HOW IDENTITY MANAGEMENT IS TRANSFORMING MODERN BUSINESS

Sarah Squire | Senior Technical Architect | @SarahKSquire
I. Identity in Ten Hundred Words
II. Zero Login
III. Zero Trust Networks
IV. One Identity Initiative
V. Open Everything
VI. Gameplan
IDENTITY
IN TEN HUNDRED WORDS
IDENTITY
IDENTITY
IDENTITY

A set of facts about a thing that make it what it is
TRUST
TRUST
TRUST
TRUST

trust
AUTHORIZATION

Allowing a person or a thing to do something
IDENTITY PROOFING
IDENTITY PROOFING

Making sure that a person is who they say they are - that their computer facts match their real life facts.
AUTHENTICATION
AUTHENTICATION
AUTHENTICATION
AUTHENTICATION

Making sure that a person or thing is the same person or thing you saw last time (which is different from them being who they say they are!)
PASSWORD
PASSWORD
PASSWORD

Something known only by the person who is supposed to know it
ATTRIBUTES
ATTRIBUTES
ATTRIBUTES

facts about a person or thing
ASSERTION
ASSERTION

fact about a person said by someone you trust
SINGLE
SIGN-ON
SINGLE SIGN-ON

letting a person or thing sign into one place and get into the other places they are allowed to go
ROLES
ROLES

a set of jobs that a person or thing does
IDENTIFIER
IDENTIFIER

The name of a thing, but only when that thing is the only thing with that name in that situation
CREDENTIALING
giving someone a thing that lets them show that they are the person you saw last time
SYSTEM OF RECORD
A place you can trust that holds the "real" things you want to know, not old out-of-date things. If two things don’t agree about facts, this one wins.
ASSURANCE
ASSURANCE

how much I believe something that was said to be a fact
PRIVACY
PRIVACY
PRIVACY

Being able to say who can know what about me
II: Zero Login
I  Ø  II: Zero Login  III  IV  V  VI

Sarah Squire  |  @SarahKSquire
ZERO TRUST NETWORKS
III: Zero Trust Networks

Authenticate the User
Authenticate the User
- something they have
- something they know
- something they are
Authenticate the Device
III: Zero Trust Networks

Authenticate the Device
- certificates or keys
III: Zero Trust Networks

Authenticate the Application
III: Zero Trust Networks

Authenticate the Application

- client credentials

- software statement
III: Zero Trust Networks

Authenticate the User

Authenticate the Device

Authenticate the Application
ONE IDENTITY INITIATIVE
IV: One Identity Initiative
IV: One Identity Initiative
Open Everything
Fitness
Fitness | Banking
---|---
Healthcare

Sarah Squire | @SarahKSquire
I  II  III  IV  V  VI:  Gameplan

Gameplan
I  II  III  IV  V  VI: Gameplan
I II III IV V VI: Gameplan

Sarah Squire | @SarahKSquire
Today

This Week

This Year
Today
Assume compromise will happen
personally identifiable information
friction is optional
**Today**

- Assume
- Compromise
- \( \text{pii} = \text{toxic} \)
- Friction is optional

**This Week**

- 

**This Year**

- 

---

*Sarah Squire | @SarahKSquire*
This Week
Common Vocabulary
Common Vocabulary

What is a token?
Common Vocabulary

What is a token?

Are these the same things?
AS  IdP  OP
Common Vocabulary

What is a token?

Are these the same things?
AS  IdP  OP Server
Common Vocabulary

What is a token?

Are these the same things?
AS  IdP  OP Server

Are these the same things?
SP  RP
Common Vocabulary

What is a token?

Are these the same things?
AS  IdP  OP Server

Are these the same things?
SP RP Client
Common Vocabulary

What is a token?
Are these the same things?
AS  IdP  OP Server

Are these the same things?
SP  RP  Client App
Common Vocabulary

What is a token?

Are these the same things?
AS  IdP  OP Server

Are these the same things?
SP  RP  Client App

Other terms: Assertion vs. Attribute
Common Vocabulary

What is a token?

Are these the same things?
AS  IdP  OP Server

Are these the same things?
SP RP Client App

Other terms: Assertion vs. Attribute, Trust
Common Vocabulary

What is a token?

Are these the same things?
AS  IdP  OP Server

Are these the same things?
SP RP Client App

Other terms: Assertion vs. Attribute, Trust, Privacy
Help with Standards
Help with Standards
Help with Standards
Transparency
Today

Assume
Compromise

pii == toxic

Friction is optional

This Week

Join IDPro

Common
Vocabulary

Help with
Standards

This Year

Sarah Squire | @SarahKSquire
Gameplan

This Year
Prepare for OpenAPIS
Prepare for OpenAPIs

- Dynamic registration
Prepare for OpenAPIs

- Dynamic registration
- Self-service identity platform
Prepare for OpenAPIs

- Dynamic registration
- Self-service identity platform
- 99.999% Uptime
One Identity Initiative
Smart MFA

Knowledge-based authentication (KBA) is a relic
Smart MFA

Knowledge-based authentication (KBA) is a relic

- bad security
- bad usability
Smart MFA

Knowledge-based authentication (KBA) is a relic

- bad security
- bad usability

One-time password over SMS is weak
Smart MFA

Knowledge-based authentication (KBA) is a relic

- bad security
- bad usability

One-time password over SMS is weak

- Public switched telephone network has extensive vulnerabilities
Smart MFA

Knowledge-based authentication (KBA) is a relic

- bad security
- bad usability

One-time password over SMS is weak

- Public switched telephone network has extensive vulnerabilities
- SMS can be sniffed
**Smart MFA**

**Knowledge-based authentication (KBA) is a relic**

- bad security
- bad usability

**One-time password over SMS is weak**

- Public switched telephone network has extensive vulnerabilities
- SMS can be sniffed
- Easy to socially engineer phone number porting/device replacement
Smart Password Policy
## Smart Password Policy

<table>
<thead>
<tr>
<th>DO</th>
<th>DO NOT</th>
</tr>
</thead>
<tbody>
<tr>
<td>Allow ridiculously long passwords</td>
<td></td>
</tr>
</tbody>
</table>
### Smart Password Policy

<table>
<thead>
<tr>
<th>DO</th>
<th>DO NOT</th>
</tr>
</thead>
<tbody>
<tr>
<td>Allow ridiculously long passwords</td>
<td></td>
</tr>
<tr>
<td>Accept spaces and special characters</td>
<td></td>
</tr>
</tbody>
</table>
## Smart Password Policy

<table>
<thead>
<tr>
<th><strong>DO</strong></th>
<th><strong>DO NOT</strong></th>
</tr>
</thead>
<tbody>
<tr>
<td>Allow ridiculously long passwords</td>
<td></td>
</tr>
<tr>
<td>Accept spaces and special characters</td>
<td></td>
</tr>
<tr>
<td>Compare to breach corpus</td>
<td></td>
</tr>
</tbody>
</table>
## Smart Password Policy

<table>
<thead>
<tr>
<th>DO</th>
<th>DO NOT</th>
</tr>
</thead>
<tbody>
<tr>
<td>Allow ridiculously long passwords</td>
<td>Require special characters</td>
</tr>
<tr>
<td>Accept spaces and special characters</td>
<td></td>
</tr>
<tr>
<td>Compare to breach corpus</td>
<td></td>
</tr>
</tbody>
</table>
### Smart Password Policy

<table>
<thead>
<tr>
<th>DO</th>
<th>DO NOT</th>
</tr>
</thead>
<tbody>
<tr>
<td>Allow ridiculously long passwords</td>
<td>Require special characters</td>
</tr>
<tr>
<td>Accept spaces and special characters</td>
<td>Force rotation</td>
</tr>
<tr>
<td>Compare to breach corpus</td>
<td></td>
</tr>
</tbody>
</table>
I: Today

Assume Compromise
pii == toxic
Friction is optional

II: This Week

Join IDPro
Common Vocabulary
Help with Standards

III: This Year

Prepare for Open APIs
One Identity
Smart MFA/passwords
Thank you, SecTor.