
What you are required to do and what do you need to do

NetSecure08

Bob Thompson, CPA
Catalyst Technology Group, Inc.
**Goals for today**

**Why use Multi-Factor Authentication (MFA)?** MFA requires you to provide something you know and something you have or something you are. Review the most common security vulnerabilities – those regarding both an organization’s internal network and Internet access.

**Who is required to use MFA?** Review what industries are required to use MFA.

**What can be used for MFA?** Provide an overview of the differences between tokens, one time passwords, site identifiers, behavioral biometrics, physical biometrics, geo-locators and when to use each independently or together.
Why use Multi-Factor Authentication?

Facts:
Consumers lost $2.8B to phishers in 2006 - 3.5M Americas are estimated to have given up sensitive information to phishers in 2006, up from 1.9M in 2005 - average loss per phishing attack was $1,244.

...more than 70% of unauthorized access to information systems is committed by employees, as are more than 95% of intrusions that result in significant financial losses.

Financial institutions that use only single factor authentication logon may not be commercially reasonable or adequate for high risk applications and transactions. Instead, multifactor techniques may be necessary.
Who is required to use MFA (and who needs to use MFA)?

- Merchants
- Medical
- Insurance
- Corporate HR
- Financial
- Municipalities
- Legal
- Business Owners
- IT Directors
- Subscription Service Providers

What would I lose if anyone could access my data? (What would I lose if I lost my laptop?)
<table>
<thead>
<tr>
<th>Vertical</th>
<th>Regulation</th>
<th>Deadline</th>
<th>Risk/Penalties</th>
<th>Applies To / Qualifications</th>
</tr>
</thead>
<tbody>
<tr>
<td>Merchants</td>
<td>PCI</td>
<td>12/31/2006</td>
<td>Termination of Payment Card Processing, Significant Fines to Merchant Banks - Merchant banks will successfully seek to recover those from Merchants.</td>
<td>All Merchants Processing over 20,000 credit card e-commerce transactions per year.</td>
</tr>
<tr>
<td>Medical</td>
<td>HIPAA - Sections: 164.306 (a)(2), 164.306 (a)(3), 164.308(a)(1), 164.308(a)(3), 164.308(a)(4), 164.308(a)(6), 164.308(a)(7), 164.308(a)(8), 164.308(b)(1), 164.312(a)(1), 164.312(b), 164.312(c)(1), 164.312(d)</td>
<td>All relevant Security and Privacy HIPAA Requirements are currently in effect.</td>
<td>From $100 per occurrence for violation of general guidelines ($25,000 per individual per year) up to prison and $250,000 personal fines for intentional violations.</td>
<td>All healthcare providers, health plans, payers, clearinghouses, and other entities that process or store personal health information must comply.</td>
</tr>
<tr>
<td>Insurance</td>
<td>State Privacy Acts</td>
<td></td>
<td>GLB - Fines levied at guilty institutions can be up to $100,000 per violation at the national level and can also expose the covered institutions, especially those in the insurance sector, to state-level sanctions in many cases. In addition, the officers and directors of these companies can be held personally liable for civil penalties up to $10,000.</td>
<td>GLB applies to financial institutions in the US, such as banks, securities firms, insurance companies, and other companies selling financial products.</td>
</tr>
<tr>
<td></td>
<td>Gramm Leach Bliley (GLB)</td>
<td></td>
<td></td>
<td>Any organization maintaining or processing Personal Health Information (PHI and EPHI)</td>
</tr>
<tr>
<td></td>
<td>HIPAA</td>
<td></td>
<td></td>
<td>Any organization processing 20,000 e-commerce transactions per year</td>
</tr>
<tr>
<td></td>
<td>PCI 1.1</td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>Vertical</td>
<td>Regulation</td>
<td>Deadline</td>
<td>Risk/Penalties</td>
<td>Applies To/Qualifications</td>
</tr>
<tr>
<td>-----------</td>
<td>-----------------------------------------------------------------------------</td>
<td>---------------------------------------------------------------------------</td>
<td>--------------------------------------------------------------------------------</td>
<td>----------------------------------------------------------------------------------------</td>
</tr>
</tbody>
</table>
| Corporate HR | Sarbanes Oxley (SOX)  
HIPAA  
PCI 1.1  
State Privacy Legislation | SOX - Companies with shares of more than $75 million, Nov. 15, 2004;  
- For their fiscal year ending on or after this date, annual reports must include an assessment of internal controls as per Section 404;  
- Companies with less than $75 million in shares, July 15, 2005 | SOX-Executives who knowingly sign falsified reports and anyone who destroys audit records can receive up to 10 years in prison and significant fines. Destroying, falsifying, or altering documents in federal investigations and bankruptcy proceedings can lead to sentences of up to 20 years in prison, in addition to fines. | SOX - Companies with shares of more than $75 million, All companies publicly traded in the United States and regulated by the Securities and Exchange Commission (SEC), including US-based companies as well as all international companies that have shares traded on a US exchange. |
| Municipalities | FISMA  
HIPAA  
State Privacy Legislation | Varies by State | Exclusion of Evidence if evidentiary chain compromised. | Schools, Government Agencies |
| Financial | Authentication in an Internet Banking Environment (FFIEC November 2005 Guidance) - FFIEC  
PCI 1.1  
Gramm Leach Billey (GLB)  
State Privacy Legislation | As this is guidance, traditional compliance dates do not apply. However, the Federal Reserve and FDIC issued a recommendation that this be addressed by the end of 2006. | Significant Fines and Prison, if violations are proven intentional. | FFIEC - All financial institutions in the U.S., including banks, brokerages, credit unions and the like, and ASPs that offer Internet banking applications. |
| Legal | State Privacy Legislation  
State Bar Association Rules | | Disbarment, fines, public relations issues | |
What does MFA address?:

General Internet Misuse Facts:
Phishing, Pharming, SpearPhishing

- The Sticky Note Problem
- Shoulder Surfing
- Password Sharing
- KeyLoggers and Spyware
## Multi-Factor Authentication Timeline

<table>
<thead>
<tr>
<th></th>
<th></th>
<th></th>
<th></th>
<th></th>
<th></th>
<th></th>
<th></th>
<th></th>
</tr>
</thead>
<tbody>
<tr>
<td>Virtual Keypad</td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>Soft PKI</td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>Grid Card</td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>One time password</td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>Transaction Authentication #</td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>Public Key Infrastructure</td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>Knowledge-based Authentication</td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>Fingerprint Biometric</td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>Voice Biometric</td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>Ocular Biometric</td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>OTP Token/Smart Card</td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>Smart Token</td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>Keystroke Dynamics</td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>Password</td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>Improved Password</td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
</tbody>
</table>
What Can Be Used For MFA?

- One Time Passwords via Tokens
- Smart Cards
- Fingerprint
- Device Tag/Profile
- One Time Passwords via Mobile Phone (an evolution of Tokens)
- Keystroke Dynamics
- Site Keys
- Is all this still enough?
How do you decide what to implement?

Security

What you Know
What you Have
What you Are

Cost - TCO  Usability
What you must know:

• What is required – who / what needs to be protected?
• What is your budget?
• How does your organization handle change management?
• How skilled and available is your help desk support?
• Do you have both internal and external (internet access) constituencies?
• What is the combination of the available technologies that best addresses your needs?

Security, Usability, and Total Cost of Ownership – What Combination Works for You!
Personal Security Questions

• What is easily surmised?
• What is a part of public record?
• What is remembered completely?
• Preference-based Security Questions (Love and Authentication – Jakobsson, Stolterman, Wetzel, Yang)
• How skilled and available is your help desk support?
Personal Security Questions

• Preference-based Security Questions
  (Love and Authentication – Jakobsson, Stolterman, Wetzel, Yang)

• Implementation
“Security is clearly the music industry’s main concern; we believe that DRM solutions employing user-friendly, non-intrusive security technologies, such as keystroke dynamics will have the clear advantage.”

John Heaven
President and CEO
Musicrypt Inc.
**Case Study – Apoteket AB**

**Apoteket AB** - Swedish drug retailer uses RSA ClearTrust® web access management to establish secure business communication channels

“When designing our new platform for identity and access management the actual technological solution was not our main concern. The most important issue was the ability to provide a safe and flexible way to provide single sign-on through all channels, whether it was over the phone or via the Internet. Once the project was defined, we started looking for the right technology to support our vision. We didn’t have to look for long—RSA ClearTrust® technology provided us with all the functionality we needed. For our purposes, RSA Security was really the only choice.”

*Lars Carlsson*
Senior IT Architect
Gartner on Multi-Factor Authentication


- **Authentication Strength**
  - High
  - Moderate
  - Low

- **TCO**
  - High (Worst)
  - Moderate
  - Low (Best)

- **Phishing/Sniffing Protection**
  - Good (8)
  - Moderate (5)
  - Low (2)
  - None (0)

- **Convenience**
  - High (8,9)
  - High (6,7)
  - Moderate (5)
  - Low/moderate (3,4)
  - Low (1,2)

- **Methods**
  - OOB (Out-of-band)
  - OTP (One time password)
  - TAN (Transaction Authentication Number)
  - PKI (Public Key Infrastructure)
  - KBA (Knowledge-based Authentication)
  - Improved Password
  - Virtual Keypad
  - Password
  - OOB (Voice Telephony) and Voice Biometric
  - OTP Token/Smart Card and Handheld Reader
  - Smart Token
  - OOB
  - Keystroke Dynamics
  - Soft PKI
  - Grid Card
  - KBA
  - Improved Password
  - Virtual Keypad
  - Password

- **Source**

- **Technology Group**
  - Catalyst
  - Where technology is everything.
Questions:
Introduction to Catalyst Technology Group

**What we offer:** Catalyst provides world class expertise in Microsoft server platforms, Cisco Networking, Computer Associates Security Solutions and best-of-breed technology consulting services.

**Where we offer it:** Indiana and Illinois, including Chicago metro areas, with some services available nationwide

**Who we service:** Our services are needed by organizations of all sizes.

**Why we’re the best choice:** We take the time to understand your business needs and deliver solutions that work, on-time.

---

**Presented by:**  
Bob Thompson  
Vice President  
Catalyst Technology Group, Inc.