FINANCIAL SERVICES TECHNOLOGY CONSORTIUM

Better Mutual Authentication Project

Recommendations & Requirements for Improving Web Authentication for Retail Financial Services

Presented to W3C Workshop on:

Transparency & Usability of Web Authentication

March 15, 2006

The Better Mutual Authentication Project Participants

- Financial Institutions & Associations
  - Major Financial Services Company
  - Major Commercial Bank
  - Major Regional Bank
  - Major Commercial Bank
  - Major Retail Securities Firm
  - Major Retail Securities Firm
  - Credit Card Association
  - Major Commercial Bank
  - Credit Card Association
  - Major Commercial Bank
  - Major Commercial Bank
- Other Associations & Government Agencies
  - Securities Industry Association
  - U.S. Dept. of the Treasury (observer)
  - General Services Administration

- Technology Vendors
  - ACI Worldwide
  - Authentify
  - Business Signatures
  - Cyota (RSA)
  - Identita Technologies
  - IronKey
  - PassMark Security
  - Private Software
  - RSA Security
  - Secure Computing
  - The 41st Parameter
  - VASCO
  - Verid
  - VeriSign
  - Yodlee

Observations

- There are a *lot* of authentication options in the market today that are deployed in *lots* of different ways
  - But very few of them are used by the consumer population at large
- The *financial industry* is being forced to *lead*
  - It has the critical need
  - But it doesn’t control much of the critical infrastructure
  - This industry can’t solve these problems on its own
- *Other industries* also face authentication challenges
  - Health Care providers, Merchants, ISPs, Cellular operators, Telcos, Content and Entertainment providers, Employers, and Governments, to name the obvious
- *Cross-industry cooperation* is essential
  - Computer hardware/software developers, authentication device manufacturers, ISPs, and third-party service providers all have vital roles to play
  - Other industries can help promote broader adoption

Threat Assessment

- Actual fraud losses are not yet a major driver, and hopefully never will be
  - However, concern about the *potential for fraud* has impeded introduction of *new* retail financial services
- Consumer confidence in the online channel is *the* major concern
- Man-in-the-Middle attacks represent today's problem
- Financial malware is tomorrow's problem, and it's already here
- Threats will continue to evolve rapidly,
  so counter-measures must be able to evolve at an equivalent pace

Key Points from BMA Project

- *Mutual* authentication is vital
  - Multi-factor without mutual authentication is of marginal value
- *Multiple authentication techniques* are needed
  - Not just multi-factor, but an array of alternatives must be available
- *Different* authentication problems require *different* approaches
  - No one size fits all
- New authentication techniques will not *displace,* but must *complement,* traditional techniques
  - *Passwords aren't going away any time soon*
- Web authentication is inherently *asymmetrical*
  - A *person* on one end, and a *machine* on the other
  - Can we tell the difference between live persons and automatons?
- Customer support is the *make or break* issue

Dimensions of Authentication Challenge

- Usability
- Mutuality
- Credibility[†]

Core Critical Requirements

- Scalability
- Availability
- Interoperability
- Flexibility
- Adaptability

[†] How much confidence should one party assume in the authentication claims made by the other party?

What needs to be done?

- Clean up current practices
- Make better use of what's available
- Fix what's broken
- Add new options, but only if they add value
- Iterate!
  - Get out of the *rut* we're in
  - Provide chickens *and* eggs
  - *Continuously improve*

The Better Mutual Authentication Project Major Deliverables & Accomplishments

- Identified relevant *use cases, vulnerabilities,* and *threats*
- Defined and updated *Authentication Terminology*
- Surveyed the available technologies and solutions
- Produced *Financial Industry Recommendations and Requirements for BMA*
  - Including a comprehensive assessment of Web Authentication requirements
- Developed *Tools* for evaluating *combinations of authentication techniques*
  - Business Evaluation Spreadsheet (tool for evaluating solution coverage)
  - Taxonomy of Authentication Techniques Spreadsheet (requirements spec tool)
- Developed a high-level *Architecture* of Authentication encompassing…
  - *Multi-factor* authentication
  - *Mutual* authentication
  - *Multi-technique* authentication
  - *Sharing* of authentication devices/techniques across FIs and other relying parties
  - *Industry-level services* to support authentication
- Preparing a *Roadmap* for evolving BMA to meet future industry needs

Where to improve?

- Usability of Web security for *persons*
  - Configuration of browser security options & parameters
  - Security indicators in browser chrome
  - Security related dialogue boxes and alerts
- Web security protocols
  - Server-side improvements (by financial service providers & vendors)
  - Browser-side improvements
- Support for challenge/response dialogues with persons
  - Financial service practices for challenge/response dialogues
  - Browser support for challenge/response dialogues
- Browser support for automated forms entry & cookies
  - Automated forms and password entry by browsers
  - Cookie management

Where to improve? (continued)

- Digital certificates and PKI
  - Digital certificates as used by financial services providers (server side)
  - Digital certificates for end user systems (client side)
  - Management of Root CAs in client applications and OSs
  - OCSP and CRL support
- Establish a comprehensive architectural framework for Web authentication
  - Incorporate people (users) into the architecture
  - Address the “final 2 feet”
  - Assimilate platform dependencies
  - Factor in the Internet and other communications channels
  - Reflect use of specialized authentication services
  - Integrate other services—*e.g.*, DNS, PKI, OCSP
  - Map to WS-* services

New approaches need to be taken…

(The old approaches haven't worked)

- Overhaul configuration management of browser security features— Enable Web site enforcement of configuration policies
- Establish rigorous, default security configurations for browsers and platforms and the ability to easily restore safe default configurations
- Exchange shared secrets (*e.g.,* passwords) with persons *only* after successfully completing other authentication measures
- Introduce new user-dialogues for handling challenge/response interactions with actual persons that facilitate mutual authentication
- Make passwords unique for each relying party via browser-based hashing
- Allow Web sites to establish and enforce policies governing use of password vaults and automated forms entry
- Thoroughly overhaul use and management of cookies

New approaches need to be taken… (continued)

- Harden browser chrome including all dialogue & alert/warning boxes
- Provide meaningful security indicators
- Explicitly tell users when weak security measures are being used
- Clarify site authentication within browser chrome—move beyond the padlock icon
- Support moving security elements in browser chrome out to trusted hardware modules

New approaches need to be taken… (continued)

- Establish new CA hierarchies that conform to financial industry policies
- Certs used by financial services sites must have sufficient key length, support OCSP, and include logotypes (RFC 3709)
- Browsers must support OCSP by default and provide rational user interfaces for dealing with OCSP exceptions
- Clean up the "Root CA Clutter" by initially disabling all built-in root CAs, and make it easy for users to safely enable the CAs they actually need
- Facilitate enrollment, installation and management of client-side key pairs and certs for both software and hardware modules
- Fully integrate use of trusted hardware modules for protecting private keys associated with client-side certs

What can financial institutions do?

(Mostly update practices)

- Clean up domain name usage so that URLs are easy to interpret
- Only use appropriate security protocols and algorithms—*i.e.*, discontinue use of outdated protocols/algorithms
- Always establish visible TLS sessions *before* exchanging any shared secrets with customers
- Utilize new authentication techniques with customers (*e.g.*, multi-factor)
- Monitor configuration settings and version levels of browsers and operating systems used by customers, and inform customers if inadequate
- Disallow use of browsers or platforms that are known to be inadequately secure, even if provided by major vendors (*i.e.*, even-handed policies)
- Upgrade site certificates to use new, higher assurance PKI hierarchies with longer keys, OCSP support, logotypes, and rational distinguished names
- When customers successfully log in, provide a summary of prior logins and login attempts so that fraudulent access can be detected

What should W3C do?

- Coordinate industry efforts to continuously improve Web authentication
  - Promote cross-industry cooperation
  - Bring together technology developers, service providers, and relying parties
- Develop a comprehensive architecture for Web authentication
  - Incorporate all viable authentication techniques
  - Map to platforms and services
  - Clarify functional roles and responsibilities
  - Establish a framework for interoperability
  - Address extensibility so authentication can be continuously improved
- Establish new standards for interoperable solutions
  - Define new or improved Web authentication techniques
  - Specify infrastructure and services to support Web authentication
  - Stipulate consistent Web authentication practices

Concluding observations

- Achieving adequate authentication is a *lot harder* than it looks
- Much more than a *technology play*—comprehensive strategies required
- *New services* are needed to manage authentication at an industry level, and even across different industries and user populations
- The financial industry must work with a variety of players and even entire other industries to address the consumer authentication problem
  - Lots of opportunities exist to align strategies with other industries and leverage multi-prong approaches to engage consumers and drive adoption
- True collaboration & cooperation is a refreshing new trend in security
  - TCG initiatives and adoption of TPM approach across a variety of platforms
  - Info Cards / Identity 2.0 as a new way for consumers to control use of their information
  - Browser overhauls are finally addressing long-standing security problems
  - Security in "Web Services" (WS-*) is being addressed more broadly
  - Federated schemes are becoming more practical
  - PKI has been rediscovered and is being approached in a more pragmatic manner
  - Cross-industry services to support authentication are emerging

How to learn more, or get involved in Phase II

- Contacting FSTC
  - Dan Schutzer, Executive Director
    eMail: Dan.Schutzer@FSTC.org
  - FSTC Web site: http://www.FSTC.org
- BMA Project Information
  - Chuck Wade, Project Leader, BMA Phase I
    eMail: Chuck.Wade@FSTC.org
    Phone: 508 435-3050
  - Project Web page
    http://www.fstc.org/projects/bma-ph-1/
- To receive future announcements of FSTC Security projects, including BMA Phase II
  - Check FSTC's Web site for announcements, or
  - Subscribe at: http://ls.fstc.org/subscriber
    For the "security-scom" email distribution list