Identity, Payments, and Bitcoin: Big Changes Ahead

Steve Kirsch
CEO, OneID

Email: stk@oneid.com
Twitter: @stkirsch

March 3, 2014

My Focus Today

Secure Payment Authorization

Authentication = Payment Authorization (*if* you do them securely)

"Log me into HSBC.com"

- Signed, Steve

"Pay 5 Euros to Amazon for Invoice #234343"

- Signed, Steve

Same protocol for authN and authZ;
only the requested action is different

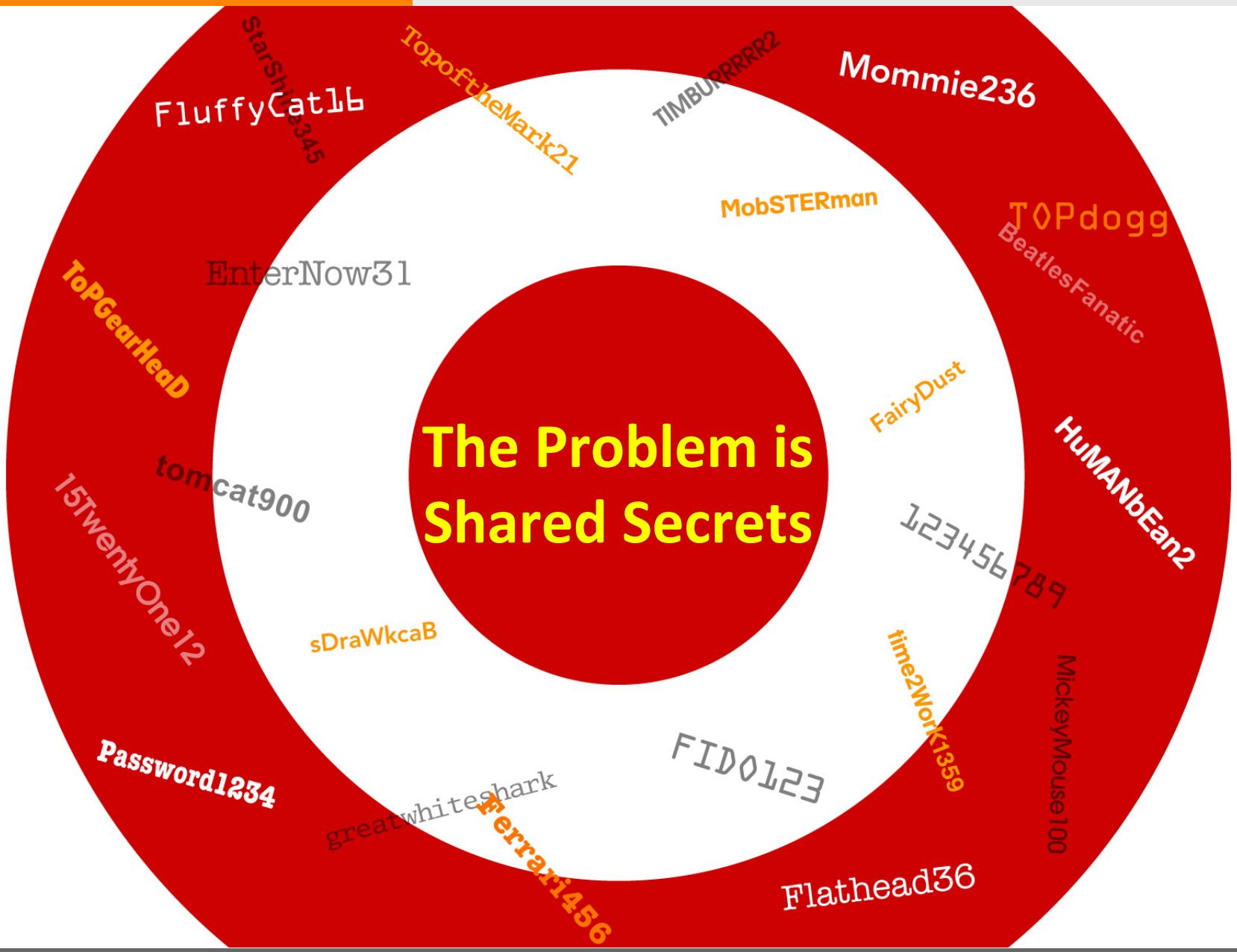
The IETF Edition

15 MYTHS

MYTH #1

There is no way to fix mass password and credit card breaches


iTunes
Hannaford
PenFed
Honda
globalpayments
altrec.com
OUTDOORS
Walgreens
The Pharmacy America Trusts
TOSHIBA
GENESCO
charles SCHWAB
CHASE
ACXIOM
ecs
reuseit.com
reusables for every part of your life
PENN STATION
EAST COAST SUBS
It's all about good taste.
cardsystems
the power of the right solution
UNM
TiVo
twitter
Dropbox
Where Restaurants Shop
Restaurant Depot
Valley National Bank
BEST BUY
Zappos.com
FIVE COUNTY
CREDIT UNION
Banking Solutions You Can Trust
Ford
J.PRESS
CollegeBoard
Principal
Financial Group
CapitalOne
bright house
NETWORKS
STEAM
citi
Google
x-rite
usbank
Genentech
ESS FOR LIFE
The Ohio State University Medical Center
serco
ascensus
SEGA
Michaels
Where Creativity Happens
GAWKER
Walmart
Save money. Live better.
DAY'S
JEWELERS
care2
make a difference
FIS
FIDELITY NATIONAL
INFORMATION SERVICES
SUBWAY
MOUNTAIN MIKE'S
PIZZA
The Hartford
ASSOCIATED
CREDIT UNION
Texas Children's Hospital
DR
Digital River
Hamilton Beach
Good Thinking
Qdoba
MEXICAN GRILL
BETHESDA
GAME STUDIOS


The Problem is Shared Secrets
StarShine345
FluffyCat16
TopoftheMark21
TIMBURRRRR2
Mommie236
MobSTERman
TOPdogg
BeatlesFanatic
EnterNow31
ToPGearHeaD
FairyDust
HuMANbEan2
tomcat900
123456789
15TwentyOne12
sDraWkcaB
time2WorK1359
MickeyMouse100
FID0123
Password1234
greatwhiteshark
Ferrari456
Flathead36

The Problem is Magnified

50% of users use the same password EVERYWHERE

Password1

Password1

Password1

Password1

How Do We Solve the Problem Once and For All?

What We Need

Solution is Easy!

OTP

TOTP

OAUTH

SS#, DOB

Pet's name

Tokenization

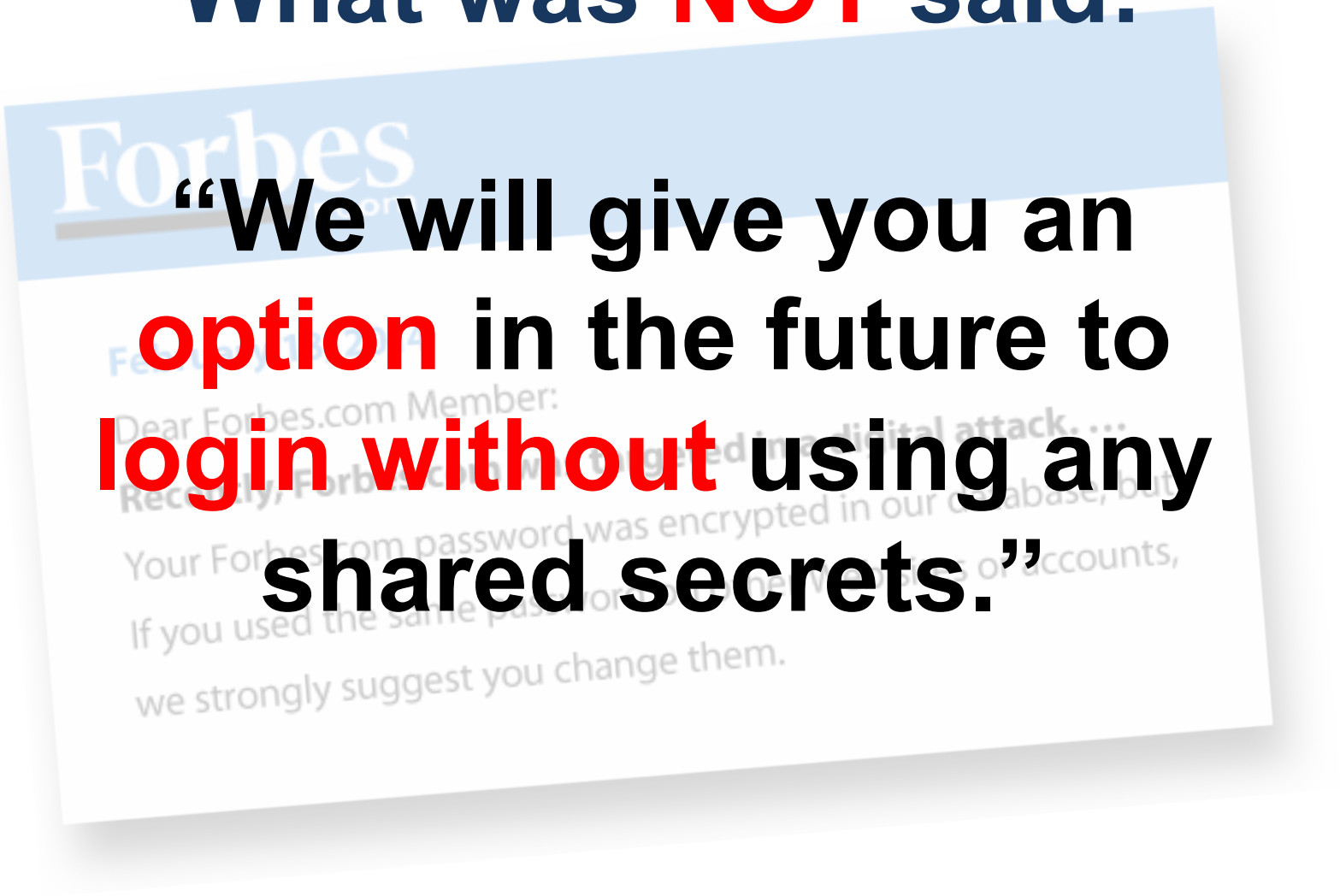
API key

- **Replace all those shared secrets with digital signatures. Duh!**

- Solutions have been available for years …
- So why aren't we using them?


Forbes
.com
February 18, 2014
Dear Forbes.com Member:
Recently, Forbes.com was targeted in a digital attack. ...
Your Forbes.com password was encrypted in our database, but
If you used the same password on other Web sites or accounts,
we strongly suggest you change them.

What was NOT said:



“We will give you an option in the future to login without using any shared secrets.”

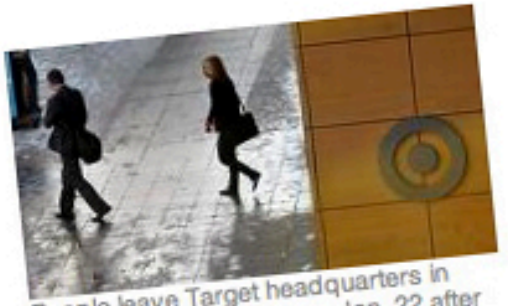
Change is Hard...
Even for a Billion Dollars!

Analyst sees Target data breach costs topping $1 billion

By Tom Webb
twebb@pioneerpress.com
POSTED: 01/30/2014 12:01:00 AM CST
UPDATED: 01/31/2014 09:59:14 AM CST

Two months into the Target security breach, fraud is turning up on 10 percent to 15 percent of the stolen card accounts, a security specialist says.

Based on that brisk level of criminal activity, one Wall Street [illegible] of the 40 million stolen



People leave Target headquarters in downtown Minneapolis on Jan. 22 after [illegible] announced layoffs. (Pioneer

AFAIK

Not one company which has been breached has **EVER** offered consumers the option of logging in (or storing their credit card info) without using any **shared secrets**.

Not One.

EVER.


Changing Behavior is HARD

Pick an Excuse for Inaction from this Handy "Feel Good" List

1. We are not interested in hearing about your solution.
2. We are too busy right now to look into this.
3. This is not on the priority list for this year
4. You don't have enough users yet to make this interesting to us
5. We aren't allowed to use this because you have to be FICAM approved (and you can't be FICAM approved because you don't have enough users)
6. Conventional wisdom solution is 2FA; I'm sticking to what the consultants tell me
7. Nobody talks about this at RSA so this can't be credible
8. What if your servers are down?
9. So what's the difference between shared secrets and digital signature again?
10. Google Authenticator is secure and free. Why do I need this?
11. I can't tell the difference between OOB vs. in-band 2FA
12. Not aware of the solution
13. It's new and different, FUD
14. Nobody else is using it so it can't be good
15. "Our users aren't asking for it"
16. This will be too hard for our users to use
17. How can we trust you?
18. I am worried this might reduce security
19. Our internal team is making the decision and your solution was not invented here

MYTH #2

Adopting 2FA eliminates password breaches

2FA Prevents Keylogging Attacks…

- **…but does NOTHING to prevent mass breaches because (99% of the time) 2FA/browser token is just another shared secret!**
- **Users get frustrated**
- **Few users adopt** (unless forced to)
- **Users hate it**
- **There are safer and easier ways**

MYTH #3

This is OOB 2FA.
Banks use this
(So it must be safe)

That's in-band 2FA!

- **Enter code on the *same* computer…**
- **MITM, MITB single point attackable**
- **Not digitally signed**

  Like signing a blank check

In-band 2FA/MFA has not reduced fraud!

Home > Articles

FFIEC Guidance: Has It Reduced Fraud?

Two Years Later, Experts Weigh In on Authentication Updates

By Tracy Kitten, July 12, 2013. Follow Tracy @FraudBlogger

Email Tweet Like Share

Username

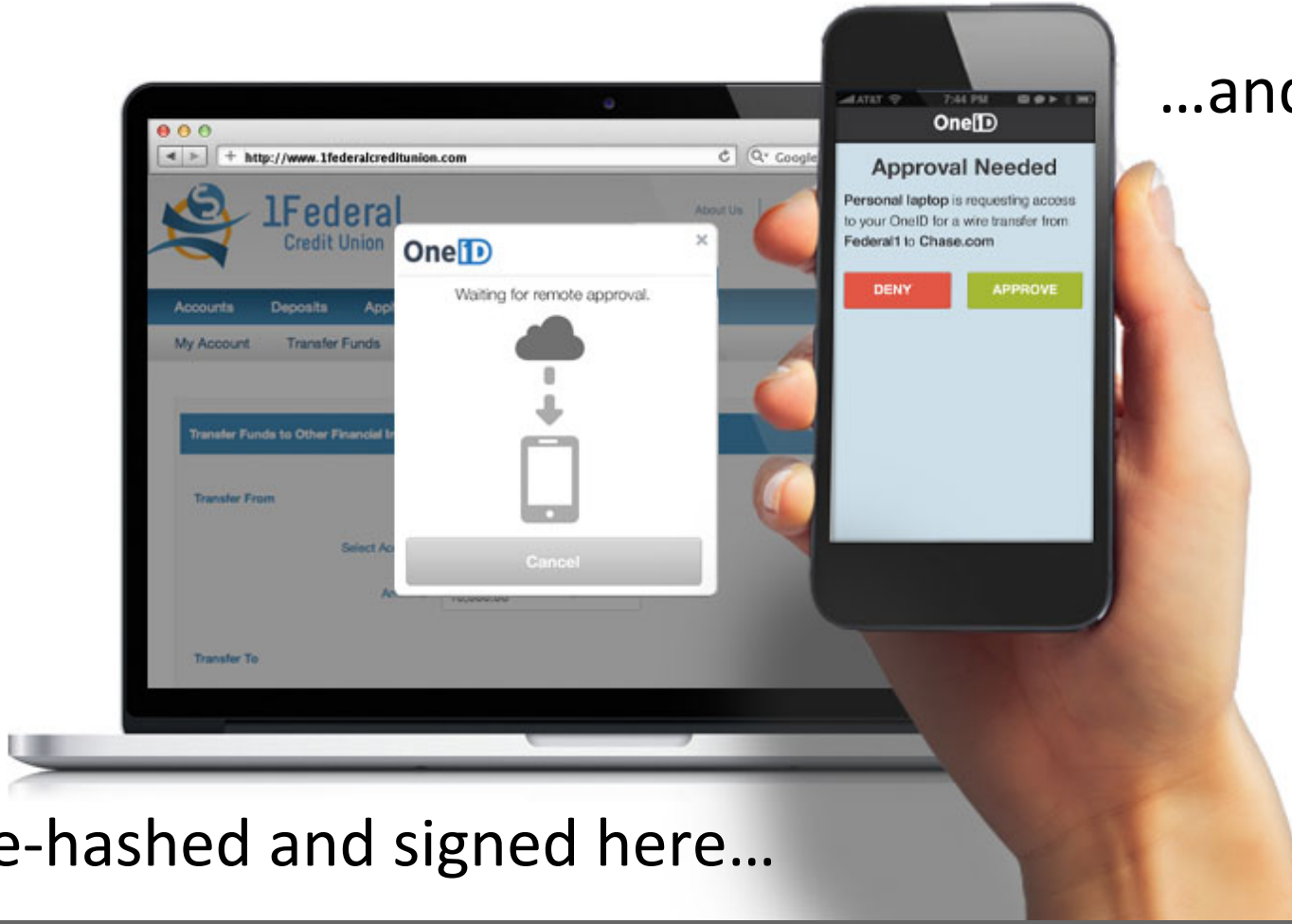
login

Password

Two years after federal banking regulators issued updated guidelines aimed at enhancing **authentication** for online-banking transactions, *BankInfoSecurity* asked industry leaders whether that new guidance has been effective at curbing account takeover losses.

Federal banking regulators declined to comment about the progress they've seen since June 2011, when the updated guidance was issued. But according to financial fraud analysts, vendors and bankers, the

This is an Example of OOB 2FA

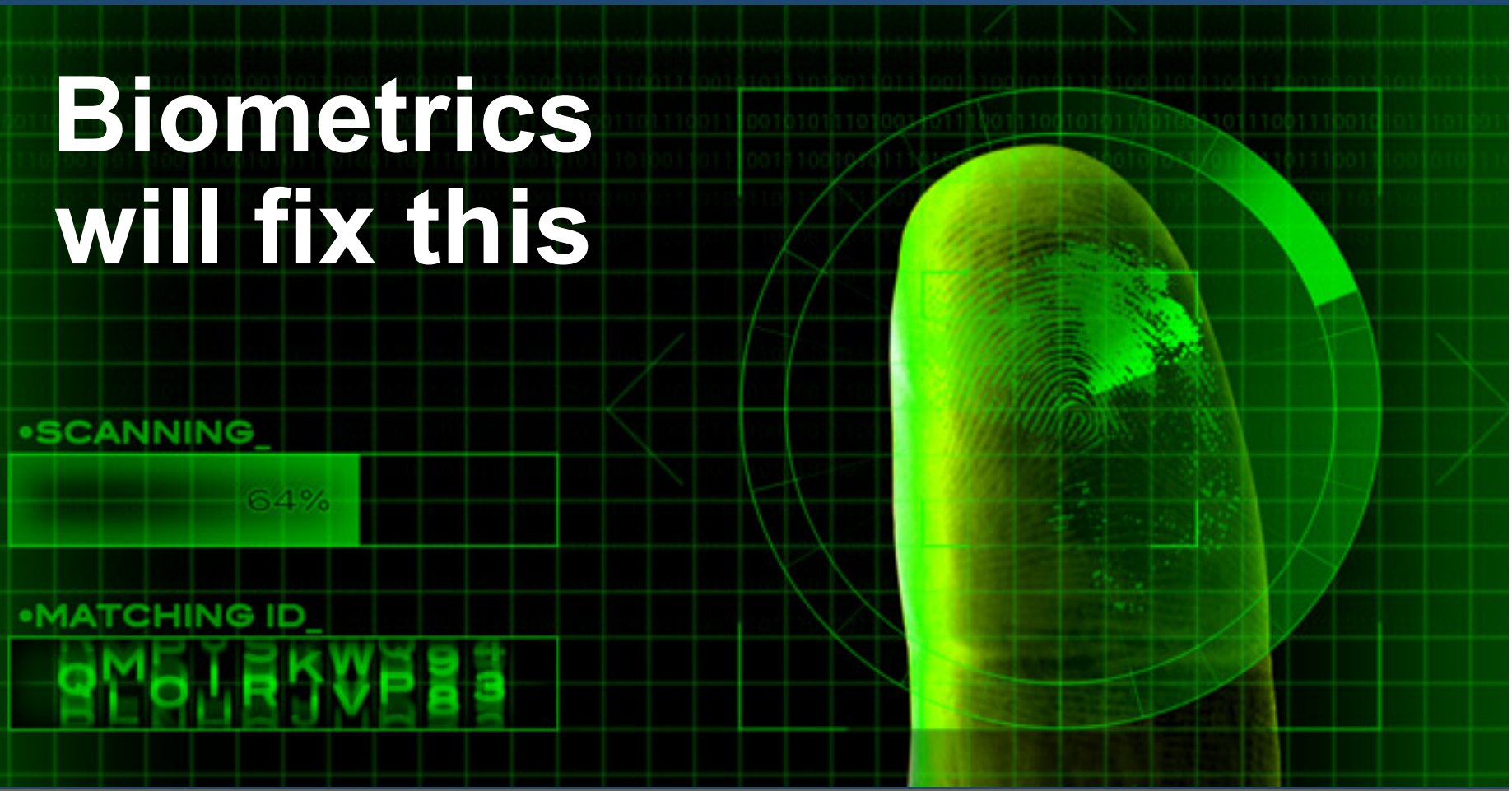


…and here

Re-hashed and signed here…

MYTH #4

Biometrics will fix this



Biometrics are a “Shared un-Secret”

- **Biometrics are like a password you cannot change**
- **Biometrics *ARE* useful locally …**
- **…if the relying party controls the reader**

MYTH #5

Storing credit cards can’t be made secure

World's safest PCI compliant vault

- **Use crypto secret on user's device to encrypt the card**
- **Store in federated identity** (in cloud)
- **When need to purchase, the user's device asks for the encrypted card data, decrypts it, passes it to merchant**
- **Over 50 NGOs using Salsa Labs are using this method today for donations**

World's Safest PCI Compliant Vault

Decryption Key
(never leaves user's device)

MYTH #6

Passwords are Bad

Passwords are Inherently Good

- **Passwords are 1 of 3 factors: "something you know"**

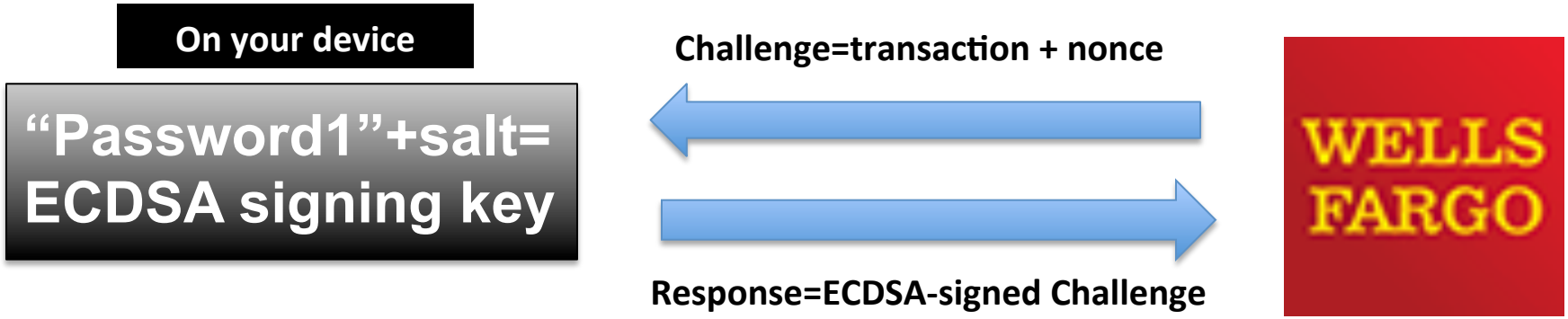
  Why would we want to eliminate that?!?
- **The problem is not passwords *per se***
- **The problem is how we use them**

"Password1" → WELLS FARGO

WRONG

(as a shared secret)

Right Way (pwd, PIN)



Combine password (or PIN) with local high entropy salt and use that as private ECDSA signing key.
Password/PIN NEVER leaves your device. NEVER!

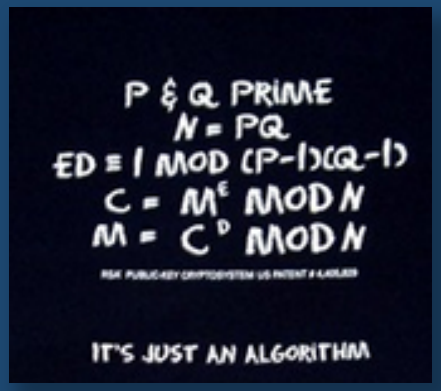
Short Passwords are Just Fine (When they aren't Shared Secrets)

- **My OneID username is:**
  `stk@oneid.com`
- **My password is:**

  `x`
- **Try to log in as me ☺**

MYTH #7

PKI, RSA Crypto, and EMV are all safe



Well…Not as Safe as you Thought

- **PKI**
  - Not end-to-end secure.
  - Proof: DigiNotar. QED.
- **RSA Crypto**
  - May be broken soon
  - Use ECC and ECDSA
- **EMV**
  - Not end-to-end secure
  - You do not know what you are approving

DigiNotar
Internet Trust Services


Math Advances Raise the Prospect of an Internet Security Crisis

Academic advances suggest that the encryption systems that secure online communications could be undermined in just a few years.

By Tom Simonite on August 2, 2013

MYTH #8

FIDO will fix all of This

WOOF, WOOF

FIDO (Fast IDentity Online) Alliance http://www.fidoalliance.org/

FIDO is Authentication Only

- **FIDO can eliminate risk of cloning private key**
- **FIDO is authentication only, not authorization**
- **FIDO is *not* a federated identity system**

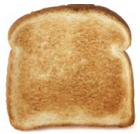
No device, key management
Point-to-point auth
If you have 10 devices and 500 RPs, painful
If you lose a device, how register the replacement everywhere?
Lots of issues left open

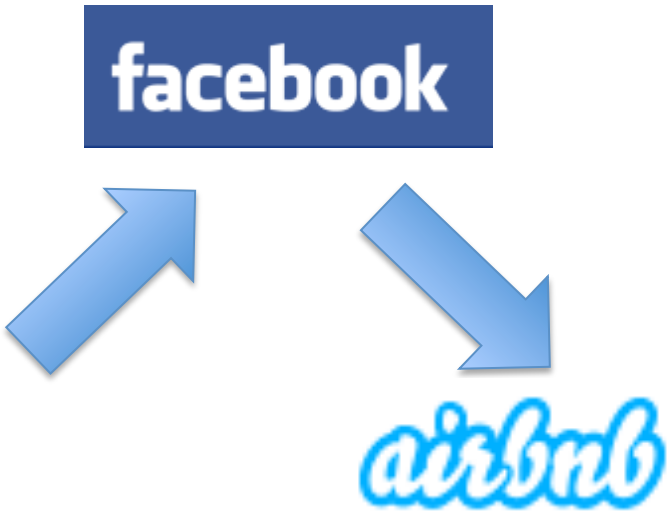
fido alliance
simpler stronger authentication

MYTH #9

All Federated Identity Providers are Untrustable

You Can't Trust Most Federated IdPs

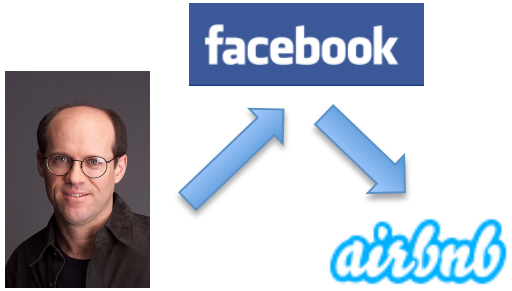
- Federated IdP examples: Facebook, Google, LinkedIn, Twitter, …
- A breach/goof @ IdP and your identity is toast 



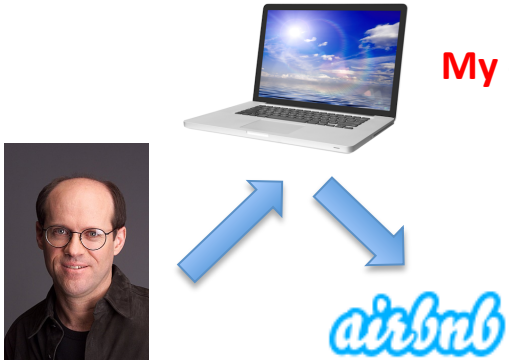
Trustable Federated Identity

- **Trustable = "IdP can't assert my identity without my express consent"** (no matter what happens @ IdP)
- **Requires a crypto secret on the user's device**

  Test: New device requires an existing device?
- **Trustable IdP uses end-to-end secure protocols**



NOT Trustable

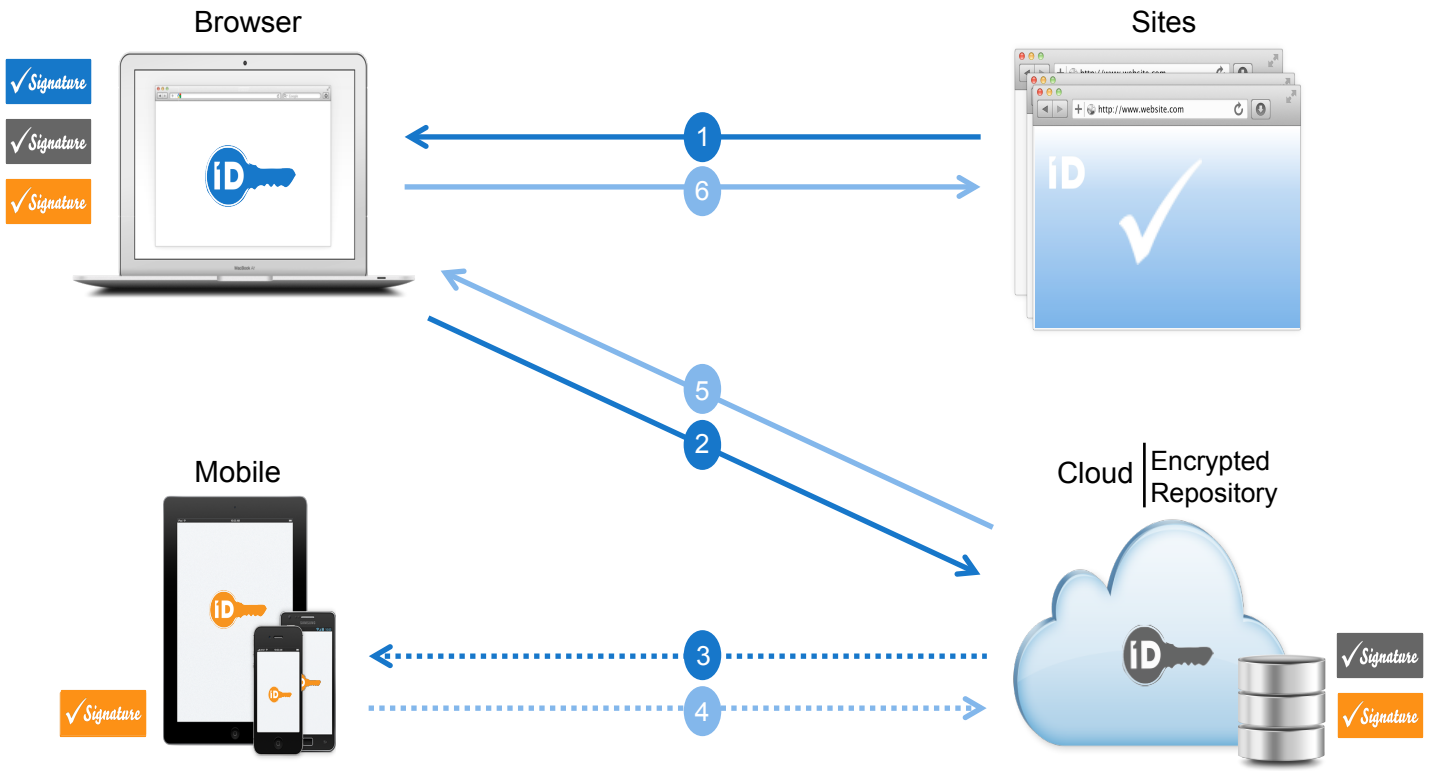


Trustable

Trustable Federated Identity (TFI)

- **Security Guaranteed by Architecture, not Operational Policy**
- **ECDSA Digital Signatures Replace all Shared Secrets**
- **Simple protocols** (complexity is the enemy of security)
- **No Single Point of Compromise**
  → Uses multiple digital signatures

A trustable federated identity: OneID



Patents granted and pending

TFI Benefits

- Store attributes securely (across all devices)
  - Private keys (e.g., for login, Bitcoin, …)
  - Secret keys
  - PII: Name, address, phone, etc.
- A user's public keys are lifetime stable @ RP
- Add 2FA to SSH, VPN
  - Simple modification to `authorized_keys` file

- One password, PIN across all sites

MYTH #10

Trustable Federated Identity is too hard to use and not as safe as Proprietary Identity

Really?! Says who?

- **TFI is so easy that most users can't tell** (feels just like "login with Facebook" button)
- **TFI is highly immune to all known threats.**
- **According to crypto security experts, for practical use, you can't get more secure than a properly designed TFI system**

MYTH #11

An IETF Standard is the Best Way to Fix This

Do not treat this presentation as a "Shared Secret"

- **Spread the word and walk the talk!**
  - **Why is IETF still using username/pwd for IETF mailing lists?**
  - **Deploy on your website, use with VPN, SSH, etc.**
  - **Share this presentation with your friends at high impact places… Target, AT&T, …**

BITCOIN MYTH #1

Bitcoin is Going to Die

New Mt. Gox logo

“Rumors of my death have been greatly exaggerated”

-*Satoshi Nakamoto*

- **Vital signs stable even after disasters**
- **Nothing on the horizon that looks lethal**


BITCOIN MYTH #2:
Bitcoin is the Future of Payments

The Future is End-to-End Secure Payments

- **Bitcoin is just a crypto currency**

  It may or may not be THE winner

- **The winner will be**

  Digitally signed end-to-end secure transactions

  Open APIs, simple money transfer protocol

```
Send(1.32, "BTC", "Amazon", "Invoice 123")
```

BITCOIN MYTH #3

Bitcoin Can't be Regulated

Bitcoin can be made compliant

- **Companies are being started now to solve the Bitcoin compliance problem in a new way that the regulators *really* like**
- **Can protect consumers from another Mt. Gox and Bitinstant disaster**

cointrust

BITCOIN MYTH #4

It is safe to keep my Bitcoin in Coinbase or Bitstamp

Steve Kirsch,
You were mentioned in a Tweet!

Aaron Pressman @ampressman

Follow

Smart: "If you have any amount [of bitcoins] in any of the exchanges today, you're a fool," @stkirsch warned 12/31/13 technologyreview.com/news/522411/bi...

06:12 PM - 26 Feb 14

Reply to @ampressman Retweet Favorite

Coinbase and Bitstamp Use the Same Protection as Mt Gox: In-band 2FA

- Can you say “shared secrets”?
- Susceptible to mass breach and malware on your computer
- Recommendation: Only keep as much as you can afford to use.
- I use “Bitcoin Armory”
- Safe *and* easy coming in 2014

How Can the IETF Help?

I'm not sure yet

Contact

stk@oneid.com

Steve Kirsch on LinkedIn