An Inside Look at the "Updated" FFIEC Guidance on Authentication

NAFCU Technology Conference
February 15, 2012

Randy Romes, CISSP, CRISC, MCP, PCI-QSA
CliftonLarsonAllen LLP
Information Security Services

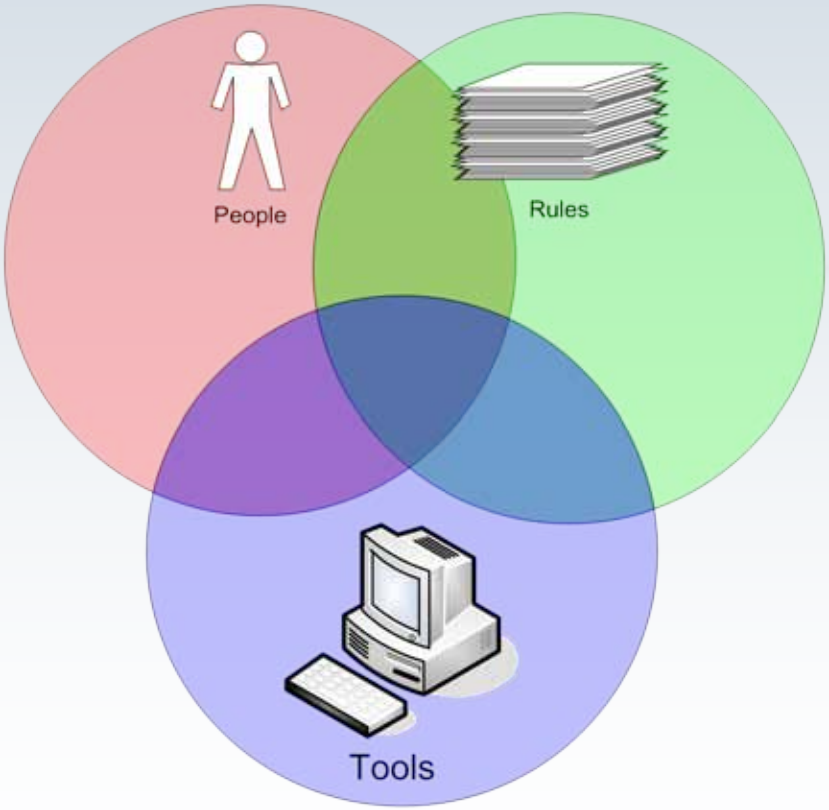
Overview

- History and evolution of threats
- Original and updated authentication guidance
- Authentication strategies
- (Case studies throughout…)

Definition of a Secure System

"A secure system is one we can depend on to behave as we expect."

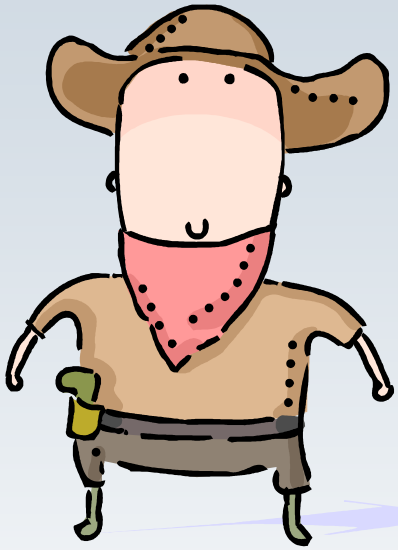
Source: "Web Security and Commerce" by Simson Garfinkel with Gene Spafford



- Confidentiality
- Integrity
- Availability

Early Threats

- History and evolution of threats
- “Mr. Jessie James, why do you rob banks???”



Original Authentication Guidance

- 2001 Authentication Guidance
- 2005 Authentication Guidance
- 2011 Authentication Guidance

Early Email Phishing

- First generation Phishing of consumers:
  - Nigerian Email Scam
  - eBay and PayPal
  - Financial Institutions
  - Resource:
  - http://www.millersmiles.co.uk/

Email Phishing – BBB Example

BBB Complaint for [redacted] - Case #D8545F0781

consumer-complaints@bbb.org

To: [redacted]

Better Business Bureau

Dear Mr./Mrs. [redacted]

You have received a complaint in regards to your business services. The complaint was filled by Mrs. Marcia E. Worthington on 05/23/2007/
Use the link below to view the complaint details:

DOCUMENTS FOR CASE #D8545F0781

Complaint Case Number: D8545F0781
Complaint Made by Consumer Mrs. Marcia E. Worthington
Complaint Registered Against: [redacted] Corporation
Date: 05/23/2007/

Instructions on how to resolve this complaint as well as a copy of the original complaint can be obtained using the link below:

DOCUMENTS FOR CASE #D8545F0781

Disputes involving consumer products and/or services may be arbitrated. Unless they directly relate to the contract that is the basis of this dispute, the following claims will be considered for arbitration only if all parties agree in writing that the arbitrator may consider them:

- **Claims based on product liability;**

Multi-Factor Authentication Solutions

- Authentication guidance calls for stronger authentication
  - Authentication factors
  - Multi-factor authentication

Email Phishing Evolves

- Phishing evolves from basic and crude attacks to more sophisticated attacks
  - Spear phishing
  - Whale phishing

Email Phishing

PayPal

Dear Member,

Because of several failed sign in attempts, your PayPal account has been restricted. To restore your PayPal features and online access, please click on the link below and carefully follow the prompts.

https://www.paypal.com/cgi-bin/webscr&verify

Please Note:If we do no receive the appropriate account verification within 24 hours, then we will assume this account is fraudulent and will be permanently restricted. After you follow the prompts your account features and online access will be restored and you will be redirected to our secured website.

Thank you,
Paypal Security

millersmiles.co.uk
Phishing scam report

http://bas6-toronto63-1128541556.dsl.bell.ca/globe/pages/www.paypal.com/

Phone Interactions

- Authentication guidance references:

  "Although this guidance is focused on the risks and risk management techniques associated with the Internet delivery channel, **the principles are applicable to all forms of electronic banking activities**"

  "The agencies consider single-factor authentication, as the only control mechanism, to be inadequate for high-risk transactions **involving access to customer information** or the movement of funds to other parties"

- http://www.ffiec.gov/pdf/authentication_guidance.pdf

Phone Interactions - Examples

- Simple phone attacks
- “…may I help you?”

Lessons Learned – Case Study

- Lessons learned from HELOC fraud events
- Dozens of Credit Unions around the country were targeted with pre-text phone calls
- Attackers used information that was available on public websites related to recent mortgage filings

Case Study – Pretext Phone Calls

- Over 20 Credit Unions around the country were targeted with pre-text phone calls

- Attackers used information that was available on public websites related to recent mortgage filings

Case Study – Pretext Phone Calls

- The attacks involved several calls to harvest small pieces of member account information

- End goal was to wire funds made available by a HELOC

Case Study – Pretext Phone Calls

Background for HELOC fraud calls

- Several calls posing as member

- Complete calls (7 calls) total over 45 minutes – including 3 minute pauses while he looks for account #

Case Study – Call #3

- Key Takeaways
  - Did not know password
  - Could not answer backup question (mother's maiden name)
  - Gave incorrect address at first

He never really authenticated!!

- Member services relied on member name, account number, and mailing address

Case Study – Call #3 (continued)

- She gave out key info and hints:
  - "Password is not the online password"
  - Validated address on the account
  - Joint account holder's first name
  - Password is a 4 digit number
  - Balances on the mortgage loan and HELOC
  - Type of car that is on the auto loan

What happened next?

- Used information from last call to authenticate
- Subsequent calls harvested more information…
- Harvested the wire transfer cut off times
- Called back the same day and requested the wire
- Used pressure – daughter needed money that day
- Had all the right information – requested the wire
- Financial Institution followed their verification procedures – stopped transfer
- Another Financial Institution was not so lucky ($700,000)

Lessons Learned

- What elements of the service culture approach put the service representatives in a position to fail?

- What things did the attacker prey on?

Lessons Learned – Pretext Phone Calls

- Train, train, train à AWARENESS
- Escalate calls to manager if security questions fail or are incomplete
- Establish a combination of authentication questions that must be answered correctly before giving out ANY information
- Attach all telephone call recordings to member numbers
  - Aids in search when one incident is detected

Example of Phone Call Procedures

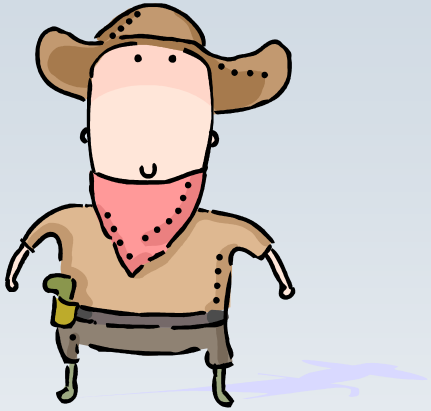
- MCS Member Identification
- All reps that deal with members requesting to access their accounts are required to ask three (3) of the twelve (12) listed below questions.

- **Date of Birth**
- **Password**
- **Last four numbers of Social Security Number**
- **Last transaction date and amount**
- **Verification of permanent mailing address (P.O. Boxes not acceptable*)**
- **Home phone number**
- **Who's joint member's name**
- **Joint member's Social Security Number**
- **Hire Date**
- **Join Date**
- **Beneficiary Names**

Phishing and ACH

- Refresher:

  "Mr. Jessie James, why do you rob banks???"



- Online banking convenience …
- Global economy…
- On-line availability of ACH

- "Corporate account take over"

Phishing and ACH – In the News

Google: "ACH fraud suit"

Bank Sues Customer

- **$800,000** fraudulent ACH transfer
- Bank retrieves $600,000
- What happens to the other $200,000?

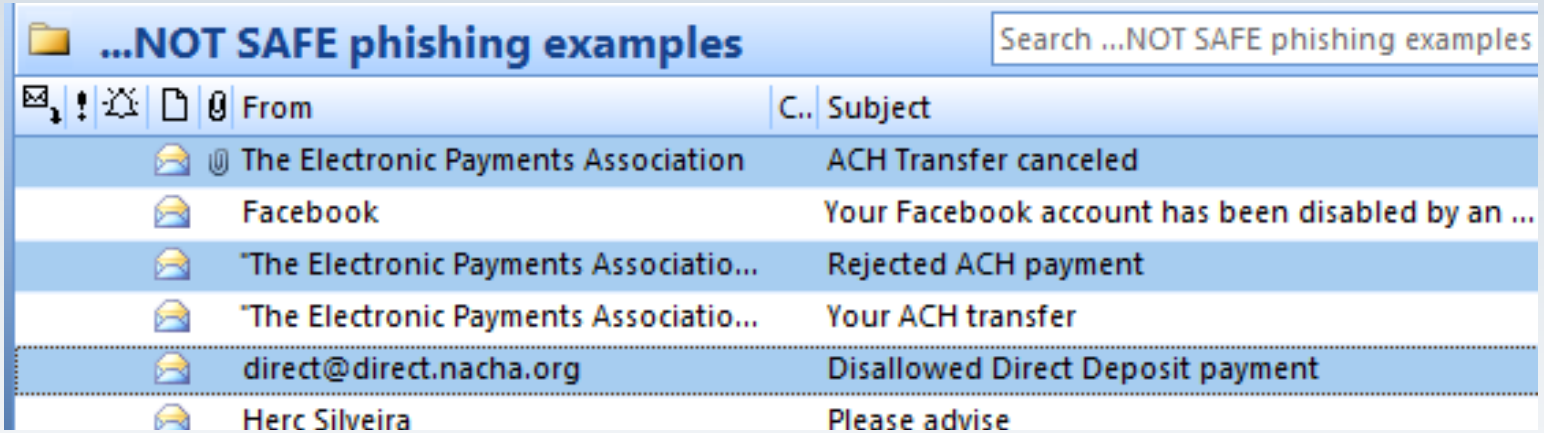
Phishing and ACH – In the News

Customer Sues Bank

- **$560,000** in fraudulent ACH transfers **to bank accounts in Russia, Estonia**, Scotland, Finland, China and the US; withdrawn soon after the deposits were made.
- Alleges that the bank failed to notice unusual activity.
- **Until the fraudulent transactions were made customer had made just two wire transfers ever**
- **In just a three-hour period, 47 wire transfers requests were made**.
- In addition, after customer became aware of the situation and asked the bank to halt transactions, the bank allegedly failed to do so until 38 more had been initiated.

Phishing and ACH – Two Direct Examples

- Business owner receives multiple emails:
- "Wire Transfer Cancelled"



- Finance staff open message – follow links
- Key logging software installed
- Fraudsters use obtained credentials
- Create 2 payroll ACH files - $500,000

Phishing and ACH – Two Direct Examples

- Finance person receives “2000 spam messages”
- Later in the day, fraudsters make three ACH transfers all within 30 minutes:
  - $8,000 to Houston
  - Two transfers for $440,000 each to Romania
- In this case, business insists the following controls were not followed:
  - Dollar limit/thresholds were exceeded
  - Call back verification did not occur
- This one is on-going…

Updated Authentication Guidance

- Risk Assessment, Risk Assessment, Risk Assessment…
- At least annually or after “changes”

Ø Changes in the internal and external threat environment,
  – including those discussed in the Appendix of the Supplement
Ø Changes in the customer base
Ø Changes in the customer functionality
Ø Actual incidents of security breaches, identity theft, or fraud experienced by the institution or industry

Updated Authentication Guidance

- Do not rely on single control
  - Controls need to increase as risk increases
  - Multi-layer
  - Additional controls at different points in transaction/interaction with member
- Technical (IT/systems) controls

Updated Authentication Guidance (2)

- Specific authentication guidance
  - Device identification
  - Challenge questions
  - Multifactor and two factor authentication
  - “Out of band” authentication

Controls for Layered Security

- Control of administrative functions
- Enhanced controls around payment authorization and verification
  - "Positive Pay" features
  - Dual authorization
  - "Call back" verification
- Detection and response to suspicious activity

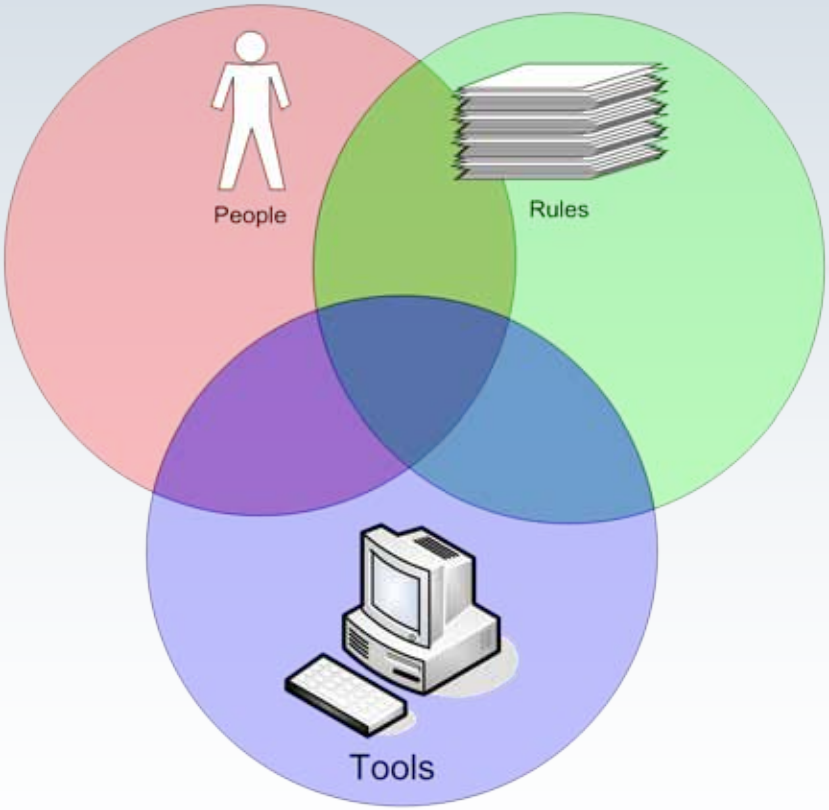
Controls for Layered Security (2)

- Customer awareness and education
  - Explanation of protections provided and not provided
  - How the credit union may contact a member on an unsolicited basis
  - A suggestion that commercial online banking members perform assessment and controls evaluation periodically;
  - A listing of alternative risk control mechanisms that members may consider implementing to mitigate their own risk
  - A listing of credit union contacts for members discretionary use to report suspected fraud

Definition of a Secure System

"A secure system is one we can depend on to behave as we expect."

Source: "Web Security and Commerce" by Simson Garfinkel with Gene Spafford



- Confidentiality
- Integrity
- Availability

Questions?

Thank you!

Randy Romes
CliftonLarsonAllen, LLP
Information Security Services
Randy.Romes@larsonallen.com
612-397-3114

CliftonLarsonAllen

References

- FFIEC
- http://ffiec.bankinfosecurity.com/
- http://www.ffiec.gov/pdf/pr080801.pdf (2001)
- http://www.ffiec.gov/pdf/authentication_guidance.pdf (2005)
- http://www.ffiec.gov/pdf/Auth-ITS-Final%206-22-11%20(FFIEC%20Formated).pdf (2011)

References

- Bank Info Security:
- http://ffiec.bankinfosecurity.com/

- FDIC ACH Advisories:
- http://www.fdic.gov/news/news/SpecialAlert/2011/index.html