status	Login Time	Device ID	Session ID	IP Address	Client Type	Alerts
11001	128	128	Success	11/11/2010 21:08:00	128	11001	202.138.208.221	Normal	
11002	128	128	Success	11/11/2010 21:08:00	128	11002	202.138.208.221	Normal	
11003	128	128	Success	11/11/2010 21:08:00	128	11003	202.138.208.221	Normal	
11004	128	128	Success	11/11/2010 21:08:00	128	11004	202.138.208.221	Normal	
11005	128	128	Success	11/11/2010 21:08:00	128	11005	202.138.208.221	Normal	
11006	128	128	Success	11/11/2010 21:08:00	128	11006	202.138.208.221	Normal	
11007	128	128	Success	11/11/2010 21:08:00	128	11007	202.138.208.221	Normal	
11008	128	128	Success	11/11/2010 21:08:00	128	11008	202.138.208.221	Normal	
11009	128	128	Success	11/11/2010 21:08:00	128	11009	202.138.208.221	Normal	
11010	128	128	Success	11/11/2010 21:08:00	128	11010	202.138.208.221	Normal	
11011	128	128	Success	11/11/2010 21:08:00	128	11011	202.138.208.221	Normal	
11012	128	128	Success	11/11/2010 21:08:00	128	11012	202.138.208.221	Normal	
11013	128	128	Success	11/11/2010 21:08:00	128	11013	202.138.208.221	Normal	
11014	128	128	Success	11/11/2010 21:08:00	128	11014	202.138.208.221	Normal	
11015	128	128	Success	11/11/2010 21:08:00	128	11015	202.138.208.221	Normal	
11016	128	128	Success	11/11/2010 21:08:00	128	11016	202.138.208.221	Normal	
11017	128	128	Success	11/11/2010 21:08:00	128	11017	202.138.208.221	Normal	
11018	128	128	Success	11/11/2010 21:08:00	128	11018	202.138.208.221	Normal	
11019	128	128	Success	11/11/2010 21:08:00	128	11019	202.138.208.221	Normal	
11020	128	128	Success	11/11/2010 21:08:00	128	11020	202.138.208.221	Normal	

Oracle Adaptive Access Manager

“Adaptive Strong Authentication” via Flexible Log-In Tools

slide 18



- A virtual authenticator device is shown on the user's browser screen
- Server-driven -- no software is downloaded
- Several from which to choose, depending on the needs of the organization
- User clicks with the mouse to enter ID, password or other info
- Can be simple (challenge questions) or complex
- These can be used in addition to other forms of strong authentication

Oracle Adaptive Access Manager

Graphical Entry of ID/Password

slide 19

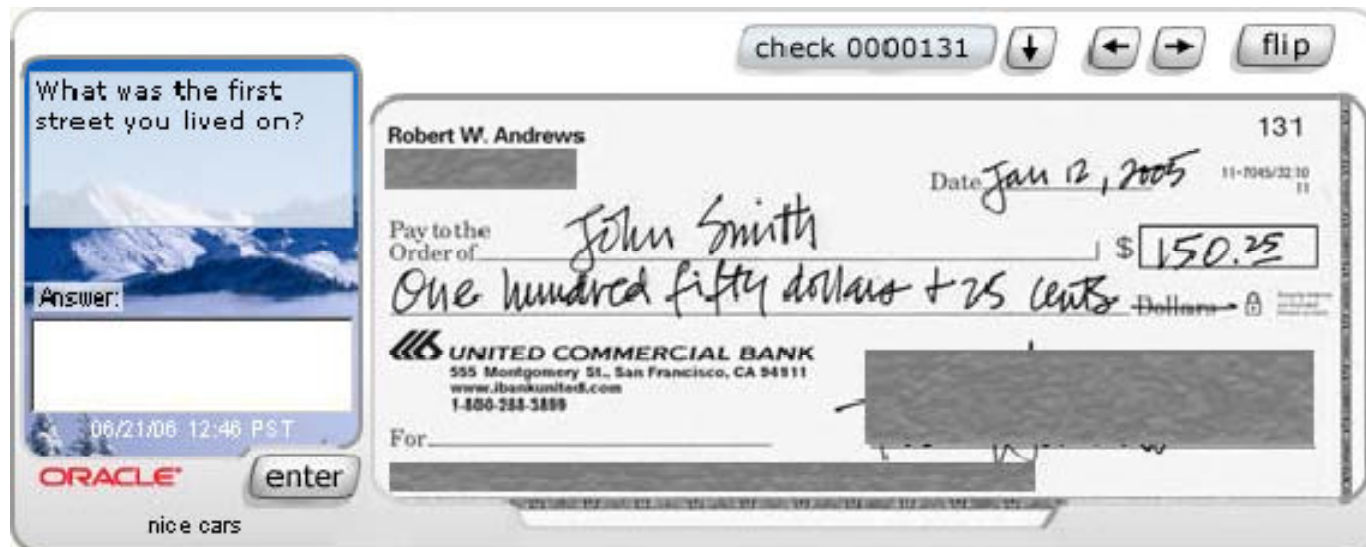


- The virtual authenticator device presents a virtual keyboard, where the user clicks on the characters
- Password is encrypted at moment of entry – never stored or transmitted in clear text
- Prevents password theft via trojans and keyboard logging – even after a device has been compromised !
- Prevents theft via man-in-the-middle attack

Oracle Adaptive Access Manager

Gated Security

slide 20



- Can present extra challenges to get to checks or other sensitive images
- CheckPad or DocPad
- Meets "Check21" legislation requirements

Oracle Adaptive Access Manager

Chose the Degree of Complexity

slide 21

The "Slider"



- For the most mission-critical applications or user types
- Present a virtual authenticator device that acts as a visual combination lock, with the users behavior serving as a factor
- The placement of the device changes each time it is presented to prevent mouse logging and screen scaping
- Size and complexity of the characters and images prevents over-the-shoulder snooping or camera snooping

Oracle Adaptive Access Manager

Two-Factor? OAM Offers Lots of Factors

slide 22

Classes of factors:

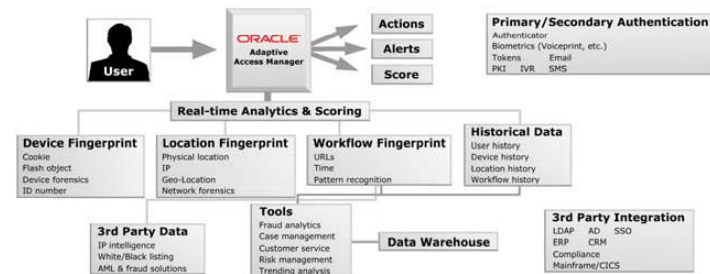
- Factor 1: something the user knows (password)
- Factor 2: something the user has (ATM card)
- Factor 3: something the user is (biometrics)

Enables compliance with key regulations:
FFIEC, HIPAA, PCI



OAM adds more factors:

- User knows and enters ID, password, other codes on virtual authenticator devices; user can answer challenge questions
- User has the virtual fingerprints of his device(s), and of his network(s), including speeds, routes, etc.
- User is the way he behaves – his workflows



Oracle Adaptive Access Manager

Also authenticates the web site to the User

slide 23



- Upon first log-in, the user selects a picture and enters a phrase
- At subsequent log-ins, the virtual authenticator devices shows the same picture and the user's phrase back to the user
- The user recognizes that this is the same home banking web site she usually uses, and feels more secure
- This mutual authentication prevents fraud via redirection (phishing and pharming)

Some customers have bought OAAM just for this mutual authentication feature



Demonstration

Save the Date!

slide 25



April 13 – 17, 2008

Colorado Convention Center

Denver, Colorado

Become a Complete Oracle Technology and Database Professional

slide 26

- **Join the IOUG online at www.ioug.org and get immediate access to:**
 - Member Discounts and Special Offers
 - SELECT Journal
 - Library of Oracle Knowledge (LoOK)
 - Member Directory
 - Special Interest Groups
 - Discussion Forums:
 - Access to Local and Regional Users Groups:
 - 5 Minute Briefing: Oracle
 - Volunteer Opportunities



IS THAT REALLY YOU?
PROVE IT!

Matt and Dan, Dan and Matt, Those Fookers!