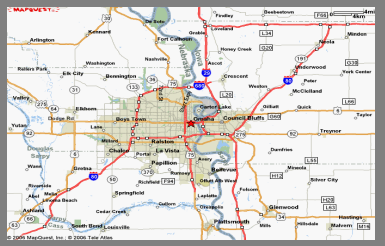
Str0nGp_w

Multifactor Authentication
August 10, 2006

NEbraska CERT Conference 2006
Computer Security and Information Assurance

Meeting OCC 2005-35 Requirements for Multifactor Authentication on eBanking Applications



Standard disclaimer, "'I never said THAT, and if you did THAT, and something broke, it's your own durn fault. Also, the views expressed here are mine, not my past, present or future employer's, and not the conference sponsor, nor any quail hunting partners. When using any tool, do no harm."

Michael T Hoesing CISA, CISSP, CIA, CCP, CMA, CPA

m-hoesing@cox.net (402) 981-7747

Learning Objectives

- Background, Drivers and Success Criteria
- Risk Assessment (always the starting point)
- Revisit “Factor” Definitions and other Mitigation
- Scope = All Customer Entry Channels
- Risk Mitigation Solution Options
- Products
- Implementation Considerations

Background

- eCommerce Applications were developed with a "time to market dot com" mindset (meaning yesterday)
- Content Delivery Preceded Transactional Capabilities
- Higher Risk Activities were layered on top of a weak base
- 10 years ago we had to fight for password authentication and even then it was set at the last 4 digits of the SSN
- FFIEC got tired of waiting, passed 2005-35

Driving Threat - Phishing

- Anatomy - eMail enticement, fake site, take authentication credentials
- Precursor to: unauthorized money movement, identity theft, disruption
- W ww.antiphishing.org
- eMail – education, sender authentication
- Fake Site – certs (if the user looks)
- Multi-factor would make credential absconding more difficult

Success Criteria

- Authentication techniques commensurate with the risk of the data on that delivery channel
- Least Disruptive to the Customer
  - Hardware (cost?)
  - User installed software
  - Portable
  - User Administration effort
- Cost/benefit? Lets face it, with the regulatory deadline , there will be no deals (watch admin costs)
- Two-Way Authentication ? (site authentication)

Risk Assessment

- Per 2005-35 High Risk requiring multi-factor includes:
  - Presents nonpublic customer information
  - Transfers funds outside of the customer's control
- Consider :
  - Corporate Sensitive
  - M&A, Contracts
  - R&D, Trade Secrets
  - Other
- Inventory all sites
- Don't forget sites hosted elsewhere
- "net residual risk" (after evaluating existing controls)

Scope

- e channel is not just “web”, consider:
  - email (SPF/SenderID)
  - IVR (ANI)
  - cellular
  - RFID
  - 802.11.b
  - bluetooth

…

Risk Mitigation

- Multifactor Authentication (more than single factor authentication) [semantics?? Is multple usage of one factor type, more than single factor?] (see also next slide)
- Operational Controls
  - Call backs
  - Transaction Limits
  - Separate masterfile creation and edits from ecommerce
  - Transaction Review/Fraud Detection
    - Before transaction execution (preventative) [batch]
    - After transaction execution (detective) [straight thru]
  - Customer Education

Technical Mitigation

- Additional Knowledge
  - Second password
  - Site authentication (phrase or picture, or both)
  - Behavior analysis (what the site knows about the user)
    - Temporal, pages used, click speed, … [aka fraud detection]
  - Passfaces w ww.realuser.com
- Something on the user's computer
  - Cookie
  - Secure Cookie
  - Computer fingerprint (cpu, memory, os, mac)
  - PKI Certificate

Technical Mitigation

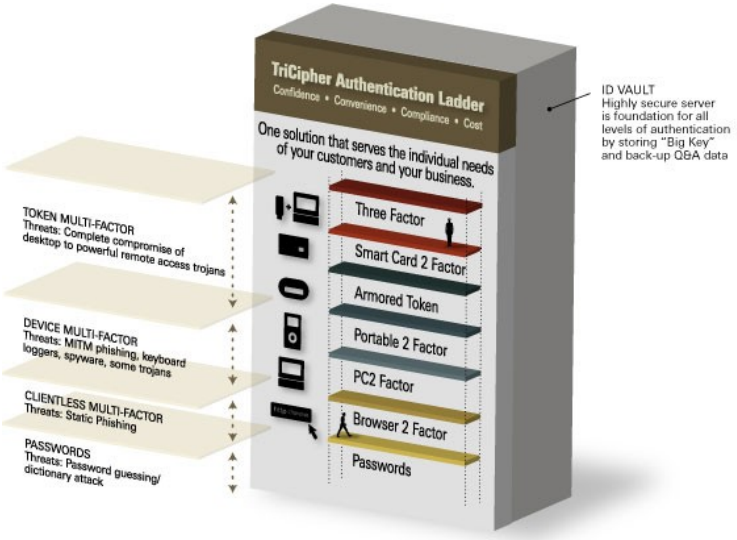
- Something in the user's possession
  - OTP
  - Scratch Card
  - Smart Card
  - Cell phone
- Biometric
  - Fingerprint reader
  - Passfaces ? w ww.realuser.com

Technical Mitigation

- The user's location
  - Geocodes from traceroute
  - GPS in smart card chip
  - Cell phone location

Products

- TriCipher (appliance,



- RSA/PassMark/Cyota (secure cookies & Macromedia Flash shared objects, site authentication, otp fob, otp to oob channel [cell phone], computer fingerprint, fraud detection, purchase or service bureau, shared fraud metrics,)
- Nuance (voiceprint biometric for IVR [4-8% EER])
- Verisign, Corrillion, Entrust

Implementation Considerations

- Configuration granularity (re-challenge, shut-off)
- Enrollment ease
- Interface with web application
- Multiple languages
- Per user fees
- Does the user need to be local administrator?
- Tie to CSR system?
- Will it play nice with your load balancer, SSL accelerator, ……. ?

Questions

- ?? (now that Bill is retiring ,who is going to demo new “blue-screens” at conferences?)
- ??
- ??