Multifactor Authentication Approaches and Multifactor for InCommon Silver

Wednesday, June 13, 2012 – 3 p.m. ET

Rob Carter, Identity Management Architect, Duke University

Mary Dunker, Director of Secure Enterprise Technology Initiatives, Virginia Tech

Rodney Petersen, Managing Director, EDUCAUSE Washington Office

Thank you to InCommon Affiliates for helping to make IAM Online possible.
Multifactor AuthN
Or: How I learned to stop worrying and love my credentials....again

Rob Carter
Duke University
rob@duke.edu
For the next 1800 seconds...

- Why should I care anyway?
- What is Multifactor Authentication, really?
- How does it work?
- If it’s so cool, why isn’t everyone already doing it?
But first, a word from the IT Security Office...
Back in Kansas...

- Few users, well versed in security
- Disorganized, dallying hackers
- Expensive, slow computing
- Low stakes -- we paid for things with cash, and kept records on paper
I don’t think we’re there anymore...

- The good lack all intention...
- The evil are consumed with a passionate intensity...
- A computer in every pocket...
- We’re playing for keeps...
The good lack all intention...

- Credulous, ill-informed users
- Up to 5% success rate for spearphishing (@ Duke)
- Some faculty spearphished > 1 time
- It's not lack of intelligence -- it's our trusting nature
The evil are passionately intense

- Hackers aren’t disorganized loners anymore...
- Anonymous?
- Stuxnet, Flame - government sponsorship
- They’re sophisticated and organized
A computer in every pocket...

- Horsepower isn’t a limiting factor
- The GPU in your laptop can crack a 6-char. pw in < 5 minutes (given its Windows hash)
- With 1000 desktop drones, 8-char < 8 hours... or with a rainbow table, seconds
We’re playing for keeps, here...

- ID Theft = asymmetric threat -- we pay $700, thieves collect $50 and pay $0

- Which would you really rather lose -- the cash in your wallet or your online banking password?
We’re playing for keeps, here...(cont’d)

- E-Harmony: 1.5 million password hashes
- LinkedIn: 6+ million password hashes
- None of those would match any of our on-site users’ passwords, would they? Or their bank codes?
And a few words from the Service Desk manager...
Aaaaaaaaaarrrrrrrrrggggggggghhhhhhhhh!
You may have heard...

“My staff can’t keep up with the calls from students who forgot their passwords over the summer (or at last weekend’s after-exams party...)”
You may have heard...

“Professor Jones called again -- she wants to know why we’re wasting her time picking these absurdly complicated 8-character passwords.”
You may have heard...

“Dr. Simpson just left in a huff -- said if she has to change this password again, she’s going to put it on a sticky note at her desk so she can remember it.”
You may have heard...

“The Vice-Provost wants to know why we’re making him use a ‘secure password’ -- can’t we keep the system secure in the first place?”
It’s not exactly Kansas

- Security says we need longer, stronger passwords
- Users say they’re fed up with hard passwords as it is
- What’s a fellah to do?
Multifactor AuthN (to the rescue)

- If passwords are the problem...
- ... maybe the solution is to stop relying on them so heavily...
- ...maybe multifactor authentication is the answer
Authentication?

- Authentication: Process by which a user proves his association with an electronic identity to a computing system.

- Distinct from: Identification (binding a user to his attributes), Authorization (associating privileges in real-time with an authN’d user)

- Usually involves presenting one or more credentials as evidence of identity

- Usually involves some kind of secret and some sort of stored information
Multifactor AuthN?

Simply: Using more than one class of credential to establish authentication

Various classes can be identified...

- Passwords, PINS, challenge question/answers
- Car keys, prox cards, smart cards, usb tokens
- Physical characteristics or habits
More technically...

- Authentication factors are grouped into classes according to how they are linked to their owners.

- Traditionally, there are three classes of factors, referred to as...
Something You Know

- Factor linked to its owner by way of secret knowledge - real-world analog = combination lock combination
- Passwords, PINs, passphrases, challenge-response questions/answers
- Includes more novel things like image selection mechanisms and touchscreen “squiggle” mechanisms (ala Android)
Something You Have

- Factor linked to the owner by physical possession - real world analog = house keys
- Prox cards, smart cards, usb dongles, key fobs
- Often construed to include X.509 certificates (although that’s debatably really SYK)
Something You Are

- Factor is an intrinsic property of the owner - real-world analog = what you look like

- Fingerprints, palmprints, retinal patterns, IR facial signatures

- Includes voiceprint recognition and actual visual recognition mechanisms

- Rumors of typing behavior as an SYA factor
Non-standard classes

- Somewhere you are
- Someone who’ll vouch for you
It’s the class, not the factor

- Common misconception: Using two instances of one class of factor is multifactor authN.
- Reality: Using two instances of one class (password + pin) is technically just single-factor authN.
- Strengths and weaknesses of classes complement one another; doubling up on a single class just increases both
Prior to needing to authenticate, the user memorizes a secret and shares it with the authenticator.

Authentication is achieved when the candidate later demonstrates (directly or indirectly) knowledge of the secret.

Security depends on secrecy; knowledge is power.
SYK - in depth

Advantages
- User controls secret (theoretically)
- No assembly required
- Easily implemented (tho' not always well)
- Widely supported
- Well understood

Disadvantages
- brute force, crypto, sniffing
- phishing
- Not tamper-evident
- No uniqueness guarantee
SYH - three ways

Unwieldy keys

The authenticator issues a token containing a key so large the user can’t possibly remember it, and registers it for safekeeping.

AuthN proceeds as in SYK, but “knowledge” of the key = possession of the token

Security = key complexity + tamper-proofing the token
SYH - three ways

- OTP Algorithms

- The authenticator issues a smart token to the user that computes a unique function - usually $f(\text{now,secret})$ or $f(\text{nonce,secret})$ and registers (secret)

- AuthN occurs when authenticator challenges user for some proof he can compute $f(n,s)$, which demonstrates control of the token

- Security = uniqueness of token
SYH - three ways

- OTA Approaches
  - The authenticator registers an addressable token for the user (say, a cellphone)
  - AuthN occurs when authenticator sends an OTP to the token address and user proves receipt of it (possibly using an SYK mechanism)
  - Security = address uniqueness
SYH - properties

Advantages
- Unphishable (hopefully :-)
- Long keys = cryptographic strength
- No dependence on neurons
- Loss-evident; copy-protectable

Disadvantages
- Some Assembly required
- Not as well-understood as SYK
- Dog ate my token.
- Batteries not included.
- RSA phenomenon
The authenticator is equipped with one or more detectors capable of collecting biometric information from a user -- fingerprints, facial imprints, voice patterns.

Authentication occurs when the system “recognizes” the characteristics of the user as matching registered characteristics for a known user.
SYA - in depth

Advantages
- No assembly required
- No “I forgot my finger” (hopefully)
- Ease of use
- Increasingly available (viz. fingerprint readers on laptops)
- Hard to spoof

Disadvantages
- Expensive instrumentation
- Creepiness; ADA; HIPAA?
- Unreliability (contact lenses, latex gloves)
- Angels & Demons scenario
Novel work-arounds

- **Cost Control**
  - BYOT solutions – cell-phone based tokens, self-printed C-R cards
  - Differential deployment by user role

- **Support Management**
  - BYOT solutions
  - Blended solutions – newer offerings support multi-modal SYH
  - Emerging recognition systems
Take Aways

- Change your LinkedIn password. Last.fm and E-Harmony, too. And their friends. And the others.

- Consider whether passwords are still “good enough”

- Remember: trust is fleeting, but it’s often the most important commodity

- Multi-factor authN isn’t rocket science

- Maybe a little brain surgery is required

- Benefits really start to outweigh the costs now, and

- YOU HAVE OPTIONS
Why consider 2 factor for InCommon Silver?

Mary Dunker
Virginia Tech
dunker@vt.edu
Is 2 factor required for Silver?

Absolutely NOT!

“SIT,” is something I know.
Decision making process

Examine the IAP criteria against single factor credentials and processes; perform gap analysis

- 4.2.1 Business, Policy, and Operational Criteria
- 4.2.2 Registration and identity proofing
- 4.2.3 Credential Technology
- 4.2.4 Credential Issuance and Management
- 4.2.5 Authentication Process
- 4.2.6 Identity Information Management
- 4.2.7 Assertion Content
- 4.2.8 Technical Environment
How can gap(s) be closed?

• Shore up current single factor process
• Examine other existing credentials and processes
• Add another factor
• Use Silver as opportunity to introduce 2 factor for other applications
• Narrow scope for who is Silver
Why 2 Factor?

- Some aspect of using single factor credentials does not meet Silver criteria (for Virginia Tech, 4.2.2.4, Identity Proofing at credential issuance time)

Do you think they know I’m a dog?
Why 2 Factor?

- Opportunity to promote stronger credentials for local campus applications that might need higher level of assurance
InCommon and Duo Security have formed a partnership to bring **phone-based two-factor authentication** to the higher education community with a low-cost site license. [www.incommon.org/duo](http://www.incommon.org/duo)

The InCommon/SafeNet partnership offers SafeNet smart cards and USB-format PKI hard tokens at significantly discounted prices. [www.incommon.org/safenet](http://www.incommon.org/safenet)

InCommon Affiliate VASCO also offers a number of strong authentication and e-signature options. [www.vasco.com](http://www.vasco.com)
Shibboleth Workshop Series
http://www.incommon.org/educate/shibboleth/

- July 16-17 – Baltimore, Maryland
- October 22-23 – Gainesville, Florida
Evaluation
Please complete the evaluation of today’s IAM Online:
www.surveymonkey.com/s/IAMOnline_June_2012

IAM Online Announcement List
Email sympa@incommon.org with the subject: subscribe iamonline

Thank you to InCommon Affiliates for helping to make IAM Online possible.