Did You Know: Trends in RSA SecurID® Two-Factor Authentication

Jeff Carpenter, Sr. Product Specialist RSA, The Security Division of EMC
Today: The Evolution of Two-Factor Authentication

- RSA SecurID is Mobile
- RSA SecurID is Enabled by Partnerships
- RSA SecurID is Moving to Contextual and Risk-Based
RSA SecurID

Time-Synchronous Authentication

- Time-based OTP has precise clock that changes password every 60 seconds
- Very hard to phish as OTP becomes invalid in one minute
- More secure than an event-based OTP where password does not expire until another one is entered into the system
- Trojan attacks must be in real-time to be able to compromise system
RSA SecurID is Mobile
“...the market will dramatically change course and the emphasis will shift towards building mobile app stores and managing the growing pool of apps and data on a burgeoning array of Smartphones and Tablets.”

Forrester, August 2011
Mobile Application Use Cases

Business (or non business) process driven

- MS Office
  - a general purpose app
  - For enterprise or consumer use

- Internal Mobile Applications
- Cloud Applications
- Personal Use Applications

- Bank of America
- amazon.com
Mobile Apps Redefine Remote Access
From Well Defined Remote Access Gateways to App Centric

VPN  VDI  OWA

Well Defined Remote Access Policy

Infrequent, highly secure access

Business Applications

Custom  Custom  Custom  SaaS  SaaS

Frequent, less controlled mobile access
Enterprise Mobile Security Challenges

**Major Security Problems**

1. **Application Security** beyond the standard support of email and calendar
2. **Service-driven authentication** aligning with continuous remote access
3. **Heterogeneous** device support

*RSA plans to solve these problems in a manner that is:*

1. Application-focused
2. Independent of traditional remote access
3. Aligned with native device usage across a variety of device types
Enterprise Mobile Usability Challenges

Balancing user convenience and security for the organization

- Provisioning strong authentication methods such as software tokens to users
- Ongoing support of users with mobile devices
- Requirement to support VPN, VDI, mobile apps to keep users productive
Mobile Authentication Strategy

Vision

Provide **application focused** authentication for enterprise use cases across a **variety of device types** with **enhanced usability**

- Support options of Invisible Authentication
- Additional step up authentication when required
- Easy provisioning of authentication options
Vision Realized:
A Different Approach to Enterprise Authentication

Mobile Device

Consumer Cloud

Internal Mobile Applications

SecurID

Appropriate authentication based on context and risk analytics – SecurID can be leveraged as an additional authentication factor

Enterprise Cloud

Trust Authority for the Cloud

The SDK may also be leveraged to have direct hooks into CTA for enterprise access from the same device

Invisible Authentication

Appropriate authentication based on context and risk analytics – SecurID can be leveraged as an additional authentication factor

The SDK may also be leveraged to have direct hooks into CTA for enterprise access from the same device
Mobile Authentication Strategy

Two Areas of Focus

**SecurID Mobile: Mobile devices as SecurID authenticators**

- Provide software token apps for the leading Smartphone platforms
- Automate provisioning of SW tokens, seamlessly and securely
- Securely store the token on the device

**Mobile Authentication: Market leading strong authentication for mobile apps**

- Ease of integration using RSA SecurID and Adaptive Authentication Mobile SDKs
- Strong auth built into the leading remote access applications
- Strong auth built into the leading mobile app development frameworks
Mobile Authentication Roadmap

Highlights

SecurID Mobile: Mobile devices as SecurID Authenticators

• Support for additional devices (Android WiFi Only Devices, Windows Phone)
• Seamless and Secure Provisioning of Software Tokens

Mobile Authentication: Market leading strong authentication for mobile apps

• Integrated Software Development Kit (SDK) for mobile apps
  • SecurID OTP Module - Import software tokens, generate OTP, user visible or invisible OTP
  • Adaptive Authentication Module - Retrieve device identifiers and location information for risk based authentication by AA
  • Transaction Signing

• Enhanced Mobile Risk based Authentication in Adaptive Authentication
  • Powered by the RSA Risk Engine
  • Added location awareness and improved device identification for mobile
SecurID Mobile:
iOS, BlackBerry, Android, Symbian, Windows Mobile, Java ME
RSA SecurID is Enabled by Partnerships
Extending the RSA Secured Program
Integration with the Broadest Range of Enterprise and Cloud-Based Apps

• More than 400 RSA Secured products with native RSA SecurID support

• A growing number of certified solutions for risk-based authentication

• Built into the leading mobile apps (Citrix, VMware, etc.)

• Federation into Cloud-based apps
  – VMWare Horizon
  – Office 365/Azure (ADFS)
  – Ping Federate

Visit www.rsa.com/rsasecured/ for a complete list of partner solutions
Secured by RSA Certified Mobile Partners

- **Appcelerator**
  - Embed RSA auth into Titanium mobile application platform

- **Citrix**
  - Embed RSA auth into Citrix Receiver and CloudGateway

- **FeedHenry**
  - Expose RSA auth from their mobile application PaaS

- **Good Technology**
  - Integrate RSA auth into Good Dynamics developer framework

- **Juniper Networks**
  - Embed RSA auth into Junos Pulse VPN

- **VMware**
  - Embed RSA auth into VMware View

- **ZScaler**
  - Integrate RSA auth with ZScaler Secure Web Gateway
RSA and Citrix

• Jointly announced in October 2011
  – Citrix Receiver (free app)
  – Embedded RSA SecurID software token

• Authenticates end-users to virtual desktops and virtual applications from iOS and Android devices

• Use case: enterprise users accessing highly sensitive applications
RSA SecurID is Moving to Contextual and Risk-Based
The Future: Intelligent Controls Framework

Activity Details

Risk Engine → Policy Mgr.

Layered Authentication

Out-of-band

Challenge

Knowledge

Case Mgmt.

Others

NetWitness

Behavior

Device

Location

Threats

© Copyright 2011 EMC Corporation. All rights reserved.
RSA Authentication Manager 8.0
Coming Early 2013

Themes

VIRTUALIZATION

RISK-BASED AUTHENTICATION

LOWERING THE COST OF ADMINISTRATION

Feature Groups

Virtual Appliance

Enterprise RBA

Core System Enhancements

Usability & User Enablement

Troubleshooting & Support
Risk-Based Authentication

How it works
SecurID Mobile
Seamless and Secure Provisioning of Software Tokens: Roadmap

Authentication Manager 8.0

- Planned enhancements to improve provisioning
- Deployment of CT-KIP in the web-tier
- Streamlined administrator flow to provision software tokens

Integration with MDM systems

- Integration with leading Mobile Device Management (MDM) systems
- Securely provision sw token when user/device is activated by the enterprise
Why RSA SecurID?

Experience
- RSA has more than 25 years in security industry
- Represents over 60% worldwide One Time Password Market
- Over 40 million authenticators are protecting resources worldwide

Strength of Security
- Built on AES algorithm
- Time synchronous is more secure than event-based

Quality & Dependability
- Authentication Manager includes redundancy, failover, and other mission critical features
- Tokens are run through a battery of tests to ensure highest quality

Breadth of Offerings
- Wide range of authenticators meet current and future needs

Application Support
- Out-of-the-box integration with over 400 applications

World Class Service & Support
- Experienced Professional Services organization to help with special requirements
- Technical support available 24 x 7 through RSA Secure Care Online, RSA’s state-of-the-art e-support system
THANK YOU