Multi-Factor Authentication: Securing the eCampus 2013

Adam Goldstein and Sean McNamara
The Password Problem - Reality

-------- Original Message --------

Subject: Thank you for scheduling a payment to Bill Me Later
Date: Wed, 3 Apr 2013 17:58:37 +0300
From: Bill Me Later <billmelater@paypal.com>
To: <stu-dent.00@Alum.Dartmouth.ORG>,

Dear Customer,

Thank you for making a payment online! We’ve received your Bill Me Later® payment of $1180.12 and have applied it to your account.

For more details please check attached file:
PP_BillMeLater_Receipt04032013_3981993.zip

Here are the details:

Your Bill Me Later Account Number Ending in: 0203

You Paid: $1180.12

Your Payment Date**: 04/03/2013

Your Payment Confirmation Number: 22866162598120726

Don’t forget, Bill Me Later is the perfect way to shop when you want more time to pay for the stuff you need. Plus, you can always find great deals and discounts at over 1000 stores. Watch this short, fun video to learn more.

**NOTE: If your payment date is Saturday, or a holiday, it will take an additional day for the payment to appear on your account. However, you will be credited for the payment as of the payment date.
The Password Problem: Reality (2)

2011 Totals: 71 DND accounts compromised
  o 18 Group/Departmental
  o 34 Faculty/Staff
  o 19 Students

2012 (With New Blitz harder to get accurate numbers.)
  o About 51 identified, mostly students

2013: 96 in March Alone!
  • 83 Students and 3 Faculty in keylogger incident
  • 10 Alumni accounts

• How?
  o Phishing
  o Easily-guessed
  o Malware

• Why?
  o Spam
  o Library resources
  o Access to Dartmouth systems to launch attacks
The Password Problem: Requirement

• NIST 800-53 (For FISMA Compliance)
  o IA 2 (CE 1-4)
    • The information system uses multifactor authentication for network access to privileged accounts.
    • The information system uses multifactor authentication for network access to non-privileged accounts.
    • The information system uses multifactor authentication for local access to privileged accounts.
    • The information system uses multifactor authentication for local access to non-privileged accounts.

• PCI DSS
  o Req 8.3
    • Implement two-factor authentication for remote access to the network by employees, administrators, and third parties.
Multi-Factor at Dartmouth: Tokens

• eTokens in use since 2006
  - USB token with protected PKI certificate (what you have) and Password to unlock (what you know)
  - ~300 current users (Staff and Researchers)
  - Requires client software (Windows and Mac)

• eToken authentication to VPN
  - Places user in special groups
  - User gets IP address from specific pools

• Firewall rules only allow VPN/eToken IP’s to certain systems
Multi-Factor at Dartmouth: Tokens(2)

• Support:
  o Not too bad!
  o Only 9 issues with forgotten passwords or broken tokens in last 12 months
  o Moved from in-house CA to DigiCert CA service simplified provisioning

• Challenges
  o Provisioning tokens to consultants/contract folks
  o Client software and OS updates
  o Scalability?
    • Users who are more mobile
    • Cost of tokens and client software
    • 300 users to 3000?
Multi-Factor at Dartmouth: OMG! The “O”-cronyms!

• How many acronyms on one slide?
• New direction: Leveraging IdM for MFA
• Products used:
  • OIF Oracle Identity Federation
  • OAM Oracle Access Manager
  • OAAM Oracle Adaptive Access Manager

  o OIF is used as a SAML IdP
  o OAM is used for standard low assurance Web SSO
  o OAAM is used for KBA Web SSO and eventually OTP
Multi-Factor at Dartmouth: OMG! The “O”-cronyms!

- OAM and OAAM are integrated
- We built a plugin to allow OIF to conditionally authenticate against either OAM or OAAM depending on SP entityId
- Setup Juniper VPN as an SAML SP
Multi-Factor at Dartmouth: Knowledge-based Authentication

• "Enhanced KBA":
  o Currently Registering security questions through account claiming process
  o Security questions are used to register new devices.
  o Once a device is registered, it is “fingerprinted” and generally the user will not be re-prompted unless behavior changes
  o Since implemented on VPN - no detected unauthorized logins
Multi-Factor at Dartmouth: Next Steps

• Adding 2nd factor:
  o Configure One-Time-Password (OTP)
  o Develop procedure for registering users mobile devices to receive OTP
  o How to handle international users, users w/o cell service…