



Access Management Landscape

Fraud and mobility

Chris Hockings
19 May 2011

The IBM[®]

SecurityStudio Tackling the illusion of absolute security



Agenda

- Traditional browser based fraud mitigation techniques
- Authorization and Authentication today
- Mobility
- Authorization++ and Authentication++
- Feedback and Comments
 - As security SMEs, customers and consumers of technology

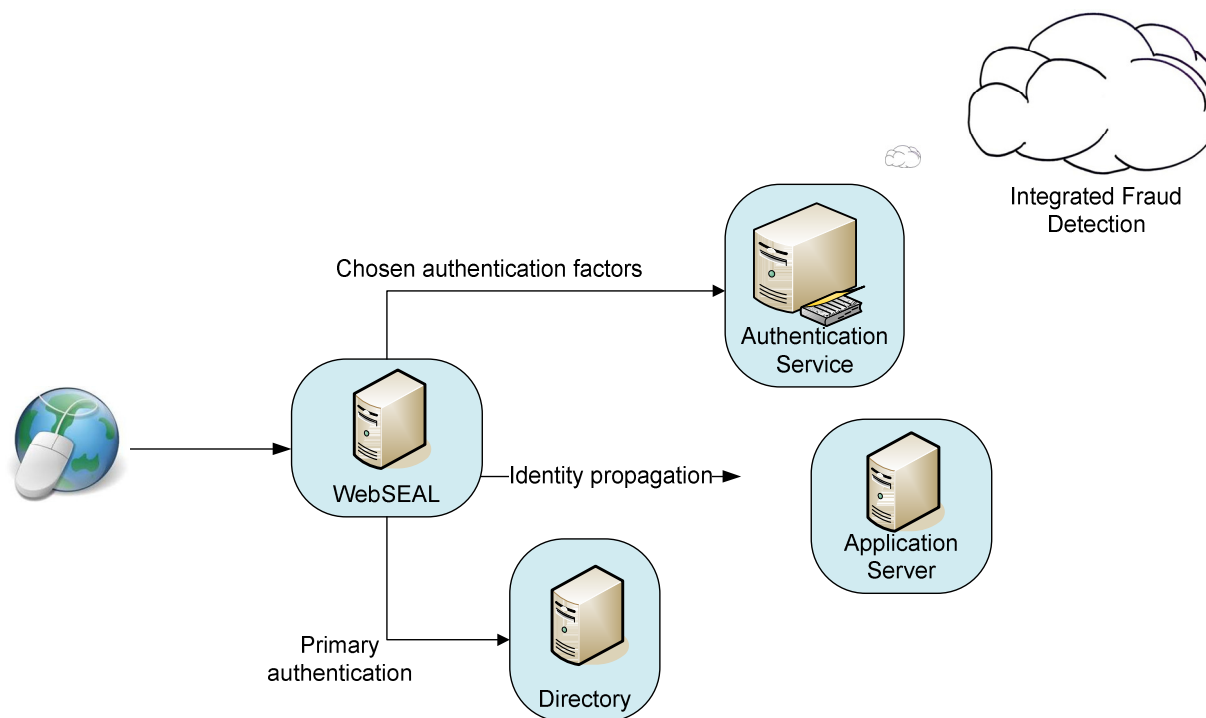
The IBM

SecurityStudio Tackling the illusion of absolute security

Access Management delivering value



- Financial loss from phishing attacks exceed US\$3B each year
 - Notwithstanding the loss of brand value
- Customers demand real-time risk based authorization as part of transaction approval
 - No longer is a delay in processing transactions acceptable to customers
- Access Management solution integrates risk analysis techniques integrated to deliver a dynamic, low cost solution that reduces financial loss

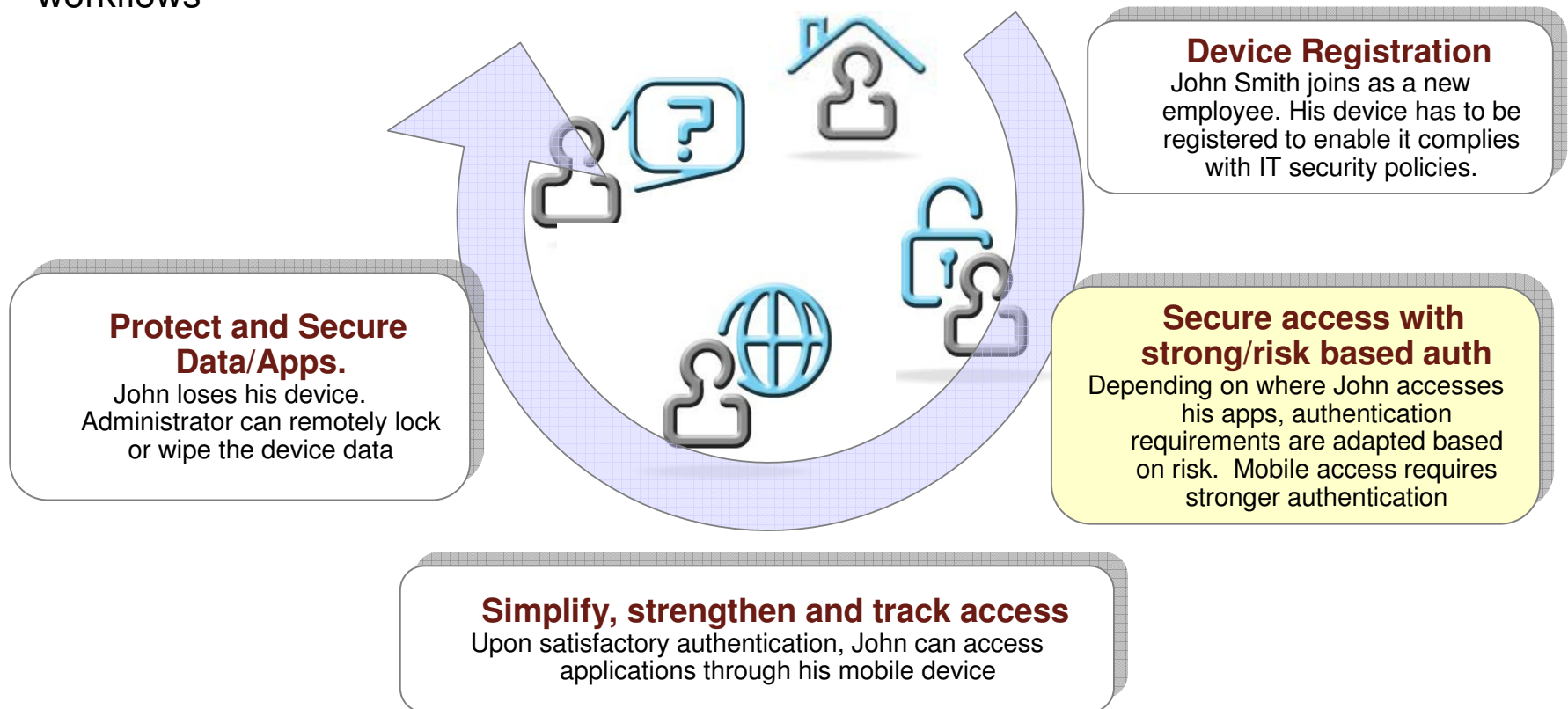


- Improved consumer trust is a tangible outcome of any solution

Access Management must now consider mobility



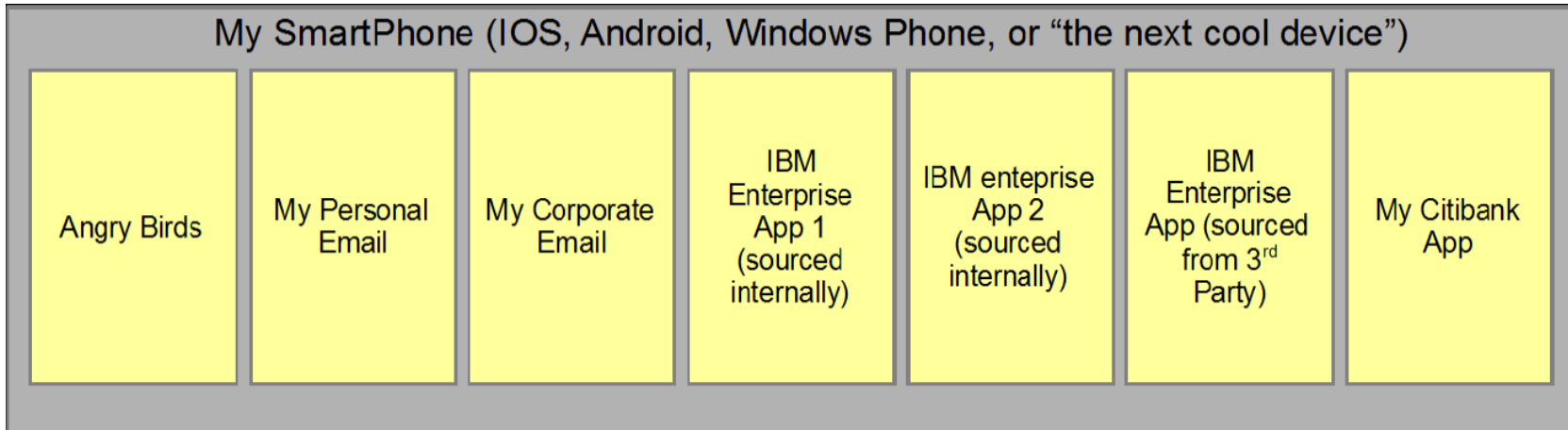
- Users are now demanding access through multiple devices
 - Creates an issue around binding identities to numerous devices with varying levels of security compliance
- Devices are context rich, creating an opportunity for greater authentication choice
 - Poor password authentication usability is becoming unacceptable to business
- Device and environment context is driving new identification and authentication workflows



The IBM

SecurityStudio Tackling the illusion of absolute security

Mobility brings many challenges



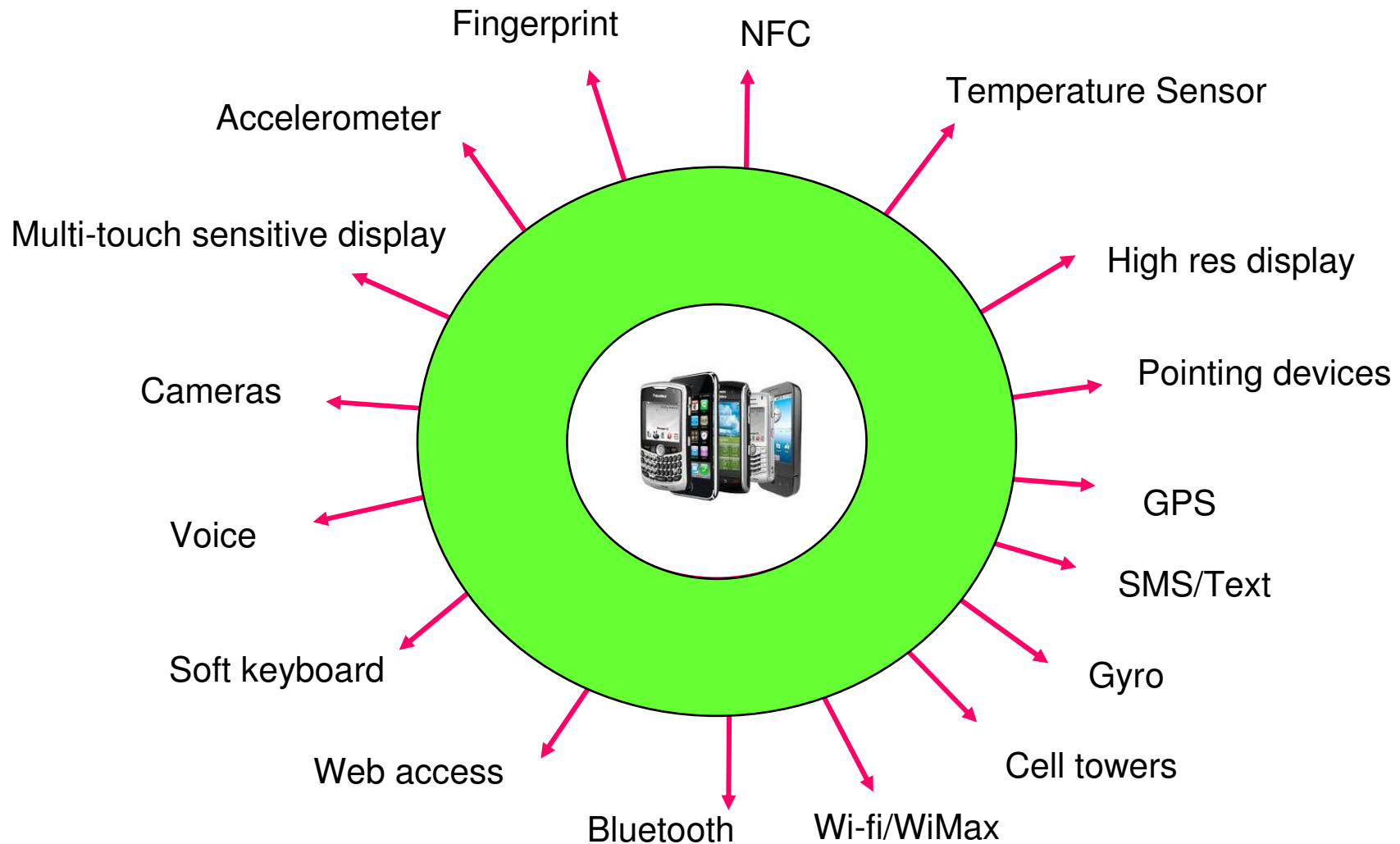
Outstanding questions that need to be addressed

- Who owns the security policies for the device or the application?
- How do I authenticate for the IBM apps? How do I authenticate to the Citibank app?
- I want to be able to play Angry Birds without IBM or Citibank authentication of the device
- How do we make the security appropriate to the application (family?) that I want to access
- When I lose the device, how do I handle informing Application Providers?
- How do I make it easy to update IBM applications?
- Where is the data stored (centrally, or by app), and is the data encrypted?
- What happens when I install an application that contains a virus or Trojan Horse?

Mobility also brings many opportunities



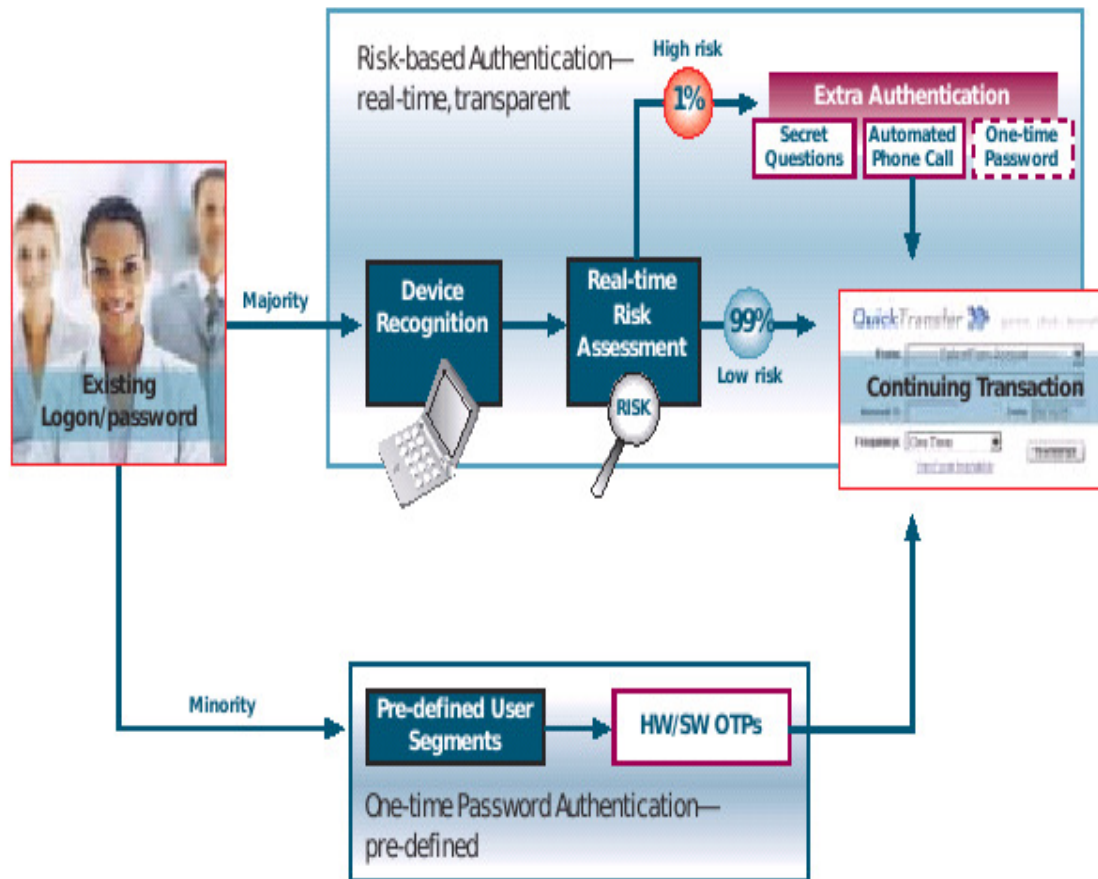
- Context needs to be considered within both authentication and authorization workflows





Where does Risk Based Auth* fit?

- Risk based authorization drives outcomes based on historical patterns of behaviour
 - Passive device focuses on the authorization aspects (which may drive authentication)
- Risk based authentication drives contextual identification (and registration)
 - With mobile devices, the focus extends to include contextual authentication
 - Continuous authentication



Device fingerprint + Behavioral pattern + Other parameters = Risk Score

Other parameters could be face/Iris scan, voice






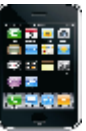



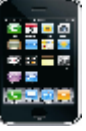


Risk Score influences the second factor for authentication (the first could be a password)

Risk based Authentication allows or deny access based on the risk score.

Mobile Security Examples


















- Glen carries a number of devices that he uses to access his IBM applications
 - These devices include personal and work devices
 - Being a mobile employee, Glen accesses applications from different locations
 - Glen hangs out with other mobile employees

Person Logging in	Device	Face Recognition	Voice Recognition	Location	1 st Access	Subsequent Access
Glen 	Glen's iPad 		NA	Gold Coast	Grant Access 	
Glen 	Glen's iPhone 		Glen's Voice	Gold Coast	Enroll new Device & Grant Access 	
Glen 	Glen's iPhone 		NA	Gold Coast		Grant Access 

Mobile Security – Demo Scenarios Continued

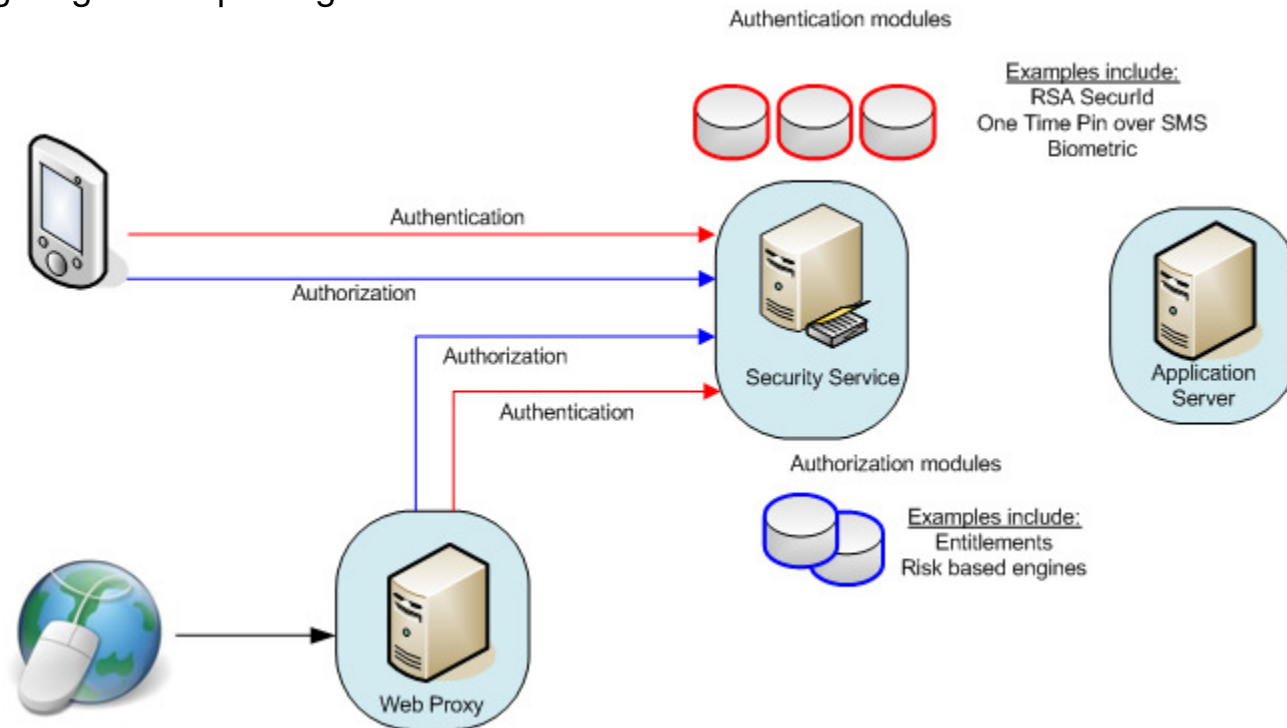


Person Logging in	Device	Face Recognition	Voice Recognition	Location	1 st Access	Subsequent Access
 Paul	 Glen's iPad		NA	Sydney	Deny Access 	
 Glen	 Glen's iPad		Glen's Voice	Sydney	Enroll & Grant Access 	
 Glen	 Glen's iPad		NA	Sydney		Grant Access 
 Paul	 Glen's iPad		NA	Sydney	Alert Glen– Someone else tried to access	



Technology Components

- Components required need to be extensible and interoperable
 - RBA modules have a role in both influencing and driving authentication
- A combination of technologies are applicable for addressing the policy management requirement
 - Risk score is combination of situational, contextual, and historical information
- For financial use cases, results in strong binding of user to transaction
 - Mitigating risk requires greater assurance



The IBM

SecurityStudio Tackling the illusion of absolute security