

IS511

Introduction to Information Security

Usable Security

Yongdae Kim



User Interface Failures

Humans

“Humans are incapable of securely storing high-quality cryptographic keys, and they have unacceptable speed and accuracy when performing cryptographic operations. (They are also large, expensive to maintain, difficult to manage, and they pollute the environment. It is astonishing that these devices continue to be manufactured and deployed. But they are sufficiently pervasive that **we must design our protocols around their limitations.**)”

— C. Kaufman, R. Perlman, and M. Speciner.
Network Security: PRIVATE Communication in a PUBLIC World.
2nd edition. Prentice Hall, page 237, 2002.

Humans are weakest link

- ✿ Most security breaches attributed to “human error”
- ✿ Social engineering attacks proliferate
- ✿ Frequent security policy compliance failures
- ✿ Automated systems are generally more predictable and accurate than humans

Why are humans in the loop at all?

- ✿ Don't know how or too expensive to automate
- ✿ Human judgments or policy decisions needed
- ✿ Need to authenticate humans

The human threat

- ❁ **Malicious** humans who will attack system
- ❁ Humans who are **unmotivated** to perform security-critical tasks properly or comply with policies
- ❁ Humans who **don't know** when or how to perform security-critical tasks
- ❁ Humans who are **incapable** of performing security-critical tasks

Need to better understand humans in the loop

- ✿ Do they know they are supposed to be doing something?
- ✿ Do they understand what they are supposed to do?
- ✿ Do they know how to do it?
- ✿ Are they motivated to do it?
- ✿ Are they capable of doing it?
- ✿ Will they actually do it?

Internet Security Warning



The server you are connected to is using a certificate that cannot be verified.

Allow access



Allow application access to keyring?

The application 'evolution-alarm-notify' (/usr/lib/evolution/2.22/evolution-alarm-notify) wants to access the password for 'Google://http://www.google.com/calendar/feeds/cristian.bravo@gmail.com/private/full' in the default keyring.

Sleep warning

Your laptop will not sleep if you shut the lid as a running program has prevented this.
Some laptops can overheat if they not sleep when the lid is closed.



Are you sure you want to turn on private browsing?

When private browsing is turned on, webpages are not added to the history, items are automatically removed from the Downloads window, information isn't saved for AutoFill (including names and passwords), and searches are not added to the pop-up menu in the Google search box. Until you close

Encryption Problems



Microsoft Office Outlook had problems encrypting this message because the following recipients had missing or invalid certificates, or conflicting or unsupported encryption capabilities:

mitsu@intermail.co.il

Continue will encrypt and send the message but the listed recipients may not be able to read it.

Send Unencrypted

Continue

Security Warning

"C:\Documents and Settings\user name\Local Settings\Temporary Internet Files\test.doc" contains macros.

Macros may contain viruses. It is usually safe to disable macros, but if the macros are legitimate, you may lose some functionality.

Disable Macros

Enable Macros

More Info

SSL Warnings



High Risk of Security Compromise

Your connection to *cameo.library.cmu.edu* is either being intercepted by another party or someone is impersonating *cameo.library.cmu.edu*.

An attacker is attempting to steal information that you are sending to *cameo.library.cmu.edu*. We advise you to contact this company by telephone or using a different computer that does not yield this warning.

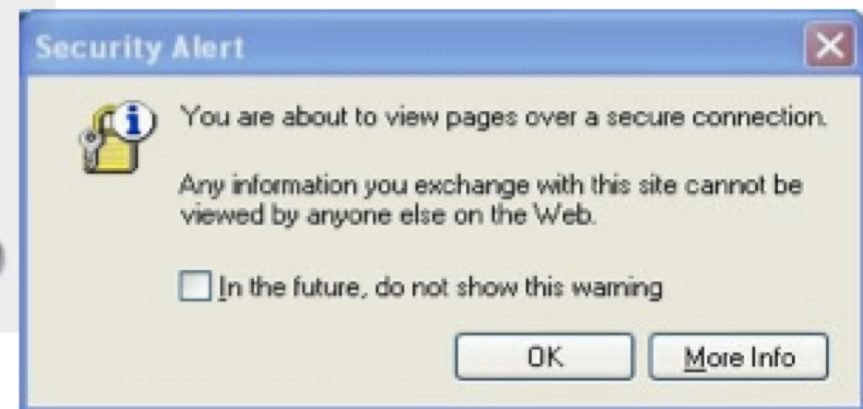
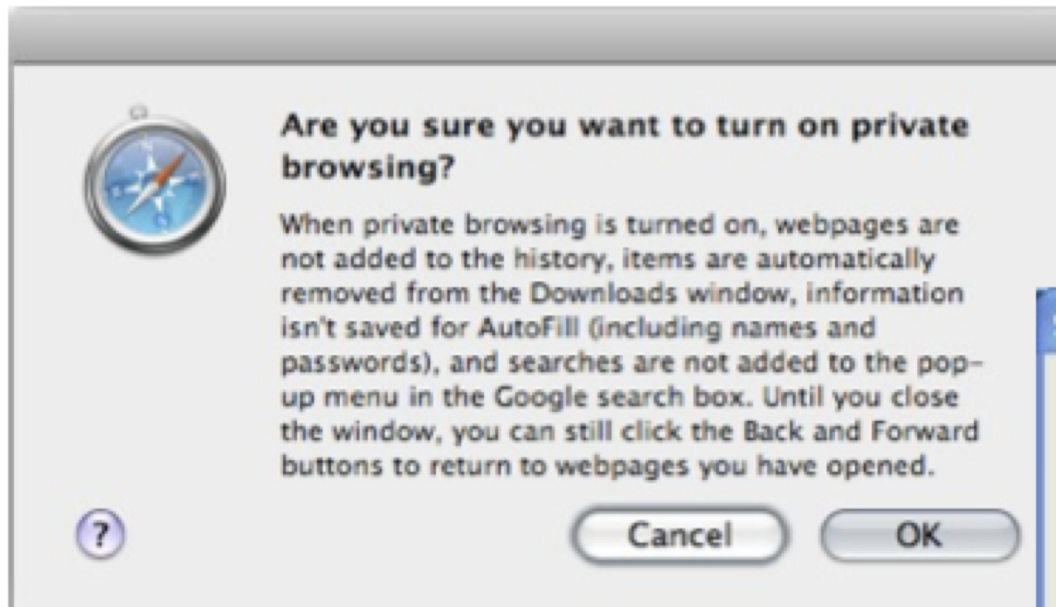
Get Me Out of Here!

Why was this site blocked?

[Ignore this warning](#)

False Alarm Effect

- ❁ “Detection system” \approx “System”
- ❁ If risk is not immediate, warning the user will decrease her trust on the system



Patco Construction vs. Ocean Bank

- ❁ Hacker stole ~\$600K from Patco through Zeus
- ❁ The transfer alarmed the bank, but ignored
 - ❁ “substantially increase the risk of fraud by asking for security answers for every \$1 transaction”
 - ❁ “neither monitored that transaction nor provided notice before completed”
 - ❁ “commercially unreasonable”
 - ▶ Out-of-Band Authentication
 - ▶ User-Selected Picture
 - ▶ Tokens
 - ▶ Monitoring of Risk-Scoring Reports

Password Authentication

Definitions

- ❁ Identification - a claim about identity
 - ▶ Who or what I am (global or local)
- ❁ Authentication - confirming that claims are true
 - ▶ I am who I say I am
 - ▶ I have a valid credential
- ❁ Authorization - granting permission based on a valid claim
 - ▶ Now that I have been validated, I am allowed to access certain resources or take certain actions
- ❁ Access control system - a system that authenticates users and gives them access to resources based on their authorizations
 - ▶ Includes or relies upon an authentication mechanism
 - ▶ May include the ability to grant coarse or fine-grained authorizations, revoke or delegate authorizations
 - ▶ Also includes an interface for policy configuration and management

Building blocks of authentication

✿ Factors

- ▶ Something you know (or recognize)
- ▶ Something you have
- ▶ Something you are

✿ Two factors are better than one

- ▶ Especially two factors from different categories

✿ What are some examples of each of these factors?

✿ What are some examples of two-factor authentication?

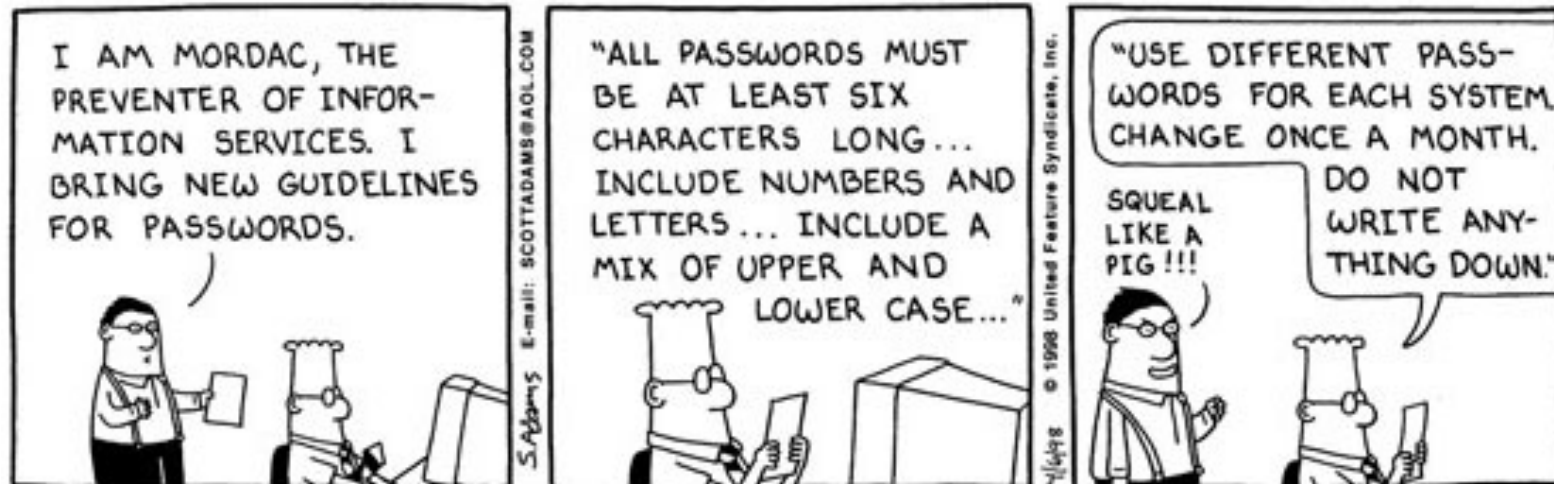
Authentication mechanisms

- ✿ Text-based passwords
- ✿ Graphical passwords
- ✿ Hardware tokens
- ✿ Public key crypto protocols
- ✿ Biometrics

Evaluation

- ✿ Accessibility
- ✿ Memorability
- ✿ Security
- ✿ Cost
- ✿ Environmental considerations

Typical password advice



© Scott Adams, Inc./Dist. by UFS, Inc.

Typical password advice

- * Pick a hard to guess password
- * Don't use it anywhere else
- * Change it often
- * Don't write it down

So what do you do when every web site you visit asks for a password?

Bank = b3aYZ
Amazon = aa66x!
Phonebill = p\$2\$ta1



Problems with Passwords

* Selection

- Difficult to think of a good password
- Passwords people think of first are easy to guess

* Memorability

- Easy to forget passwords that aren't frequently used
- Difficult to remember “secure” passwords with a mix of upper & lower case letters, numbers, and special characters

* Reuse

- Too many passwords to remember
- A previously used password is memorable

* Sharing

- Often unintentional through reuse
- Systems aren't designed to support the way people work together and share information

Mnemonic Passwords

Four score and seven years ago, our Fathers

First letter of each word (with punctuation)

Substitute numbers for words or similar-looking letters

4sa7ya,oF

Substitute symbols for words or similar-looking letters

4s&7ya,oF

Source: Cynthia Kuo, SOUPS 2006



KAIST

The Promise?

- ❁ Phrases help users incorporate different character classes in passwords
 - ▶ Easier to think of character-for-word substitutions
- ❁ Virtually infinite number of phrases
- ❁ Dictionaries do not contain mnemonics

Source: Cynthia Kuo, SOUPS 2006

Mnemonic password evaluation

- ✿ Mnemonic passwords are not a panacea for password creation
- ✿ No comprehensive dictionary today
- ✿ May become more vulnerable in future
 - Many people start to use them
 - Attackers incentivized to build dictionaries
- ✿ Publicly available phrases should be avoided!

Source: Cynthia Kuo, SOUPS 2006



Password keeper software

- * Run on PC or handheld
- * Only remember one password

Single sign-on

- * Login once to get access to all your passwords

Biometrics



Fingerprint Spoofing

* Devices

- ▶ Microsoft Fingerprint Reader
- ▶ APC Biometric Security device



* Success!

- ▶ Very soft piece of wax flattened against hard surface
- ▶ Press the finger to be molded for 5 minutes
- ▶ Transfer wax to freezer for 10-15 minutes
- ▶ Firmly press modeling material into cast
- ▶ Press against the fingerprint reader

* Replicated several times

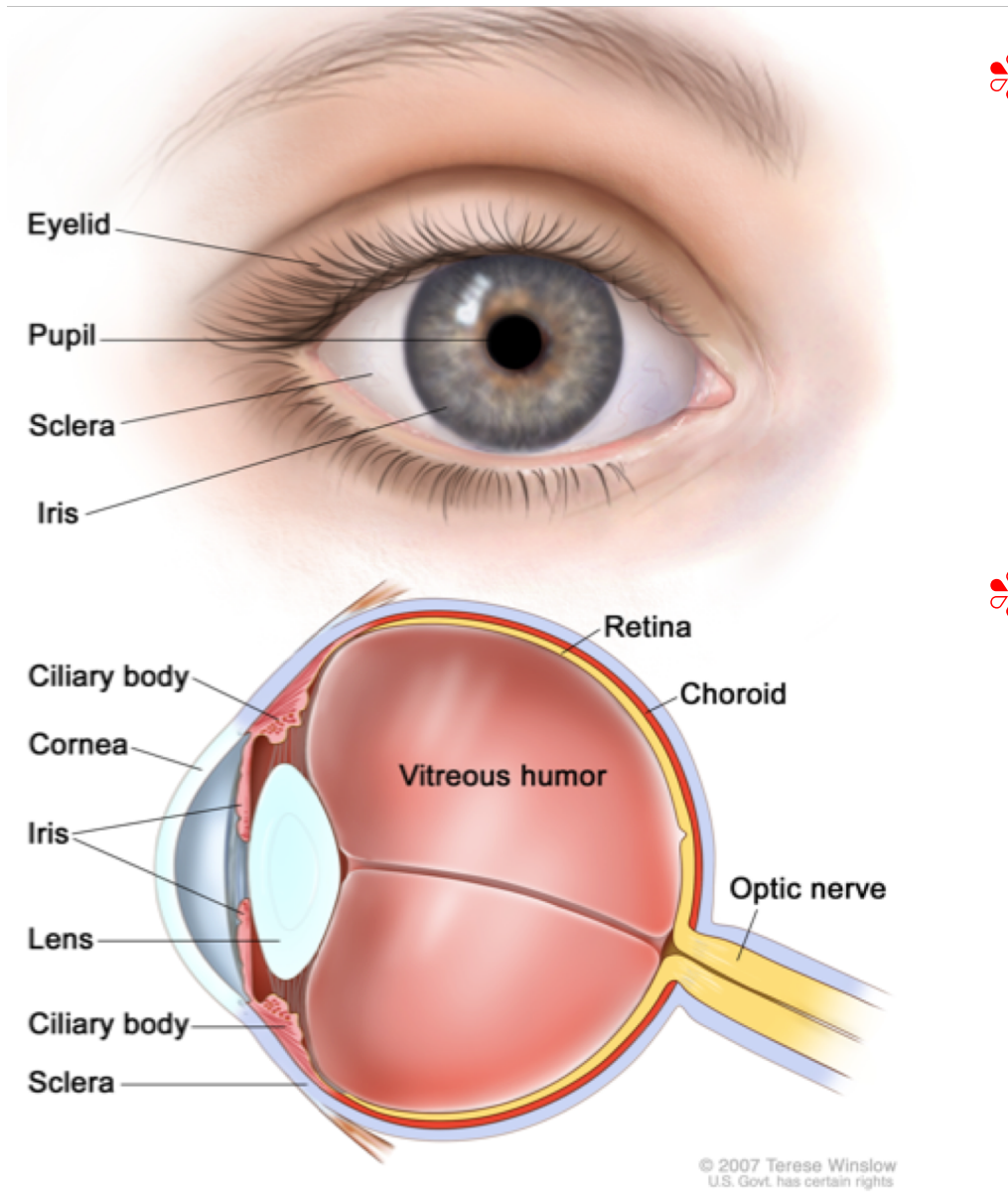
Retina/Iris Scan

* Retinal Scan

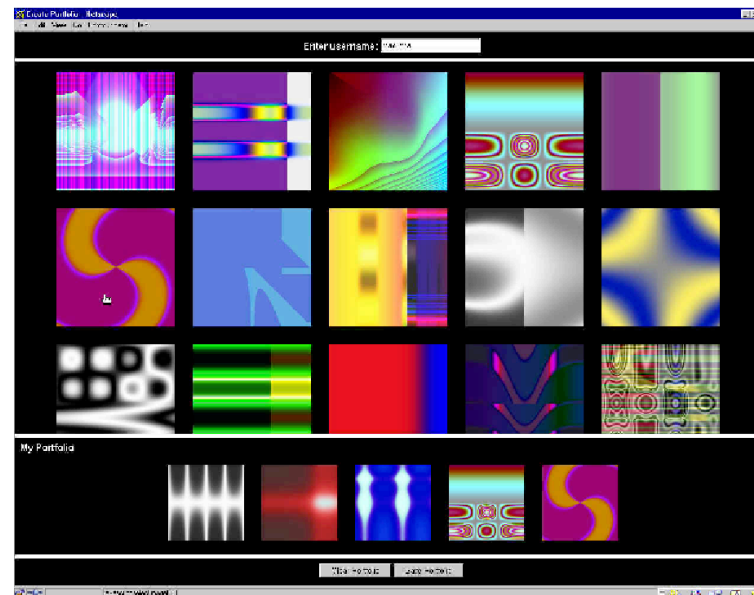
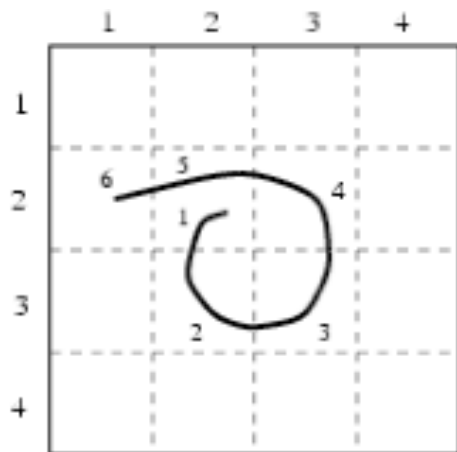
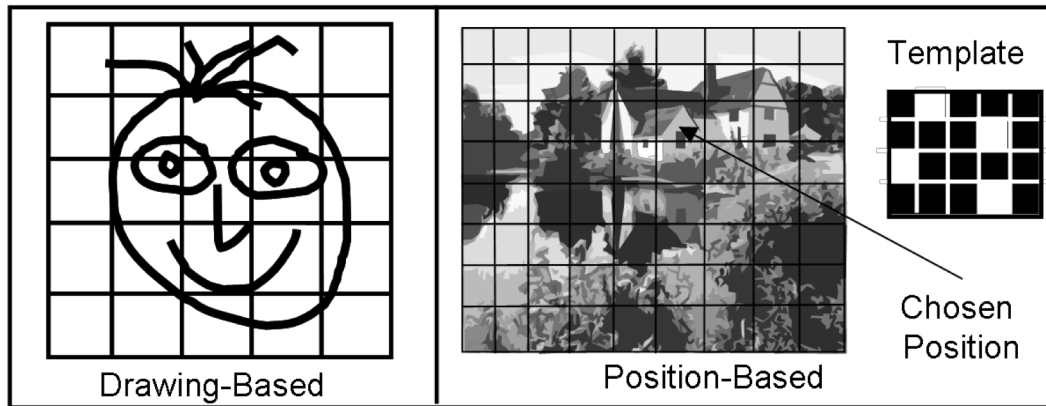
- ▶ Must be close to camera (IR)
- ▶ Scanning can be invasive
- ▶ Not User friendly
- ▶ Expensive

* Iris Scan

- ▶ Late to the game
- ▶ Requires advanced technology to properly capture iris
- ▶ Users do not have to consent to have their identity tested

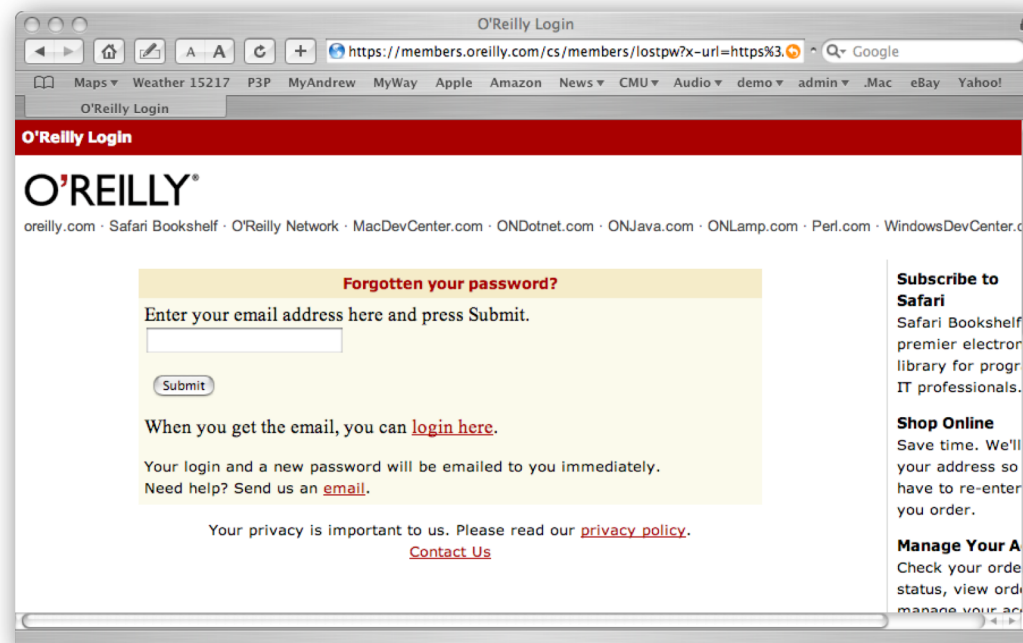


Graphical passwords



“Forgotten password” mechanism

- ✿ Email password or magic URL to address on file
- ✿ Challenge questions
- ✿ *Why not make this the normal way to access infrequently used sites?*



Convenient SecureID 1

- ✿ What problems does this approach solve?
- ✿ What problems does it create?



Source:

http://worsethanfailure.com/Articles/Security_by_Oblivity.aspx

KAIST

Convenient SecureID 2

- ✿ What problems does this approach solve?
- ✿ What problems does it create?



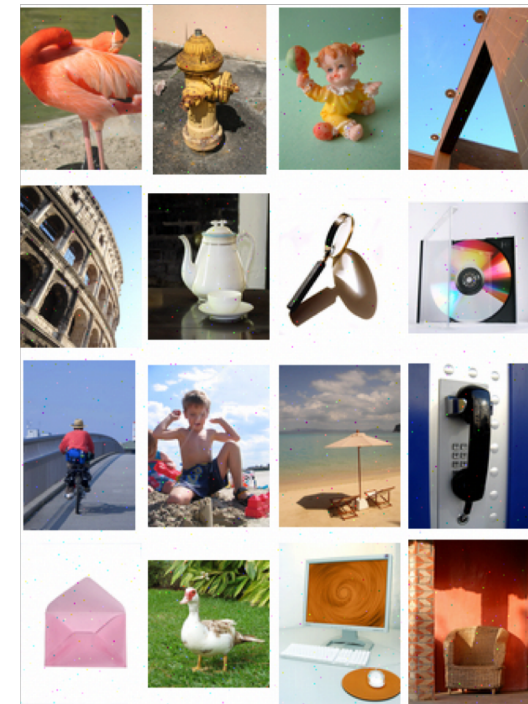
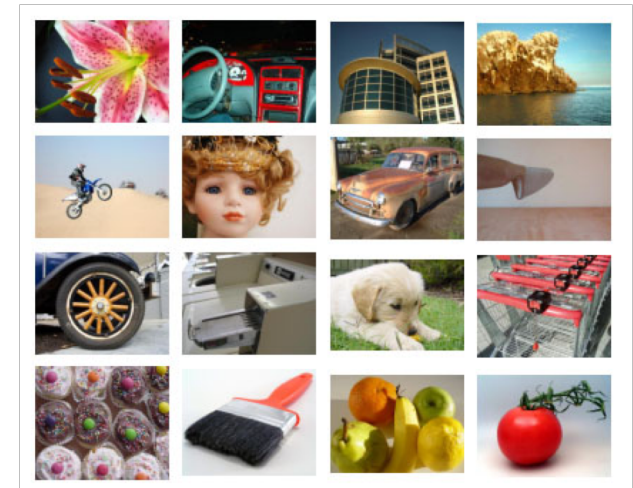
Previously available at:

<http://fob.webhop.net/>



Browser-based mutual authentication

- ❁ Chris Drake's "Magic Bullet" proposal
- ❁ <http://lists.w3.org/Archives/Public/public-usable-authentication/2007Mar/0004.html>
 - User gets ID, password (or alternative), image, hotspot at enrollment
 - Before user is allowed to login they are asked to confirm URL and SSL cert and click buttons
 - Then login box appears and user enters username and password (or alternative)
 - Server displays set of images, including user's image (or if user entered incorrect password, random set of images appear)
 - User finds their image and clicks on hotspot
 - Image manipulation can help prevent replay attacks
- ❁ What problems does this solve?
- ❁ What problems doesn't it solve?
- ❁ What kind of testing is needed



Phishing

Spear Phishing (Targeted Phishing)

- ✿ Personalized mail for a (small) group of targeted users
 - ▶ Employees, Facebook friends, Alumni, eCommerce Customers
 - ▶ These groups can be obtained through identity theft!
- ✿ Content of the email is personalized.
 - ▶ Different from Viagra phishing/spam
- ✿ Combined with other attacks
 - ▶ Zero-day vulnerability: unpatched
 - ▶ Rootkit: Below OS kernel, impossible to detect with AV software
 - ▶ Key logger: Further obtain ID/password
 - ▶ APT (Advanced Persistent Threat): long-term surveillance

Examples of Spear Phishing

SoundbyteF10 | X | Inbox | X

Print all Expand all Forward all

☆ from **Michael Jordan** cs_umn_news@yahoo.com [hide details](#) Feb 21 [Reply](#)

to hopper@cs.umn.edu

date Mon, Feb 21, 2011 at 6:11 AM

subject SoundbyteF10

mailed-by cs.umn.edu

signed-by yahoo.com

View our news and recent events:
[News and Recent Events\(pdf\).](#)

News and Events Contacts
External Relations Coordinator
4-192 Keller Hall
200 Union Street SE
Minneapolis, MN 55455
Phone: [\(612\) 625-2424](tel:6126252424)
Email: news@cs.umn.edu (External Relations Coordinator)

[Reply](#) [Reply to all](#) [Forward](#)

Good Phishing example

Blizzard Entertainment Cataclysm beta

From: **Blizzard Entertainment** (WOWbetaUS@blizzard.com)

⚠ You may not know this sender. [Mark as safe](#) | [Mark as junk](#)


Sent: Tuesday, July 20, 2010 1:20:12 AM

To: 

world of warcraft: Cataclysm Beta Test Invitation!

Get those opt-ins ready for the World of Warcraft: Cataclysm closed beta! The sundering of Azeroth is nigh, and you don't want to be left out in the cold of Northrend when you could be enjoying the sun-drenched beaches on the goblin isle of Kezan. To ensure you're opted-in and eligible as a potential candidate, you'll need a World of Warcraft license attached to your Battle.net account, have your current system specifications uploaded to the Battle.net Beta Profile Settings page, and have expressed interest through the franchise-specific check boxes.

Get the Installer - Log in to your Battle.net account :



Enjoy the game!

Policy and Usability

Amazon.com Privacy Notice

Last updated: October 1, 2008. To see what has changed, [click here](#).

Amazon.com knows that you care how information about you is used and shared, and we appreciate your trust that we will do so carefully and sensibly. This notice describes our privacy policy. **By visiting Amazon.com, you are accepting the practices described in this Privacy Notice.**

- [What Personal Information About Customers Does Amazon.com Gather?](#)
- [What About Cookies?](#)
- [Does Amazon.com Share the Information It Receives?](#)
- [How Secure Is Information About Me?](#)
- [What About Third-Party Advertisers and Links to Other Websites?](#)
- [Which Information Can I Access?](#)
- [What Choices Do I Have?](#)
- [Are Children Allowed to Use Amazon.com?](#)
- [Does Amazon.com Participate in the Safe Harbor Program?](#)
- [Conditions of Use, Notices, and Revisions](#)
- [Examples of Information Collected](#)

What Personal Information About Customers Does Amazon.com Gather?

The information we learn from customers helps us personalize and continually improve your shopping experience at Amazon.com. Here are the types of information we gather.

- **Information You Give Us:** We receive and store any information you enter on our Web site or give us in any other way. [Click here](#) to see examples of what we collect. You can choose not to provide certain information, but then you might not be able to take advantage of many of our features. We use the information that you provide for such purposes as responding to your requests, customizing future shopping for you, improving our stores, and communicating with you.
- **Automatic Information:** We receive and store certain types of information whenever you interact with us. For example, like many Web sites, we use "cookies," and we obtain certain types of information when your Web browser accesses Amazon.com or advertisements and other content served by or on behalf of Amazon.com on other Web sites. [Click here](#) to see examples of the information we receive.
- **E-mail Communications:** To help us make e-mails more useful and interesting, we often receive a confirmation when you open e-mail from Amazon.com if your computer

E-mail Communications

To help us make e-mails more useful and interesting, we often receive a confirmation when you open e-mail from Amazon.com if your computer supports such capabilities. We also compare our customer list to lists received from other companies, in an effort to avoid sending unnecessary messages to our customers. If you do not want to receive a mail or other mail from us, please adjust your [Customer Communication Preferences](#).

Information from Other Sources

We might receive information about you from other sources and add it to our account information. [Click here](#) to see examples of the information we receive.

What About Cookies?

Cookies are alphanumeric identifiers that we transfer to your computer's hard drive through your Web browser to enable our systems to recognize your browser and to provide features such as [A-Z](#) purchasing, [Personalized](#), [Personalized](#) advertisements on other Web sites (e.g., [Amazon Associates](#) with content served by Amazon.com and Web sites using [CheckOut by Amazon](#) payment service), and storage of items in your [Shopping Cart](#) between visits. The main portion of the toolbar on most browsers will tell you how to prevent your browser from accepting new cookies, how to have the browser notify you when you receive a new cookie, or how to disable cookies altogether. Additionally, you can disable or delete similar data used by browser add-ons, such as Flash cookies, by changing the add-on's settings or visiting the Web site of its manufacturer. However, because cookies allow you to take advantage of some of Amazon.com's essential features, we recommend that you leave them turned on. For instance, if you block or otherwise reject our cookies, you will not be able to add items to your [Shopping Cart](#), proceed to [CheckOut](#), or use any Amazon.com products and services that require you to log in.

Does Amazon.com Share the Information It Receives?

Information about our customers is an important part of our business, and we are not in the business of selling it to others. We share customer information only as described below and with subsidiaries Amazon.com, Inc. controls that other are subject to this Privacy Notice or follow practices at least as protective as those described in this Privacy Notice.

Affiliated Businesses We Do Not Control

We work closely with affiliated businesses. In some cases, such as [Warehouse](#) sellers, these businesses operate stores at Amazon.com or sell offerings to you at Amazon.com. In other cases, we operate stores, provide services, or sell product lines jointly with these businesses. [Click here](#) for some examples of co-branded and joint offerings. You can tell when a third party is involved in your transactions, and we share customer information related to these transactions with that third party.

Third-Party Service Providers

We employ other companies and individuals to perform functions on our behalf. Examples include fulfilling orders, delivering packages, handling postal mail and e-mail, removing repetitive information from customer lists, analyzing data, providing marketing assistance, providing search results and links (including paid listings and links), processing credit card payments, and providing customer service. They have access to personal information needed to perform their functions, but may not use it for other purposes.

Franchised Offers

Sometimes we send offers to selected groups of Amazon.com customers on behalf of other businesses. When we do this, we do not give that business your name and address. If you do not want to receive such offers, please adjust your [Customer Communication Preferences](#).

Business Transfers

As we continue to develop our business, we might sell or buy stores, subsidiaries, or business units. In such transactions, customer information generally is one of the transferred business assets but remains subject to the promises made in any pre-existing Privacy Notice (unless, of course, the customer consents otherwise). Also, in the unlikely event that Amazon.com, Inc., or substantially all of its assets are acquired, customer information will of course be one of the transferred assets.

Protection of Amazon.com and Others'

We release account and other personal information when we believe release is appropriate to comply with the law, enforce or apply our [Conditions of Use](#) and other agreements, or protect the rights, property, or safety of Amazon.com, our users, or others. This includes exchanging information with other companies and organizations for fraud prevention and credit risk reduction. Obviously, this does not include selling, renting, sharing, or otherwise disclosing personally identifiable information from customers for commercial purposes in violation of the commitments set forth in this Privacy Notice.

Web Site Content

Other than as set out above, you will receive notice when information about you might go to third parties, and you will have an opportunity to choose not to share the information.

How Secure Is Information About Me?

We work to protect the security of your information during transmission by using [Secure Sockets Layer \(SSL\)](#) software, which encrypts information you send. We reveal only the last five digits of your

When Your Browser Closes or an Error Occurs

you will receive notice when information about you might go to third parties, and you will have an opportunity to choose not to share the information.

How Secure Is Information About Me?

- We work to protect the security of your information during transmission by using [Secure Sockets Layer \(SSL\)](#) software, which encrypts information you send.
- We reveal only the last five digits of your credit card numbers when confirming an order. Of course, we transmit the entire credit card number to the appropriate credit card company during order processing.
- It is important for you to protect against unauthorized access to your password and to your computer. Be sure to sign off when finished using a shared computer. [Click here](#) for more information on how to sign off.

What About Third-Party Advertisers and Links to Other Websites?

Our site includes third-party advertising and links to other Web sites. We do not provide any personally identifiable customer information to these advertisers or third-party Web sites. [Click here](#) for more information about our advertising notices and specifications.

These third-party Web sites and advertisers, or Internet advertising companies working on their behalf, sometimes use technology to send (or "serve") the advertisements that appear on our Web site directly to your browser. This technology requires your IP address when this happens. They may also use cookies, JavaScript, web beacons (also known as action tags or single-pixel gifs), and other technologies to measure the effectiveness of their ads and to personalize advertising content. We do not have access to or control over cookies or other features that they may use, and the information practices of these advertisers and third-party Web sites are not covered by this Privacy Notice. These contact them directly for more information about their privacy practices. In addition, the [Federal Advertising Initiative](#) offers useful information about Internet advertising companies (also called "ad networks" or "network advertisers"), including information about how to opt out of their information collection.

Amazon.com also displays personalized third-party advertising based on personal information about customers, such as purchases at Amazon.com, visits to Amazon Associates Web sites, or use of payment services like [CheckOut](#) by Amazon on other Web sites. [Click here](#) for more information about the personal information that we gather. Although Amazon.com does not provide any personal information to advertisers, advertisers (including ad-serving companies) may assume that users who interact with or click on a personalized advertisement meet their criteria to personalize the ad (for example, users in the neighborhood listed above who bought or browsed for classical music). If you do not want us to use personal information that we gather to allow third parties to personalize advertisements we display to you, please adjust your [Marketing Preferences](#).

Which Information Can I Access?

Amazon.com gives you access to a broad range of information about your account and your interactions with Amazon.com for the limited purpose of viewing and, in certain cases, updating that information. [Click here](#) to see some examples, the list of which will change as our Web site evolves.

What Choices Do I Have?

- As discussed above, you can always choose not to provide information, even though it might be needed to make a purchase or to take advantage of such Amazon.com features as [Buy with 1-Click](#), [Web Logs](#), [Customer Reviews](#), and [Amazon Prime](#).
- You can tell or update certain information on pages such as those referenced in the ["Your Information Can I Access?"](#) section. When you update information, we usually have a view of the prior version for our internal use only.
- If you do not want to receive e-mail or other mail from us, please adjust your [Customer Communication Preferences](#). If you do not want to receive [CheckOut by Amazon](#) and other legal notices from us, such as this Privacy Notice, these notices will still govern your use of Amazon.com, and it is your responsibility to review them for changes.
- If you do not want us to use personal information that we gather to allow third parties to personalize advertisements we display to you, please adjust your [Marketing Preferences](#).
- The Help portion of the toolbar on most browsers will tell you how to prevent your browser from accepting new cookies, how to have the browser notify you when you receive a new cookie, or how to disable cookies altogether. Additionally, you can disable or delete similar data used by browser add-ons, such as Flash cookies, by changing the add-on's settings or visiting the Web site of its manufacturer. However, because cookies allow you to take advantage of some of Amazon.com's essential features, we recommend that you leave them turned on. For instance, if you block or otherwise reject

Are Children Allowed to Use Amazon.com?

Amazon.com does not sell products for purchase by children. We will shoo products for purchase by adults. If you are under 18, you may use Amazon.com only with the involvement of a parent or guardian.

Does Amazon.com Participate in the Safe Harbor Program?

Amazon.com is a participant in the Safe Harbor program developed by the U.S. Department of Commerce and the European Union. We have certified that we adhere to the Safe Harbor Privacy Principles agreed upon by the U.S. and the E.U. For more information about the Safe Harbor and to view our certification, visit the [U.S. Department of Commerce Safe Harbor](#) Web site. If you would like to contact Amazon.com directly about the Safe Harbor program, please send an e-mail to [safeharbor@amazon.com](#).

Conditions of Use, Notices, and Revisions

If you choose to visit Amazon.com, your visit and any disclosure you provide is subject to this Notice and our [Conditions of Use](#), including limitations on damages, resolution of disputes, and application of the law of the state of Washington. If you have any concern about privacy at Amazon.com, please [contact us](#) with a thorough description, and we will try to resolve it. Our business changes constantly, and our Privacy Notice and the [Conditions of Use](#) will change also. We may e-mail periodic reminders of our notices and conditions, unless you have indicated an e-mail opt-out choice. Check our Web site frequently for any recent changes. Unless stated otherwise, our current Privacy Notice applies to all information that we have about you and your account. We stand behind the promises we make, however, and will never intentionally change our policies and practices to make them less protective of customer information collected in the past without the consent of affected customers.

Related Practices and Information

- [Conditions of Use](#)
- [Discussion Board](#)
- [Community Rules](#)
- [Your Account](#)
- [Your Account Dashboard](#)
- [Your Amazon.com Marketing Preferences](#)

Examples of Information Collected

Information You Give Us

You provide that such information when you search, buy, sell, add, and participate in a contest or questionnaire, or communicate with customer service. For example, you provide information when you search for a product, place an order through Amazon.com or one of our third-party sellers, provide information in [Your Profile](#) (and you might have more than one if you have used more than one e-mail address when shopping with us) or [Your Email](#), communicate with us by phone, e-mail, or otherwise, complete a questionnaire or a contest entry form, complete [Buy with 1-Click](#) or other gift registries, provide employer information when opening a corporate account, participate in [Discussion Boards](#) or other community features, provide and rate [Reviews](#), specify a [Special Question](#), provide information with [Amazon Events](#), and employ other Personal Notification Services, such as [Available to Order Notifications](#). As a result of these actions, you might supply us with such information as your name, address, and phone numbers, credit card information, people to whom purchases have been shipped, including addresses and phone numbers; journal (with addresses and phone numbers) listed in [A-Z](#) selling; e-mail addresses of [Amazon Direct](#) and other people; content of reviews and e-mails to us; personal description and photograph in [Your Profile](#); and financial information, including Social Security and driver's license numbers.

Automatic Information

Examples of the information we collect and analyze include the Internet protocol (IP) address used to connect your computer to the Internet, logs, e-mail address, password, cookie and connection information such as browser type, version, and time zone setting, browser plug-in types and versions, operating system, and platform; purchase history, which we sometimes aggregate with similar information from other customers to create features such as [Discussion Boards](#) and [Buy with 1-Click](#); the full contents of [Your Profile](#) and [Your Reviews](#); by, through, and from our Web site, including date and time; cookie number; products you viewed or searched for; and the phone number you use to call our 800 number. We may also use browser data such as cookies, Flash cookies (also known as [Flash Local Shared Objects](#)), or similar

Information from Other Sources

We might receive information about you from other sources and add it to our account information. Examples include information from our [Warehouse](#) sellers, [Amazon.com](#) or other businesses that sell offerings to you at Amazon.com, [Amazon.com](#) or other businesses that we operate, [Amazon.com](#) or other businesses that we provide services or sell product lines jointly with, [Amazon.com](#) or other businesses that we employ, and other companies and individuals that we employ to perform functions on our behalf. Examples include fulfillment providers, delivery services, handling postal mail and e-mail, removing repetitive information from customer lists, analyzing data, providing marketing assistance, providing search results and links (including paid listings and links), processing credit card payments, and providing customer service. They have access to personal information needed to perform their functions, but may not use it for other purposes.

Third-Party Service Providers

We employ other companies and individuals to perform functions on our behalf. Examples include fulfilling orders, delivering packages, handling postal mail and e-mail, removing repetitive information from customer lists, analyzing data, providing marketing assistance, providing search results and links (including paid listings and links), processing credit card payments, and providing customer service. They have access to personal information needed to perform their functions, but may not use it for other purposes.

Franchised Offers

Sometimes we send offers to selected groups of Amazon.com customers on behalf of other businesses. When we do this, we do not give that business your name and address. If you do not want to receive such offers, please adjust your [Customer Communication Preferences](#).

Business Transfers

As we continue to develop our business, we might sell or buy stores, subsidiaries, or business units. In such transactions, customer information generally is one of the transferred business assets but remains subject to the promises made in any pre-existing Privacy Notice (unless, of course, the customer consents otherwise). Also, in the unlikely event that Amazon.com, Inc., or substantially all of its assets are acquired, customer information will of course be one of the transferred assets.

Protection of Amazon.com and Others'

We release account and other personal information when we believe release is appropriate to comply with the law, enforce or apply our [Conditions of Use](#) and other agreements, or protect the rights, property, or safety of Amazon.com, our users, or others. This includes exchanging information with other companies and organizations for fraud prevention and credit risk reduction. Obviously, this does not include selling, renting, sharing, or otherwise disclosing personally identifiable information from customers for commercial purposes in violation of the commitments set forth in this Privacy Notice.

Web Site Content

Other than as set out above, you will receive notice when information about you might go to third parties, and you will have an opportunity to choose not to share the information.

Cost of Reading Policy Cranor et al.

❁ $T_R = p \times R \times n$

- ▶ p is the population of all Internet users
- ▶ R is the average time to read one policy
- ▶ n is the average number of unique sites Internet users visit annually

❁ $p = 221$ million Americans online (Nielsen, May 2008)

❁ $R = \text{avg time to read a policy} = \# \text{ words in policy} / \text{reading rate}$

- ▶ To estimate words per policy:

- 🌿 Measured the policy length of the 75 most visited websites

- 🌿 Reflects policies people are most likely to visit

❁ Reading rate = 250 WPM Mid estimate: 2,514 words / 250 WPM = 10 minutes

* n = number of unique sites per year

▶ Nielsen estimates Americans visit 185 unique sites in a month:

▶ but that doesn't quite scale x12, so 1462 unique sites per year.

* $T_R = p \times R \times n$

= 221 million x 10 minutes x 1462 sites

* $R \times n = 244$ hours per year per person

P3P: Platform for Privacy Preferences

- ✿ A framework for automated privacy discussions
 - ▶ Web sites disclose their privacy practices in standard machine-readable formats
 - ▶ Web browsers automatically retrieve P3P privacy policies and compare them to users' privacy preferences
 - ▶ Sites and browsers can then negotiate about privacy terms

Acme Privacy Summary

Scope

This policy discloses what information we gather about you when you visit any of our Web sites (all acme.com and Acme Network sites) or buy product directly from us. For more details, please refer to our [full privacy policy](#).

Personal Information

Acme collects two kinds of information about users:

1. data that users volunteer by signing up to receive news and product information, entering contests, completing surveys, or buying directly from us
2. aggregated tracking data we collect when users interact with us, such as access logs and web cookies

For more information about our information collection practices, please see our [full policy](#).

Uses

- We use the personal information you provide voluntarily to send information you've requested and to fulfill orders.
- When you sign up online to receive Acme Network newsletters, Acme product and company news, and to participate in talkbacks on our sites you must provide your name, email address, and a password. We never sell or rent your email address or other personally identifiable information you provide us under these circumstances.
- When you register for an Acme conference, or sign up for a conference email list, we will send you email announcements and updates about Acme conferences. We send conference brochures to past conference attendees.
- When you order books directly from us, or request book catalogs, we add you to our snailmail list, and we'll send you catalogs and other marketing pieces.
- When you enter a contest or sweepstakes, we may ask for your name, address, and email

The Acme Policy

types of information	how we use your information					who we share your information with	
	provide service & maintain site	research & development	marketing	telemarketing	profiling	other companies	public forums
contact information	!	!	OUT	OUT	☐	IN	☐
cookies	!	!	OUT	OUT	☐	IN	☐
demographic information	☐	☐	☐	☐	☐	☐	☐
financial information	☐	☐	☐	☐	☐	☐	☐
health information	☐	☐	☐	☐	☐	☐	☐
preferences	!	!	OUT	OUT	☐	IN	!
purchasing information	!	!	OUT	OUT	☐	IN	☐
social security number & govt ID	!	☐	☐	☐	☐	☐	☐
your activity on this site	!	!	OUT	OUT	☐	IN	!
your location	☐	☐	☐	☐	☐	☐	☐