Two-Factor Authentication

The key to compliance for secure online banking
Legal Notice

© Copyright 2008 Aladdin Knowledge Systems Ltd. All rights reserved.

Aladdin, Aladdin Knowledge Systems, HASP®, eToken™ and eSafe® are only a few of Aladdin Knowledge Systems Ltd’s (“Aladdin”) proprietary trademarks. The Aladdin Knowledge Systems logo is also proprietary to Aladdin.

The information contained in this presentation is protected by international copyright laws. The copyrights are owned by Aladdin or the original creator of the material. The information contained herein is provided to you for informational purposes only, and except and to the extent specifically permitted, no portion of this presentation may be copied, reproduced (or the like), distributed or used in any way whatsoever whether directly or indirectly.

In addition to Aladdin’s trademarks, logos, content and information, this presentation may contain references to trademarks and/or logos owned by other entities. Aladdin expressly disclaims any proprietary interest in trademarks and/or logos owned by other entities and makes no representation of any association, sponsorship, affiliation, or endorsement with or by the owners of such trademarks and/or logos.

This presentation may contain references and use of third party web sites for purposes of providing examples relevant to this course. Aladdin assumes no responsibility and/or liability for any content and/or information contained in such third party web sites. Aladdin further does not endorse the companies or contents of any referenced sites.

Aladdin does not assume any responsibility or liability for the accuracy of the information contained in this presentation. The information contained in this presentation is provided "as is" and does not constitute a warranty of any kind, either express or implied. Aladdin disclaims all warranties, expressed or implied, including but not limited to implied warranties of merchantability, fitness for a particular purpose, and non-infringement.
Topics Covered in This Presentation

- The identity theft issue
- Passwords are not enough!
- Strong authentication
- USB smartcard tokens – Strong authentication with added value
- Strong authentication check list
(fish´ing) (n.) The act of sending an email to a user falsely claiming to be an established legitimate enterprise in an attempt to scam the user into surrendering private information that will be used for identity theft. The email directs the user to visit a Web site where they are asked to update personal information, such as passwords and credit card, social security, and bank account numbers, that the legitimate organization already has. The Web site, however, is bogus and set up only to steal the user’s information.

Source: Anti-Phishing Working Group
Major Problem: Global Identity Fraud

- The number of U.S. adult victims of identity fraud in 2006: **8.9 million**
- Amount of fraud in 2006: **$56.6 billion**
- The mean fraud amount per victim rose from $5,249 in 2003 and $5,885 in 2005 to **$6,383** in 2006

“Targeted, financially motivated attacks have already started and define the protections that will be needed to win (or at least survive) the next battle.”

“Augment Security Processes to Deal With the Changing Internet Threat”, Gartner, John Pescatore, March 2006

Source: Javelin/Better Business Bureau Survey - January 2006
What Do Your Customers Think?

Nearly 60 percent of U.S. consumers are worried about identity theft.

27 percent of online bankers use less online banking functionality due to security concerns.

31 percent of online users will not bank online due to security concerns.

Source: IDC/Financial Insights, 2005

How Security Concerns Affect Customers’ Online Activity

Source: JupiterResearch, 2005

Perhaps the biggest impact is a newfound and serious consumer distrust of e-mail. More than 80 percent of online consumers…say that their concerns about online attacks have affected their trust in e-mail from companies or individuals they don’t know personally. Of these, more than 85 percent delete suspect mail without opening it.”

“Increased Phishing and Online Attacks Cause Dip in Consumer Confidence”, Gartner, Aviva Litan, June 2005
Many Access Points For Customer Identity Data

- Online banking web sites
- Portals
- Internal networks
- Employee computers / laptops
Attacks..

- **Employees**
  - March 2005 – 670,000 customers of 4 banks, including Bank of America and Wachovia, had their personal data illegally sold by bank employees to someone posing as a collection agency representative.
  - June 2005 – over 40 million credit card owners had their card data stolen by an employee of payment processor CardSystems.

- **Partners**
  - April 2005 – a total of $350,000 was stolen from Citibank customers by 12 employees of an outsourced call center firm in India, who defrauded the customers of their credentials.

- **Outsiders**
  - April 2005 – a laptop containing ID information of 16,500 MCI Inc. employees was stolen from the car of a company financial analyst.
  - July 2006 - researchers spotted a phishing website targeting Citibank's Citibusiness service that attempted to steal user names and passwords as well as OTP values for user accounts.

*Sources: newsfactor.com; CNN/Money; E-Commerce Times; MSNBC, VNunet*
What Are Regulators Saying?

- **U.S. Senate** – introducing legislation to protect consumers from ID theft
  - Example: Identity Theft Protection Act – *requires entities that collect sensitive data (e.g. social security numbers) to secure the data, and notify consumers when the data is compromised*

- **U.S. Federal Deposit Insurance Corp. (FDIC)**
  - Recommends financial institutions to upgrade their customer authentication systems from single-factor to **two-factor**

- **EU Directive on Data Protection (Directive 95/46/EC)**
  - Protects individuals with regard to the processing and transfer of **personal data** throughout the European Union

What is Strong Authentication?

1. What you know
2. What you have
3. What you are

Strong authentication means using two or more authentication methods.

Example 1

Example 2
Keys Offer Protection

We all use keys to protect our valuable possessions
Secure Access to My Data

Why not use a key to protect our Data PC/laptop?
How Keys Protect Your Data PC/Laptop

- Using data encryption together with pre-boot authentication is in fact locking your data
- The encryption key is the key to your computer
- The success of your security scheme depends on where you place your key
Where to Save Your Key

- Placing your key on the PC/Laptop is not safe!
  - It is exposed to malicious software and insider attacks
- The key must be kept outside of the computer on an external device
- The question is – On which device?
Devices in the Market

- There are many devices available
  - USB ‘Smart’ tokens
  - Flash tokens
  - Hybrid tokens
  - Smart Cards
  - And more…

- But which device is the one you need?
Smartcard Tokens

Smartcard tokens allow secure key storage, and are also:

- Most flexible
- Most portable
- Easy to use
- Easy to deploy

“Gartner projects that [smart tokens] will become the single most common strong authentication method across enterprises by the end of 2010.”

Gartner, June 2007
How Does It Work? (Encryption)

For a user to reach the data he/she must:
1. Insert the eToken device into the USB port
2. Enter the eToken password

As a result:
- Only authorized users can decrypt sensitive data
- The private key stored on-board the token
  - Key does not reside in the vulnerable PC Environment
How Does It Work? (Pre-Boot Authentication)

For a user to start the boot procedure he/she must:

1. Insert the eToken device into the USB port
2. Enter the eToken password

As a result:

- Only authorized users can boot the PC
- With encryption – impossible to target hard disk directly
USB Smart Card Tokens – Key Features

- Secure
- Easy to use
- Portable – no need for a separate smart card reader
- Enable easy and secure implementation of certificate-based (PKI) solutions
  - Automatic generation of PKI keys on-board the token
  - Secure and portable storage of PKI keys and certificates
- Enable a variety of security applications in one device – secure Web access, password management, laptop protection, secure e-mails, and more

“The smart card is the user's “Swiss army knife.””
Add Value with Certificate-Based Solutions

Secure Network Access
- **VPN Access** – Certificate-based authentication to your VPN
- **Web Access** – Secure access to your protected Web sites using certificates for SSL authentication
- **Smartcard Logon** – Internal network logon using certificates

Data Security
- **E-mail Signing & Encryption** – Secure two-way e-mail communication between the bank and your customers and partners
- **Digital Signing (Non-Repudiation)** – Signing of transactions and documents using certificates
Benefits

- Establish mutual trust between your organization, your customers, and partners by implementing end-to-end data and network security.

- Increase your online banking revenues
  - Higher confidence in online banking → increased usage

- Decrease your operational costs
  - Increase online vs. offline activities
  - Significantly decrease password-related helpdesk costs

The Result: Significant ROI
Strong Authentication
Check List

...What should I look for in a strong authentication solution?
Strong Authentication Solution Check List

- **Secure**
  - Smart-card-based (USB Token, SC)
  - Provides secure on-board generation of keys
  - Enables secure storage of personal credentials such as passwords and digital certificates
  - Robust strong authentication process – requires strong passwords

- **Easy to Deploy**
  - Enables easy token deployment via automated distribution, enrollment and personalization (i.e. individual or group characteristics) capabilities
  - Provides user self-service token enrollment
Strong Authentication Solution Check List

- **Easy to Use**
  - Easy and intuitive for users

- **Easy to Manage**
  - Comprehensive system for managing the solution
  - Doesn’t require extensive changes and heavy investments in IT infrastructure OS support certificate.
  - Enables a range of token life-cycle management functions
    - Token enrollment, maintenance, revocation, and more
    - Automatic backup and restoration of user credentials
    - Handling of lost and damaged tokens
  - Provides user self-service management capabilities
Strong Authentication Solution Check List

➢ **Portable**
  – Functional in a range of environments, including home, work and public locations, such as Internet cafés
  – Fully portable and easy to carry

➢ **Value-Added Enabler**
  – Gives you the ability to provide a wide variety of security services – all with the same token:
    • Laptop security
    • Credential management
    • File encryption
    • And more…
Aladdin Vision & Product Lines

Aladdin’s vision is to be the leading provider of security solutions to:

- Protect Digital Assets
- Enable Secure Business
- Create, Sell, Distribute and Use Digital Content

**Software Rights Management**

HASP SRM
Hardware or software-based protection and licensing solution for software vendors
Target Market: Software Publishers and System Vendors

**Authentication**

eToken, SafeWord
Devices for two-factor authentication, password and digital identity management
Target Market: Enterprise, Education, Banking, Pharmacy, Government

**Content Security**

eSafe
Gateway-based anti-virus protection, anti-spyware, content security, web browsing security and proactive email security
Target Market: Enterprise and ISP’s
Chen Arbel
Vice President, Strategic Development
Authentication Unit & Software DRM
Aladdin Knowledge Systems

Chen.Arbel@Aladdin.com
www.aladdin.com