piocon

EXPLOITING TECHNOLOGY for your advantage.

Oracle Adaptive Access Manager: What, Why, How

Dan Norris

dnorris@piocon.com

http://www.dannorris.com/

Thanks to Matt Topper for his help preparing this presentation.

Agenda

- Who is Dan?
- Web Application Security Problems
- Business Drivers
- Solution Overview
- Admin Console Review

Who is Dan?

- Virgo
- Scuba Diver (PADI Advanced OW, Nitrox)
- Over 21, under 35
- Oracle DBA & UNIX Admin background
- Certifiable: OCM, ACE Director, RHCE
- Consultant, mostly fixing things that are broken
- Active community participant: RAC SIG, SIG Council, DBA Track Manager, blogger, tweeter
- ESA Practice Manager at Piocon Technologies

Web Application Vulnerabilities

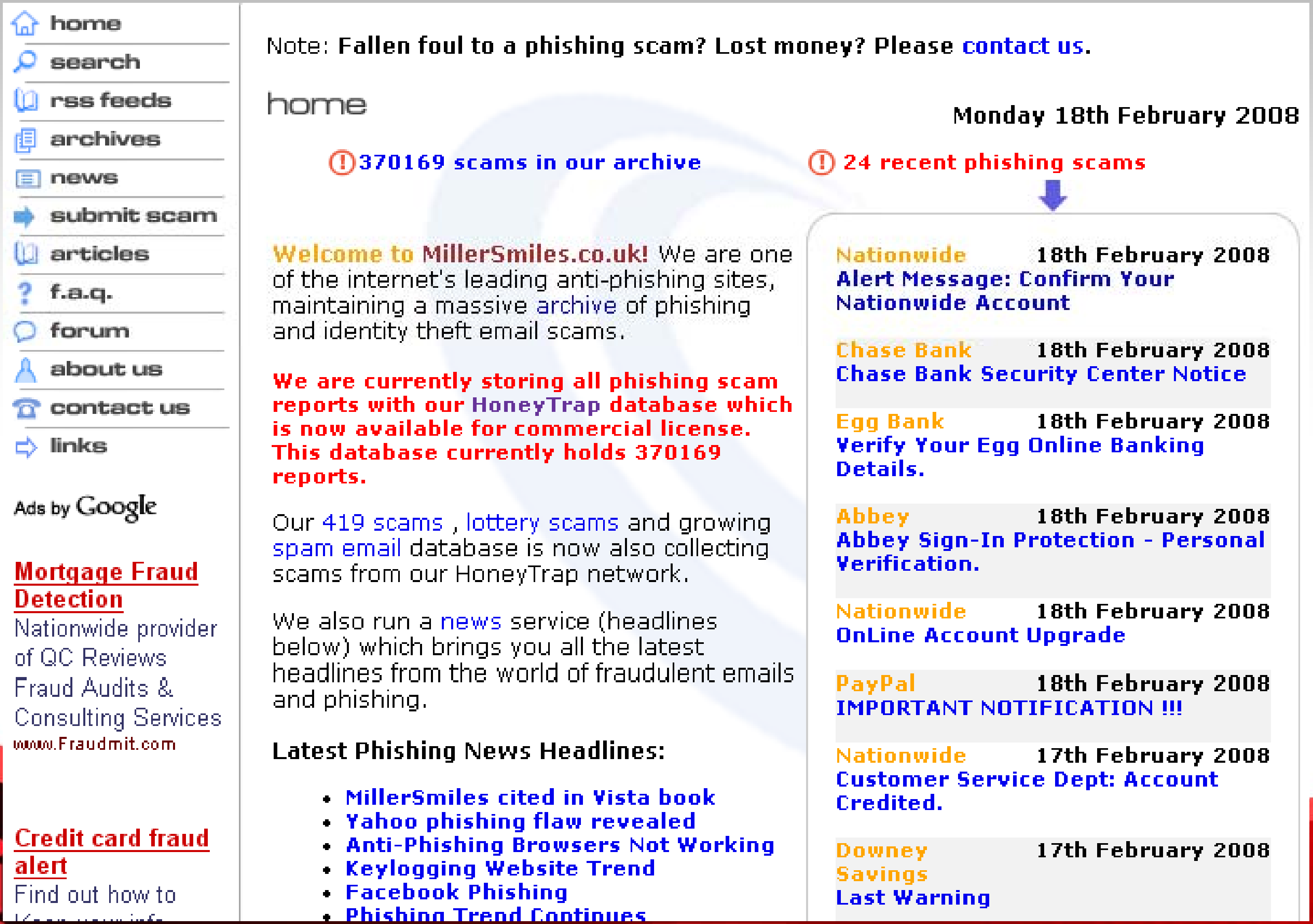
- The Classics
  - SQL Injection
  - Unvalidated Input
  - Broken Access Controls
  - Cross Site Scripting
  - Improper Error Handling
  - Denial of Service
- The Newbies (OK, not completely new)
  - Phishing
  - Key Logging
  - Pharming

Common Problems

A Few Headlines

- *“11.9 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 £12m”*
- *“Swedish bank hit by 'biggest ever' online heist”*
- *“Swedish Bank loses $1 Million through Russian hacker”*

MillerSmiles.co.uk



Note: **Fallen foul to a phishing scam? Lost money? Please contact us.**

home

Monday 18th February 2008

370169 scams in our archive

24 recent phishing scams

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 370169 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**

Nationwide 18th February 2008
Alert Message: Confirm Your Nationwide Account

Chase Bank 18th February 2008
Chase Bank Security Center Notice

Egg Bank 18th February 2008
Verify Your Egg Online Banking Details.

Abbey 18th February 2008
Abbey Sign-In Protection - Personal Verification.

Nationwide 18th February 2008
OnLine Account Upgrade

PayPal 18th February 2008
IMPORTANT NOTIFICATION !!!

Nationwide 17th February 2008
Customer Service Dept: Account Credited.

Downey Savings 17th February 2008
Last Warning

Experiments at Indiana University

- 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

- 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

- 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)

- 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

- 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

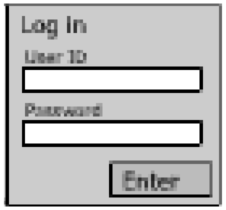
Bharosa - Acquisition

- 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:

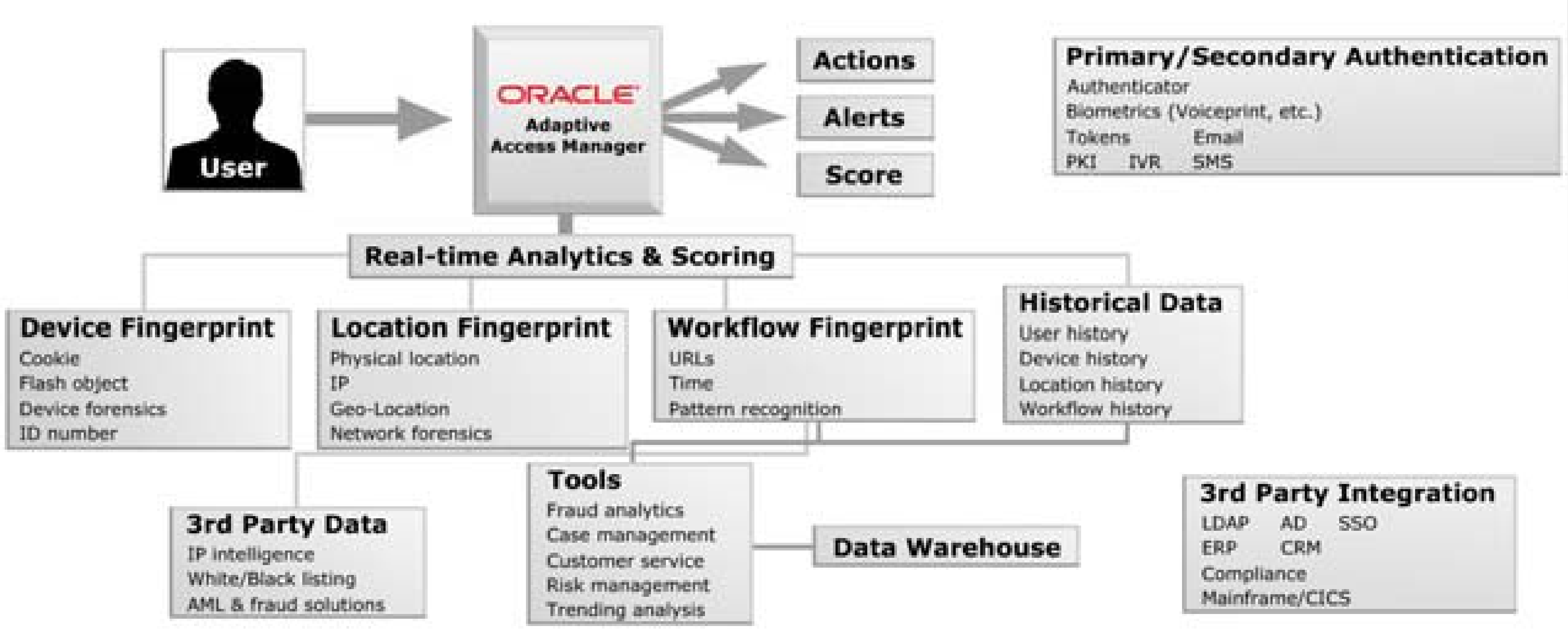
Typical security



Oracle Adaptive Access Manager

After:

Advanced real-time risk assessment combines many factors:



User

ORACLE
Adaptive
Access Manager

Actions

Alerts

Score

Primary/Secondary Authentication
Authenticator
Biometrics (Voiceprint, etc.)
Tokens Email
PKI IVR SMS

Real-time Analytics & Scoring

Device Fingerprint
Cookie
Flash object
Device forensics
ID number

Location Fingerprint
Physical location
IP
Geo-Location
Network forensics

Workflow Fingerprint
URLs
Time
Pattern recognition

Historical Data
User history
Device history
Location history
Workflow history

3rd Party Data
IP intelligence
White/Black listing
AML & fraud solutions

Tools
Fraud analytics
Case management
Customer service
Risk management
Trending analysis

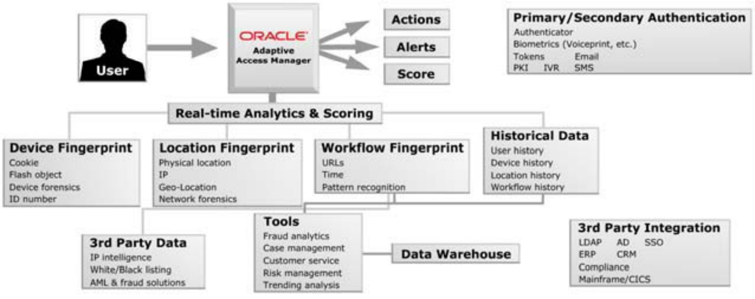
Data Warehouse

3rd Party Integration
LDAP AD SSO
ERP CRM
Compliance
Mainframe/CICS

Oracle Adaptive Access Manager

“Adaptive Risk Manager”

- 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.



User

ORACLE Adaptive Access Manager

Actions

Alerts

Score

Primary/Secondary Authentication
Authenticator
Biometrics (Voiceprint, etc.)
Tokens Email
PKI IVR SMS

Real-time Analytics & Scoring

Device Fingerprint
Cookie
Flash object
Device forensics
ID number

Location Fingerprint
Physical location
IP
Geo-Location
Network forensics

Workflow Fingerprint
URLs
Time
Pattern recognition

Historical Data
User history
Device history
Location history
Workflow history

3rd Party Data
IP intelligence
White/Black listing
AML & fraud solutions

Tools
Fraud analytics
Case management
Customer service
Risk management
Trending analysis

Data Warehouse

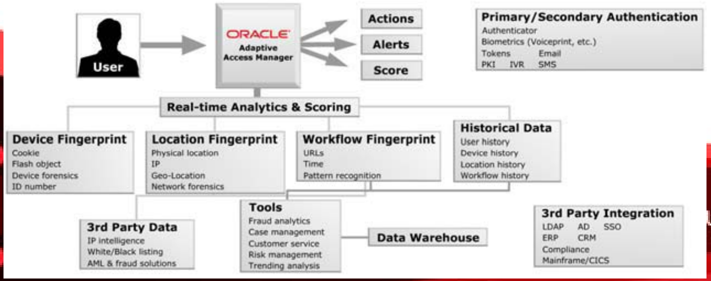
3rd Party Integration
LDAP AD SSO
ERP CRM
Compliance
Mainframe/CICS

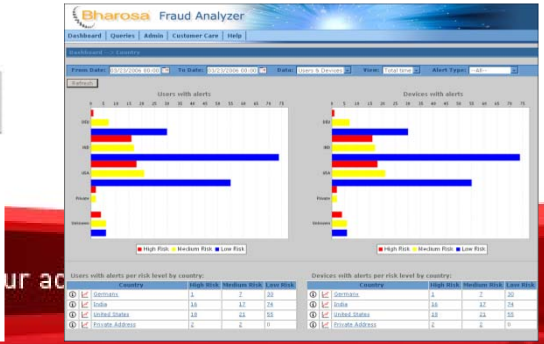
Compares “virtual fingerprints” and actions to known fraud models

Oracle Adaptive Access Manager

Real-Time Risk Assessment Capabilities

- 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





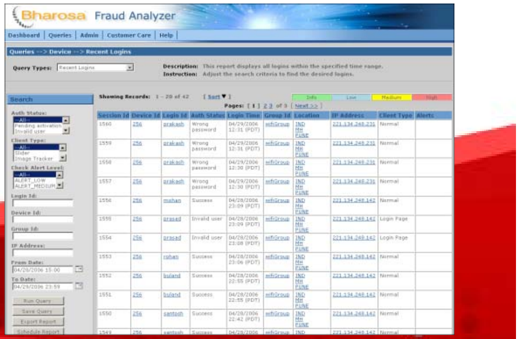
From Date: 03/23/2006 00:00 To Date: 03/23/2006 00:00 Data: Users & Devices View: Total time Alert Type: --All--

Users with alerts per risk level by country:

Country	High Risk	Medium Risk	Low Risk
Germany	1	7	30
India	16	17	74
United States	18	21	55
Private Address	2	2	0

Devices with alerts per risk level by country:

Country	High Risk	Medium Risk	Low Risk
Germany	1	7	30
India	16	17	74
United States	18	21	55
Private Address	2	2	0



Query Types: Recent Logins

Description: This report displays all logins within the specified time range.
Instruction: Adjust the search criteria to find the desired logins.

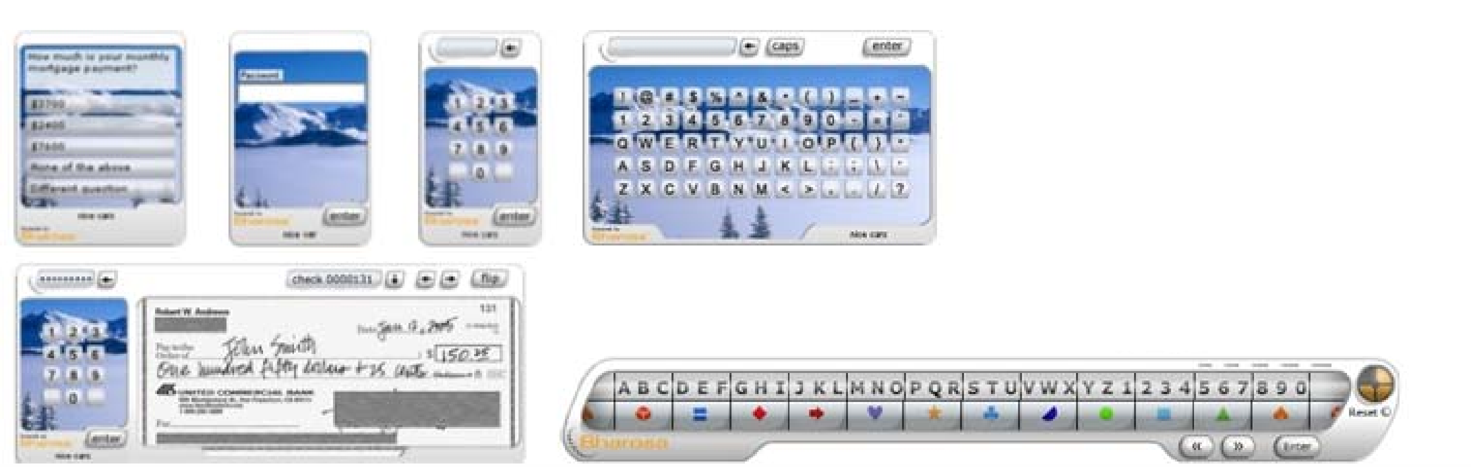
Auth Status: --All-- Pending activation Invalid user
Client Type: --All-- Slider Image Tracker
Check Alert Level: --All-- ALERT_LOW ALERT_MEDIUM
Login Id:
Device Id:
Group Id:
IP Address:
From Date: 04/28/2006 15:00
To Date: 04/29/2006 23:59

Showing Records: 1 - 20 of 42 [Sort ▼]
Pages: [1] 2 3 of 3 [Next >>]

Session Id	Device Id	Login Id	Auth Status	Login Time	Group Id	Location	IP Address	Client Type	Alerts
1560	256	prakash	Wrong password	04/29/2006 12:31 (PDT)	wifiGroup	IND MH PUNE	221.134.248.231	Normal	
1559	256	prakash	Wrong password	04/29/2006 12:31 (PDT)	wifiGroup	IND MH PUNE	221.134.248.231	Normal	
1558	256	prakash	Wrong password	04/29/2006 12:30 (PDT)	wifiGroup	IND MH PUNE	221.134.248.231	Normal	
1557	256	prakash	Wrong password	04/29/2006 12:30 (PDT)	wifiGroup	IND MH PUNE	221.134.248.231	Normal	
1556	256	mohan	Success	04/28/2006 23:09 (PDT)	wifiGroup	IND MH PUNE	221.134.248.142	Normal	
1555	256	prasad	Invalid user	04/28/2006 23:09 (PDT)	wifiGroup	IND MH PUNE	221.134.248.142	Login Page	
1554	256	prasad	Invalid user	04/28/2006 23:08 (PDT)	wifiGroup	IND MH PUNE	221.134.248.142	Login Page	
1553	256	rohan	Success	04/28/2006 23:06 (PDT)	wifiGroup	IND MH PUNE	221.134.248.142	Normal	
1552	256	buland	Success	04/28/2006 22:55 (PDT)	wifiGroup	IND MH PUNE	221.134.248.142	Normal	
1551	256	buland	Success	04/28/2006 22:55 (PDT)	wifiGroup	IND MH PUNE	221.134.248.142	Normal	
1550	256	santosh	Success	04/28/2006 22:42 (PDT)	wifiGroup	IND MH PUNE	221.134.248.142	Normal	
1549	256	santosh	Success	04/28/2006	wifiGroup	IND	221.134.248.142	Normal	

Oracle Adaptive Access Manager

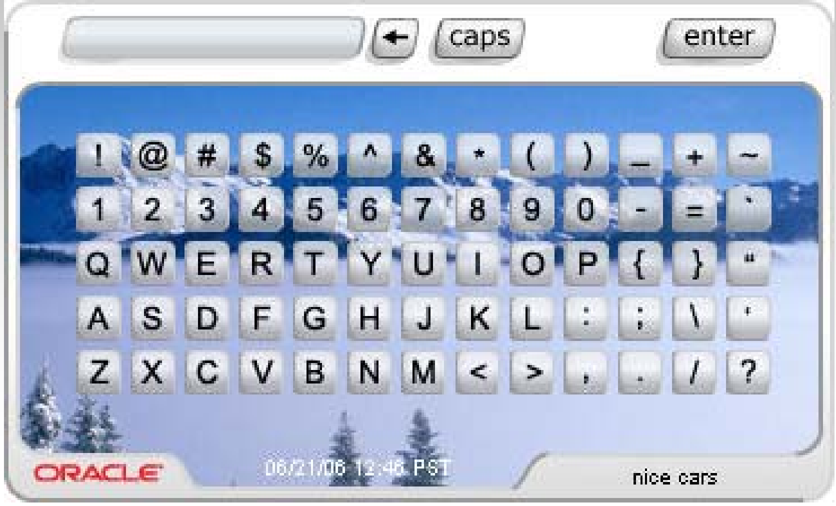
“Adaptive Strong Authentication” via Flexible Log-In Tools


How much is your monthly mortgage payment?
None of the above
Different question
Password
enter
caps
check 0000131
flip
A B C D E F G H I J K L M N O P Q R S T U V W X Y Z 1 2 3 4 5 6 7 8 9 0
Reset
Enter
Bharosa

- 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


caps
enter
! @ # $ % ^ & * ( ) _ + ~
1 2 3 4 5 6 7 8 9 0 - = `
Q W E R T Y U I O P { } "
A S D F G H J K L : ; \ '
Z X C V B N M < > , . / ?
ORACLE

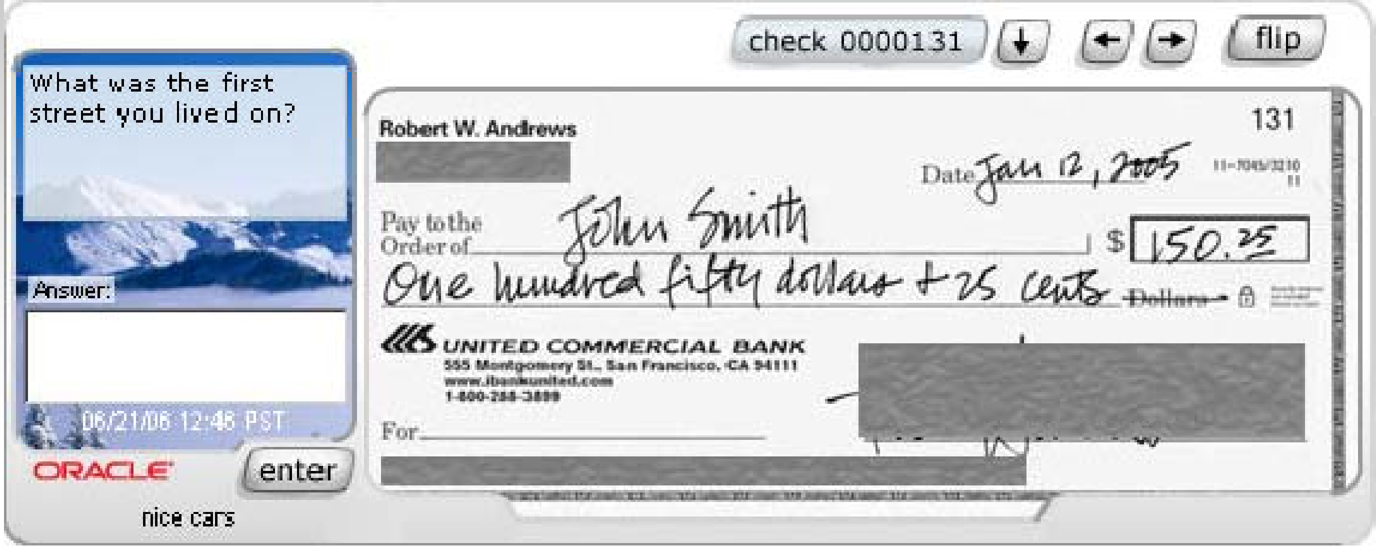
06/21/06 12:46 PST

nice cars

- The virtual authenticator device presents a virtual keyboard, where the user clicks on the characters
- Password is <u>encrypted at moment of entry</u> – 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



What was the first street you lived on?

Answer:

06/21/06 12:48 PST

Robert W. Andrews

[redacted]

131

Date Jan 12, 2005

11-7045/3210
11

Pay to the Order of John Smith $ 150.25

One hundred fifty dollars + 25 cents Dollars

UNITED COMMERCIAL BANK
555 Montgomery St., San Francisco, CA 94111
www.ibankunited.com
1-800-288-3899

For

[redacted]

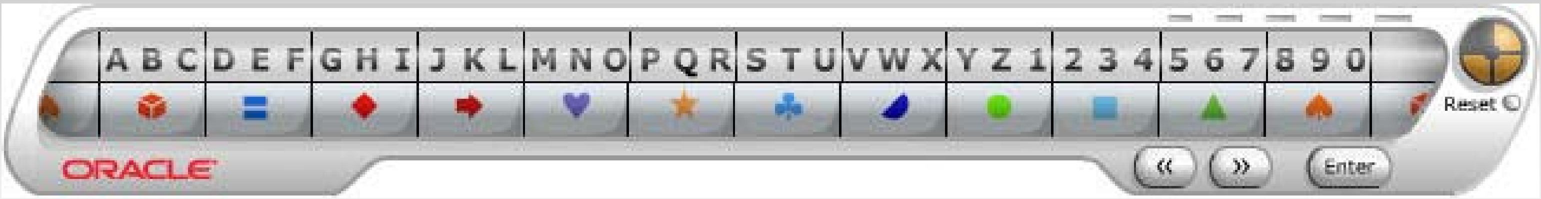
[redacted]

- 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

The “Slider”


A B C D E F G H I J K L M N O P Q R S T U V W X Y Z 1 2 3 4 5 6 7 8 9 0
Reset
ORACLE
«
»
Enter

- 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? OAAM Offers Lots of Factors

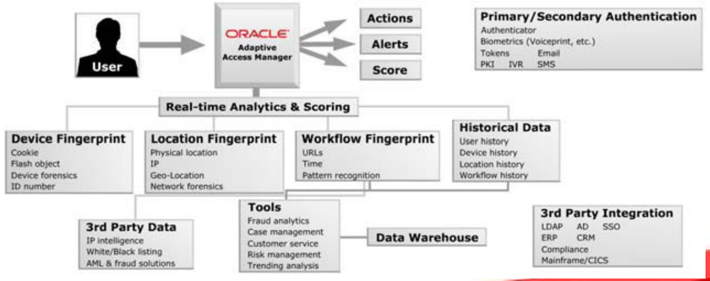
Classes of factors:

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

OAAM adds more factors:

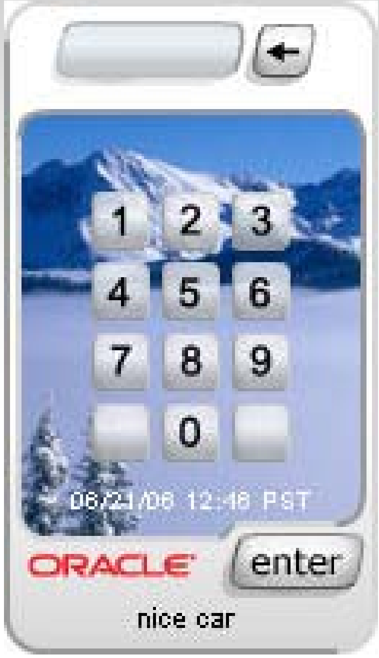
- User knows and enters ID, password, other codes on virtual authenticator devices; user can answer challenge questions
- User has the virtual fingerprints of his device(s), and of his network(s), including speeds, routes, etc.
- User is the way he behaves – his workflows

Enables compliance with key regulations: FFIEC, HIPAA, PCI



Oracle Adaptive Access Manager

Also authenticates the web site to the User



- 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

ADMIN CONSOLE REVIEW

piocon EXPLOITING TECHNOLOGY for your advantage.

Save the Date!

COLLABORATE08

Technology and **Applications** Forum for the **Oracle** Community

April 13 – 17, 2008

Colorado Convention Center

Denver, Colorado

www.ioug.org/collaborate08

RAC SIG Events

- See www.oracleracsig.org for details
  - **Webcasts:** Average 2x per month, live
  - **Conference Events:** Panels, Networking/QA sessions
  - **Forums (via OTN):** Lots of participation from RAC SIG as well as Oracle gurus
- Join the RAC SIG at www.oracleracsig.org!

Oracle RAC SIG Home - Microsoft Internet Explorer

Hot Items

RAC Forum
Online forum to share experiences with other RAC SIG members.

RAC in the News
Latest RAC News from Google.

RAC Home on Oracle.com
Official site for RAC information.

About the RAC SIG

To attend the web seminars all that is required is to register and provide details of your 10g RAC configuration. If already registered please login.

Announcements

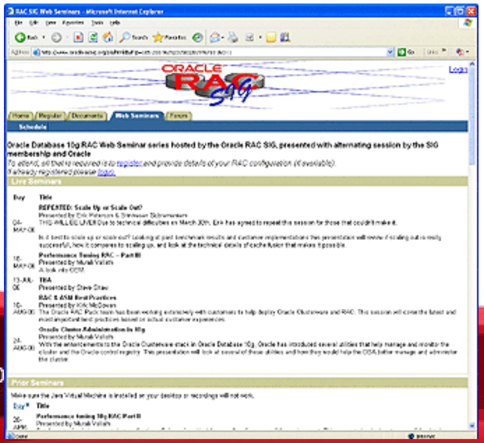
No Announcements at this Time

Next Live Web Seminar

16-MAY-06 Performance Tuning RAC – Part II
Presented by Murali Vallath
A look into OEM

New Items

This site is not associated with Oracle Corporation, and the opinions expressed within are not necessarily those of Oracle Corporation



RAC SIG Web Seminars - Microsoft Internet Explorer

Oracle Database 10g RAC Web Seminar series hosted by the Oracle RAC SIG, presented with alternating session by the SIG membership and Oracle

To attend, all that is required is to register and provide details of your RAC configuration (if available). If already registered please login.

Live Seminars

Day	Title
04-MAY-06	REPEATED: Scale Up or Scale Out?
16-MAY-06	Performance Tuning RAC – Part II Presented by Murali Vallath A look into OEM
13-JUL-06	TBA Presented by Steve Shaw
10-AUG-06	RAC & ASM Best Practices Presented by Kirk McGowan
24-AUG-06	Oracle Cluster Administration in 10g Presented by Murali Vallath

Prior Seminars

Make sure the Java Virtual Machine is installed on your desktop or recordings will not work.

Forum - Microsoft Internet Explorer

A great forum to share experiences with other customers. At the moment the forum server works off a different database and thus a different registration system as the main site.

Oracle RAC SIG Forums

Forum	Topics	Replies
Announcements	14	16
Installation & Configuration by Platform	147	226
RAC High Availability	34	52
RAC Performance & Scalability	38	71
RAC Consolidation	5	16
10g RAC & ASM	19	43

piocon

EXPLOITING TECHNOLOGY for your advantage.

Oracle Adaptive Access Manager: What, Why, How

Dan Norris

dnorris@piocon.com

http://www.dannorris.com/

Thanks to Matt Topper for his help preparing this presentation.

Legal

The information contained herein should be deemed reliable but not guaranteed. The author has made every attempt to provide current and accurate information. If you have any comments or suggestions, please contact the author at:

dnorris@piocon.com

You may request redistribution permission from dnorris@piocon.com.