PIVOTGROUP
SOLUTIONS TAILORED, NOT RESOLD.

Multi-Factor Authentication: What You Need to Know

by Faith M. Heikkila, Pivot Group Information Security Consultant

The Federal Financial Institutions Examination Council (FFIEC) has issued guidelines for safeguarding high risk transactions, such as online money transfers. The confidentiality, integrity, availability, and non-repudiation of customer information must be protected. The guidelines mandate that financial institutions develop an appropriate security program by utilizing a risk assessment, then use authentication appropriate for the level of risk.

The FFIEC states that single-factor authentication is clearly an unacceptable control mechanism for high risk transactions involving personally identifiable customer information. Hence, it is suggested that multi-factor authentication, multi-layered (defense-in-depth) security, and other controls reasonable to mitigate risk be implemented.

1. **Federal Financial Institutions Examination Council (FFIEC) Standards and Federal Deposit Insurance Corporation (FDIC) Studies**
   - FFIEC – *Authentication in an Electronic Banking Environment* – August 8, 2001
   - FFIEC – *Authentication in an Internet Banking Environment* – October 12, 2005
     - Updates the August 8, 2001 Guide
     - Conduct risk-based assessments
     - Evaluate customer awareness programs
     - Develop reliable authentication security measures
       - Single-factor is not an acceptable authentication solution for high-risk transactions involving customer information or fund movement
       - Defense-in-depth security to mitigate risks identified by risk assessment
       - Customer acceptance is crucial
   - FDIC – *Putting an End to Account-Hijacking Identity Theft* – December 2004
     - Outlines the use of technology to mitigate account-hijacking identity theft
     - The New FFIEC Guidelines build on the technologies outlined in this document
   - FDIC – *Putting an End to Account-Hijacking Identity Theft Study Supplement* – June 17, 2005
     - Discusses the comments received on the original report
     - Adds seven additional technologies not previously discussed
       - The majority of these technologies were included in the *Authentication in an Internet Banking Environment* guidelines
       - Adds Trusted Platform Module (TPM) Chip
         - Hardware-based system with an embedded chip for encryption purposes
         - Only allows trusted applications
         - Uses PKI
         - Chip must be enabled on new computers that have the chip installed
         - Won't be applicable for older computers

- Federal Reserve Board – *Interagency Guidelines Establishing Information Security Standards* – December 14, 2005
  - Help financial institutions comply with the *Gramm-Leach-Bliley Act § 501(b) Protection of Non-Public Personal Information Security Guidelines*
  - Build an appropriate security program – utilize a risk assessment
    - Identification of risks result in:
      - Authentication appropriate for the level of risk
      - Multi-factor authentication
      - Multi-layered (defense-in-depth) security
      - Other controls reasonable to mitigate risk
  - Guidelines Requiring the Proper Disposal of Consumer Information
    - Proper disposal of customer information by financial institutions and their third party service providers pursuant to the Fair and Accurate Credit Transactions Act (FACT Act) of 2003 December 28, 2004 (69 Fed. Reg. 248, 77610-77621)
  - Require third parties, such as service providers, to contractually secure and protect customer sensitive information

Multi-factor authentication methodologies discussed in: FDIC – Putting an End to Account-Hijacking Identity Theft – December 2004 and FFIEC – Authentication in an Internet Banking Environment – October 12, 2005 are outlined here. The three factors related to authentication methodologies are: Something a person knows, Something a person has, and Something a person is.

2. Multi-factor Authentication Techniques, Processes, & Methodologies

- Shared Secrets (something a person knows)
  - Shared by both institution and customer offline
  - Faces
- Tokens (something a person has)
  - Costly to distribute
  - Forget or lose token
  - USB tokens
  - Smart Card
  - Password-Generating Token – one time password changes usually every 60 seconds
- Biometrics (something a person is)
  - Costly
  - Reliability issues – false positives and false rejections
  - Privacy issues with providing personal biometrics – how will they be protected
  - Fingerprint recognition
  - Face recognition
  - Iris recognition
  - Voice recognition
  - Keystroke recognition
  - Handwriting recognition
- Non-Hardware based one-time password scratch card (something a person has)
  - Less costly
  - Low tech, easy to use
  - Bingo Card
  - Choose character randomly from cell in grid

- Out-of-band Authentication (something a person knows)
  - Relatively inexpensive
  - Authenticated through a second medium such as a cell phone, telephone, fax, or e-mail message
  - Cumbersome for customer
- Internet Protocol Address location (something a person has)
  - Match IP addresses previously used with customers
  - Use of public access point in airport or hotel not available
  - Traveling – difficulties using this technology
  - Privacy issues
- Device Authentication (something a person has)
  - Authenticates the computer being used is in fact the customer's computer
- Geo-location (something a person has)
  - Calculates location
  - Not suitable for wireless connection
- Mutual Authentication (something a person has)
  - Digitally signed certificates to authenticate the financial institution's Web site
  - Digitally signed certificates to authenticate the customer
  - Certificate Authority (CA) issuing the certificates can be financial institution or a third party CA
- Challenge question verification techniques (something a person knows)
  - Positive verification
  - Logical verification
  - Negative verification

It should be noted that the multi-factor authentication solution chosen should be interoperable, reliable, scalable for future growth, and readily accepted by the customers. Additionally, it should be appropriate for the level of risk. The following section provides links to some possible solutions for multi-factor authentication. These links are provided for educational and research purposes and Pivot Group does not endorse any of these solutions.

3. Multi-factor Authentication Technologies

- Shared Secrets (something a person knows)
  - Bank of America uses SiteKey by Passmark for picture recognition along with shared secrets – http://www.bankofamerica.com/privacy/passmark
  - Entrust – http://www.entrust.com
  - PassMark– http://www.passmarksecurity.com
  - Safe2Login – http://www.safe2login.com

- Tokens (something a person has)
  - Aladdin – http://www.aladdin.com
  - Authenex – http://www.authenex.com
  - Entrust – http://www.entrust.com
  - Vasco Digipass – http://www.vasco.com
  - PointSec – http://www.pointsec.com
  - RSA SecurIDs – http://www.rsasecurity.com
  - Verisign – http://verisign.com

- Biometrics (something a person is)
  - Fingerprint Recognition
    - Entrust – http://www.entrust.com
    - Sonic Foundry's Unified Security View – http://www.sonicfoundry.com

  - Face Recognition
    - Entrust – http://www.entrust.com
    - Face Recognition – http://www.face-rec.org
    - Sensible Vision – http://www.sensiblevision.com
    - EPIC Privacy Issues – http://www.epic.org/privacy/facerecognition
    - Government sponsored testing of face recognition software –http://www.frvt.org
    - Sonic Foundry's Unified Security View – http://www.sonicfoundry.com

  - Iris Recognition
    - Entrust – http://www.entrust.com
    - Gens Software – http://www.genssoft.com/iridian.html
    - Iridian Technologies – http://www.genssoft.com/iridian.html
    - Sonic Foundry's Unified Security View – http://www.sonicfoundry.com

  - Voice Recognition
    - ANOVEA Authentication Technologies – http://www.anovea.com/
    - Bio ID – http://www.bioid.com/
    - Entrust – http://www.entrust.com
    - InterVoice SpeechAccess – n http://www.intervoice-brite.com
    - Keywares Centralized Authentication Server (CAS) – http://www.keyware.com
    - Nuance Verifier – http://www.nuance.com
    - Persay's Orpheus – http://www.persay.com/homepage.asp?fd=1
    - Sonic Foundry's Unified Security View – http://www.sonicfoundry.com
    - VeriVoice Security Lock (SL) – http://www.verivoice.com
    - Vocent Voice Secure Suite – http://www.vocent.com/site/do/index
    - VoiceVault Services – http://www.voicevault.com
    - Biometric Roundup Evaluates voice recognition software – http://www.biometritech.com/features/roundup030102.htm

- Non-Hardware based one-time password scratch card (something a person has)
  - Entrust – http://www.entrust.com
  - PassMark– http://www.passmarksecurity.com
  - TriCipher – http://www.tricipher.com

- Out-of-band Authentication (something a person knows)
  - Cyota – http://www.cyota.com
  - Entrust – http://www.entrust.com
  - PassMark– http://www.passmarksecurity.com
  - TriCipher – http://www.tricipher.com

- Internet Protocol Address Location (something a person has)
  - Entrust – http://www.entrust.com
  - HostIP.info - http://www.hostip.info/
  - GeoIP –http://www.maxmind.com/app/ip_location
  - PassMark– http://www.passmarksecurity.com

- Device Authentication (something a person has)
  - PassMark– http://www.passmarksecurity.com
  - TriCipher – http://www.tricipher.com
  - Safe2Login – http://www.safe2login.com

- Geo-location (something a person has)
  - Entrust – http://www.entrust.com
  - NetGeo – http://www.netgeo.com/ip.geolocation.htm
  - PassMark– http://www.passmarksecurity.com
  - Quova – http://www.quova.com
  - NSA Fact Sheet – http://www.nsa.gov/techtrans/techt00031.cfm
  - USA Today article: "Geo-location software puts Net surfers on map" – http://www.usatoday.com/tech/news/techinnovations/2002-11-18-bonus-quova_x.htm

- Mutual Authentication (something a person has)
  - Entrust – http://www.entrust.com
  - imX Solutions – http://www.imx-solutions.com/bankingsecurity.asp
  - PassMark– http://www.passmarksecurity.com
  - Safe2Login – http://www.safe2login.com

- Challenge Question verification techniques (something a person knows)
  - Cyota – http://www.cyota.com
  - Digital Resolve– http://www.digital-resolve.net/solutions/login_authentication.html
  - PassMark– http://www.passmarksecurity.com
  - Safe2Login – http://www.safe2login.com

- TPM Chip (something a person has)
  - PassMark– http://www.passmarksecurity.com
  - TriCipher – http://www.tricipher.com

You should contact your online banking software provider to find out how they are handling multi-factor within their software packages. The following are a few online banking software packages utilized by financial institutions and what their solution to multi-factor authentication appears to be at this time.

4. Online Banking Software and Their Solution Partners

- Andera – http://www.andera.com
  - Digital Resolve– http://www.digital-resolve.net/solutions/login_authentication.html
- Digital Insight – http://www.digitalinsight.com
  - Cyota – http://www.cyota.com/product_7.asp
  - TriCipher – http://www.tricipher.com
- Fiserv – http://www.fiserv.com
  - PassMark Security primary partner – http://www.passmarksecurity.com
- Open Solutions – http://www.opensolutions.com/
  - Utilizing its own Security Matrix Two-Factor Authentication – one time password wallet sized matrix card
- S1 Corporation – http://www.s1.com
  - PassMark Security primary partner – http://www.passmarksecurity.com
- Symitar – http://symitar.com partners:
  - Cyota – http://www.cyota.com/product_7.asp
  - Trustdata- http://www.trustdatasolutions.com
  - Digital Resolve– http://www.digital-resolve.net/solutions/login_authentication.html

The Risk Assessment is a necessary component of discovering what the threats, vulnerabilities, and risks are to the financial institution's online security.

5. **Risk Assessment Features**
   - FFIEC – *Authentication in an Internet Banking Environment* – October 12, 2005 that risk assessment is necessary:
     - Evaluate by Customer Needs (retail or commercial)
     - Customer transactions available online – online bill paying, and transfer of funds, loan origination
     - Personally identifiable information of customer being communicated by both customer and financial institution
     - User-friendliness of communication is effortless
     - Volume of online transactions
     - Identify and assess the risks
     - Identify and implement mitigation of risk options
     - Assess customer awareness training efforts
     - Revise security program pursuant to findings
       - Changes to technology
       - Sensitivity of customer information
       - Incident response to internal or external threats
     - Build an appropriate security program – utilize a risk assessment
       - Identification of risks result in:
         - Authentication appropriate for the level of risk
         - Multi-factor authentication
         - Multi-layered (defense-in-depth) security
         - Other controls reasonable to mitigate risk

   - *Interagency Guidelines Establishing Information Security Standards* – December 14, 2005 that risk assessment is necessary:
     - Security policy and procedure development and review is crucial
       - Procedures for proper disposal of customer information
       - Ramifications of improper disposal of customer information
       - Customer awareness training
     - Automated vulnerability assessment tools should only be one tool not the only tool used
     - An option is to hire an outside consultant to conduct the risk assessment
       - Allow access to entire set of computer networks
       - Include physical controls as well as technical controls
       - Security policy review should also be evaluated
     - Risk Assessments are an ongoing process
     - Insurance coverage is not a defense
     - Incident response plan must be in place

Because we are technology neutral, Pivot Group can assist you with Assessing, Developing and Implementing a program that meets the FFEIC guidelines for safeguarding high risk transactions. Each Risk Assessment, Implementation Plan, and Solution is customized to match the needs and resources of the particular financial institution.

6. **look, plan, act, repeat**
   - **look** – business assessment of your needs through a risk assessment
     - Identify critical assets, such as customer online accounts & systems, to be protected
     - Identify the threats and vulnerabilities to the confidentiality, integrity, and availability of customer online accounts & systems
     - Evaluate the probability, likelihood, and impact of threats occurring
   - **plan** – build a proactive strategy
     - Identify how to mitigate risks
       - Technical controls
       - Management controls
       - Operational controls
     - Draft or revise security policies to cover these risks
     - Set Up Framework
     - Select Potential Technologies
     - Education Plan for employees and customers
     - Develop Effective Monitoring & Reporting Procedures & Techniques
   - **act** – take action on the plan
     - Implement the processes, controls, and technologies
     - Revise security policies as required
     - Train customers and employees on security best practices
     - Monitor, Review, & Report activities on a regular basis.
   - **repeat** – the life cycle of information security is a process not a destination
     - Ongoing basis – repeat it on a regular basis as security best practices indicate
     - Schedule regular risk assessments & update policies and controls regularly
     - If new technology is employed, schedule a risk assessment
     - If business requirements change, schedule a risk assessment

Faith M. Heikkila is a Pivot Group Security Consultant and currently a Ph.D. Candidate in Information Systems – Nova Southeastern University specializing in information assurance. She has over 18 years of paralegal and IT Project Management experience with two law firms in Michigan. She is a member of Association for Computing Machinery (ACM), Association of Information Technology Professionals (AITP), Computer Security Institute (CSI), Institute of Electrical and Electronics Engineers, Inc. (IEEE), Information Systems Security Association (ISSA).