Trusted Identities for Electronic Health Records
A National Strategy

Jeremy Grant

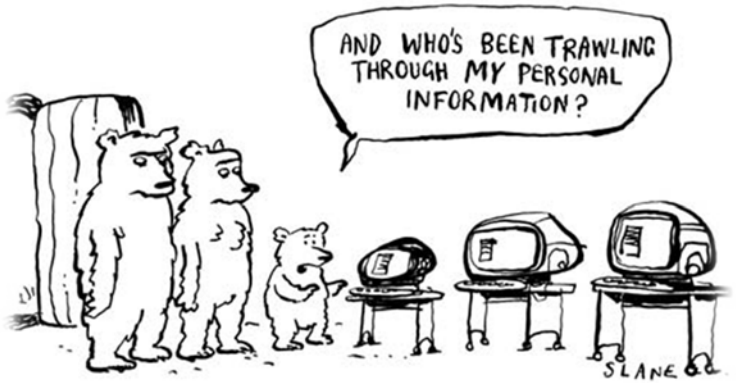
Senior Executive Advisor, Identity Management

National Strategy for Trusted Identities in Cyberspace (NSTIC)

National Institute of Standards and Technology (NIST)

Why does digital identity matter to health care?

Identity is central to…



Why does digital identity matter to health care ?

Identity + Authentication challenges abound:

- Providers and patients juggling multiple credentials to access different resources…many lacking sufficient security
- Identity verification is essential to ensure proper delivery of care and protect privacy
- Need for repeatable, standards-based solutions that scale to very small and large entities

Sharing data is good.

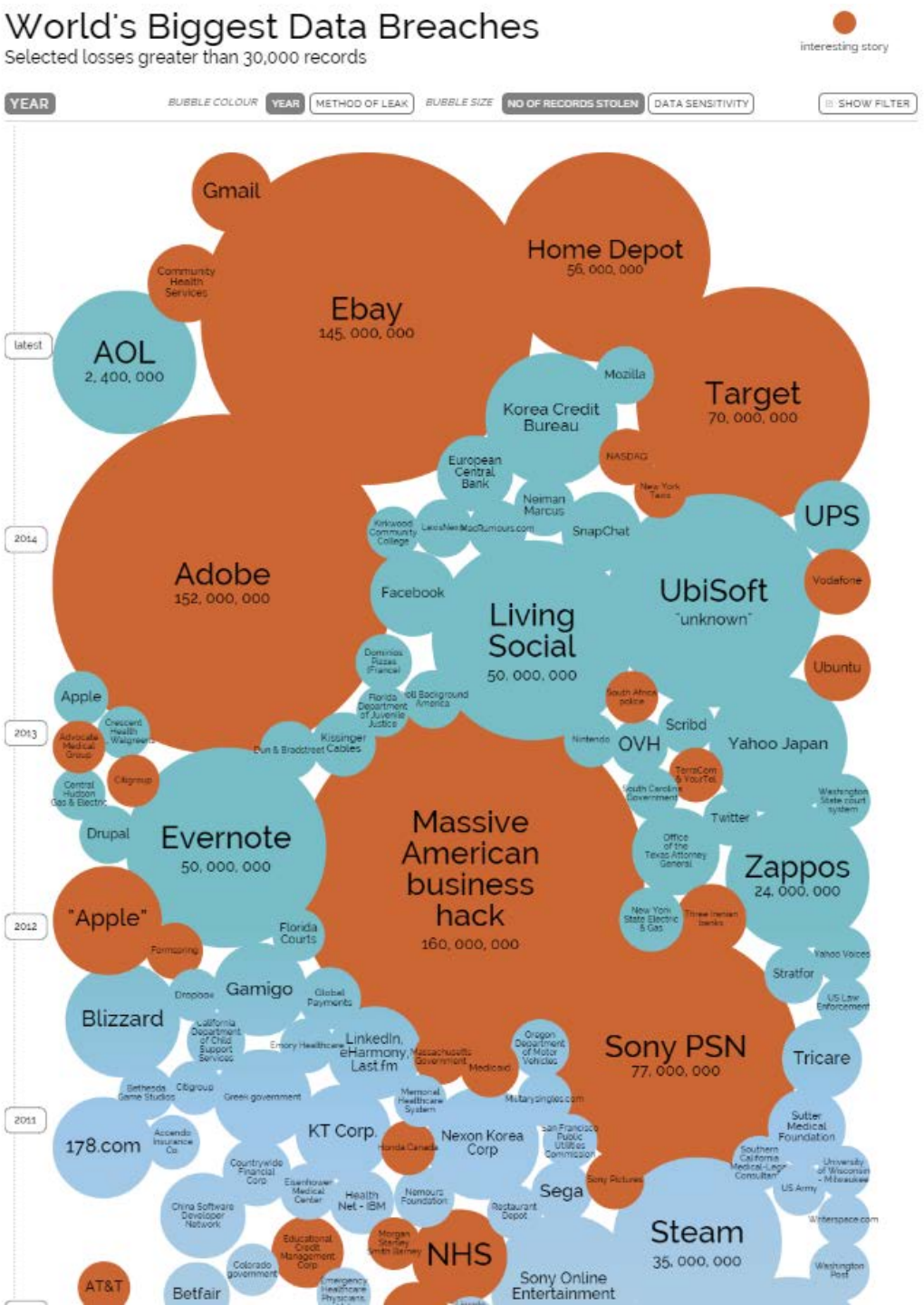
Sharing personal data is really good…

…with the right person.

But after 21 years, we still struggle with this.

"On the Internet, nobody knows you're a dog."

And now we've got this happening.



http://www.informationisbeautiful.net/visualizations/worlds-biggest-data-breaches-hacks/

And now we've got this happening.

Russian Hackers Amass Over a Billion Internet Passwords

By NICOLE PERLROTH and DAVID GELLES AUG. 5, 2014

Email
Share
Tweet
Save
More

A Russian crime ring has amassed the largest known collection of stolen Internet credentials, including 1.2 billion user name and password combinations and more than 500 million email addresses, security researchers say.

The records, discovered by Hold Security, a firm in Milwaukee, include confidential material gathered from 420,000 websites, including household names, and small Internet sites. Hold Security has a history of uncovering significant hacks, including the theft last year of tens of millions of records from Adobe Systems.

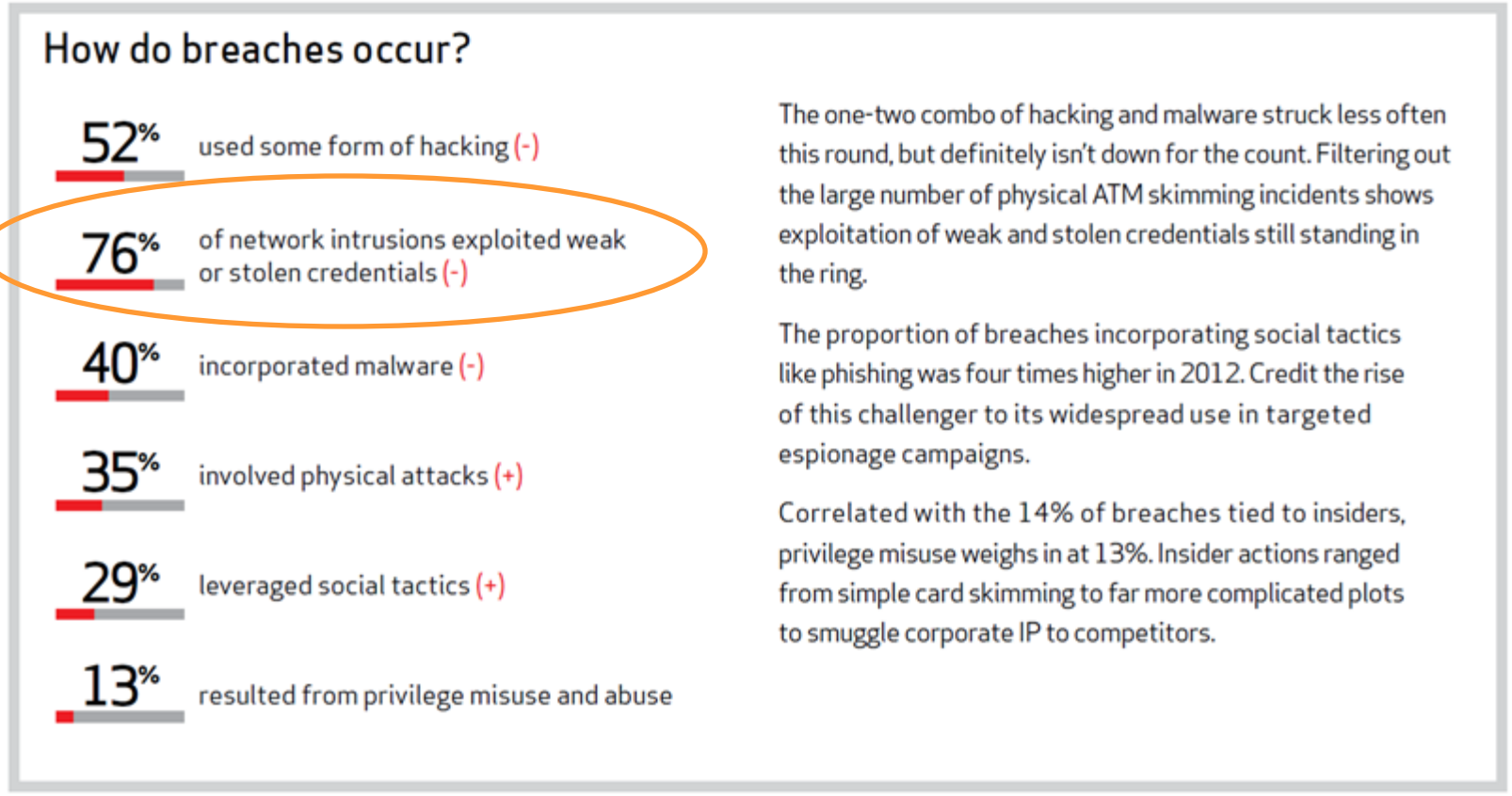
TECH 9/02/2014 @ 3:00AM | 91,809 views

iCloud Data Breach: Hacking And Celebrity Photos

+ Comment Now + Follow Comments

A few days ago a group calling themselves hackappcom posted a proof of concept script on the popular code repository called Github that would allow for a user to attempt to breach iCloud and access a user account. This script would query iCloud services via the "Find My iPhone" API to guess username and password combinations. The problem here was that apparently Apple AAPL -0.06% was not limiting the number of queries. This allowed for attackers to have numerous chances to guess password combinations without the fear of being locked out.

Securing personal data with just a password is a bad idea.



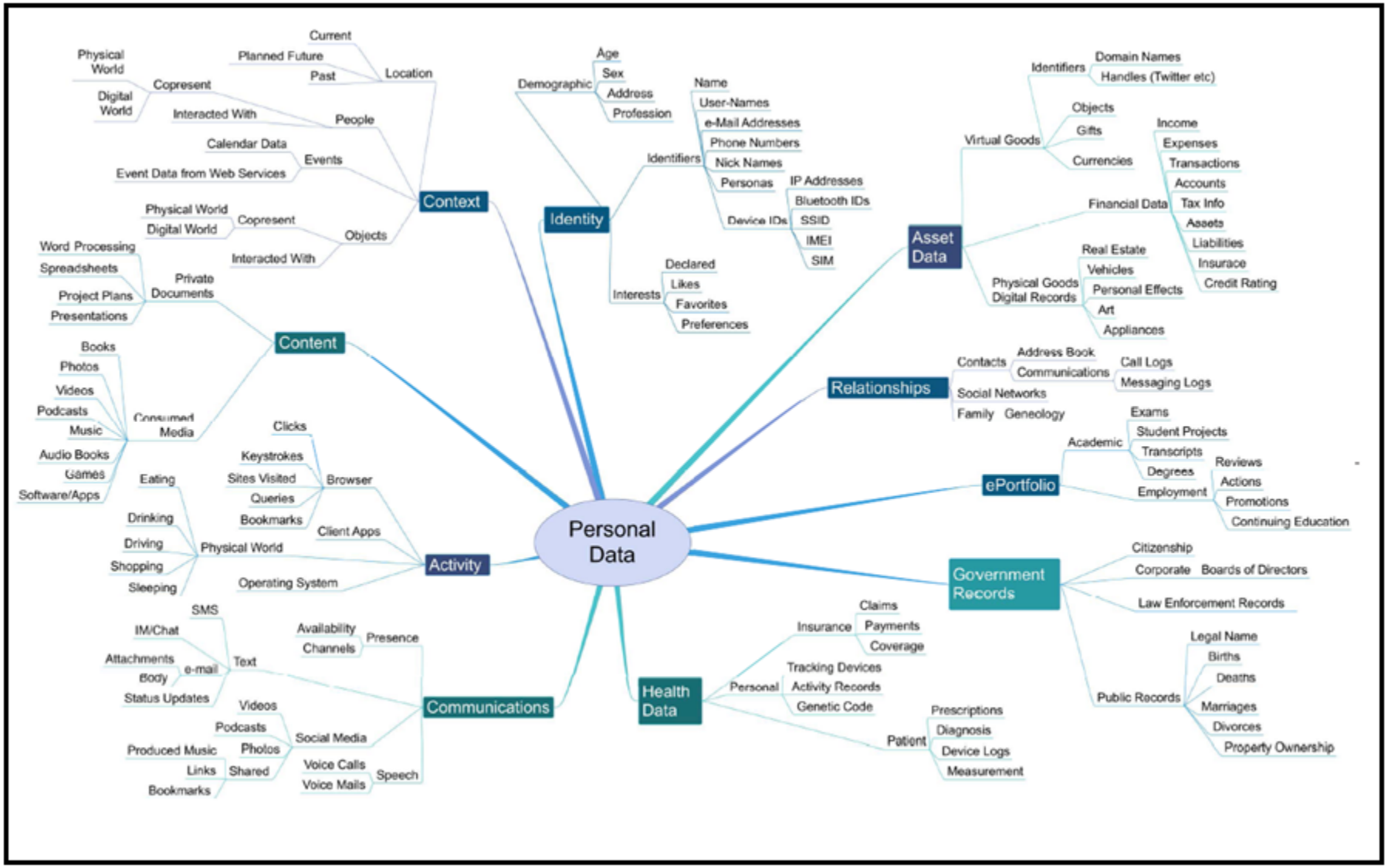
Source: 2013 Data Breach Investigations Report, Verizon and US Secret Service

Multi-Factor Authentication Matters.

Passwords Aren't Just Bad for Security

- 75% of customers will avoid creating new accounts.
- 54% leave the site or do not return when asked to create a new password
- 45% of consumers will abandon a site rather than attempt to reset their passwords or answer security questions

And…privacy is a growing concern



Source: World Economic Forum, *"Rethinking Personal Data: Strengthening Trust,"* May 2012

Trust matters to online business

$2 Trillion

The total projected online retail sales across the G20 nations in 2016

$2.5 trillion

What this number can grow to if consumers believe the Internet is more worthy of their trust

$1.5 Trillion

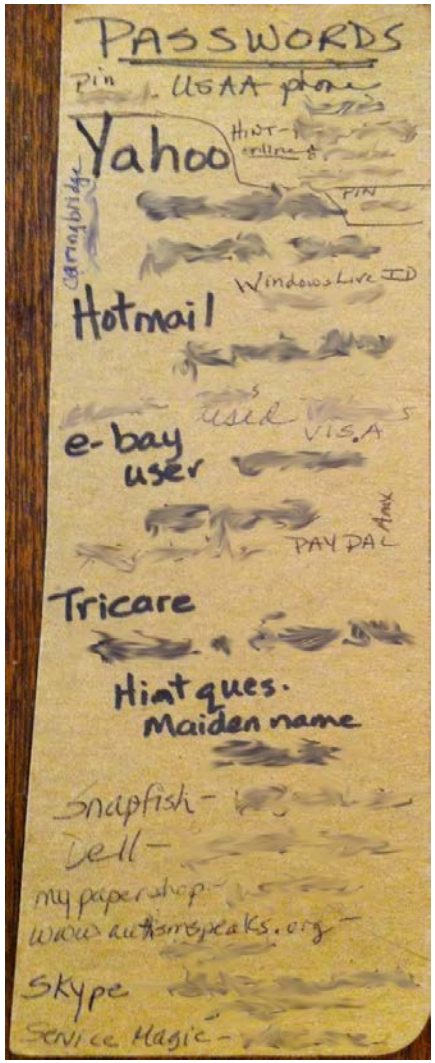
What this number will fall to if Trust is eroded

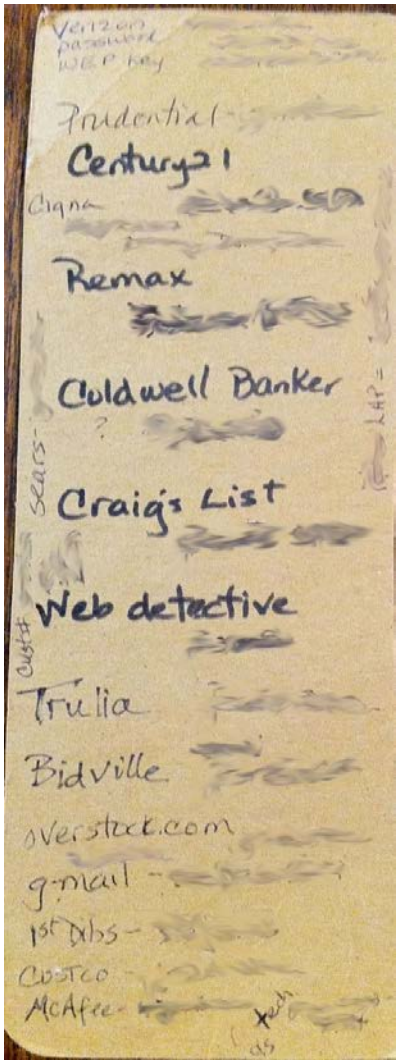
Source: *Rethinking Personal Data: Strengthening Trust*. World Economic Forum, May 2012.

Health could try to solve this with a siloed approach.

But…

When consumers already manage this:

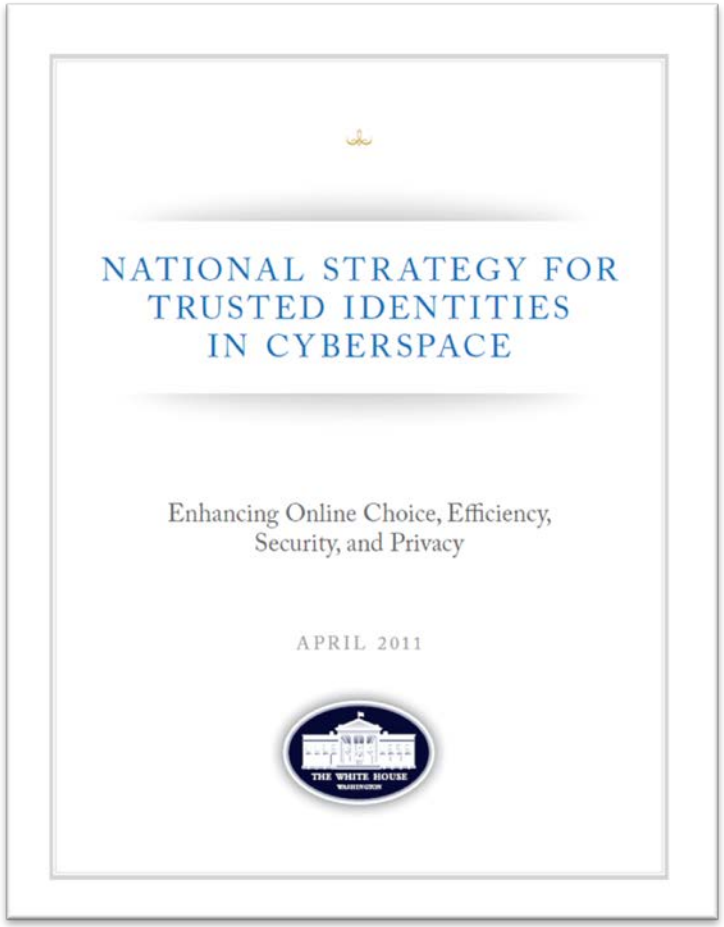




They aren't eager to add another.

Consumers should be able to use a single, secure, convenient, privacy-enhancing credential across multiple sites – public and private – in lieu of passwords.

The President agrees.



NSTIC calls for an **Identity Ecosystem**, "an online environment where individuals and organizations will be able to trust each other because they follow agreed upon standards to obtain and authenticate their digital identities."

Guiding Principles

Identity solutions will be privacy-enhancing and voluntary

Identity solutions will be secure and resilient

Identity solutions will be interoperable

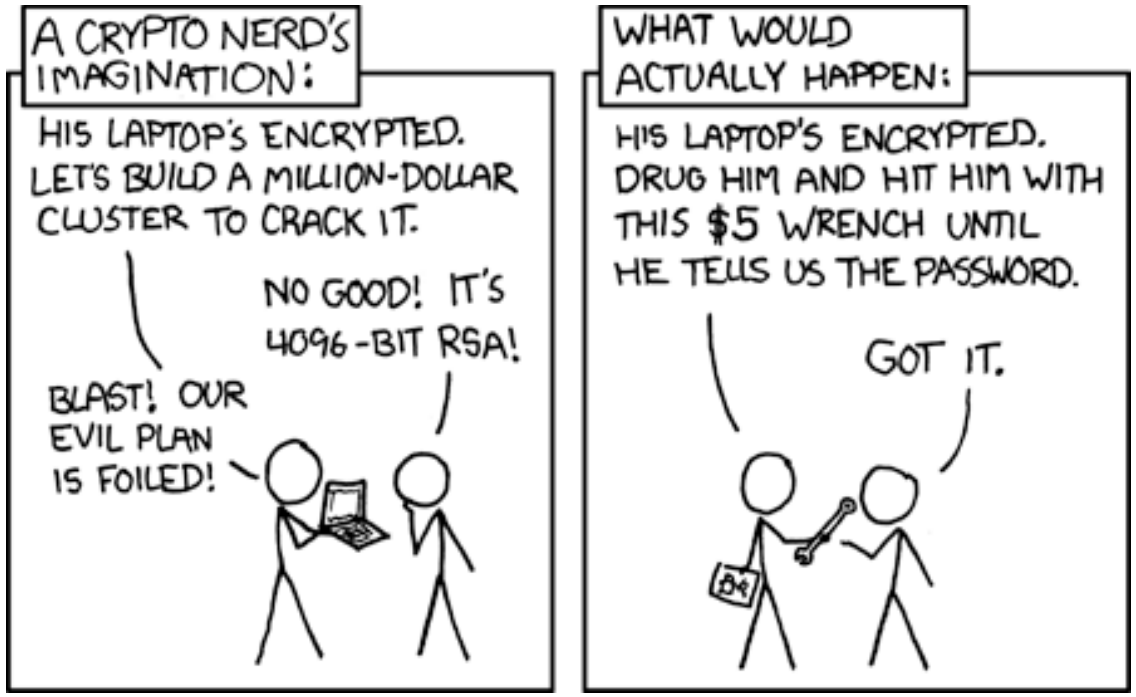
Identity solutions will be cost-effective and easy to use

National Strategy for Trusted Identities in Cyberspace

Why NSTIC?

There is a marketplace today – but there are barriers the market has not yet addressed on its own

It’s not all about security



Source: *xkcd*

Usability

Liability

Privacy

Business Models

Interoperability

Why NSTIC?

There is a marketplace today – but there are barriers the market has not yet addressed on its own.

Government can serve as a convener and facilitator, and a catalyst.

What does NSTIC call for?

Our Ultimate Goal

Catalyze the marketplace – so that all Americans can soon choose from a variety of new types of solutions that they can use in lieu of passwords…

…for online transactions that are more secure, convenient and privacy-enhancing.

Key Implementation Steps

Convene the Private Sector

- August 2012: Launched privately-led **Identity Ecosystem Steering Group (IDESG).** Funded by NIST grant, IDESG tasked with crafting standards and policies for the Identity Ecosystem Framework http://www.idecosystem.org/
- October 2013: IDESG incorporates as 501(c)3, prepares to raise private funds
- July 2014: NIST awards IDESG Inc. follow-on grant

Fund Innovative Pilots to Advance the Ecosystem

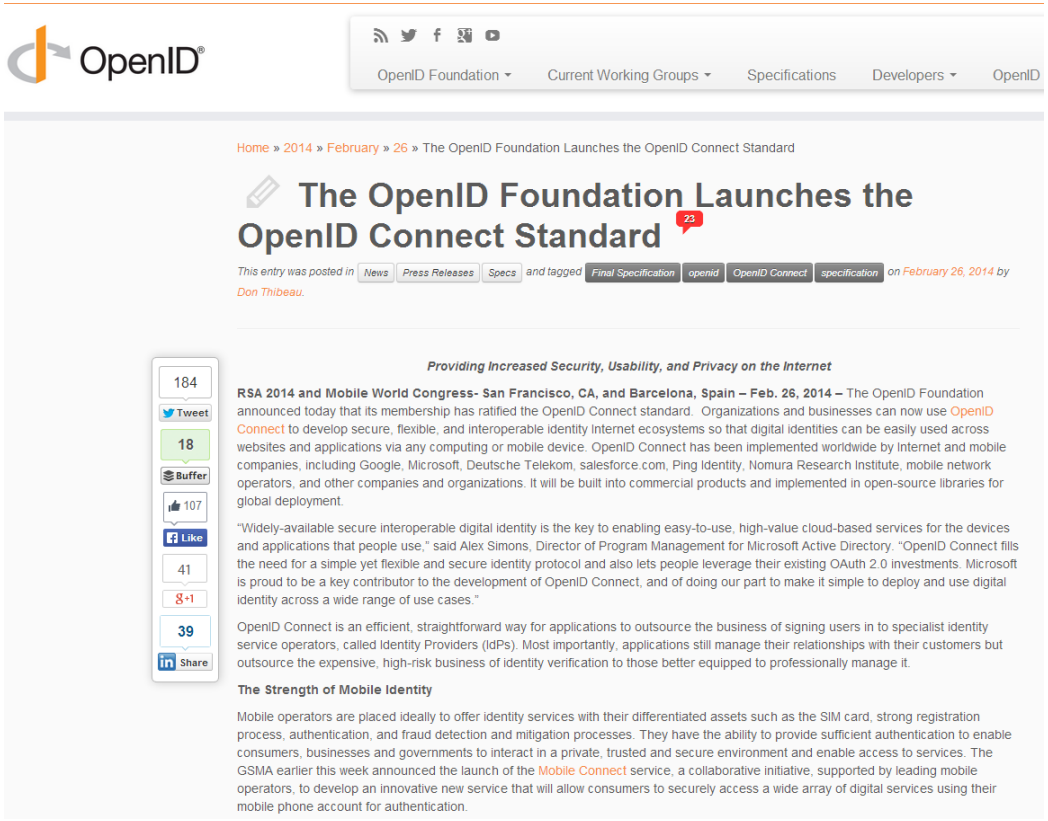
- Three rounds of pilot grants in 2012 and 2013; **10 pilots now active**
- 3 new awards due next month.

Government as an early adopter to stimulate demand

- White House effort to create a **Federal Cloud Credential Exchange** (FCCX)
- Last summer: USPS awards FCCX contract; Now: rethink how USG buys identity services
- Next month: FCCX goes live! FedRAMP certified. Rename as "Connect.gov"

Where do we stand?

The marketplace has started to respond



OpenID®

OpenID Foundation ▾ Current Working Groups ▾ Specifications Developers ▾ OpenID

Home » 2014 » February » 26 » The OpenID Foundation Launches the OpenID Connect Standard

The OpenID Foundation Launches the OpenID Connect Standard

This entry was posted in News Press Releases Specs *and tagged* Final Specification openid OpenID Connect specification *on February 26, 2014 by Don Thibeau.*

184 Tweet 18 Buffer 107 Like 41 +1 39 Share

Providing Increased Security, Usability, and Privacy on the Internet

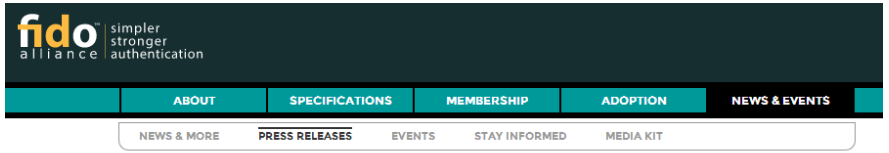
RSA 2014 and Mobile World Congress- San Francisco, CA, and Barcelona, Spain – Feb. 26, 2014 – The OpenID Foundation announced today that its membership has ratified the OpenID Connect standard. Organizations and businesses can now use OpenID Connect to develop secure, flexible, and interoperable identity Internet ecosystems so that digital identities can be easily used across websites and applications via any computing or mobile device. OpenID Connect has been implemented worldwide by Internet and mobile companies, including Google, Microsoft, Deutsche Telekom, salesforce.com, Ping Identity, Nomura Research Institute, mobile network operators, and other companies and organizations. It will be built into commercial products and implemented in open-source libraries for global deployment.

"Widely-available secure interoperable digital identity is the key to enabling easy-to-use, high-value cloud-based services for the devices and applications that people use," said Alex Simons, Director of Program Management for Microsoft Active Directory. "OpenID Connect fills the need for a simple yet flexible and secure identity protocol and also lets people leverage their existing OAuth 2.0 investments. Microsoft is proud to be a key contributor to the development of OpenID Connect, and of doing our part to make it simple to deploy and use digital identity across a wide range of use cases."

OpenID Connect is an efficient, straightforward way for applications to outsource the business of signing users in to specialist identity service operators, called Identity Providers (IdPs). Most importantly, applications still manage their relationships with their customers but outsource the expensive, high-risk business of identity verification to those better equipped to professionally manage it.

The Strength of Mobile Identity

Mobile operators are placed ideally to offer identity services with their differentiated assets such as the SIM card, strong registration process, authentication, and fraud detection and mitigation processes. They have the ability to provide sufficient authentication to enable consumers, businesses and governments to interact in a private, trusted and secure environment and enable access to services. The GSMA earlier this week announced the launch of the Mobile Connect service, a collaborative initiative, supported by leading mobile operators, to develop an innovative new service that will allow consumers to securely access a wide array of digital services using their mobile phone account for authentication.



fido alliance simpler stronger authentication

ABOUT SPECIFICATIONS MEMBERSHIP ADOPTION NEWS & EVENTS

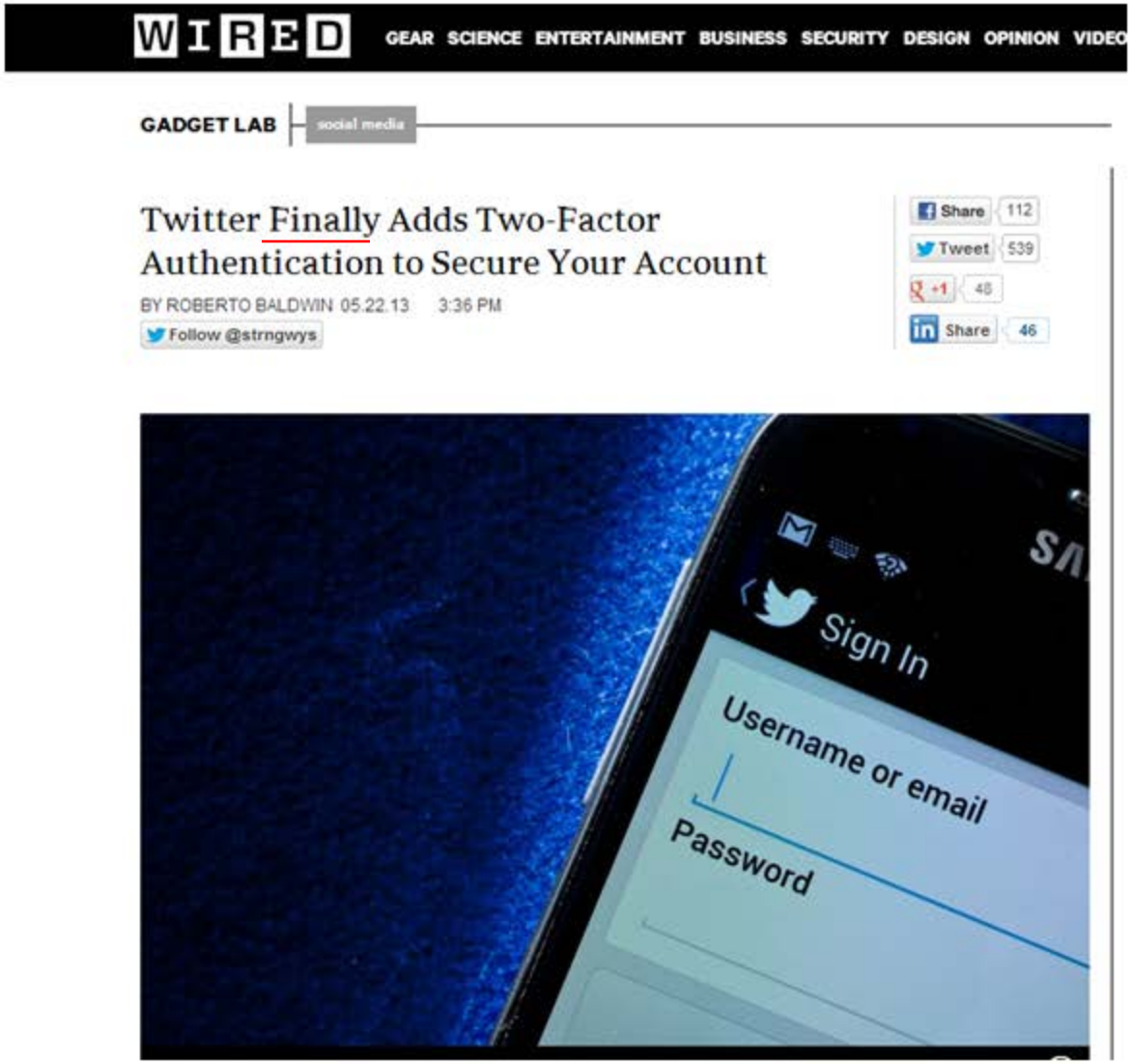
NEWS & MORE PRESS RELEASES EVENTS STAY INFORMED MEDIA KIT

FIDO Alliance Opens Technology for First Public Review to an Industry Desperate for Simpler, Stronger Authentication

Mountain View, CA - February 11, 2014 - The FIDO (Fast IDentity Online) Alliance (http://www.fidoalliance.org/), an open industry consortium delivering standards for simpler, stronger authentication, achieved a historic milestone today by releasing its first public review draft technology specifications. These open technologies have been collaboratively developed by a rapidly increasing number of the most innovative companies in the world to enable simpler, stronger authentication to scale in the market.

The Q1 2013 Forrester Wave™: Enterprise Fraud Management asserts the online services industry is seeing upwards of $200B in annual losses from password breaches and related hacks that exploit the vulnerabilities inherent in single-factor password systems. According to the Verizon 2013 Network Investigations Data Breach Report, 76 percent of network intrusions exploit weak or stolen credentials. According to Gartner, 20 to 50 percent of all help desk calls are for password resets. Forrester Research estimates help desk labor cost at $70 per password reset*. In Mobile Consumer Insights, Jumio reports that 68 percent of smartphone and tablet owners have attempted to make purchases on their device. Due to problems during

The marketplace has started to respond



But I now am managing one-off 2FA solutions for

The Good News

- **This can be fixed – with a Framework of standards and operating rules that enables interoperability**
- **Both at a technical and policy level**

The Identity Ecosystem Steering Group

Source: Phil Wolff, http://www.flickr.com/photos/philwolff/7789263898/in/photostream

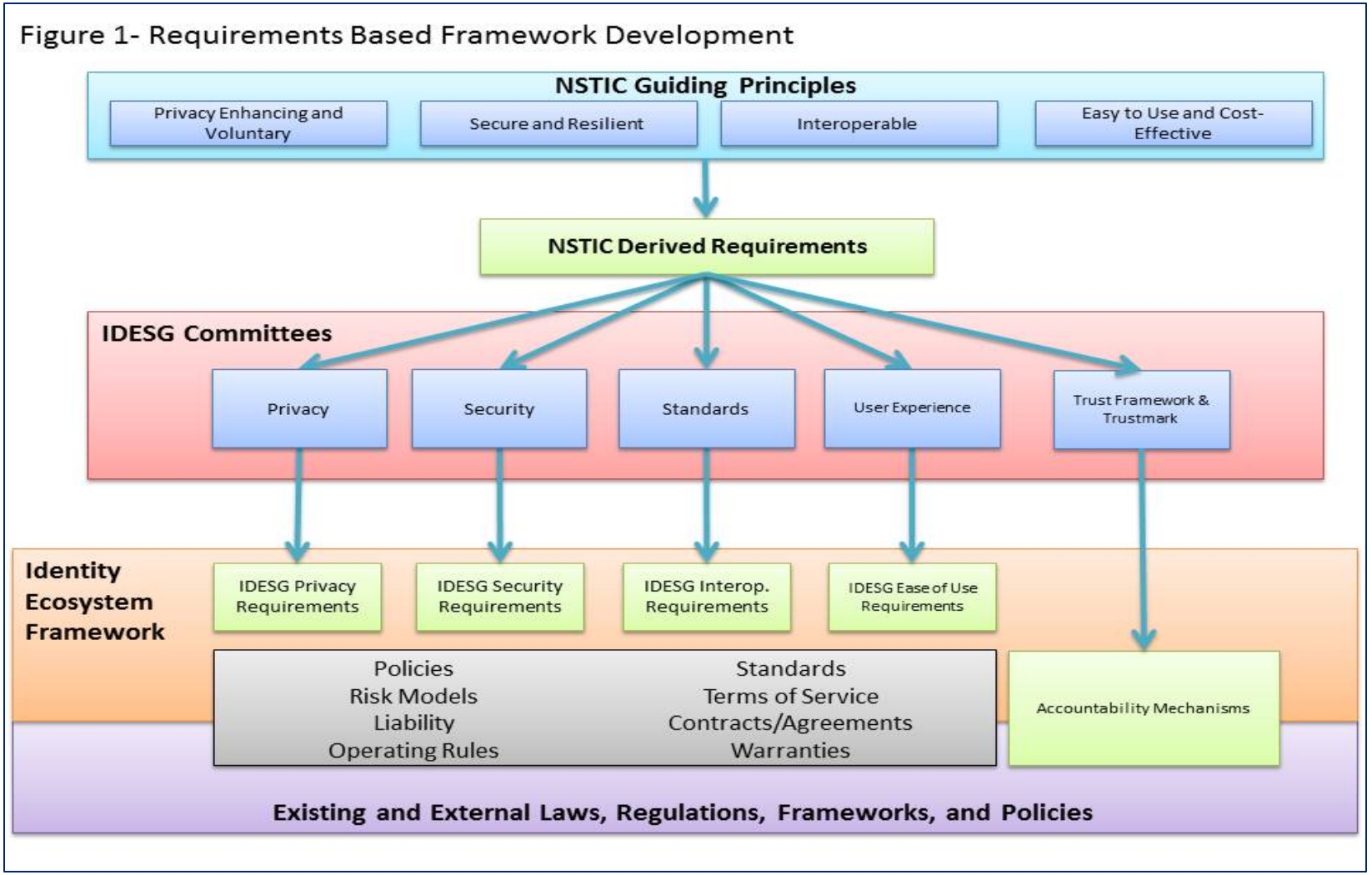
Identity Ecosystem Steering Group (IDESG)

- 200+ firms/organizations; 60+ individuals
- Elected Plenary Chair (Kim Little/LexisNexis) and Management Council Chair (Peter Brown); Elected 16 delegates to Management Council
- Member firms include: Verizon, Visa, PayPal, Fidelity, Citigroup, Mass Mutual, IBM, Bank of America, Microsoft, Oracle, 3M, CA, Symantec, Kaiser Permanente, Experian, Neiman Marcus, NBC Universal, Aetna, United Health, Intel.
- Also: AARP, ACLU, EPIC, EFF, and more than 65 universities. Participants from 12 countries.
- Committees include:
  - Standards
  - Policy
  - Privacy
  - Usability
  - Security
  - Trust Frameworks/Trustmarks
  - **Health Care**
  - Financial Sector
  - International Coordination

www.idecosystem.org

Identity Ecosystem Steering Group Progress

Private Sector Stakeholders Leading Framework Development



NSTIC Pilots are Advancing the Ecosystem

Four rounds of pilots awarded thus far

- 5 “core” NSTIC pilots in September, 2012; another 4 in September, 2013 and 3 in September, 2014
- 2 state pilots – focused on improvement of state government services – funded by Partnership Fund for Program Integrity Innovation

Among 14 pilots, 7 have some nexus with health care

NSTIC Pilots Impact

More than **140 universities** are deploying **smartphone-based MFA**, thanks to the Internet2 pilot

More than **180,000 kids** have been authorized by parents – **in compliance with COPPA** – to access content at websites (PRIVO)

Inova Health Systems is enabling **1500 patients** to securely obtain their personal health record, leveraging validated attributes from **Virginia's DMV** (AAMVA)

A Broadridge/Pitney Bowes JV has launched targeting **140 million customers** for **secure digital delivery** of financial services content, bill presentment and bill pay, enabled by the ID/Dataweb identity solution

More than **300,000 Veterans** can access online services from more than **70 organizations** without having to share documents containing sensitive PII to prove Veteran status (ID.me)

NSTIC Can Accelerate Health IT

- Health leverages a broader Identity Ecosystem – driven by **common standards** and **business rules** that cross sectors.
- Patients can use a **single trusted credential** to log on to an electronic health record application in the cloud
- Benefits
  - ✓ Increased security, privacy and convenience
  - ✓ Patients no longer need to manage numerous user names and passwords – or wrestle with their usability challenges
  - ✓ A single credential unlocks access to a provider or other health data service – both public and private – and securely enables the sharing of health information between those applications

Benefits of Standards-based Trusted Identities

- Streamlined provider and patient access to multiple systems, including via Blue Button
- Improved care through secure exchange of electronic medical records
- Secure patient access to health information
- Address “identity resolution” challenges such as patient matching via exchange of attributes…while also enhancing privacy

Collaboration with ONC: Blue Button Plus

- Blue Button Plus is looking at improving the security and privacy of patient access to their electronic health records
- This includes updating Blue Button with innovative new cloud identity architectures, such as enabling third party applications to selectively “pull” individual health record elements, with strong user controls
- To enable this, ONC is working with NSTIC on solutions that will provide secure, privacy enhancing, interoperable, and user friendly access to Blue Button Plus systems

Key Takeaways

- Don’t secure sensitive health information with only a password
- Recognize that the best approach for providers and patients is one where secure, privacy-enhancing credentials can be used interoperably across domains
- Get engaged in the Identity Ecosystem Steering Group (IDESG) (www.idecosystem.org) to help create better standardized approaches for strong identity and authentication in health care

For More Information

Jeremy Grant

Jgrant@nist.gov

+1 202.482.3050

Twitter: @NSTICNPO, #NSTIC

Blog: NSTIC Notes, http://nstic.blogs.govdelivery.com/