Cardinal Key

Going Passwordless @ Stanford

October 9, 2019

Michael Duff, Chief Information Security Officer
Vision
Characteristics of Poor Authenticators

• Secret is provided as part of authentication process
  • Static passwords
  • Credit card numbers, CSC, expiration date
  • SSNs and DOBs
  • Biometrics

• Same secret is provided to multiple services
  • Reused passwords
  • Credit card numbers, CSC, expiration date
  • SSNs and DOBs
  • Biometrics

• Secret is an identifier (vs. authenticator)
  • Credit card numbers
  • SSNs and DOBs
  • Biometrics
Authenticator Value vs. Knowledge of Secret

Knowledge of Secret

Auth Value

1 2
Password managers store your passwords securely and offer a mechanism for logging into websites without the need to remember all of your passwords. The
Incidents as Catalysts
Stanford University Is Investigating An Apparent Security Breach, Urges Community To Reset Passwords

Posted Jul 25, 2013 by Billy Gallagher (@gallagherbilly)

Stanford University urged network users to change their passwords late Wednesday evening, explaining that it “is investigating an apparent breach of its information technology infrastructure.”

Randall Livingston, Stanford’s chief financial officer, emailed the entire Stanford community, noting that Stanford does “not yet know the scope of the intrusion.”

Livingston’s full email, which was sent via an IT Services announce email but signed by the school’s CFO, reads:
Two Factor Authentication (Since Fall 2013)
Stanford reports fifth big HIPAA breach

Stolen laptop at children’s hospital compromises PHI of 13,000

By Erin McCann | June 13, 2013 | 10:14 AM

Officials at Stanford University's Lucile Packard Children's Hospital are notifying nearly 13,000 patients that their protected health information has been compromised following the theft of a hospital laptop.

An employee notified the hospital May 8 that an unencrypted laptop containing medical information on pediatric patients had been stolen from a badge-access controlled area of the hospital. Officials say the laptop contained patient names, ages, medical record numbers, surgical procedures, names of physicians involved in the procedures and telephone numbers.

This is the fifth big HIPPA breach for Stanford University.

Following Stanford's most recent HIPAA breach in January, hospital officials said they were "redoubling efforts to ensure that all computers and devices containing medical information are encrypted."
Encryption at Stanford

The University has established a requirement to verifiably encrypt all Windows and Mac computers, as well as Apple and Android mobile devices that are used by employees on the campus network.

Encrypt your devices  View frequently asked questions
MyDevices

Enrollment App  BigFix  MDM  VLRE  LDAP  NetDB  Auth Logs  Exceptions

MyDevices Portal: mydevices.stanford.edu
Ad Hoc Reports: bi.stanford.edu

Compliance Database

Automated Notifications and Enforcement

High ROI
## Registered Devices

This page contains information about devices you use, according to University records. Changes to source systems may take up to 24 hours to display. If you have questions or concerns about the data, please contact your local IT support or submit a help ticket.

<table>
<thead>
<tr>
<th>Model</th>
<th>Name</th>
<th>Type</th>
<th>Operating System</th>
<th>Ownership</th>
<th>Compliance Status</th>
</tr>
</thead>
<tbody>
<tr>
<td><img src="image" alt="Apple - MacBookPro15,2" /></td>
<td>ISO-C02XH4H6JHD2</td>
<td>Laptop</td>
<td>Mac OS X 10.14.6</td>
<td>Stanford</td>
<td>Compliant</td>
</tr>
<tr>
<td><img src="image" alt="iPad Pro with Wi-Fi (128 GB Space Gray)" /></td>
<td>mjduff iPad iOS 13.1.2 DQTQR3HKGMLL</td>
<td>Mobile</td>
<td>iOS 13.1.2</td>
<td>Stanford</td>
<td>Compliant</td>
</tr>
<tr>
<td><img src="image" alt="iPhone X (256 GB Space Gray)" /></td>
<td>mjduff iPhone iOS 13.1.2 F17VN78NJCL8</td>
<td>Mobile</td>
<td>iOS 13.1.2</td>
<td>Personal</td>
<td>Compliant</td>
</tr>
</tbody>
</table>

Learn about Stanford’s Encryption Requirements
Imagine not needing to enter your username and password anymore, all while being dramatically more secure…
Cardinal Key
Simplicity and Security
Get a Cardinal Key
Why are we doing this?
Integration Points

• VPN

• Web SSO

• Secure Wireless
VPN Connections with Username + Password + Two-Step

1. Ready to connect.
   - VPN: su-vpn.stanford.edu
   - Connect

2. Enter SUNet ID and password:
   - Group: Default Stanford split-tunnel
   - Username: jdoe
   - Password: *************

3. Answer:
   - Two-step code or option # (1-7) from below:
   - 1. Push to My iPad (iOS)
   - 2. Push to My Phone
   - 3. Push to My Tablet
   - 4. Push to My Computer
   - 5. Push to My TV
   - 6. Push to My Smart TV
   - 7. Push to My Set Top Box

4. Connected...
VPN Connections with a Cardinal Key
Web Logins with Username + Password + Two-Step

Logged In

Every 90 days
Web Logins with a Cardinal Key

Two-step authentication is required every 90 days.

Logged In
Rollout
3 Years, 3 Phases

• Year 1: Infrastructure to support opt-in participation

• Year 2: UX improvements and broad adoption

• Year 3: Require for central services
## Supported Platforms

<table>
<thead>
<tr>
<th>PLATFORM</th>
<th>BROWSERS</th>
<th>VPN CLIENTS</th>
</tr>
</thead>
<tbody>
<tr>
<td></td>
<td>CHROME</td>
<td>SAFARI</td>
</tr>
<tr>
<td>Windows</td>
<td>✔️</td>
<td></td>
</tr>
<tr>
<td>Mac</td>
<td>✔️</td>
<td>✔️</td>
</tr>
<tr>
<td>iOS</td>
<td>✔️</td>
<td>✔️</td>
</tr>
<tr>
<td>Android</td>
<td></td>
<td></td>
</tr>
<tr>
<td>Linux</td>
<td></td>
<td></td>
</tr>
</tbody>
</table>

Cardinal Key is not supported on Android and Linux platforms at this time.
Simplicity and security: the future of logins has arrived. Wouldn’t it be nice to skip typing in your SUNet ID and password every day, while protecting your credentials from phishing? With Cardinal Key, you can do just that. University IT has made this new service available to all, with the understanding that it is a preliminary rollout and not yet fully refined.

“Cardinal Key is a triumph of usability and security,” said Michael Duff, chief information security officer. “This is the culmination of six years of concerted effort, and the Stanford community will reap the benefits for decades to come. While Cardinal Key is still in beta, the advantages are too compelling to wait any longer.”

More than 1,000 staff and faculty are already using Cardinal Key as early adopters. Students are welcome to use Cardinal Key, but their devices must adhere to the same cybersecurity standards that apply to university employees.
Getting a Cardinal Key in 60 Seconds

1. Client
2. Web Login
3. Two-Step
4. Install

cardinalkey.stanford.edu
Which Device Are You Using?

Please provide a name for the device that you are activating:

Device Name: Michael's MacBook
To access the secure network, follow the instructions below based on your computer's operating system.

**Mac OS X**

Download for Mac 10.7 & Newer
Installs Stanford Client Configuration Profile
Quid Pro Quo

Incentives
• Simplified logins
• Protection against credential phishing

Requirements
• Must have endpoint agent
• Must meet our cybersecurity standards
Opt-in Security Doesn’t Work

(even when the benefits are overwhelmingly compelling)
Stanford Information Security Goals

No incidents attributable to a lack of best practices

Automated standards enforcement wherever possible

Uniform solutions across the University, Hospitals and SLAC

Balance security with usability and personal privacy

Stanford as a recognized leader in information security
Adoption
### Stanford Cardinal Key Report

**Source:** Auth_Radius_Cert & auth_idp logs

#### GlobalTimePicker

- **Last 30 days**

#### VPN: Total Cardinal Key Authorizations (Success & Rejects)

**Source:** Radius VPN

- **29,547**

#### VPN: Unique Cardinal Key Users

**Source:** Radius VPN

- **1,736**

#### Web SSO: Enrollment ID Count

**Source:** auth_idp

- **4,058**

#### Web SSO: User Count

**Source:** auth_idp

- **1,860**
“Life Changing”
How It Works
<table>
<thead>
<tr>
<th><strong>Subject Name</strong></th>
<th><strong>Common Name</strong></th>
</tr>
</thead>
<tbody>
<tr>
<td></td>
<td>mjdff/Enrollment-EAE917EB-8EAF-4E9D-8793-97937B95592F</td>
</tr>
</tbody>
</table>

**Organization**: Stanford University

**Organizational Unit**: MyDevices

**Country**: US

**Title**: Michael's MacBook

**Issuer Name**

**Country**: US

**Organization**: Stanford University

**Common Name**: Stanford University MyDevices Intermediate CA

**Trust**

- This certificate is valid

**Details**

- Expires: Monday, April 10, 2023 at 5:18:21 PM Pacific Daylight Time

**5 Year Lifetime**

**Identifies user and device**
Mapping Cardinal Keys to Devices

Cardinal Key $k$ is on Device $x$
**Device Information**

<table>
<thead>
<tr>
<th>Field</th>
<th>Value</th>
</tr>
</thead>
<tbody>
<tr>
<td>Model</td>
<td>Apple - MacBookPro15,2</td>
</tr>
<tr>
<td>Name</td>
<td>ISO-C02XH4H6JHD2</td>
</tr>
<tr>
<td>Type</td>
<td>Laptop</td>
</tr>
<tr>
<td>Serial Number</td>
<td>C02XH4H6JHD2</td>
</tr>
<tr>
<td>Operating System</td>
<td>Mac OS X 10.14.4</td>
</tr>
<tr>
<td>Encryption Status</td>
<td>Encrypted Last checked at 2019-05-14 15:25:29 Recover your encryption key</td>
</tr>
<tr>
<td>Hardware Address(es)</td>
<td>3c:07:54:30:be:d5 f0:18:98:60:5b:aa</td>
</tr>
<tr>
<td>SUNet ID</td>
<td>mjduff</td>
</tr>
</tbody>
</table>

**Cardinal Key Information**

<table>
<thead>
<tr>
<th>Field</th>
<th>Value</th>
</tr>
</thead>
<tbody>
<tr>
<td>Cardinal Key</td>
<td>Work MacBook Valid from 2018-10-21 to 2023-10-21</td>
</tr>
</tbody>
</table>
Public Key Cryptography

Secret Key

Hi!

0011010
1101110
1001010

Bye!

0110101
1100011

Public Key

Hi!

1110000
0110101
1100011

Bye!
**Public Key**

mjduff/Enrollment-EAE917EB-8EAF-4E9D-8793-97937B95592F

*Issued by:* Stanford University MyDevices Intermediate CA

*Expires:* Monday, April 10, 2023 at 5:18:21 PM Pacific Daylight Time

- This certificate is valid

### Trust

### Details

| Subject Name: mjduff/Enrollment-EAE917EB-8EAF-4E9D-8793-97937B95592F
<table>
<thead>
<tr>
<th></th>
<th></th>
<th></th>
<th></th>
<th></th>
</tr>
</thead>
<tbody>
<tr>
<td><strong>Common Name</strong></td>
<td>mjduff/Enrollment-EAE917EB-8EAF-4E9D-8793-97937B95592F</td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td><strong>Organization</strong></td>
<td>Stanford University</td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td><strong>Organizational Unit</strong></td>
<td>MyDevices</td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td><strong>Country</strong></td>
<td>US</td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td><strong>Title</strong></td>
<td>Michael's MacBook</td>
<td></td>
<td></td>
<td></td>
</tr>
</tbody>
</table>

<table>
<thead>
<tr>
<th><strong>Issuer Name</strong></th>
</tr>
</thead>
<tbody>
<tr>
<td><strong>Country</strong></td>
</tr>
<tr>
<td><strong>Organization</strong></td>
</tr>
<tr>
<td><strong>Common Name</strong></td>
</tr>
</tbody>
</table>
Authentication

Client
- Login request
- Decrypt challenge with secret key
  - 477dfa 54ede2 8e2f36

Cardinal Key
- Certificate Standard
  - 111000 001101 011101

Server
- Generate random challenge
  - 477dfa 54ede2 8e2f36
- Encrypt with public key
  - Key
- Verify match
  - 477dfa 54ede2 8e2f36

Cardinal Key = 477dfa 54ede2 8e2f36
Cardinal Key-Based Logins

1) Client authenticates to IdP via HTTPS handshake.
2) Is key valid? Verify and check validity period. Check against CRL.
3) Extract key components of Cardinal Key user ID and device ID.
4) Confirm user account is valid and active.
5) User account is valid and active.
6) Require two-step once every 90 days.
7) What is compliance status of device x?
8) Device x is fully compliant.
9) Authentication successful. Redirect to O365 with login assertion.
10) O365 login assertion.
1) Client authenticates to IdP via HTTPS handshake.

2) Device posture check + Cardinal Key status check.

3) User account status check.

4) Require two-step every 90 days.

5) Auth successful. Redirect to O365 with SAML login assertion.

6) O365 SAML login assertion.
Resources

- cardinalkey.stanford.edu
- uit.stanford.edu/service/mydevices
- twostep.stanford.edu
- encrypt.stanford.edu
- riskclass.stanford.edu
- minsec.stanford.edu
CA Key Ceremony

- Undisclosed location
- Recording (via Zoom)
- Raspberry Pi (instead of HSM) – no networking
- Standard keyboard & monitor
- Keys generated with OpenSSL → RAM disk
- No other computing devices permitted
- 10 pages of rehearsed step-by-step instructions
- 7 people x 10 hours
Key Ceremony

Key Masters: A, B, C, D

Use Shamir Secret Sharing instead
Cert Cache

- Transactional, HA MySQL database
  - Feature of Shibboleth IdP
  - Maps cert CN → device and cert status
- REST API written in node.js
  - Invoked by Shibboleth IdP, MyDevices, and CloudPath
Certificate Hierarchy

- Root CA (20 yrs): cn=Stanford University MyDevices Root CA, o=Stanford University, c=US

- Intermediate CA (10 yrs): cn=Stanford University MyDevices Intermediate CA, o=Stanford University, c=US

- User/device (5 yrs): cn=userID/deviceID, title=Device Name, ou=MyDevices, o=Stanford University, c=US
  - Subject Alternative Name: rfc822Name = emailAddress
Stanford University MyDevices Root CA

Root certificate authority
Expires: Saturday, January 9, 2038 at 8:20:44 AM Pacific Standard Time

Details

<table>
<thead>
<tr>
<th>Subject Name</th>
<th>Stanford University MyDevices Root CA</th>
</tr>
</thead>
<tbody>
<tr>
<td>Country</td>
<td>US</td>
</tr>
<tr>
<td>Organization</td>
<td>Stanford University</td>
</tr>
<tr>
<td>Common Name</td>
<td>Stanford University MyDevices Root CA</td>
</tr>
</tbody>
</table>

Issuer Name

| Country               | US                                    |
| Organization          | Stanford University                   |
| Common Name           | Stanford University MyDevices Root CA |
Stanford University MyDevices Intermediate CA
Intermediate certificate authority
Expires: Sunday, January 9, 2028 at 9:20:45 AM Pacific Standard Time

Details

Subject Name
Country US
Organization Stanford University
Common Name Stanford University MyDevices Intermediate CA

Issuer Name
Country US
Organization Stanford University
Common Name Stanford University MyDevices Root CA
SaaS Certificate Issuing Service

Root CA private key:
Never online and requires
3 people to reassemble

Intermediate private key:
Stored in CloudPath and
used to generate certs

CloudPath

User/device
certs
Key Design Decision Summary

- Campus-wide 2FA
- Building MyDevices
- Device-specific user certs
- Certs do not convey device posture status → ID only
- 5-year user/device cert lifetimes
- Cert hierarchy, fields, and 4K key sizes
- CA key ceremony
- Requiring 2FA for cert fetch and web SSO (periodically)
- SaaS cert issuing service
- Cert cache infrastructure
- Mapping certs to devices in MyDevices
Lessons Learned

• Most calendar time consumed by design decisions
• MyDevices wildly successful, yet resource-intensive to build
  • Open source platforms now available: Netflix Stethoscope
  • Similar: Google’s BeyondCorp, Duo Beyond
• UX improvements have a powerful impact
• Importance of branding
• Opt-in security doesn’t work