Improving Authentication Security

IAM Online
April 8, 2015 – 2 pm EDT

Kristin Judge, Program Lead, National Cyber Security Alliance
Jeff Shultz, Trusted Identity Analyst, National Strategy for Trusted Identities in Cyberspace
Brett McDowell, Executive Director, FIDO Alliance
Stephan Somogyi, Google
Theresa Semmens, Chief Information Security Officer, North Dakota State University
Improving Authentication Security

National Cyber Security Alliance

National Strategy for Trusted Identities in Cyberspace

FIDO (Fast IDentity Online) Alliance
NCSA's mission is to educate and therefore empower a digital society to use the Internet safely and securely at home, work, and school, protecting the technology individuals use, the networks they connect to, and our shared digital assets.

www.staysafeonline.org
NCSA Board Companies

- AT&T
- ADP
- Bank of America
- Comcast
- EMC
- ESET
- Facebook
- Google
- Intel
- McAfee
- Microsoft
- Visa
- Verizon
- Raytheon
Core Initiatives

National Cyber Security Awareness Month

RE:CYBER
POWERED BY BENS AND NCSA

DATA PRIVACY DAY

TWO STEPS AHEAD
PROTECT YOUR DIGITAL LIFE
STOP. THINK. CONNECT.™ is the national cybersecurity awareness campaign to help all digital citizens stay safer and more secure online.

www.stopthinkconnect.org
National Cyber Security Awareness Month

National Cyber Security Awareness Month (NCSAM) – celebrated every October – was created as a collaborative effort between government and industry to ensure every American has the resources they need to stay safer and more secure online.

Since its inception under leadership from the U.S. Department of Homeland Security and the National Cyber Security Alliance, NCSAM has grown exponentially, reaching consumers, small and medium-sized businesses, corporations, educational institution, and young people across the nation.
About Data Privacy Day


Now annually on January 28th!
DATA PRIVACY DAY

PRIVACY is Good for Business

consumers make BUYING DECISIONS based on privacy

39% of people said they’d made a buying decision based on privacy concerns.\(^1\)
27% of millennials abandoned a purchase online because of security or privacy concerns in the past month.\(^2\)
32% of US adults always consider a company’s privacy policies when choosing which websites to visit or online services to use.\(^3\)

PRIVACY IS GOOD FOR BUSINESS TIPS

If you collect it, protect it.
Follow reasonable security measures to keep individuals’ personal information safe from inappropriate and unauthorized access.

Be open and honest about how you collect, use and share consumers’ personal information.
Think about how the consumer may expect their data to be used.

Build trust by doing what you say you will do.
Communicate clearly and concisely to the public about what privacy means to your organization and the steps you take to achieve and maintain privacy.

Create a culture of privacy in your organization.
Explain to and educate employees about the importance and impact of protecting consumer and employee information as well as the role they play in keeping it safe.

Don’t count on your privacy notice as your only tool to educate consumers about your data practices.

Conduct due diligence and maintain oversight of partners and vendors.
You are also responsible for how they collect and use personal information.
Two Steps

Resources

- Poster
- Video
- How To Library
- Links to Instructions

Be more secure.
2-step authentication uses another factor to make sure you're really trying to access your information. It can be as simple as a code a website sends to your phone and then asks you to enter it for verification.

Be modern.
Passwords need companions to provide modern security and a newer way to be safer and more secure.

Be empowered.
More and more websites and applications are implementing 2-step authentication. So, take control of the safety of your online accounts.

StopThinkConnect.org/2StepsAhead

facebook.com/StopThinkConnect
© 2016 STOP THINK CONNECT Messaging Convention, Inc.
<table>
<thead>
<tr>
<th>Kalamazoo, MI</th>
<th>Brooklyn, NY</th>
<th>Sioux Falls, SD</th>
</tr>
</thead>
<tbody>
<tr>
<td>Washington, DC</td>
<td>Dallas, TX</td>
<td>Topeka, KS</td>
</tr>
<tr>
<td>Tallahassee, FL</td>
<td>Ohio</td>
<td>Wisconsin</td>
</tr>
</tbody>
</table>

kristin@staysafeonline.org
THANKS TO OUR CALIFORNIA PARTNERS:

STOPTHINKCONNECT.ORG
KEEP A CLEAN MACHINE.

Having the latest security software, web browser, and operating system are the best defenses against viruses, malware, and other online threats.

TURN ON TWO-FACTOR AUTHENTICATION

Use a username and password and another form of identification, often times a security code. Some examples are voice ID, facial recognition, iris recognition and fingerscanning.

WHEN IN DOUBT, THROW IT OUT.

Links in email, tweets, posts, and online advertising are often the way cybercriminals compromise your computer. If it looks suspicious, even if you know the source, it’s best to delete or if appropriate, mark as junk email.

PROTECT ALL DEVICES THAT CONNECT TO THE INTERNET

Along with computers, smart phones, gaming systems, and other web-enabled devices also need protection from viruses and malware.

Visit dhs.gov/stophinkconnect
BUILD A CULTURE OF CYBERSECURITY

$3CURITY4L1F3

Use a better password
Improve your defenses by making passwords that you can remember, are hard to guess, preferably use capital and lowercase letters, numbers and symbols and are different for all accounts.

GET TWO STEPS AHEAD
Switch on two-step verification or multi-factor authentication wherever offered to make your accounts more secure.

KEEP A CLEAN MACHINE
Keep software up-to-date on all Internet connected devices to reduce risk of infection and malware.

WHEN IN DOUBT, THROW IT OUT
Links in email, posts and texts are often the ways cybercriminals try and steal your information or infect your devices.

THINK BEFORE YOU APP
Understand and be comfortable with what information (i.e., location, your contacts, social networking profiles, etc.) the app would access and share before you download it.

POST ONLY ABOUT OTHERS WHAT YOU WOULD HAVE THEM POST ABOUT YOU
It's the golden rule on the Internet, too.

Enjoy the Internet with more peace of mind.
Visit: www.stopthinkconnect.org for more.
Online Safety Materials
www.stopthinkconnect.org
www.staysafeonline.org

- Posters – English, Spanish, French and more
- Tip sheets
- Videos
- Games
- Social Media Posts
- Infographics
- Template certificates of achievement for employees who are good data stewards
Reach Us Online

- Data Privacy Day #DPD15
- Two-Steps Campaign #2stepsahead
- Twitter Chats #ChatDPD or #ChatSTC
- @stopthnkconnect
- @staysafeonline
- Facebook – STOP.THINK.CONNECT
- Facebook – National Cyber Security Alliance
- www.stopthinkconnect.org
- www.staysafeonline.org
Improving Authentication Security

National Cyber Security Alliance

National Strategy for Trusted Identities in Cyberspace

FIDO (Fast IDentity Online) Alliance
National Strategy for Trusted Identities in Cyberspace

White House initiative (April 2011)

NSTIC Goal: Catalyze the marketplace so we can choose from a variety of new types of solutions to use in lieu of passwords for online transactions that are more secure, convenient, and privacy-enhancing.
The Gears that Move NSTIC

Identity Ecosystem Steering Group (IDESG):
• A privately-led group across sectors furthering the NSTIC vision to develop a more secure, private, and easy-to-use online environment for all

Pilot Projects:
• Catalyzing a marketplace of solutions and infrastructure

Connect.Gov (formerly FCCX):
• Creates a secure, privacy-enhancing service that conveniently connects people to government services and applications online using an approved digital credential they may already have and trust
What’s this ‘Identity Ecosystem’ all about?

- The foundation of enhanced online trust, reduced fraud and better customer experiences
- Individuals can choose among multiple identity providers and digital credentials for convenient, secure, and privacy-enhancing transactions anywhere, anytime
- Providing a list of self-assessment criteria of different roles for organizations wishing to participate in a collaborative trusted manner online
Why do we need it?

• A marketplace exists – but there are barriers the market has not yet addressed on its own
• Private sector will lead the effort
• Private sector is in the best position to drive solutions...and ensure the Identity Ecosystem offers improved online trust and better customer experiences
• The Federal government can serve as a convener, facilitator, and a catalyst...states maybe could do more
• Executive Order – Improving the Security of Consumer Financial Transactions
What are we going to do?

**Guiding Principles**

Identity solutions will be:

- Privacy-Enhancing and Voluntary
- Secure and Resilient
- Interoperable
- Cost-Effective and Easy To Use

**Implementation Steps**

Convene the private sector:

- Identity Ecosystem Steering Group
- Catalyze a marketplace
- 15 pilot grants, ~$29M in 3 years
- Connect.Gov launch with commercial CSPs
- FICAM updates for modularity
NSTIC Pilots

GSMA - As part of the pilot, GSMA and the 4 major Mobile Network Operators will collaborate on creation of a hub that will allow any organization to easily accept identity solutions from any of the four MNOs with a single integration point – reducing a significant barrier to online service providers accepting mobile-based credentials.

MorphoTrust – Capability to use a ‘Selfie’ to your photo on record to eliminate the need for in-person proofing. The pilot will leverage North Carolina’s state driver’s license solution to create a digital credential for those applying for the North Carolina (DHHS) Food and Nutrition Services (FNS) Program online.

Confyrm - Pilot a “shared signals” solution to mitigate the impact of account takeovers and fake accounts through early fraud detection and notification, with special emphasis on consumer privacy. Online account compromises – and the subsequent misuse of identity – result in destruction of personal information, damage to individual reputations, and financial loss.
So where do we go?

• Strong authentication with verified attributes used in government applications with Connect.Gov

• Pilots are expanding, commercializing, moving to production, and integrating with each other to form a real, live ecosystem

• Solutions are budding elsewhere and consumers are showing an increasing hunger for change

• Like an umbrella trust framework, IDESG provides the means for multilateral trust between these parties and all the others that come to the table
The National Strategy for Trusted Identities in Cyberspace (NSTIC) NPO has just announced a privacy pilot funding opportunity! This new initiative focuses on turning theoretical privacy-enhancing technologies (PET) into commercially viable solutions.

The privacy-enhancing NSTIC guiding principle addresses concerns that the development of more trusted and federated identity solutions could create risks for privacy and civil liberties—like tracking and profiling of individuals. But barriers exist to the implementation of PET that could address these risks, including lack of understanding of appropriate PET, deployable protocols or standards, and lack of demonstrated proof of performance and scalability.

The NSTIC NPO is soliciting applications to fund projects that are intended to overcome the PET implementation barriers while advancing the NSTIC vision.

Email: NSTIC@NIST.gov | Twitter: @NSTICNPO | Blog: http://tinyurl.com/NSTICblog
Thanks!

Jeffrey Shultz
Trusted Identity Analyst, NSTIC National Program Office
National Institute of Standards and Technology

jeffrey.shultz@nist.gov
www.nstic.gov
Improving Authentication Security

National Cyber Security Alliance

National Strategy for Trusted Identities in Cyberspace

FIDO (Fast IDentity Online) Alliance
EXPERIENCE SIMPLER, STRONGER AUTHENTICATION
Data Breaches are out of control
IN 2014...

708 data breaches
82 million personal records stolen
$3.5 million average cost per breach
We have a **PASSWORD PROBLEM**
TOO MANY TO REMEMBER, DIFFICULT TO TYPE, AND TOO VULNERABLE
Adding more authentication has largely been rejected by users.
ONE-TIME PASSCODES
Improve security but aren’t easy enough

- SMS Reliability
- Token Necklace
- Poor User Experience
- Still Phishable
WE NEED A NEW MODEL
Fast IDentity Online
THE OLD PARADIGM

OTP 2FA

Passwords

PINs

SECURITY

USABILITY
THE FIDO PARADIGM

SECURITY

Weak

Poor

Strong

Good

USABILITY

Passwords

PINs

OTP

2FA
HOW DOES FIDO WORK?

USER VERIFICATION ← AUTHENTICATOR ← FIDO AUTHENTICATION

AUTHENTICATOR
Passwordless Experience (FIDO UAF Standards)

1. Transaction Detail
   - $10,000
   - Transfer Now

2. User Authentication

3. Success
   - Done

Second Factor Experience (FIDO U2F Standards)

1. Login & Password

2. Insert dongle
   - Press Button

3. Success
   - Done
FIDO Registration

1. Registration Begins

2. User Approval

3. New Key Created

4. Key Registered using Public Key Cryptography
FIDO Login

1. Login Challenge
2. User Approval
3. Key Selected
4. Login Complete

Login Response using Public Key Cryptography
online authentication using
public key cryptography
FIDO UNIVERSAL 2\textsuperscript{ND} FACTOR

Is a user present?

USER VERIFICATION

FIDO AUTHENTICATION

AUTHENTICATOR

Same authenticator as registered before?
Step 1
U2F AUTHENTICATION DEMO EXAMPLE
Step 2
U2F AUTHENTICATION DEMO EXAMPLE
Step 3
U2F AUTHENTICATION DEMO EXAMPLE
Step 4
U2F AUTHENTICATION DEMO EXAMPLE
USABILITY, SECURITY and PRIVACY
No 3rd Party in the Protocol

No Secrets on the Server side

Biometric data (if used) never leaves device

No link-ability between Services or Accounts
Better Security for **online services**

Reduced cost for the **enterprise**

Simple & Safe for **consumers**
The FIDO Alliance is an open association of more than 180 diverse member organizations
- Online Services
- Chip Providers
- Device Providers
- Biometrics Vendors
- Enterprise Servers
- Platform Providers

---

**Board Members**

- Discover
- PayPal
- MasterCard
- Bank of America
- Google
- Microsoft
- Lenovo
- Samsung
- ARM
- Synaptics
- NOK
- ARM Labs
- IdentityX
- CrucialTec
- NXP
- Alibaba Group
- VISA
- RSA
- Oberthur Technologies

---

**FIDO Alliance**
FIDO TIMELINE

- Alliance Announced: FEB 2013 (6 Members)
- FIDO Ready Program: DEC 2013 (59 Members)
- Specification Review Draft: FEB 2014 (84 Members)
- First UAF & U2F Deployments: FEB-OCT 2014 (129 Members)
- FIDO 1.0 FINAL Specification: DEC 9 2014 (152 Members)
PayPal continues FIDO enablement in improved mobile wallet app.

Google has FIDO in Chrome and 2-Step Verification.

Samsung adds touch to Galaxy® S6 and ships FIDO on all Galaxy® devices

2014 Deployments
Windows used by 1.5 billion users
Windows 10 in 190 countries by Q3
Free upgrade

Windows Hello lets you sign into Windows 10 devices with your face or finger

Windows For Your Business
Microsoft Announces FIDO Support Coming to Windows 10
Market leader to ship FIDO client
85+ OEMs as of Q4
>1 billion Android devices shipped
Innovative sensor

FIDO in Snapdragon

Qualcomm launches Snapdragon fingerprint scanning technology

Summary: Based on government-grade technology, Qualcomm's Snapdragon Sense ID is said to go far beyond current biometric scanners.

Qualcomm is currently the leader in the global cellular baseband chip market as well as the smartphone applications processor market, with a 64% and 51% share in the two segments, respectively. According to research firm Strategy Analytics, LTE basebands...
FIDO in Healthcare

- First healthcare deployment
- Physician access to health records
- Up to 50 million Healthcare users

FIDO Alliance Members MedImpact and Nok Nok Labs to Deliver FIDO Authentication to Physicians, an Industry First for Healthcare

March 23, 2015: 10:00 AM ET

The FIDO (Fast Identity Online) Alliance, an industry consortium launched in 2013 to revolutionize online security with open standards for simpler, stronger authentication that can be used for online transactions, released new industry capabilities today. FIDO Alliance members MedImpact and Nok Nok Labs will launch a new FIDO authentication-based physician access portal to enable physicians to access health records for patients who need same-day care.
A range of **FIDO PRODUCTS** is now available
<table>
<thead>
<tr>
<th>Category</th>
<th>Companies</th>
</tr>
</thead>
<tbody>
<tr>
<td>Online Services</td>
<td>Alibaba.com, PayPal, Google, PushCoin</td>
</tr>
<tr>
<td>Chip Providers</td>
<td>ARM, Infineon, NXP, GTI</td>
</tr>
<tr>
<td>Device Providers</td>
<td>GO-Trust, Samsung, FEITIAN, yubico, Sonovation</td>
</tr>
<tr>
<td>Biometrics Technology Providers</td>
<td>AGNITIO, CrucialTec, DDS, Sonovation</td>
</tr>
<tr>
<td>Enterprise Servers</td>
<td>Nok Labs, Duo, Entersekt, RCDevs, StrongAuth</td>
</tr>
<tr>
<td>Open Source</td>
<td>Google, yubico, WordPress</td>
</tr>
<tr>
<td>Mobile Apps/ Clients</td>
<td>Samsung, Nok Labs, Entersekt, Google, Android</td>
</tr>
<tr>
<td>WWW Browsers</td>
<td>Chrome, Firefox</td>
</tr>
</tbody>
</table>
JOIN THE
FIDO ALLIANCE
EXPERIENCE SIMPLER, STRONGER AUTHENTICATION
Evaluation

Please complete the evaluation of today’s webinar

https://www.surveymonkey.com/s/IAM_Online_April_2015
InCommon Shibboleth Training Workshops

May 14-15, 2015 – George Washington University Science and Technology Campus, Ashburn, VA

June 11-12, 2015 – OARnet, Columbus, OH

September 17-18, 2015 – DeAnza College, Cupertino, CA

October 19-20, 2015 – University of Texas – Arlington, Arlington, TX
Upcoming Events

April 26-30 – Internet2 Global Summit, Washington, DC

May 13, 2015 – IAM Online – Use of Social Identities – Real-World Examples

October 4-7 – Technology Exchange, Cleveland, OH