Security - 510: Social Mobile Security

Shane Weeden

(thanks to David Robinson, Simon Canning)

Pulse2012

Optimizing the World's Infrastructure

Please note:

- IBM's statements regarding its plans, directions, and intent are subject to change or withdrawal without notice at IBM's sole discretion.
- Information regarding potential future products is intended to outline our general product direction and it should not be relied on in making a purchasing decision.
- The information mentioned regarding potential future products is not a commitment, promise, or legal obligation to deliver any material, code or functionality. Information about potential future products may not be incorporated into any contract. The development, release, and timing of any future features or functionality described for our products remains at our sole discretion.
- Performance is based on measurements and projections using standard IBM benchmarks in a controlled environment. The actual throughput or performance that any user will experience will vary depending upon many factors, including considerations such as the amount of multiprogramming in the user's job stream, the I/O configuration, the storage configuration, and the workload processed. Therefore, no assurance can be given that an individual user will achieve results similar to those stated here.

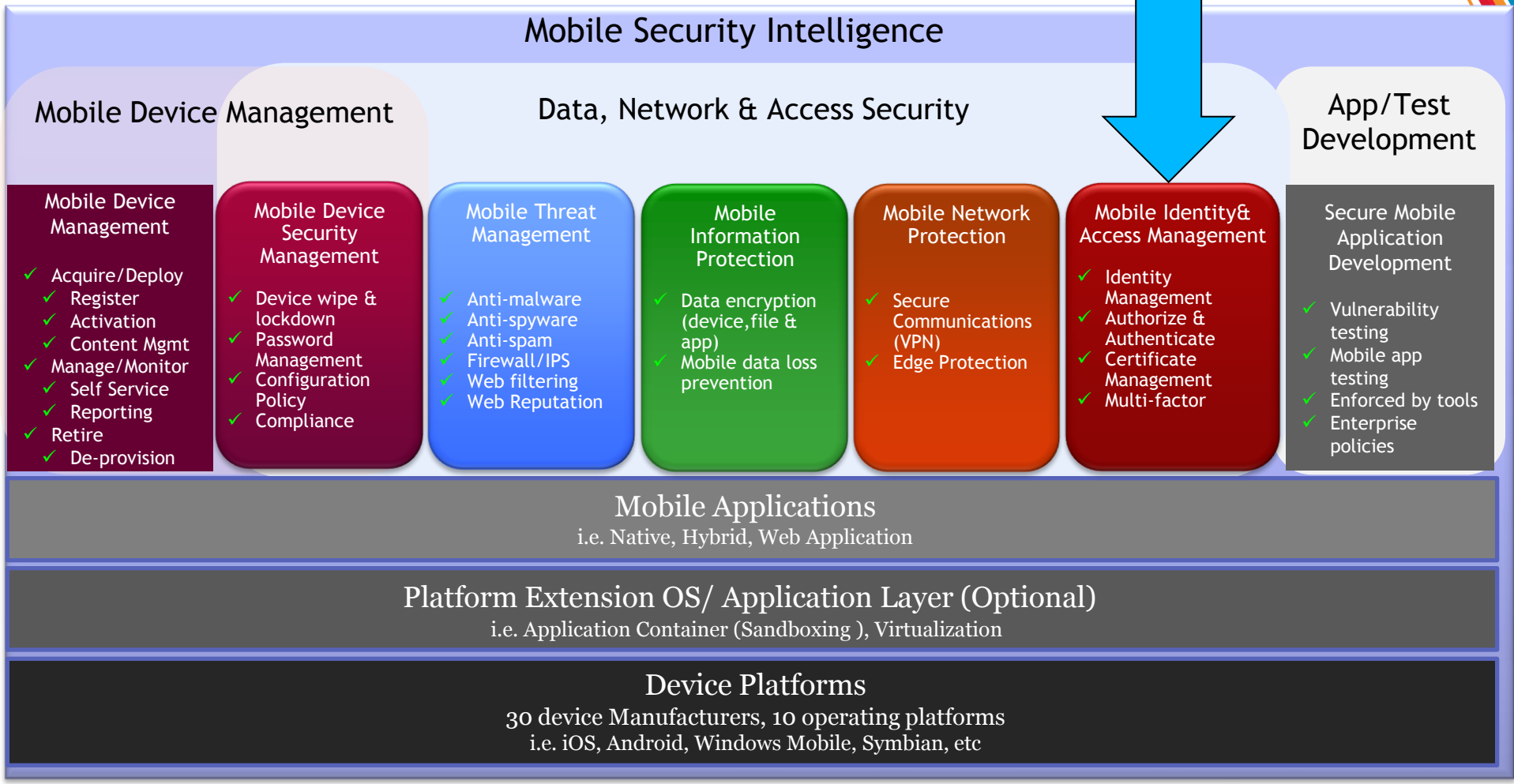
Agenda - Social Mobile Security

- The secure, social, mobile problem space
  - A brief introduction
- Use Case 1: Simple security model for mobile business apps
  - Overview
  - Demonstration: Lifecycle example of a native mobile application
  - The architecture
- Use Case 2: A mobile desktop for Change Management
  - Overview
  - Demonstration: Management of an RFC process from a mobile device
  - The architecture
- Good Practices and Common Themes
  - Techniques behind mobile applications

IBM's Mobile Security Strategy

Today's demonstrations

Mobile security is multi-faceted, driven by customers



The evolving mobile landscape

How do I ever make my apps and data secure in *this* environment ?

67% of respondents said they use their own personal device for work related activities
W3C Social Business Jam Results, November 2011

- Companies want to be able to support a broad range of devices that their employees might leverage
  - How do I do this securely ?
- Apps are “mobile” too between devices that are different
  - The same app should be able to behave differently relative to security on different devices
- Important to focus on application security features
  - Apps are how we interact with mobile devices –
    - A key control point
  - Native and browser-based apps are equally relevant
  - Audit and traceability are still important

Mobile access to enterprise applications

How *do* I make my existing applications mobile ?

57% of respondents said they are concerned about application support and network access for doing work from their mobile device W3C Social Business Jam Results, November 2011

"Social" technologies can help

- Enabling the desktop to go mobile
- Enabling mobile desktop to be secure
- Integrating data

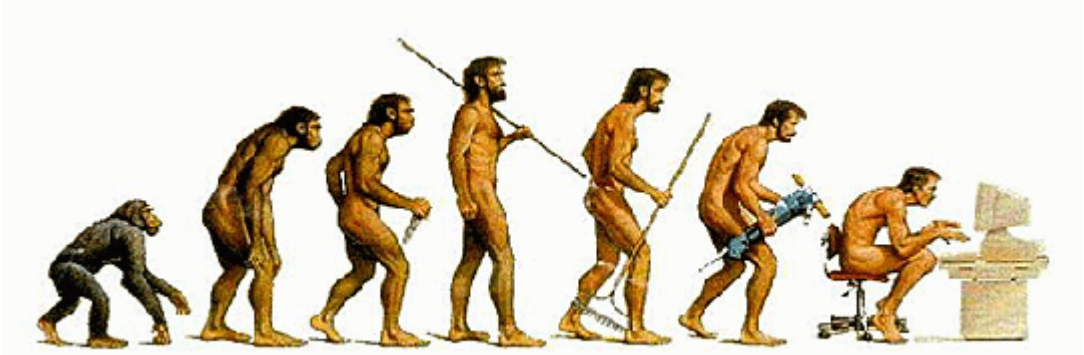
- "Social" has many meanings
  - Describes lineage of technologies – where they came from
  - Describes what technologies do – connect people
  - Much deeper than "social media"
  - Some technologies labeled "social" might surprise

Loose coupling is the new integration model

- Rapid federation with new partners to quickly solve new scenarios
  - Happens more “on the fly”
  - Need security that supports this model

- Authorized access to data and API’s is:
  - granted by the owner of the data
  - differing levels of trust

- Enter OAuth for delegated authorization
  - Shown in the demos



No IT ⟹ Internal IT ⟹ Web 1.0 ⟹ Business via API

Standards foster key interoperability

- What if my e-mail system could not read your e-mails?
  - Standards are important to the smooth functioning of social technologies

- Social Business standards benefit you
  - foster interoperability
  - simplify application development
  - Provide consistent deployment models
  - Ease the move between on-premise and cloud delivery models

- IBM is active in over 20 “social” business standards including:
  - OpenSocial, ActivityStreams, OAuth, HTML 5, CMIS, OSLC and Linked Data, OpenAjax…to name a few
  - A new opportunity and group at the W3C to talk “social business”
    - To learn more: http://www.w3.org/community/groups/#socbizcg

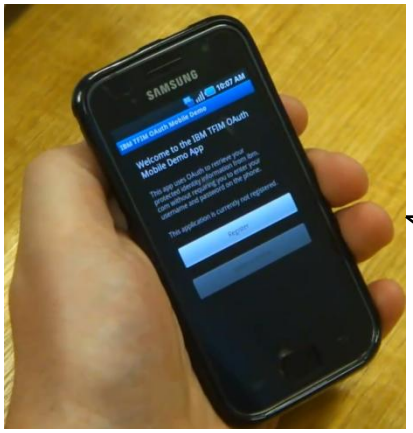
Agenda - Social Mobile Security

- Use Case 1: Security model for mobile business apps
  - Overview
  - Demonstration: Sample lifecycle of a native mobile application
  - Architecture

Use case 1: Simple security model for mobile business apps

- A banking customer wants a low-risk mobile application to perform their most common operations:
  - View balance
  - Perform transfers to pre-authorized payee list
  - Limited daily transfer total
  - View transaction history
- Loss of the mobile, or a compromised application installation should not compromise the entire account
  - Application should not have my banking username/password
- Different copies of the same application may be installed on different devices
  - Each may be managed independently
  - Each may have different authorized capabilities

Use case 1: Overview



Call API with access token

Complete registration

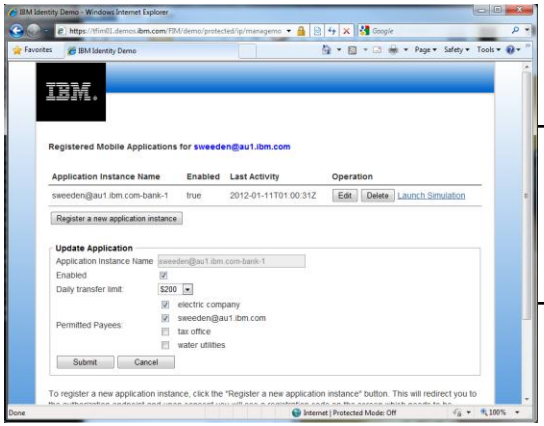
Mobile Banking API's

Security

getBalance
getPayees
transferMoney
getTxnHistory

$

Validate



Initiate registration

List, enable, modify, revoke application instances

Application Management

Authorization Server / STS

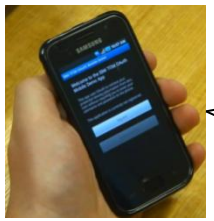
Application Administration

Users, Token state

Use Case 1: Native application demonstration

The Banking Demo

Use case 1: Architecture



Native Application

Access Token
Refresh Token

Browser Access

Tivoli Access Manager WebSEAL

OAuth EAS

Authenticated

access tokens

azn code

uid, pwd

authorized scope

Mobile Banking Application API's

Tivoli Federated Identity Manager

OAuth Server

/token

/authorize

STS

validate

Application instance administration

Users, Token state

Agenda - Social Mobile Security

- Use Case 2: A mobile desktop for Change Management
  - Overview
  - Demonstration: Management of an RFC process from a mobile device
  - Architecture

Scenario capabilities shown:

Tivoli Federated Identity Manager

Tivoli Access Manager WebSEAL

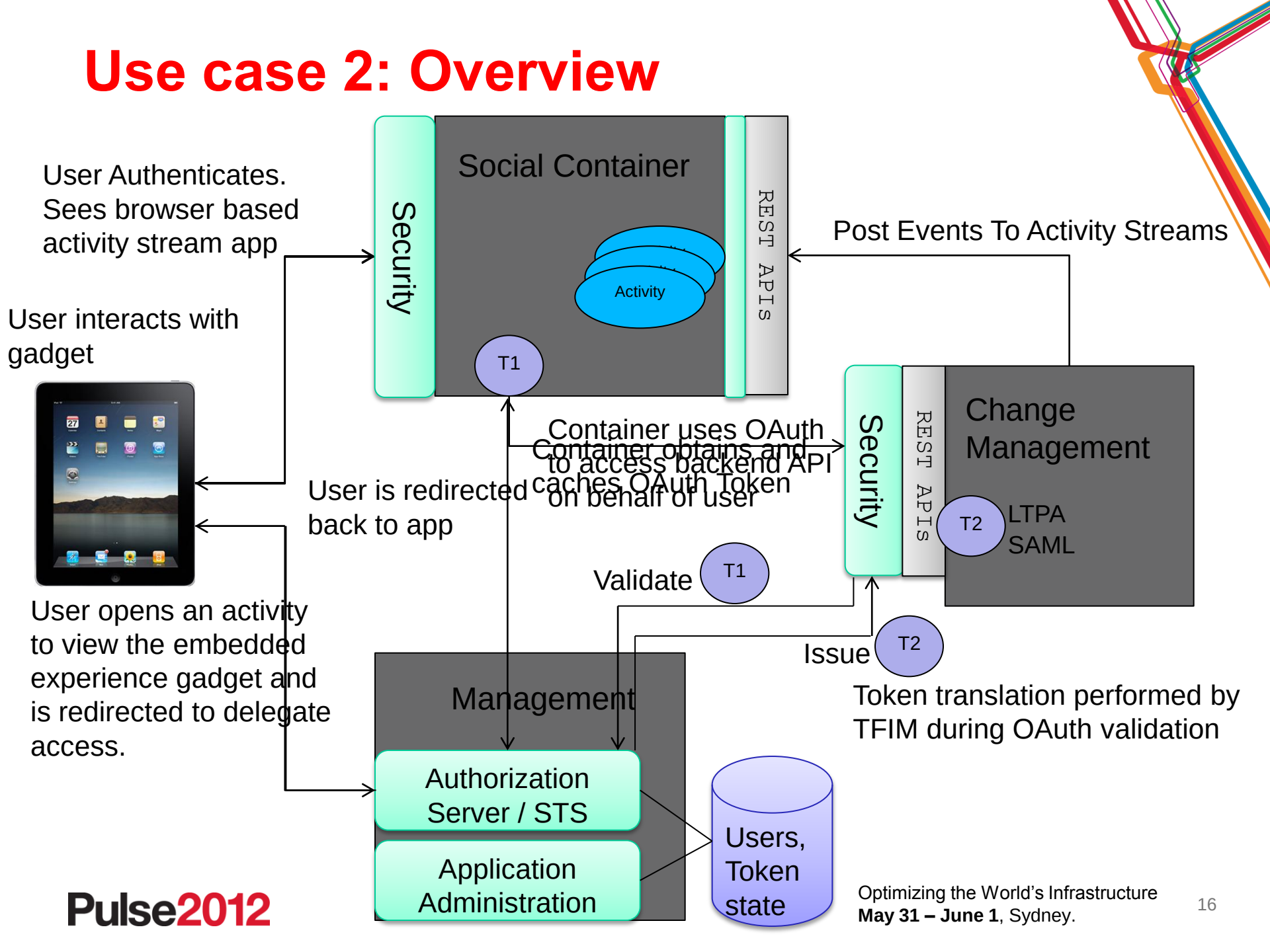
Tivoli Change Management

Lotus Connections Next

Use case 2: Mobile activity streams for change management

- An organization needs a mobile way to participate in the ITIL based request for change process
  - Need multi device support
  - Need secure, auditable access
  - Need roll based application behaviour
- An Enterprise app goes mobile
  - Need to somehow get an enterprise application on a mobile device
- Single application model
  - Only want to code a single mobile application, not dozens

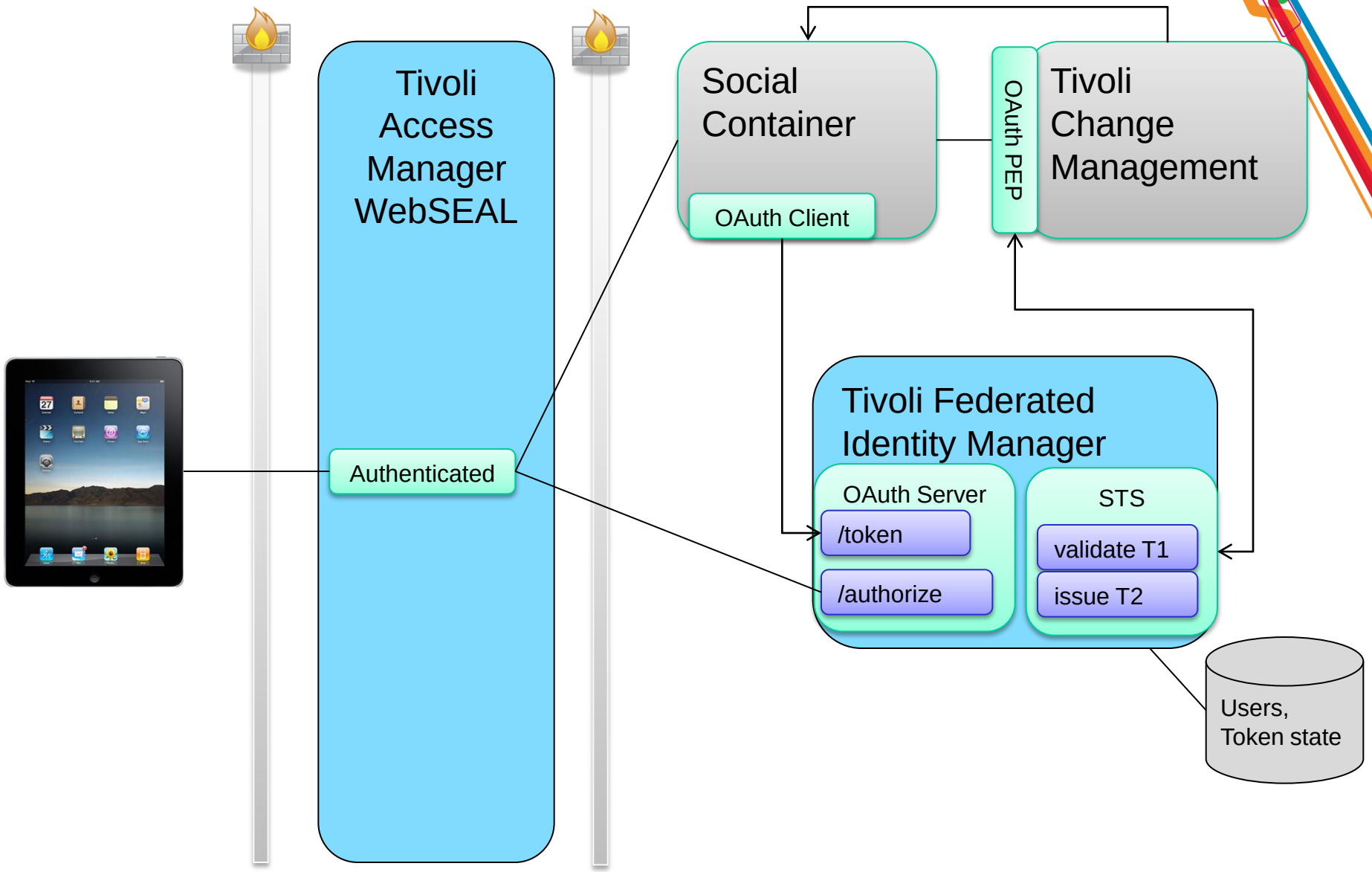
Use case 2: Overview



Use Case 2: Mobile Activity Stream Demonstration

The Activity Stream For Change Management

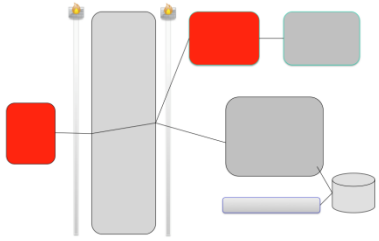
Use case 2: Architecture



Social Mobile Security – Standards Help

- Judicious use of standards can make your mobile life easier
  - activity streams
  - embedded experience gadgets
  - social container
  - OAuth 2 security
  - OSLC and Linked Data

To learn more:
OpenSocial : http://docs.opensocial.org/display/OS/Home
Activity Streams: http://activitystreams.org
IETF: https://datatracker.ietf.org/doc/draft-ietf-oauth-v2



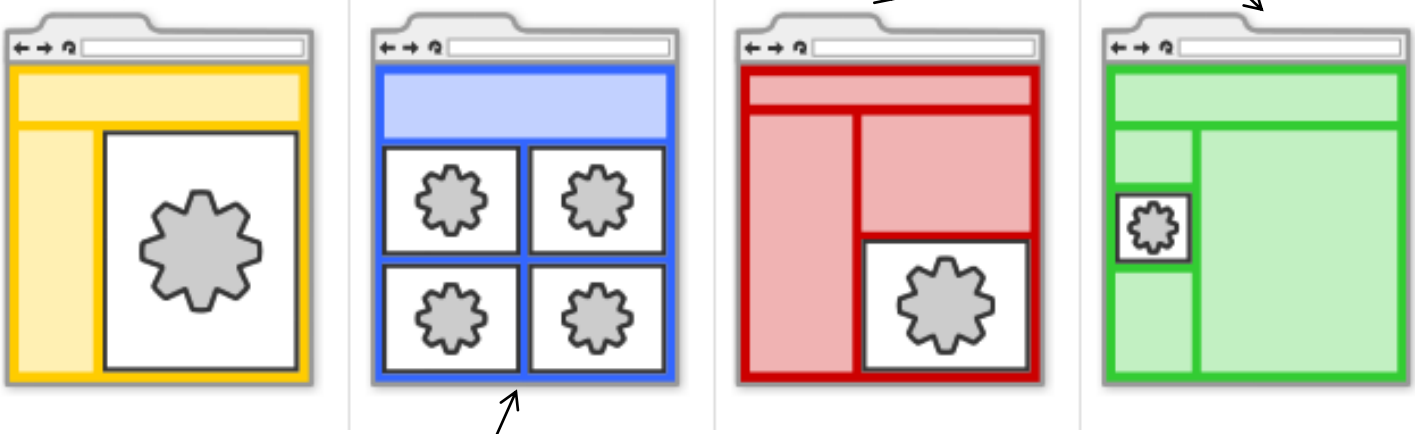
Social Mobile Security - Flexibility

The right technologies can get you flexibility in mobile for “free”…
Can also make use of the CSS media tag to detect specific devices

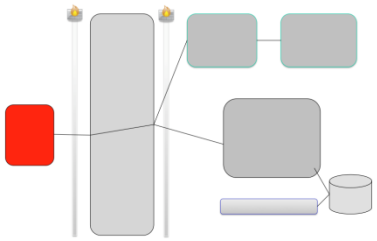
<view=”canvas”>

< view=”profile">

< view=”home">



< view=”dashboard">



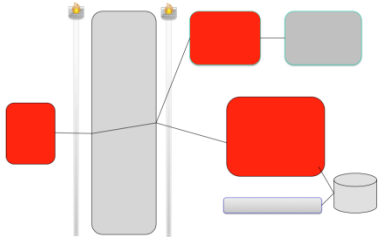
Social Mobile Security - Passwords

- Eliminate the password: "password anti-pattern"
  - A user id and password bind a user and all the operations they perform to a 'site' and should not be shared with third-party sites or native/desktop applications
  - Auditing – who **really** performed this operation?
  - Minimizes the profile for phishing attacks
  - Constantly entering a user id and password is a poor user experience

Open Authorization 2

(http://tools.ietf.org/html/draft-ietf-oauth-v2)

Delegated authorization to access data

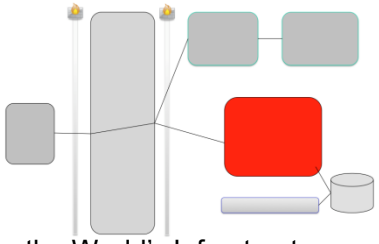


Social Mobile Security – Going Beyond…

There is more than meets the eye behind OAuth 2 security:

- Suitable entropy and life time for security tokens
- Carefully considered scopes for mobile and native applications
  - Social technologies can help with what features are/are not available on mobile
- Consider both behavioural contextual security requirements
  - phishing resistant authentication mechanisms
  - geolocation and habit monitoring
  - challenge with additional measures if necessary
- Support user and admin-driven revocation of tokens

Ref: http://tools.ietf.org/html/draft-ietf-oauth-v2-threatmodel



Social Mobile Security - What you've seen

Social technologies provide high-value user experiences for business applications across a wide range of devices

Mobile devices are becoming pervasive and employees and customers expect BYOD service that works

Security is fundamental to providing safe, successful, standardized business applications

IBM has solutions to deliver your next generation of business applications – no matter what your mobile platform

Thank You!

Trademarks and disclaimers

The customer examples described are presented as illustrations of how those customers have used IBM products and the results they may have achieved. Actual environmental costs and performance characteristics may vary by customer.

Information concerning non-IBM products was obtained from a supplier of these products, published announcement material, or other publicly available sources and does not constitute an endorsement of such products by IBM. Sources for non-IBM list prices and performance numbers are taken from publicly available information, including vendor announcements and vendor worldwide homepages. IBM has not tested these products and cannot confirm the accuracy of performance, capability, or any other claims related to non-IBM products. Questions on the capability of non-IBM products should be addressed to the supplier of those products.

All statements regarding IBM future direction and intent are subject to change or withdrawal without notice, and represent goals and objectives only.

Some information addresses anticipated future capabilities. Such information is not intended as a definitive statement of a commitment to specific levels of performance, function or delivery schedules with respect to any future products. Such commitments are only made in IBM product announcements. The information is presented here to communicate IBM's current investment and development activities as a good faith effort to help with our customers' future planning.

Performance is based on measurements and projections using standard IBM benchmarks in a controlled environment. The actual throughput or performance that any user will experience will vary depending upon considerations such as the amount of multiprogramming in the user's job stream, the I/O configuration, the storage configuration, and the workload processed. Therefore, no assurance can be given that an individual user will achieve throughput or performance improvements equivalent to the ratios stated here.

Prices are suggested U.S. list prices and are subject to change without notice. Starting price may not include a hard drive, operating system or other features. Contact your IBM representative or Business Partner for the most current pricing in your geography.

Photographs shown may be engineering prototypes. Changes may be incorporated in production models.