

Two Factor Pilot Project

Security Liaisons

4/10/13

Joshua Beeman

Melissa Muth


Talk Outline

- Overview of Multi Factor Authentication (MFA)
- MFA at Penn
 - History
 - Current Pilot

Two Factor/Multi-Factor



Common Knowledge Factors



Password: *****

Something You
Know



Something You
Are



Something You
Have

What problem are we solving?

CNET > News > Privacy & data protection
February 25, 2004 7:25 AM PST

Gates predicts death of the password

By Munir Kotadia

Related Stories

- Security in the spotlight at RSA show
- February 25, 2004
- Gates: 'Every impacted by s concerns
- February 24, 2004
- Microsoft tear RSA on pass protection

SAN FRANCISCO--Microsoft predicted the demise of the cannot "meet the challenge" secure.

WIRED GEAR SCIENCE ENTERTAINMENT BUSINESS SECURITY DESIGN OPINION VIDEO

Politics | Business | Tech | Entertainment | Health | Sexes | National | Global | China

SAP® Sybase® Adaptive Server Enterprise [Learn More >](#)

Forbes New Posts [+3 posts this hour](#) Popular [\\$100 M](#)

Kashmir Hill, Forbes Staff
Welcome to The Not-So Private Parts where technology
[+ Follow](#) (1,265) [Follow](#) (176k)

GADGET LAB | miscellaneous

The Password is Dead: Better Online Security

TECH | 4/15/2011 @ 3:52PM | 1,595 views

Kill the Password: Why a String of Characters Can't Protect Us Anymore

BY MAT HONAN 11.15.12 6:30 AM
[Follow @mat](#)

2 comments, 2 called-out [+ Comment Now](#) [+ Follow](#)

The username/password approach to security woefully insecure and in need of updating. Passwords (hello, Gawker), email addresses are stolen (hello, phishing attacks tend to hook the unwary, and stolen.

The White House proposes a solution in the National Security Agency's report on Trusted Identities in Cyberspace, a report released last week.

[Like](#) 23k
[Tweet](#) 6,090
[+1](#) 1.9k
[Share](#) 2,783



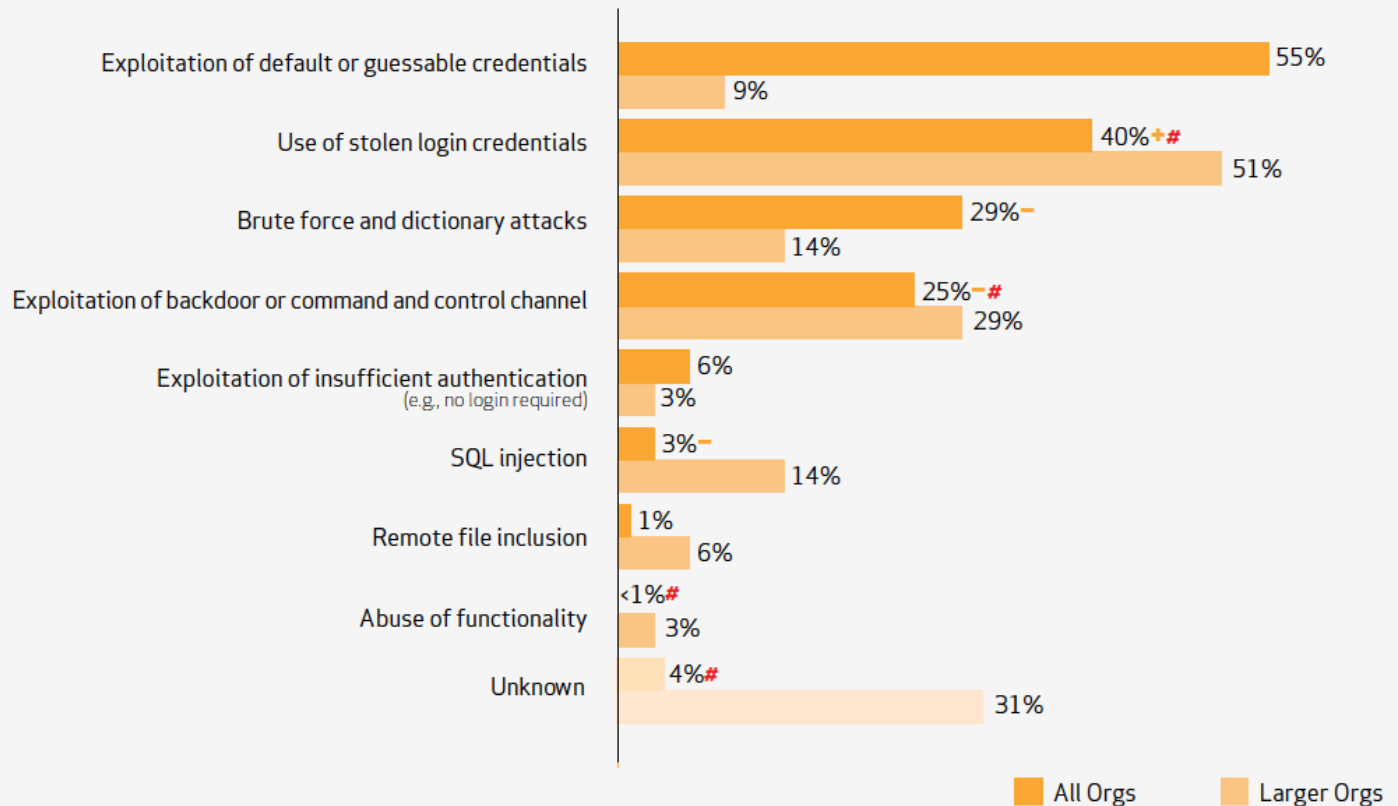
What problem are we solving?

Table 7. Top 10 Threat Action Types by number of breaches and records

Rank	Variety
1	Keylogger/Form-grat
2	Exploitation of
3	Use of stolen
4	Brute force and dictionary attacks
5	Exploitation of backdoor or command and control channel
6	Exploitation of insufficient authentication (e.g., no login required)
7	SQL injection
8	Remote file inclusion
9	Abuse of functionality
10	Unknown

Figure 20. Malware functionality

Figure 21. Hacking methods by percent of breaches within Hacking



What problem are we solving?

HOW SECURE IS MY PASSWORD?

SHOW SETTINGS

It would take a desktop PC about
58 years
to crack your password

HIDE DETAILS

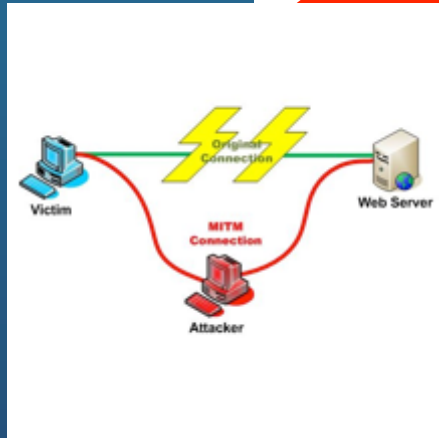
Length: 10 characters

Character Combinations: 77

Calculations Per Second: 4 billion

Possible Combinations: 7 quintillion

Not a magic bullet



Man in the Middle



Trojan/
Piggybacking

MFA in Popular Commercial Services



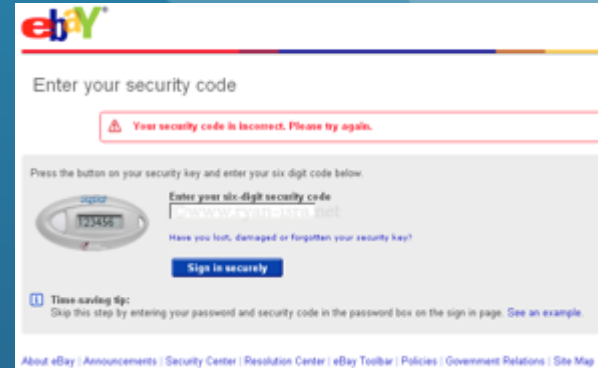
Enable two-step verification



Two-step verification adds an extra layer of protection to your account. Whenever you sign in to the Dropbox website or link a new device, you'll need to enter both your password and also a security code sent to your mobile phone.

[Learn more](#)

[Get started](#)



Turn on Login Approvals

What is Login Approvals?

Login Approvals is a security feature that requires you to enter a code that we text to your phone when you log in from an unrecognized computer. You can enable this feature in a few simple steps.

If you ever lose access to your phone, you can always return to a previously-recognized computer to regain access to your account.

Note: You'll need to have your mobile phone with you to complete this process.

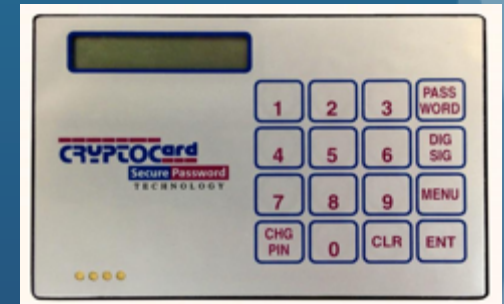
[Next](#)

[Cancel](#)



Common Past MFA Experience

- One-time funding & long term cost
- Technology limitations
 - RSA tokens (expensive, proprietary)
 - CryptoCard (too complex for some?)
- Specific use case (OOB network)
- Hard to get prioritized
 - Affecting individuals, not apps
 - Other more pressing concerns



History of MFA at Penn

RSA Agrees to Replace Security Tokens After Admitting Compromise

BY KIM ZETTER 06.07.11 12:41 PM

[Follow @KimZetter](#)

[Like](#) 122
[Tweet](#) 95
[+1](#) 2
[Share](#) 67



Nearly three months after RSA Security was breached by hackers, the company has announced it will replace the security tokens for nearly all of its SecurID customers.



History of MFA at Penn

Lessons Learned

1. Proprietary vs. open source
2. Power of personal mobile devices was real
3. Cost - and who pays it - can make or break it
 - What application and/or how it MFA is deployed matters (self-provisioning, opt-in, “remember this device”)
4. Security (PhoneFactor spoofing)

MFA Small Ball

If you know there is value (there is a risk)...

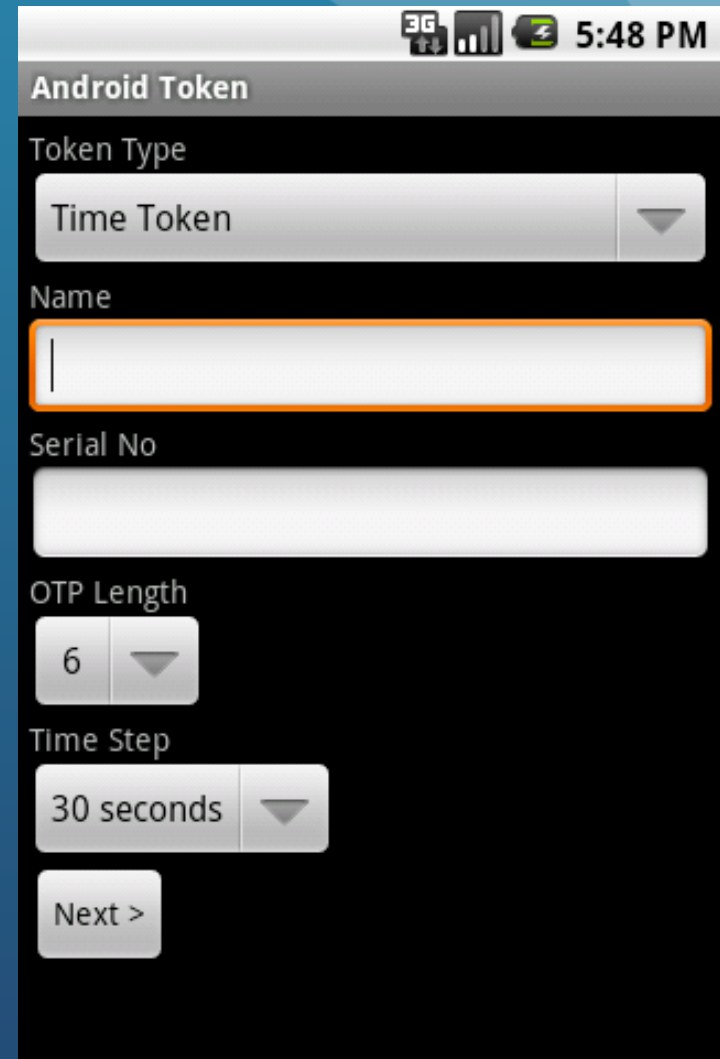
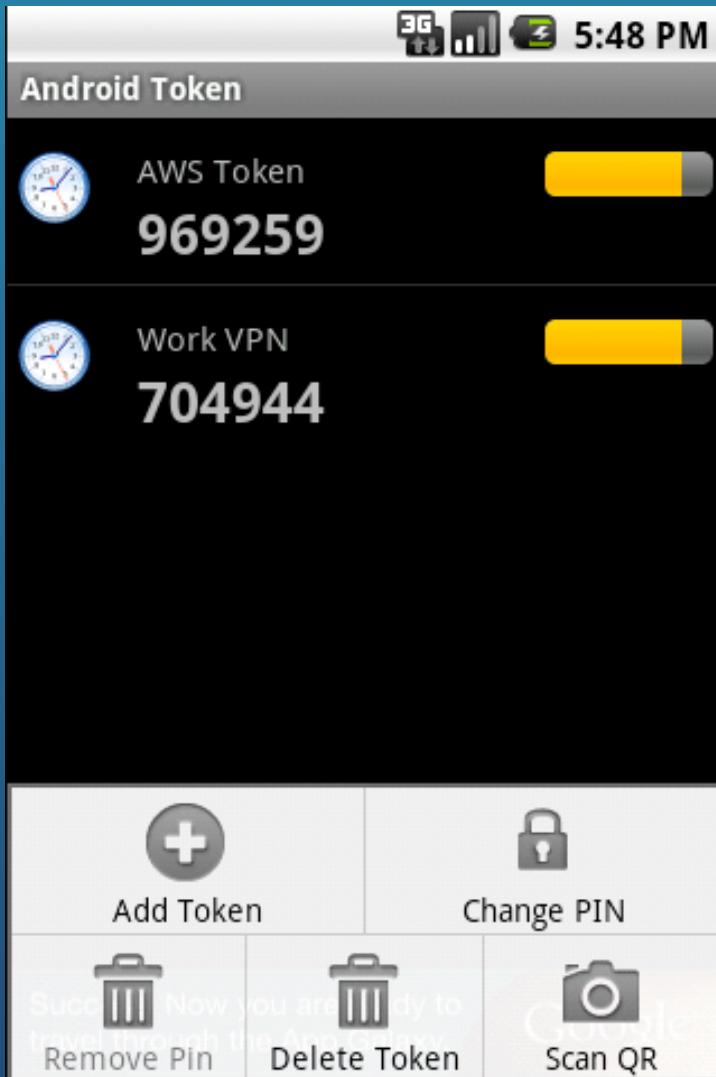
If you think you can find a solution...

Set the table and wait for the chance to score.

FY12 Goal: Evaluate and draft white paper on open-source, standards-based, one-time passcode generators for mobile platforms.

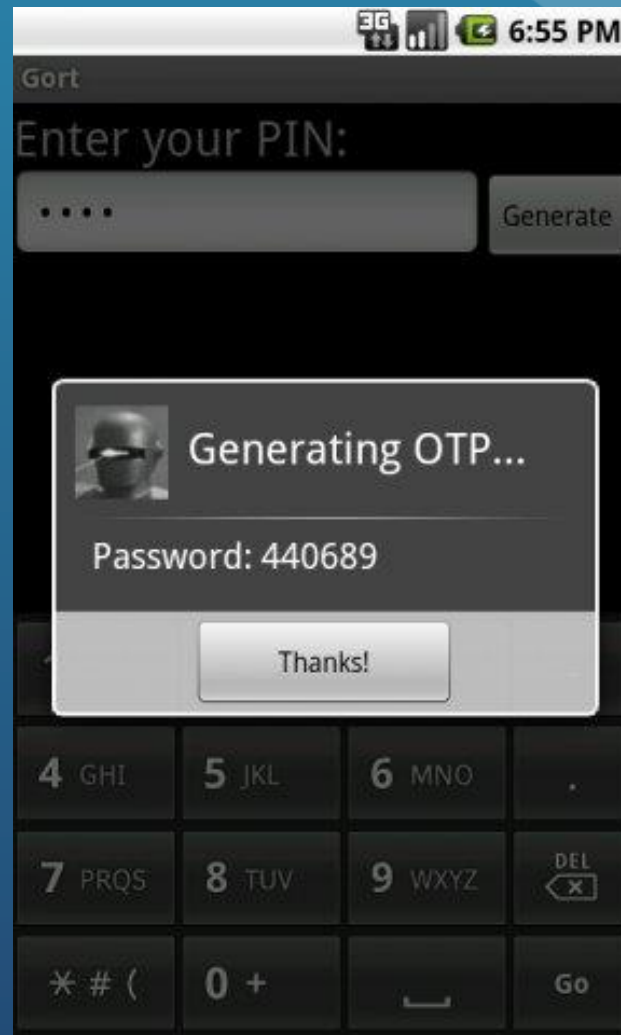
FY 13 Goal: Implement a pilot two-factor service using Google Authenticator and CoSign for individual users who opt in, including the infrastructure for provisioning and management of tokens.

Client Options



Client Options

Barada's Gort



Client Options

Edit Token [Cancel] [Done]

Token Name
Acme Portal Login

Token Secret Key
a938f92e5054a83fb284f7205537d0...

[Generate Random Key](#)

Event Based Time Based

Counter Value

Number of digits to display

Display digits in hex OFF

Lock down token* OFF

*Permanently prevents further edits of this token

OATH Token [New]

VPN Access >

Acme Portal Login >

Investment Account

139267

i

Client Options

Google Authenticator



Winner: Google Authenticator

- Server-side authentication component
- QR code generation for easy provisioning
- Generation of printable backup codes
- Broad platform support (iOS, Android, Blackberry, Linux)



Found: [partial] Open Source Solution

Provisioning ✓

Management

Client ✓

+ Cosign
integration

Authentication
(server) ✓



Goal: Pilot Two-Factor Service

- Opt-in by user (not just service)
- Option for user to “trust” a browser
- Self-service interface
 - Opt in/out
 - Regenerate scratch codes
 - Change secret
 - Revoke browser trust
- Integrate with web authN (Cosign)

Pilot Project

- Team:
 - Development, Info Sec, Support, Networking, Data Administration
- Timeline (Sept 2012 - May 2013)
 - Definition & Planning: Sep 2012-Oct 2012
 - Development: Nov 2012-Feb 2013
 - Testing & Documentation: Mar 2013
 - Pilot Rollout: May 2013



Decision Points

- Which group should run the service?
 - Development group: web service for all 2f functionality
 - Networking group: integrate 2f with Cosign
- When/how to display second factor prompt
 - Only if user authenticates successfully with 1st factor, and has opted in
 - Requires modification to Cosign; alternative (showing 2f only if cookie present) would leave users in dark about when to provide 2f.

Decision Points

- What to call it
 - PennKey Token? PennToken?
 - Two-step verification
- How to support it
 - Push the one-time codes!
 - Alternate phone number
 - Designee to opt the user out
- Whom to invite
 - Must be in online directory
 - IT & Security contacts

2F status

- Self-serve UI nearly complete
- Cosign integration underway
- [screen shots]



Penn
UNIVERSITY of PENNSYLVANIA

Penn WebLogin

Enter your credentials to initiate
a 10-hour Penn WebLogin session.

The session provides single sign-on access
to many protected University web resources.

PennKey

Password

[About Penn WebLogin](#)

Log in



Penn
UNIVERSITY of PENNSYLVANIA

Penn WebLogin

Additional authentication is required.

Please enter a valid PennToken code to continue.

✓ PennKey authentication complete

PennToken

[About Penn WebLogin](#)

Log in



Penn WebLogin Two Factor

Two Factor authentication is optional. If you do opt in, you can greatly reduce the risk of unauthorized access to your and to Penn's data by providing not only a password, but also a second factor - one-time passwords displayed by your phone. For more details, see [About Penn WebLogin Two Factor](#), below.

[Manage my two factor](#)

[I am having trouble logging in](#)

[About Penn WebLogin Two Factor](#)



Penn

Penn WebLogin Two Factor

Two Factor authentication is optional. If you do opt in, you can greatly reduce the risk of unauthorized access to your and to Penn's data by providing not only a password, but also a second factor - one-time passwords displayed by your phone. For more details, see [About Penn WebLogin Two Factor](#), below.

You are not currently enrolled in this service.

[Profile](#)[Opt in](#)[View recent activity](#)[Help a colleague](#)[Admin console](#)

[About Penn WebLogin Two Factor](#)

Penn WebLogin Two Factor - Opt in

Note: your two factor enrollment is not complete until you test your device below

Step 1 of 3: [Install Google Authenticator](#) in your mobile device

Step 2 of 3: Scan this QR code or or enter this secret value into your device(s)

Base 32 (e.g. Google Authenticator): **WLGV ECHT VQVE JMC3** ([Other options](#))

Note: This QR code and secret value should not be stored anywhere but inside the two-factor device (phone or token).



Step 3 of 3: Test the second factor

Two factor 6 digit pass

Submit

Home

[About Penn WebLogin Two Factor](#)



Penn

Penn WebLogin Two Factor - Opt in success

You have been successfully enrolled in Two Factor.

Important: If you lose your phone, run out of charge, or do not have it, *you will not be able to log in to WebLogin.* We **strongly recommend** that you click the 'Show one-time codes' button below and then print out and store them securely, for the event you do not have your phone.

[Home](#)[Show one-time codes](#)

[About Penn WebLogin Two Factor](#)

Penn WebLogin Two Factor - Show one-time codes

Note: Keep these codes safe since they are your passwords.
Use your browser Print function to print these codes and instructions.

Instructions: you can use each 6-digit password once in order. If you forget which password you are on, you can use two that have not been used (separated by a space). Generally these are used if you lose your phone or do not have it available. If you lose your printed codes you must invalidate them so no ones else uses them.

Note: all codes before the ones on this screen are now invalid

- | | |
|------------|------------|
| 1. 392146 | 11. 007181 |
| 2. 073332 | 12. 559526 |
| 3. 800432 | 13. 523248 |
| 4. 768860 | 14. 411788 |
| 5. 236396 | 15. 811581 |
| 6. 377212 | 16. 356830 |
| 7. 839041 | 17. 338517 |
| 8. 787762 | 18. 179087 |
| 9. 440100 | 19. 971353 |
| 10. 931292 | 20. 719261 |

[Home](#)

Almost there...