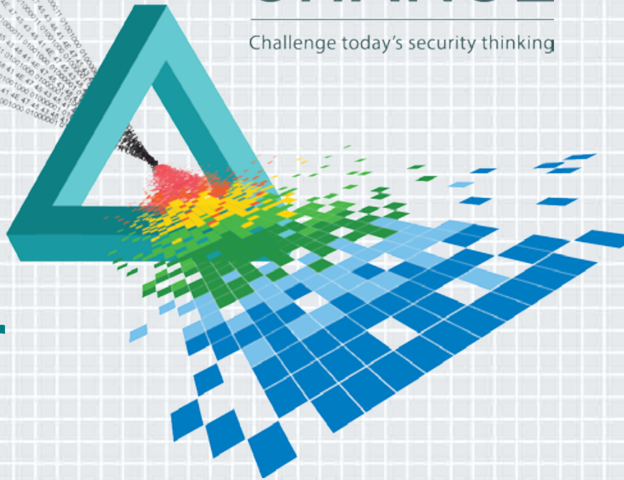
RSAConference2015

San Francisco | April 20-24 | Moscone Center

CHANGE

Challenge today's security thinking

SESSION ID: IDY-R03



Use Context to Improve Your User Identification Odds

Eve Maler

VP Innovation & Emerging Technology

ForgeRock

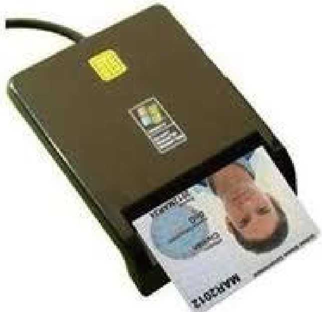
@xmlgrrl

#RSAC

We’re in authentication Bizarro World

These have been hacked

2011



2012

2015

I have heard this said by bank security architects, with my own ears

Oh yes, of course we have two-factor authentication. We protect accounts with a password, and then if the customer forgets the password, they have to answer security questions.

A good case can be made that…

this:

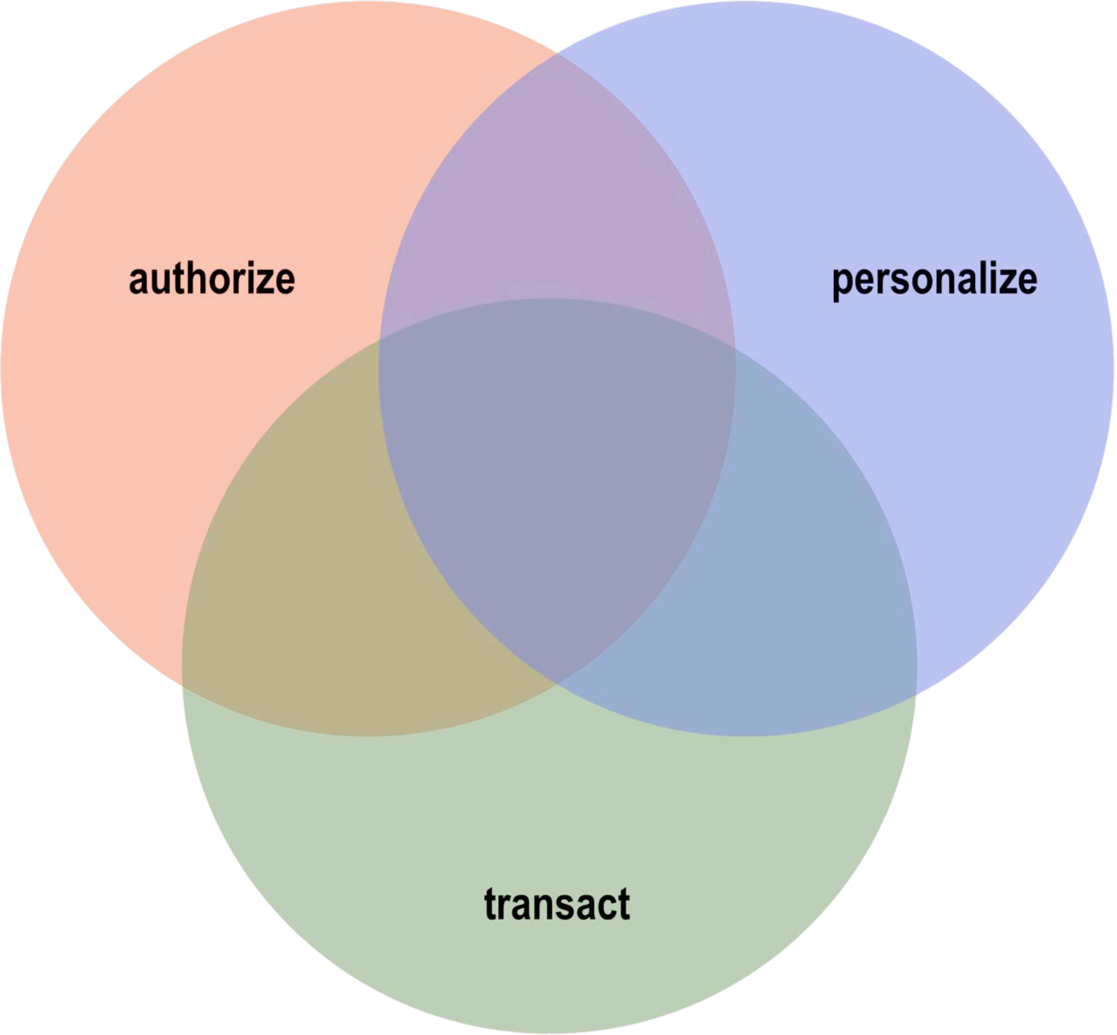
Provider of trusted identity claims for your birth date, gender, and postal code:

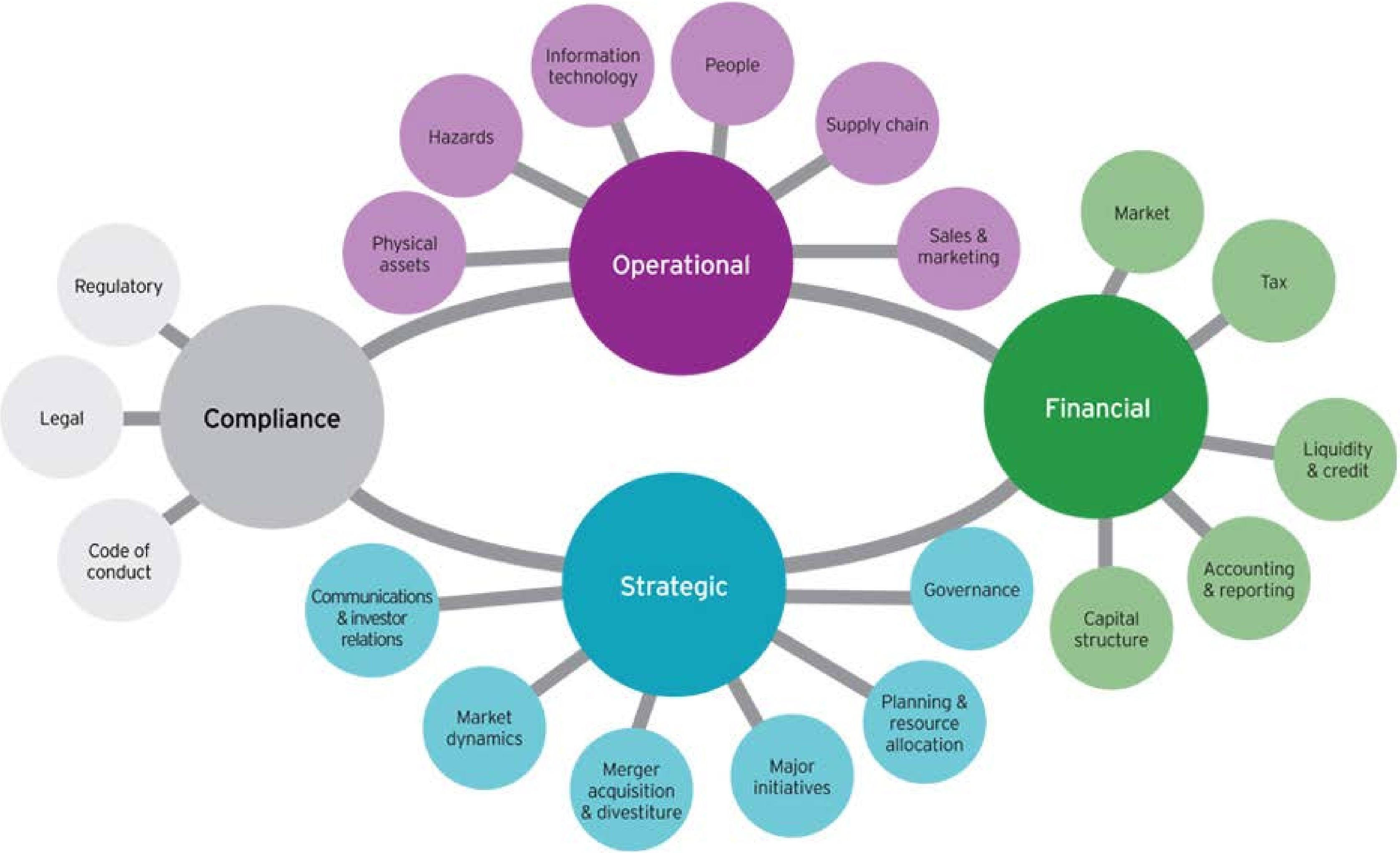
…is lower-risk than this:

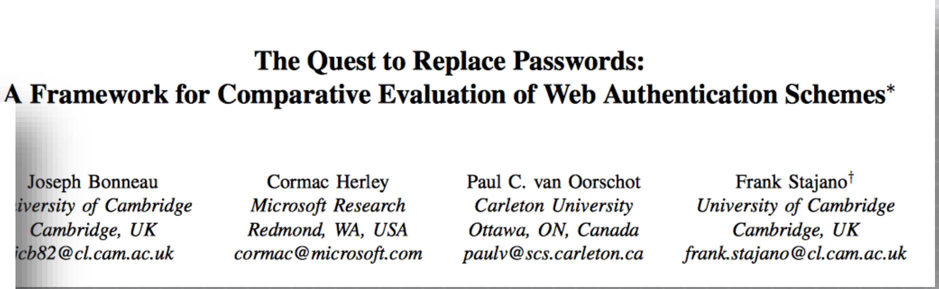
Username:

Password:

Why were we performing authentication in the first place?


authorize
personalize
transact


Operational
Physical assets
Hazards
Information technology
People
Supply chain
Sales & marketing
Financial
Market
Tax
Liquidity & credit
Accounting & reporting
Capital structure
Strategic
Governance
Planning & resource allocation
Major initiatives
Merger acquisition & divestiture
Market dynamics
Communications & investor relations
Compliance
Regulatory
Legal
Code of conduct



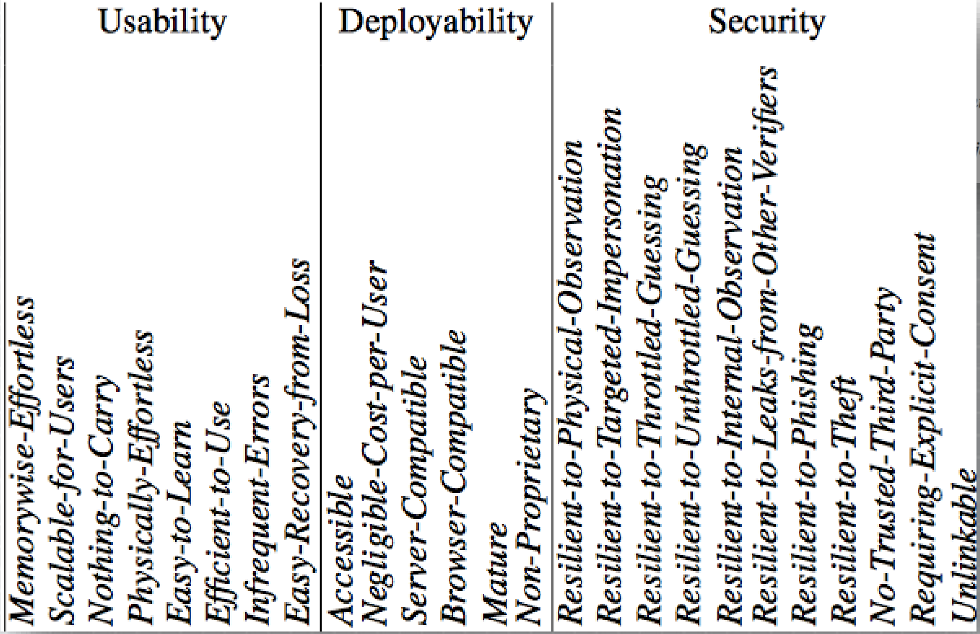
The Quest to Replace Passwords:
A Framework for Comparative Evaluation of Web Authentication Schemes*

Joseph Bonneau
iversity of Cambridge
Cambridge, UK
jcb82@cl.cam.ac.uk

Cormac Herley
Microsoft Research
Redmond, WA, USA
cormac@microsoft.com

Paul C. van Oorschot
Carleton University
Ottawa, ON, Canada
paulv@scs.carleton.ca

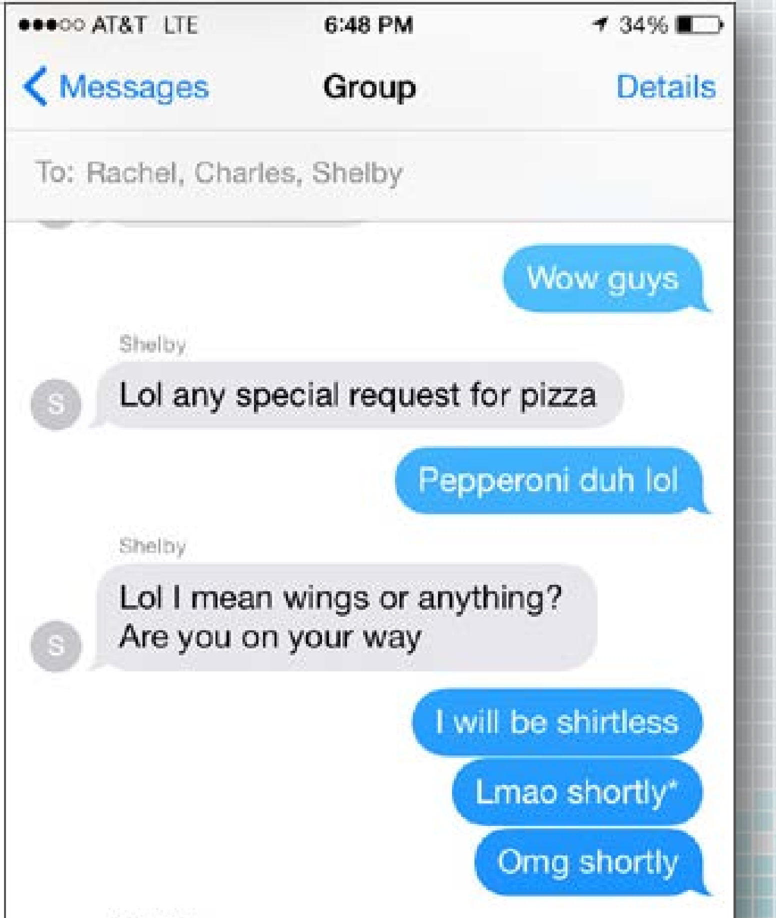
Frank Stajano†
University of Cambridge
Cambridge, UK
frank.stajano@cl.cam.ac.uk



Usability								Deployability						Security										
Memorywise-Effortless	*Scalable-for-Users*	*Nothing-to-Carry*	*Physically-Effortless*	*Easy-to-Learn*	*Efficient-to-Use*	*Infrequent-Errors*	*Easy-Recovery-from-Loss*	*Accessible*	*Negligible-Cost-per-User*	*Server-Compatible*	*Browser-Compatible*	*Mature*	*Non-Proprietary*	*Resilient-to-Physical-Observation*	*Resilient-to-Targeted-Impersonation*	*Resilient-to-Throttled-Guessing*	*Resilient-to-Unthrottled-Guessing*	*Resilient-to-Internal-Observation*	*Resilient-to-Leaks-from-Other-Verifiers*	*Resilient-to-Phishing*	*Resilient-to-Theft*	*No-Trusted-Third-Party*	*Requiring-Explicit-Consent*	*Unlinkable*

But we’re making the tradeoffs all wrong

Customer experiences often suffer from dismal security *and* usability



●●●○○ AT&T LTE 6:48 PM 34%

Messages Group Details

To: Rachel, Charles, Shelby

Wow guys

Shelby

Lol any special request for pizza

Pepperoni duh lol

Shelby

Lol I mean wings or anything? Are you on your way

I will be shirtless

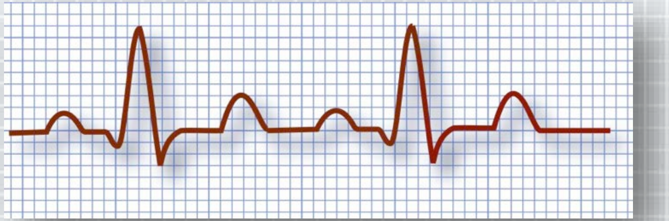
Lmao shortly*

Omg shortly

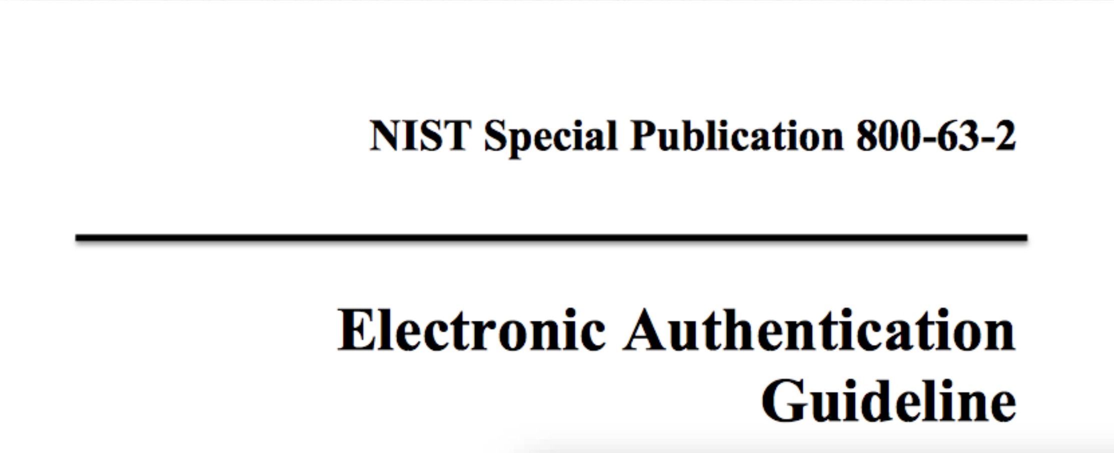
Hey SKINNY! ...YER RIBS ARE SHOWING!
DON'T LET HIM HIT YOU, JOE!
WATCH WHAT YOU SAY, FELLA...
HERE'S A LOVE-TAP FROM THAT "BAG OF BONES" REMEMBER?
WHAT A MAN
AND HE USED TO BE SO SKINNY!
I Can Make YOU a New Man, Too, In Only 15 Minutes a Day!
CHARLES ATLAS

What makes authentication "strong"?

The three ~~*pigs*~~ ~~*wishes*~~ ~~*billy goats gruff*~~ factors

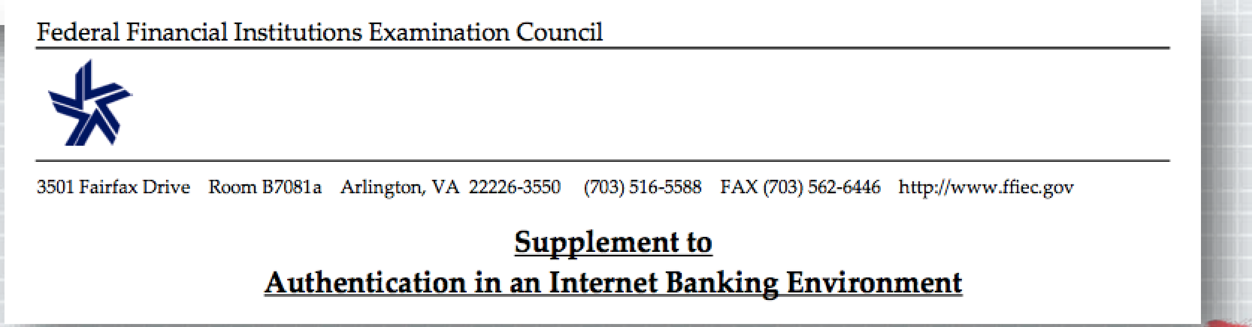


Regulations tend to be backwards-looking



NIST Special Publication 800-63-2

Electronic Authentication Guideline

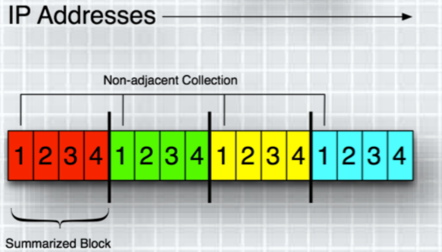


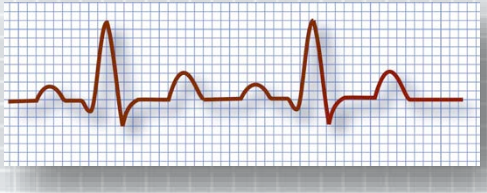
Federal Financial Institutions Examination Council

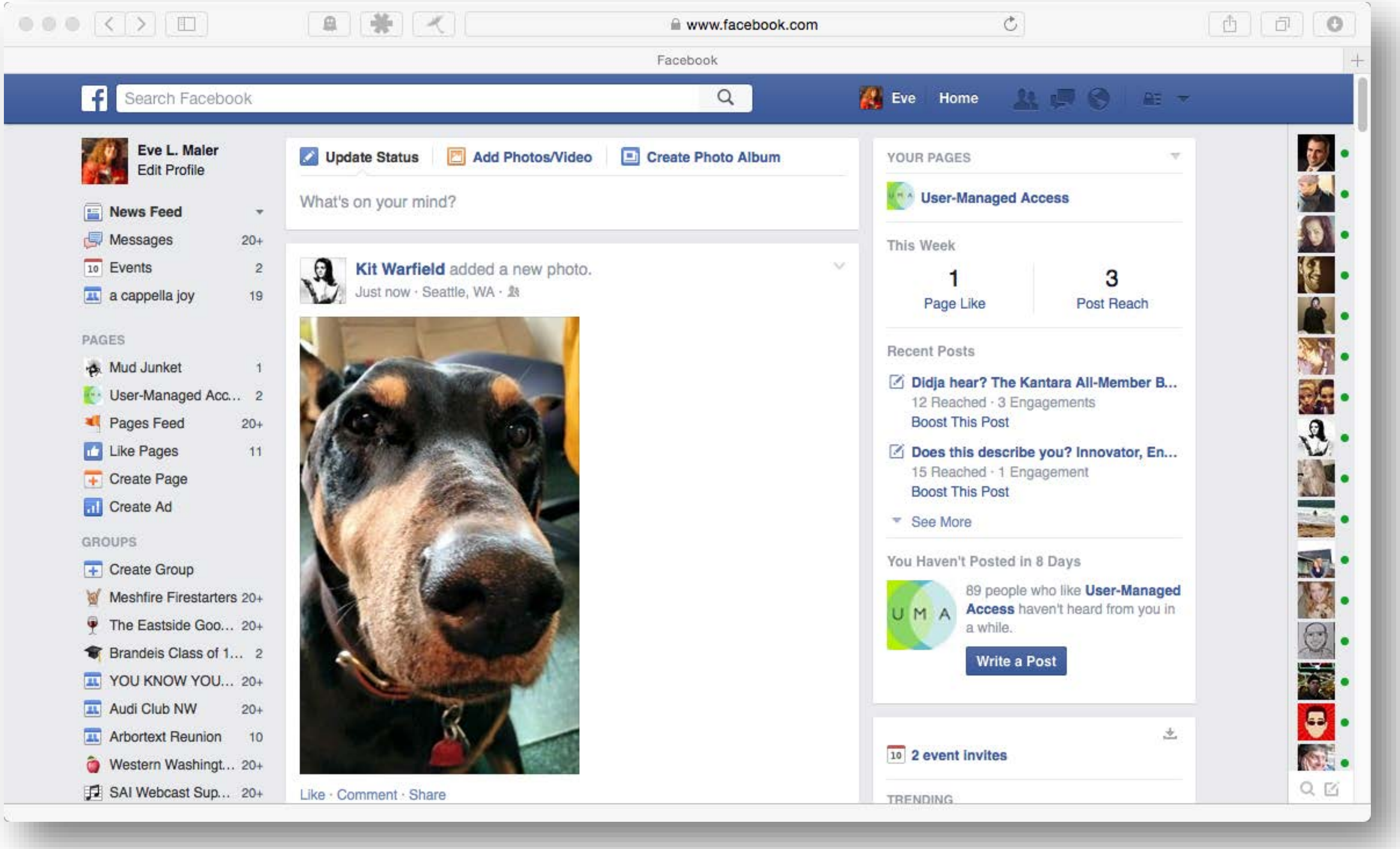
3501 Fairfax Drive Room B7081a Arlington, VA 22226-3550 (703) 516-5588 FAX (703) 562-6446 http://www.ffiec.gov

Supplement to
Authentication in an Internet Banking Environment

Context has become a fourth “factor”: everything you are observed to do







www.facebook.com

Facebook

Search Facebook

Eve Home

Eve L. Maler
Edit Profile

News Feed	
Messages	20+
Events	2
a cappella joy	19

PAGES

Mud Junket	1
User-Managed Acc...	2
Pages Feed	20+
Like Pages	11
Create Page	
Create Ad	

GROUPS

Create Group	
Meshfire Firestarters	20+
The Eastside Goo...	20+
Brandeis Class of 1...	2
YOU KNOW YOU...	20+
Audi Club NW	20+
Arbortext Reunion	10
Western Washingt...	20+
SAI Webcast Sup...	20+

Update Status · Add Photos/Video · Create Photo Album

What's on your mind?

Kit Warfield added a new photo.
Just now · Seattle, WA ·

Like · Comment · Share

YOUR PAGES

User-Managed Access

This Week

1 Page Like · 3 Post Reach

Recent Posts

Didja hear? The Kantara All-Member B...
12 Reached · 3 Engagements
Boost This Post

Does this describe you? Innovator, En...
15 Reached · 1 Engagement
Boost This Post

See More

You Haven't Posted in 8 Days

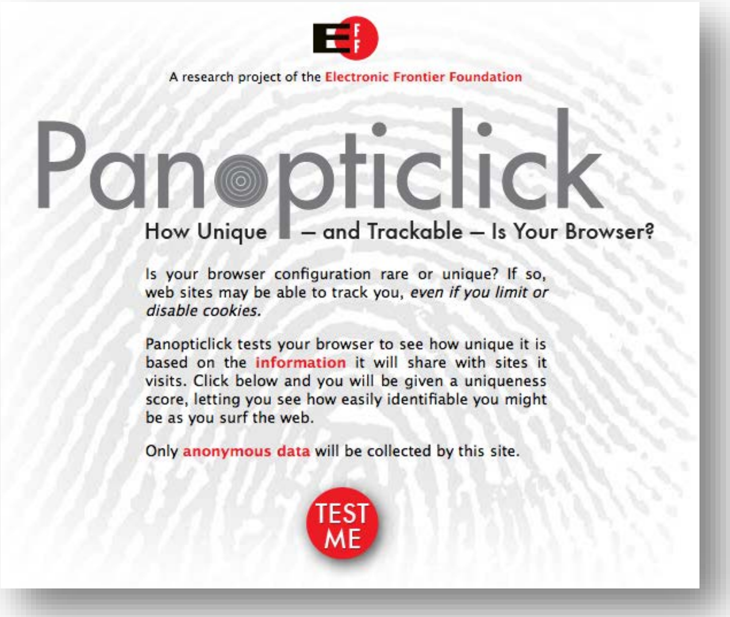
U M A

89 people who like User-Managed Access haven't heard from you in a while.

Write a Post

2 event invites

TRENDING



A research project of the **Electronic Frontier Foundation**

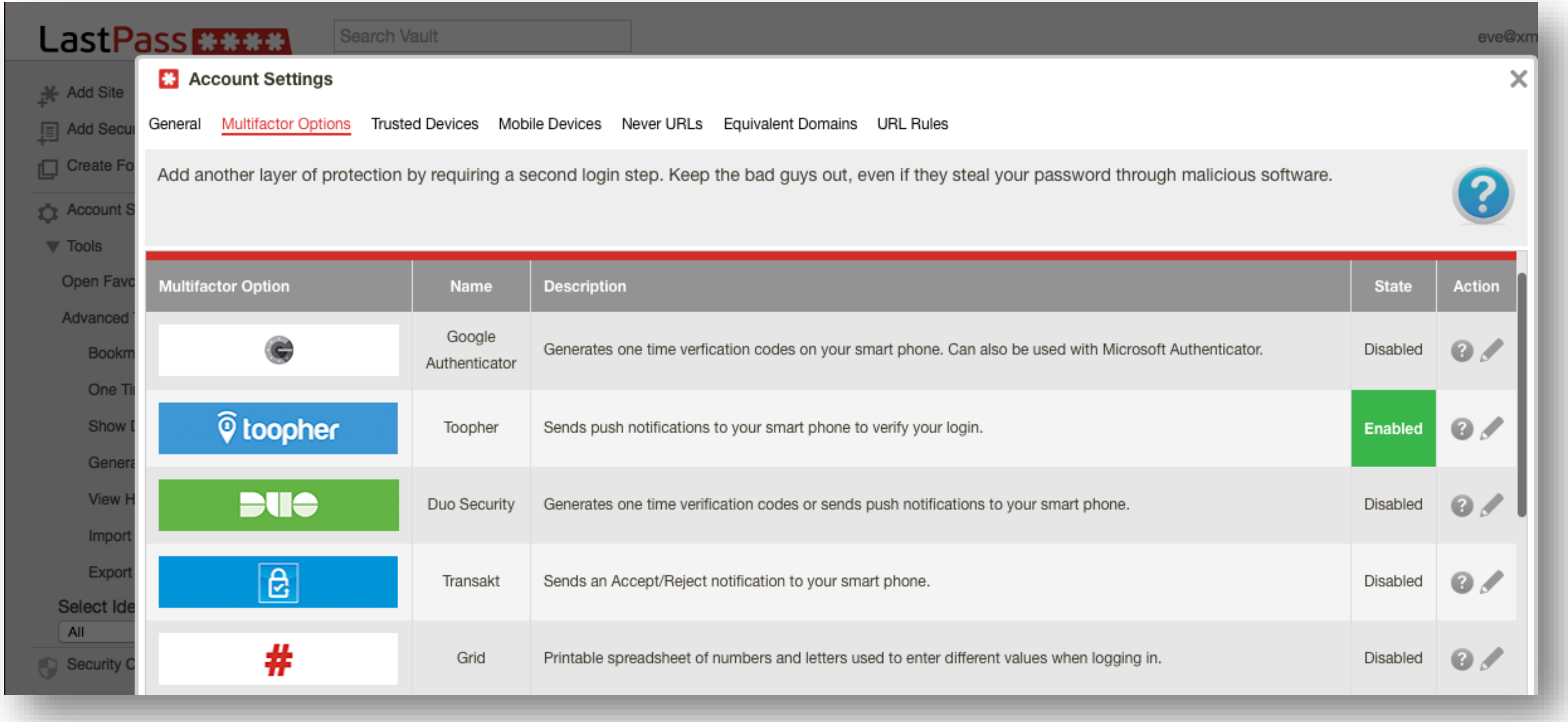
Panopticlick

How Unique — and Trackable — Is Your Browser?

Is your browser configuration rare or unique? If so, web sites may be able to track you, *even if you limit or disable cookies.*

Panopticlick tests your browser to see how unique it is based on the **information** it will share with sites it visits. Click below and you will be given a uniqueness score, letting you see how easily identifiable you might be as you surf the web.

Only **anonymous data** will be collected by this site.



Add another layer of protection by requiring a second login step. Keep the bad guys out, even if they steal your password through malicious software.

Multifactor Option	Name	Description	State	Action
	Google Authenticator	Generates one time verfication codes on your smart phone. Can also be used with Microsoft Authenticator.	Disabled	
toopher	Toopher	Sends push notifications to your smart phone to verify your login.	Enabled	
DUO	Duo Security	Generates one time verification codes or sends push notifications to your smart phone.	Disabled	
	Transakt	Sends an Accept/Reject notification to your smart phone.	Disabled	
#	Grid	Printable spreadsheet of numbers and letters used to enter different values when logging in.	Disabled	

Identification is about more than authentication “factors”

Authentication has always needed other elements too

Bandness

Hygiene

Form factor

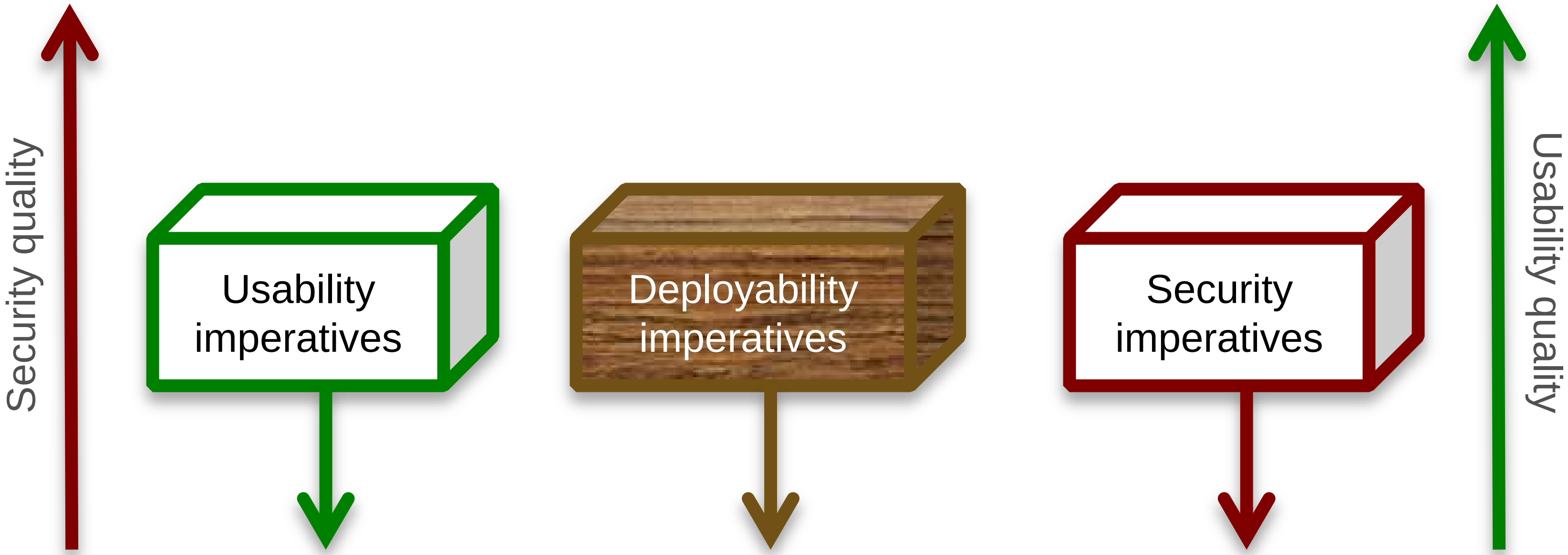
Layering

Resistance to creativity

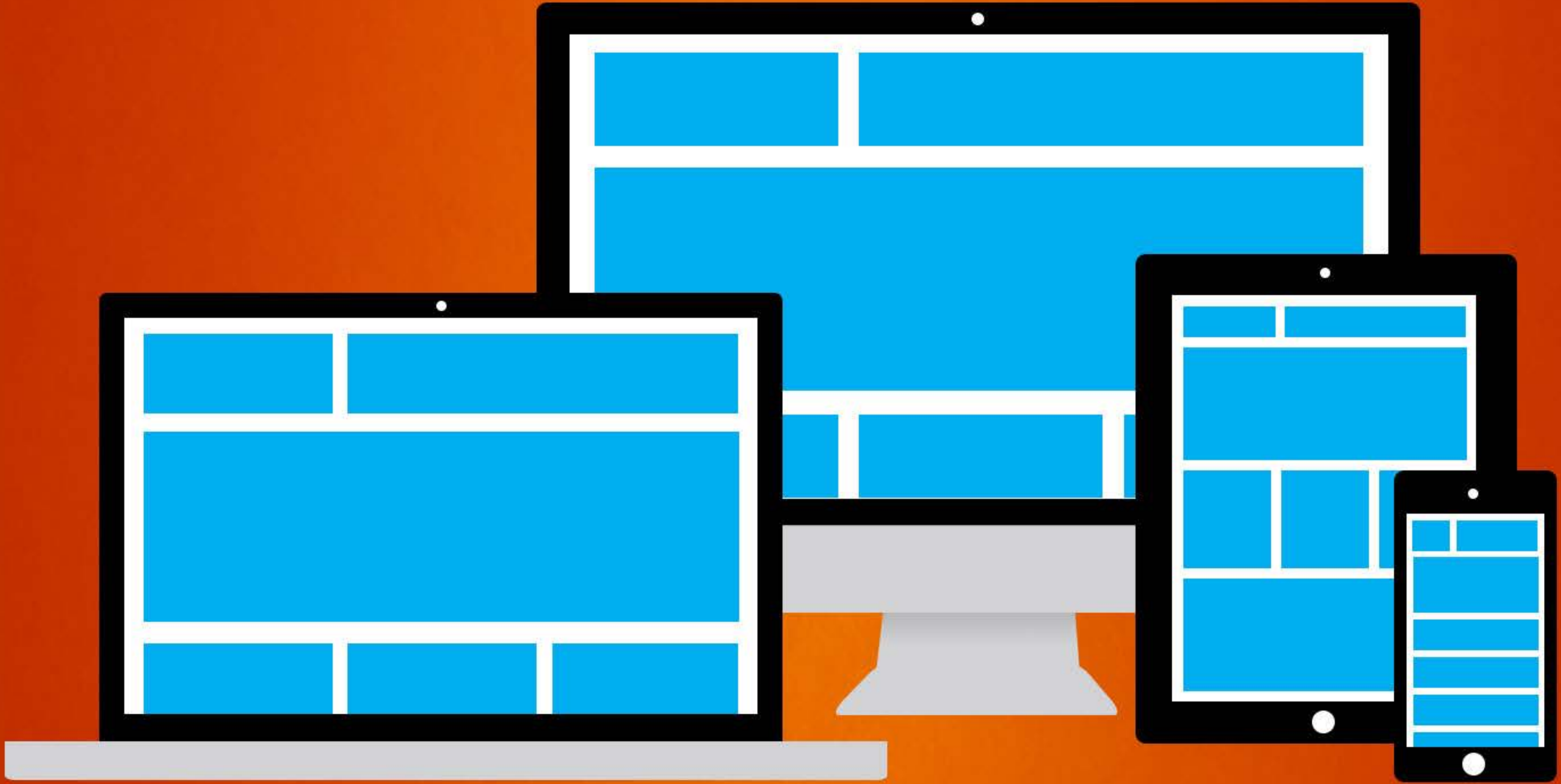
Trust chain

What are the benefits of the contextual approach? You can…

- Mobile-fuel your digital transformation
- Provide immediate personalization with privacy and risk backstops
- Save annoying security interactions for higher-risk transactions
- Enable progressive, finer-grained authorization
- Tune your risk exposure through policy

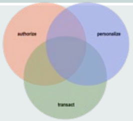
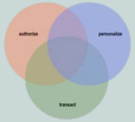


…but it doesn’t have to be a zero-sum game



Bring responsive design to authentication

Maximize your success by assessing your scenarios’ unique aspects

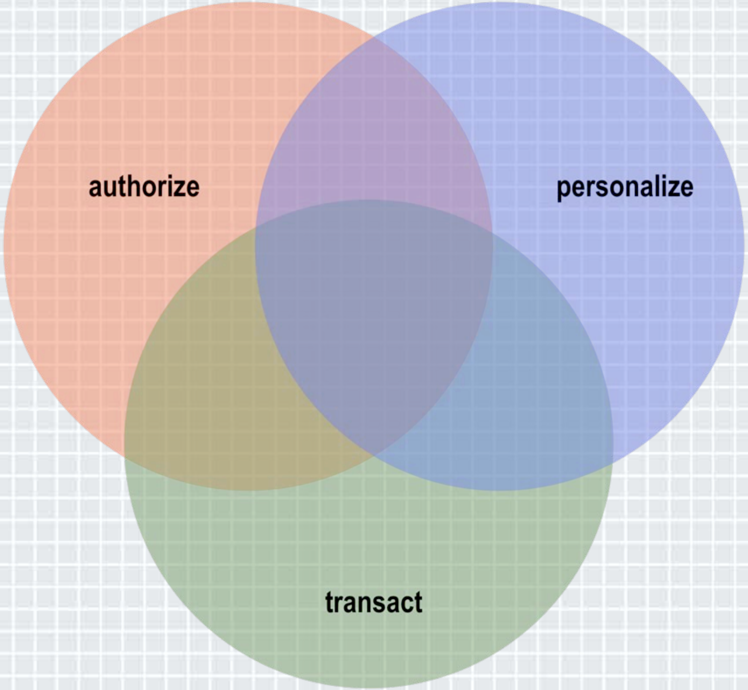
Phase	Goal	Potential tasks	Upside potential vs. downside risk
Initial approach	Create record, issue credential	Register, verify, link, set attributes	New relationship and upsell vs. identity theft
Front door		Authenticate/correlate	Routine transaction vs. fraud
High-risk transaction		Step up authentication/check attributes	High-risk/reward transaction vs. high-level fraud
In-session	Prevent takeover	Various	Convenience of long session vs. sophisticated attack
Lost credential	Prevent takeover	*High-risk + Initial approach*	Reestablished relationship vs. high-level fraud and identity theft

Kill security theater

Taking it home

Apply what you’ve learned today

- If your organization has lost sight of the identification forest for the authentication trees…
- Next week, document your concerns – you know what they are!
- Next month, research ways to fix them and reach out to your business (or operational) counterparts
  - See The Quest to Replace Passwords
- Within three months, pick the lowest hanging fruit for pilots that leverage context


authorize
personalize
transact