Participants

Individuals

Enabling System Trust fo ~~Users~~

L Jean Camp

People

infosecon.net

Brain Surgeons

ljean.com

Outline

- Theoretical discussion of security decisions as risk communication
- Risk perception, expressed preference
- Example of two systems
- Intermittent snark examples

An Aside

Mental models of designers also matter.

Participants engage with us on risk decisions in a given context.
Users Use (and are used by).

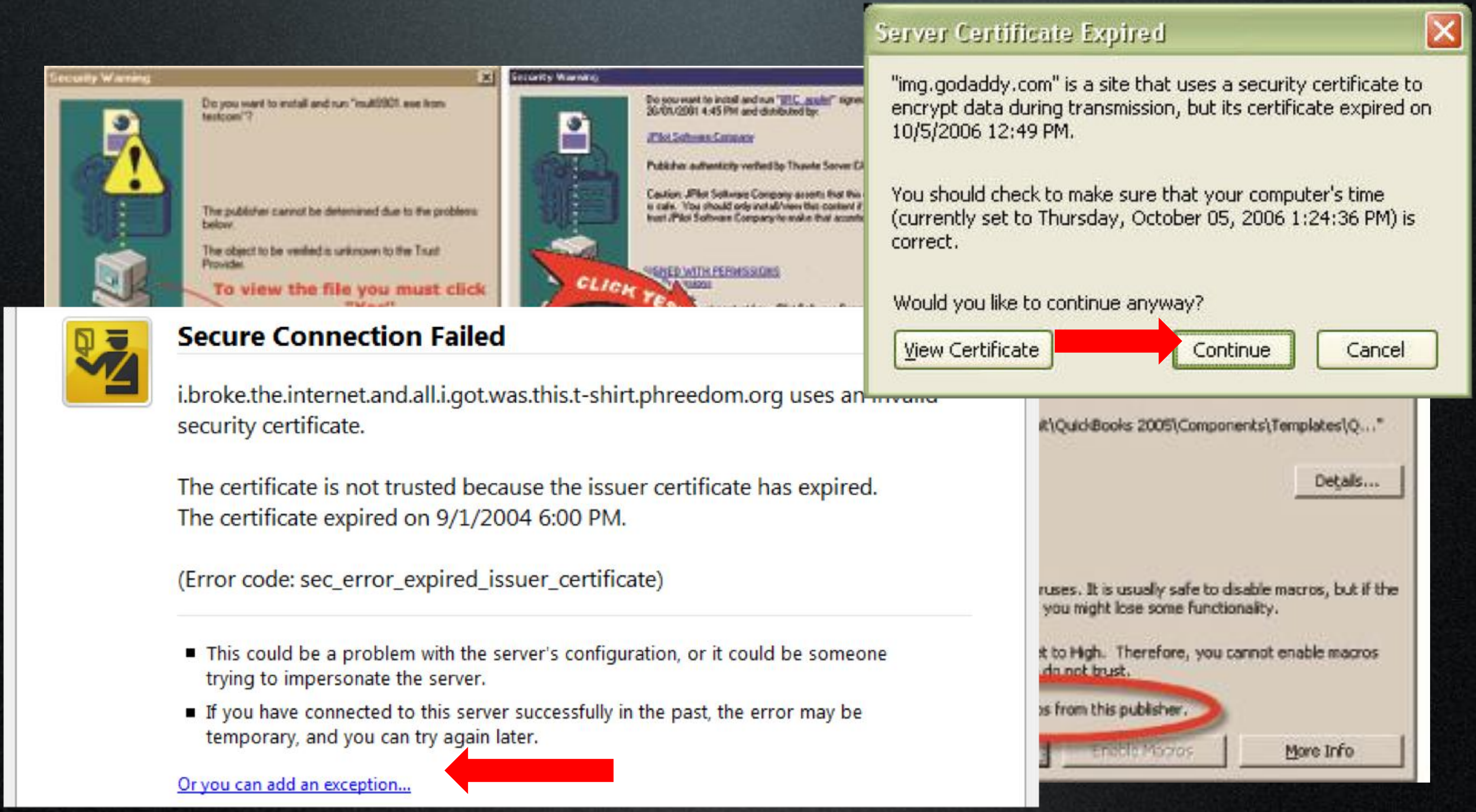
People Do Not Engage in the Calculus of Risk

- Consider two failures
  - A pop-up notification of a change in privacy policy
  - A display of another person’s information (cc#, DoB, details)
  - Individuals responded significantly more strongly to the first
  - A failure in benevolence more critical than competence

Individual Risk Decision

- A specific person making a potentially irrational risk decision
  - Using local client records of that individual
  - Using risk perspectives from other domains
  - Depending on their mental models for decision guidance
- Solve the problem of the homophilus individual as well as the problem of the heterogeneous network

Decades of Consistent Security Training



Security Warning

Do you want to install and run "msft0901.exe from testcom"?

The publisher cannot be determined due to the problems below

The object to be verified is unknown to the Trust Provider

To view the file you must click "Yes!"

Security Warning

Do you want to install and run "IRC_applet" signed 20/01/2001 4:45 PM and distributed by:

JPilot Software Company

Publisher authenticity verified by Thawte Server CA

Caution: JPilot Software Company asserts that this is safe. You should only install/view this content if trust JPilot Software Company to make that assertion

SIGNED WITH PERMISSIONS

Server Certificate Expired

"img.godaddy.com" is a site that uses a security certificate to encrypt data during transmission, but its certificate expired on 10/5/2006 12:49 PM.

You should check to make sure that your computer's time (currently set to Thursday, October 05, 2006 1:24:36 PM) is correct.

Would you like to continue anyway?

Secure Connection Failed

i.broke.the.internet.and.all.i.got.was.this.t-shirt.phreedom.org uses an invalid security certificate.

The certificate is not trusted because the issuer certificate has expired. The certificate expired on 9/1/2004 6:00 PM.

(Error code: sec_error_expired_issuer_certificate)

- This could be a problem with the server's configuration, or it could be someone trying to impersonate the server.
- If you have connected to this server successfully in the past, the error may be temporary, and you can try again later.

Or you can add an exception…

it\QuickBooks 2005\Components\Templates\Q…"

ruses. It is usually safe to disable macros, but if the you might lose some functionality.

t to High. Therefore, you cannot enable macros do not trust.

s from this publisher.

Somehow there is still a problem

Why Usable Security is Not Usability

- People rarely want to perform security tasks
- People often want to subvert, minimize, or ignore security
- People need to trust their machines, achieving suspicion is not a goal

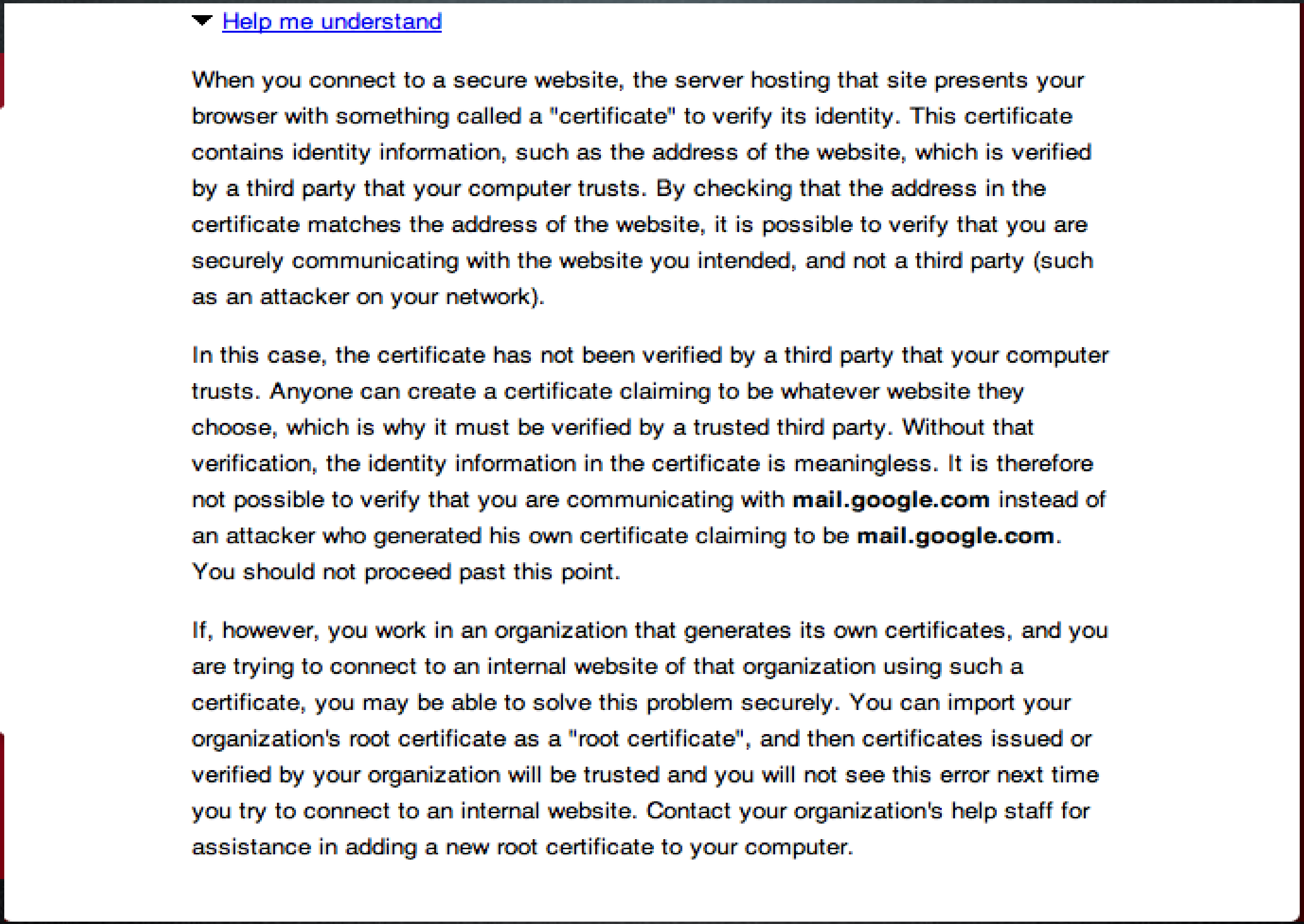
Usable Transparent Design

- Make the connection between action and consequence clear
- Risk is inherently probabilistic
  - There may be no consequence
  - Consequence is very likely to be delayed
  - Consequence may prove catastrophic
  - Action-risk-consequence information may be overwhelming

Opaque

- Security as a default
- Require explicit confirmation
- May be disabling
  - So individuals disable it

Opaque Stops Actions



▼ Help me understand

When you connect to a secure website, the server hosting that site presents your browser with something called a "certificate" to verify its identity. This certificate contains identity information, such as the address of the website, which is verified by a third party that your computer trusts. By checking that the address in the certificate matches the address of the website, it is possible to verify that you are securely communicating with the website you intended, and not a third party (such as an attacker on your network).

In this case, the certificate has not been verified by a third party that your computer trusts. Anyone can create a certificate claiming to be whatever website they choose, which is why it must be verified by a trusted third party. Without that verification, the identity information in the certificate is meaningless. It is therefore not possible to verify that you are communicating with **mail.google.com** instead of an attacker who generated his own certificate claiming to be **mail.google.com**. You should not proceed past this point.

If, however, you work in an organization that generates its own certificates, and you are trying to connect to an internal website of that organization using such a certificate, you may be able to solve this problem securely. You can import your organization's root certificate as a "root certificate", and then certificates issued or verified by your organization will be trusted and you will not see this error next time you try to connect to an internal website. Contact your organization's help staff for assistance in adding a new root certificate to your computer.

Translucent Security

- Context dependent
- Designed for the task and the risk
- A single interaction or narrative
- Incentives must be visible, but also participants must be allowed to pay the risk price
- Participants understand the context, security engineers understand the risk

Online and Offline Risks

- Offline risks inherently physical
- No true fear online
- Classic nine-dimensional risk perception model
- How can we use knowledge of offline risks to design security online?
    - Examine dimensions of perception that inform risk decisions

One of Nine

- Voluntariness or Involuntary

Smoking vs. Air pollution

Two of Nine

- Immediacy

Jaywalking vs. Global warming

Three of Nine

- Knowledge about the risk to the exposed

Genetically modified crops vs. a hot stove

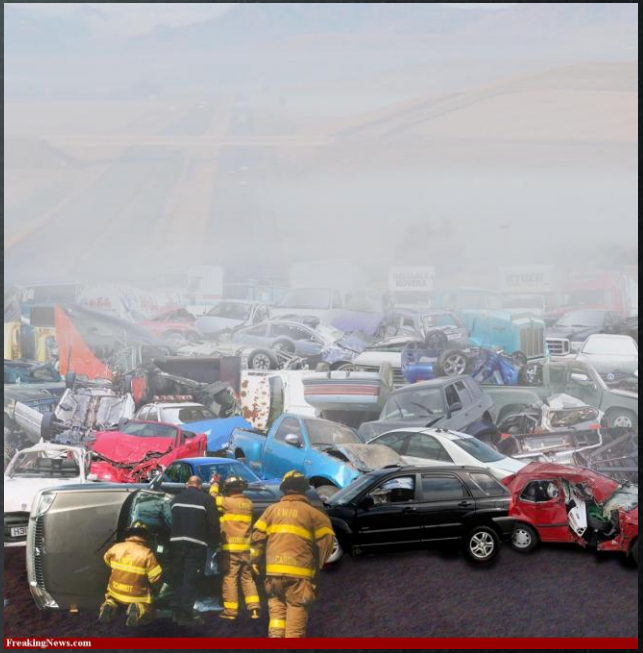
Four of Nine

- Knowledge of the risk to science

Pharmaceutical interaction vs. alcohol

Five of Nine

- Controllability



Airplane crash vs. an automobile crash

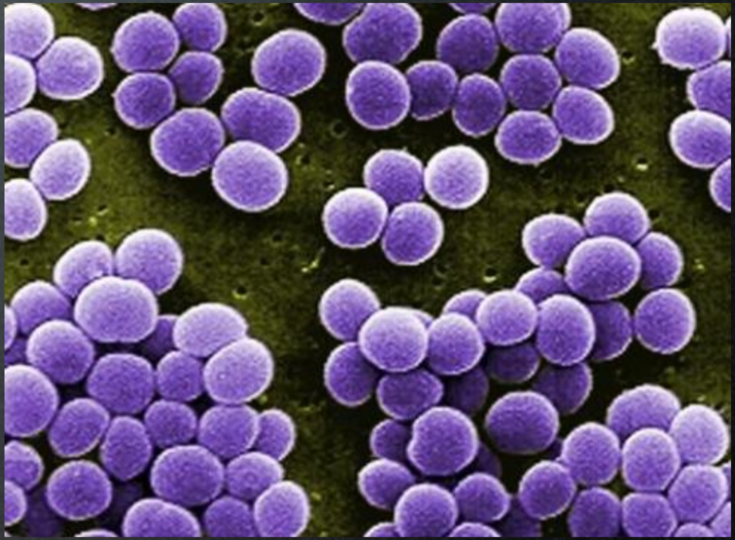
Six of Nine

- Newness

Coal-burning facility vs. Catawba nuclear facility

Seven of Nine

- Common-Dread



Snake bite vs. the flu

Eight of Nine

- Chronic-Catastrophic

Nine of Nine

- Severity

Sky diving vs. chopping & cutting

What About Virtual Risks?

- Virus, Botnets, Trojan, Malware, Spam, Identify Theft, Phishing, Key Loggers, Surveillance, Worms, Virtual Stalking, Cookies, Zombies, Spoofing, and Spyware
- n=95

Computing Risks Are
Not Scary or Scary ?

- Not apparently immediate
- Chronic
- Not dreadful
- Perceived as being understood by experts

- New
- Not understood

- **Severity!!**
- Voluntary?
- Uncontrollable?

Use What We Can

- Condensed to four dimension
  - temporal impact (newness and common-dread)
  - control (voluntariness and controllability)
  - familiarity (knowledge to science, knowledge to the exposed)
  - impact (severity, chronic, immediacy)

Make Risk Appear Immediate
With Timely Warnings and Mitigation

Beyond Usability

- Computing will not be scary so mitigation has to be very easy
- Risk information may be unpleasant
- Visible user-action-system-consequence may be overwhelming or context-dependent
- Be timely, careful, targeted, & personalized

Voluntary & Uncontrollable?

- Folk Practices
  - Eavesdropping: Turn screens sideways
  - Big fish/ targeted crime: nothing
  - Infectious/street crime: back-up
  - Patching, rarely
  - Firewalls, never
  - Updated anti-virus: medical model, ubiquitous
- Current knowledge
  - Be careful what websites you visit
  - Don’t click on attachments

Risk Communication

- Communication of specific risk
- Effective automation/ support of risk mitigation
- No communication is welcome if ill-timed

Phishing Video

- Informative
- Nontechnical
- Useful
- Actionable
- Grounds risk in an available mental model
- Makes risk appear immediate

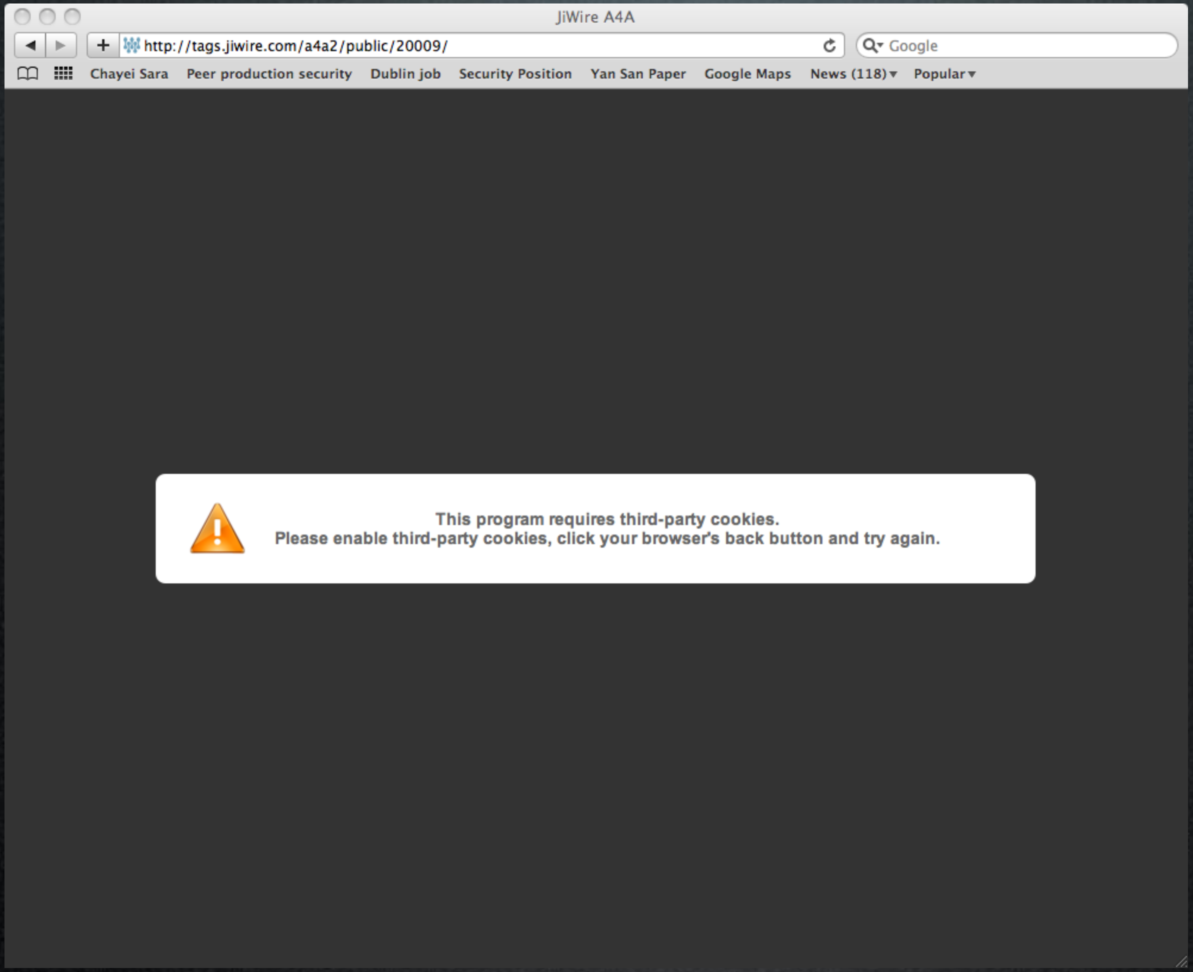
Informative

WATCH OUT!!

THIS IS A BARREL

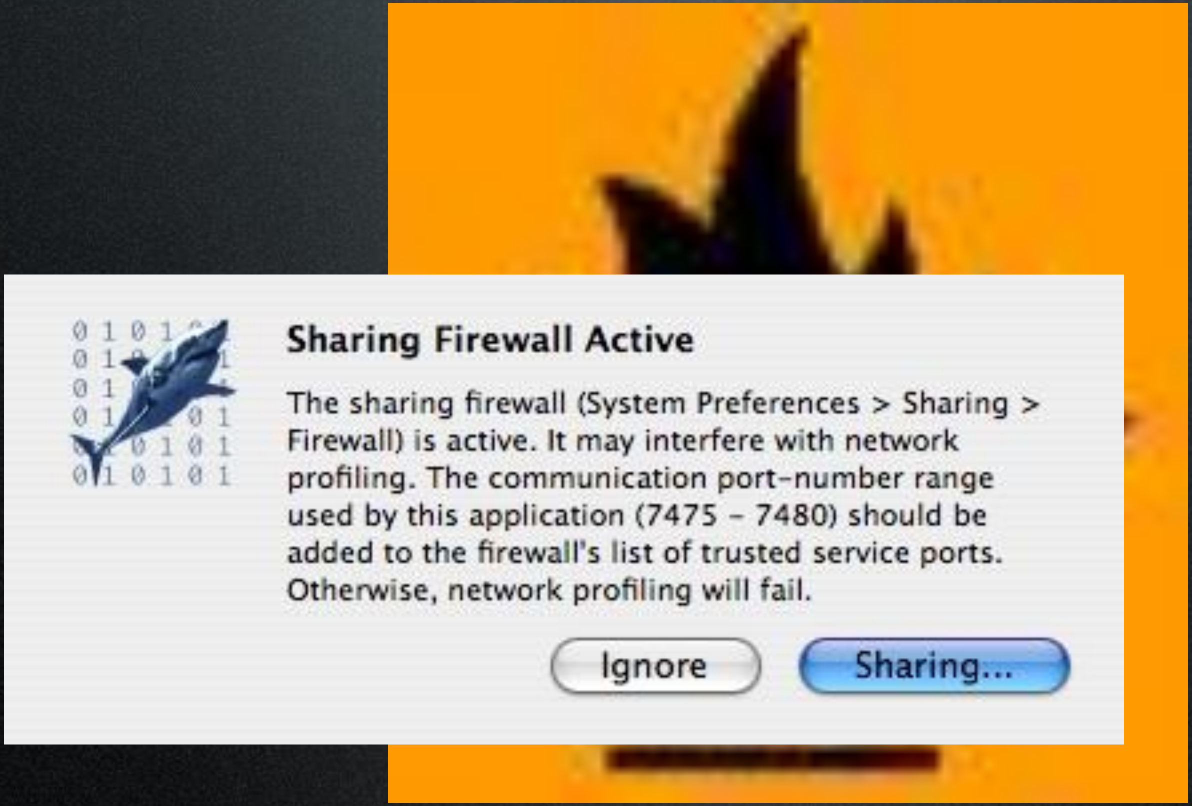
SOMETHING MAY BE IN IT

Useful?



This program requires third-party cookies.
Please enable third-party cookies, click your browser's back button and try again.

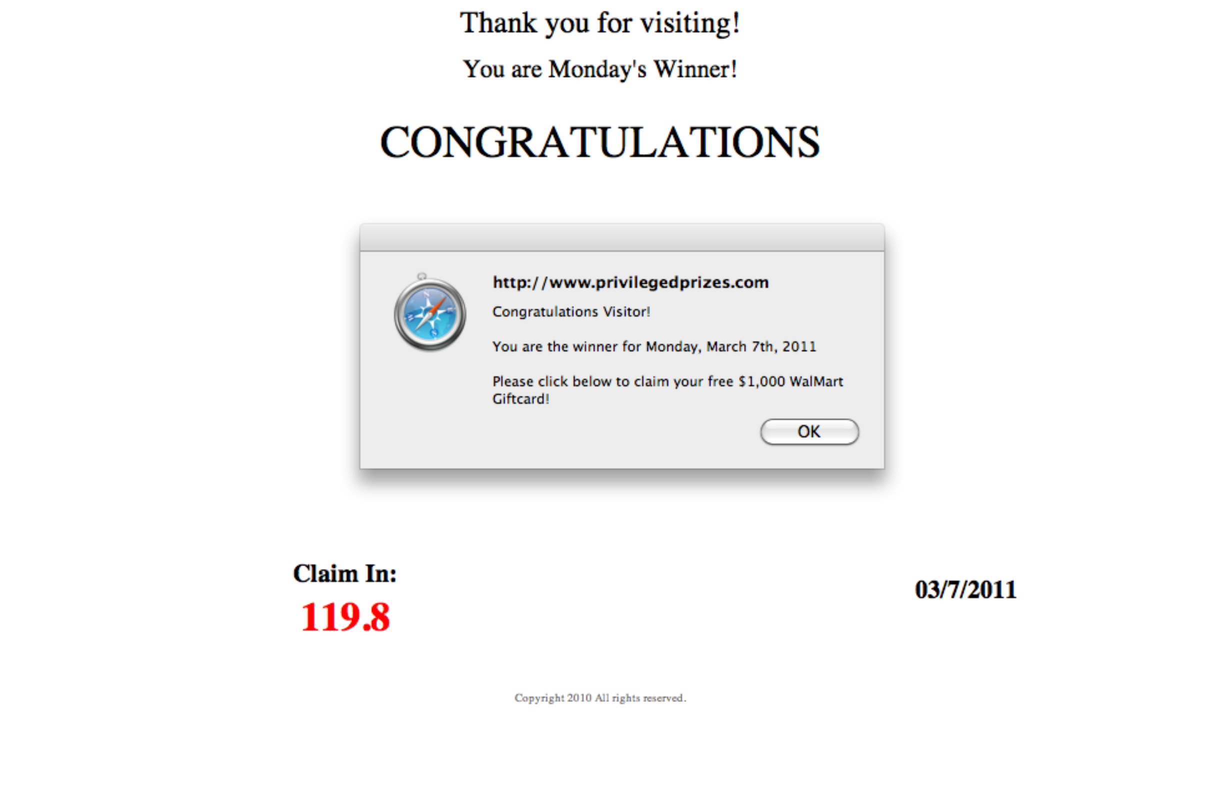
Clear and Actionable



Sharing Firewall Active

The sharing firewall (System Preferences > Sharing > Firewall) is active. It may interfere with network profiling. The communication port-number range used by this application (7475 – 7480) should be added to the firewall's list of trusted service ports. Otherwise, network profiling will fail.

Actionable?



Thank you for visiting!

You are Monday's Winner!

CONGRATULATIONS

http://www.privilegedprizes.com

Congratulations Visitor!

You are the winner for Monday, March 7th, 2011

Please click below to claim your free $1,000 WalMart Giftcard!

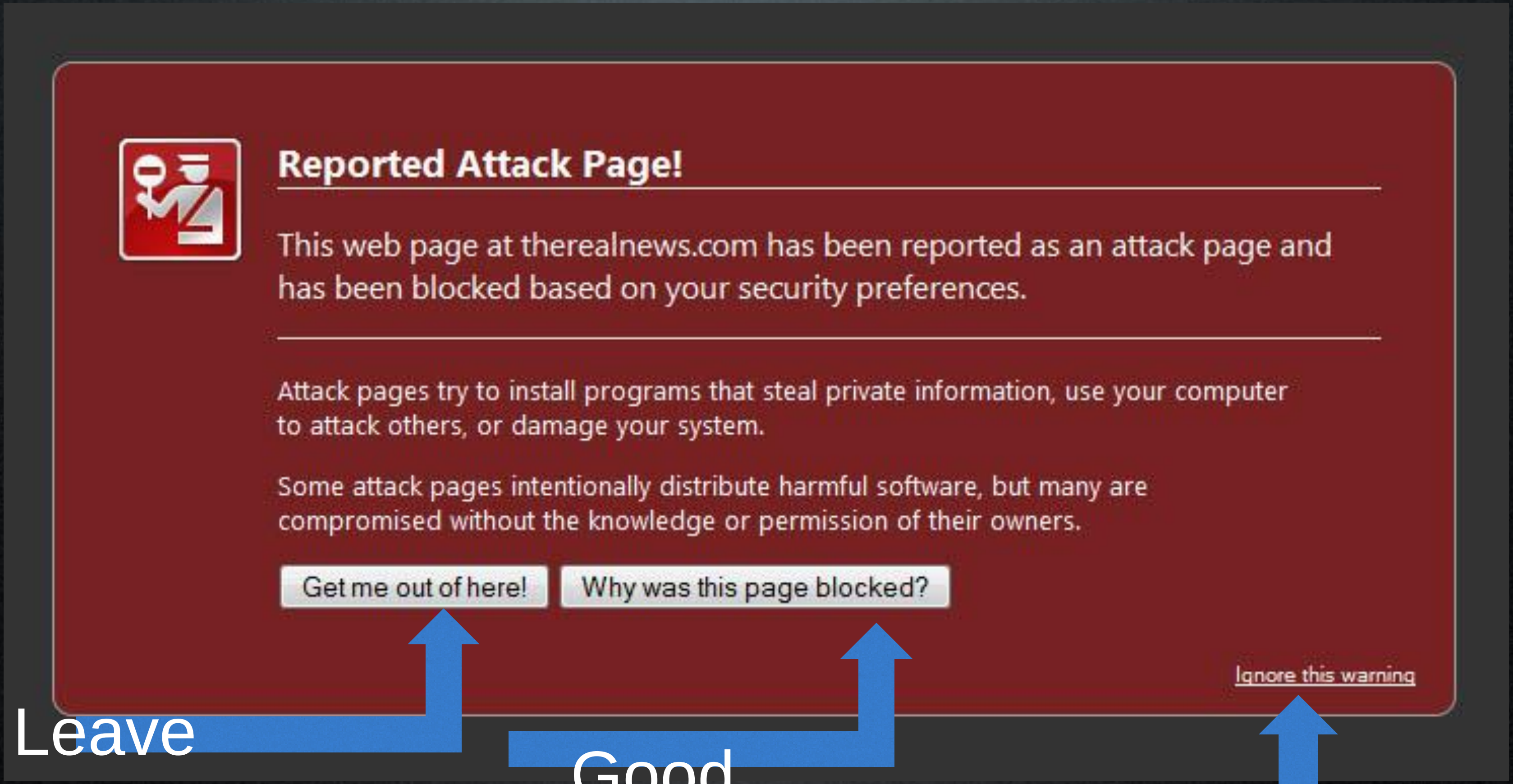
Claim In:

119.8

03/7/2011

Copyright 2010 All rights reserved.

Grounded in Useful Mental Models



Reported Attack Page!

This web page at therealnews.com has been reported as an attack page and has been blocked based on your security preferences.

Attack pages try to install programs that steal private information, use your computer to attack others, or damage your system.

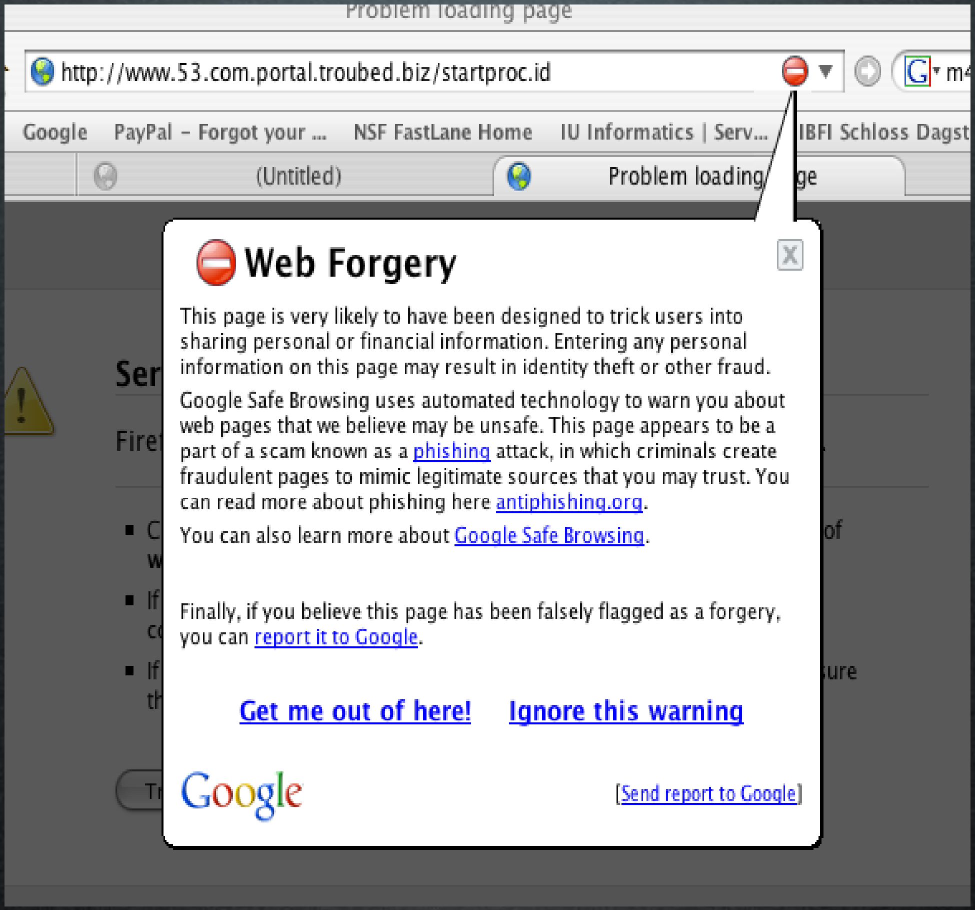
Some attack pages intentionally distribute harmful software, but many are compromised without the knowledge or permission of their owners.

Leave

Good Luck!

Stay

A Safe Place: Technical



Web Forgery

This page is very likely to have been designed to trick users into sharing personal or financial information. Entering any personal information on this page may result in identity theft or other fraud.

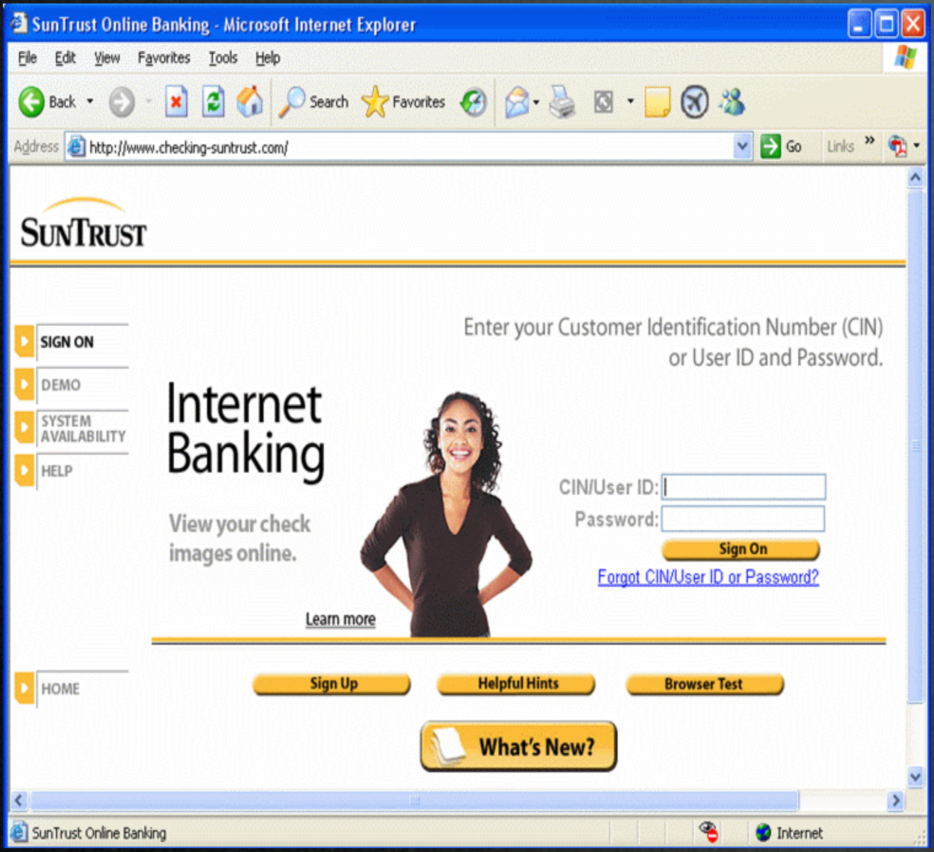
Google Safe Browsing uses automated technology to warn you about web pages that we believe may be unsafe. This page appears to be a part of a scam known as a phishing attack, in which criminals create fraudulent pages to mimic legitimate sources that you may trust. You can read more about phishing here antiphishing.org.

You can also learn more about Google Safe Browsing.

Finally, if you believe this page has been falsely flagged as a forgery, you can report it to Google.

Structured the problem incorrectly, we lose by design

Identify the Bank



SunTrust Online Banking - Microsoft Internet Explorer

Address: http://www.checking-suntrust.com/

Enter your Customer Identification Number (CIN) or User ID and Password.

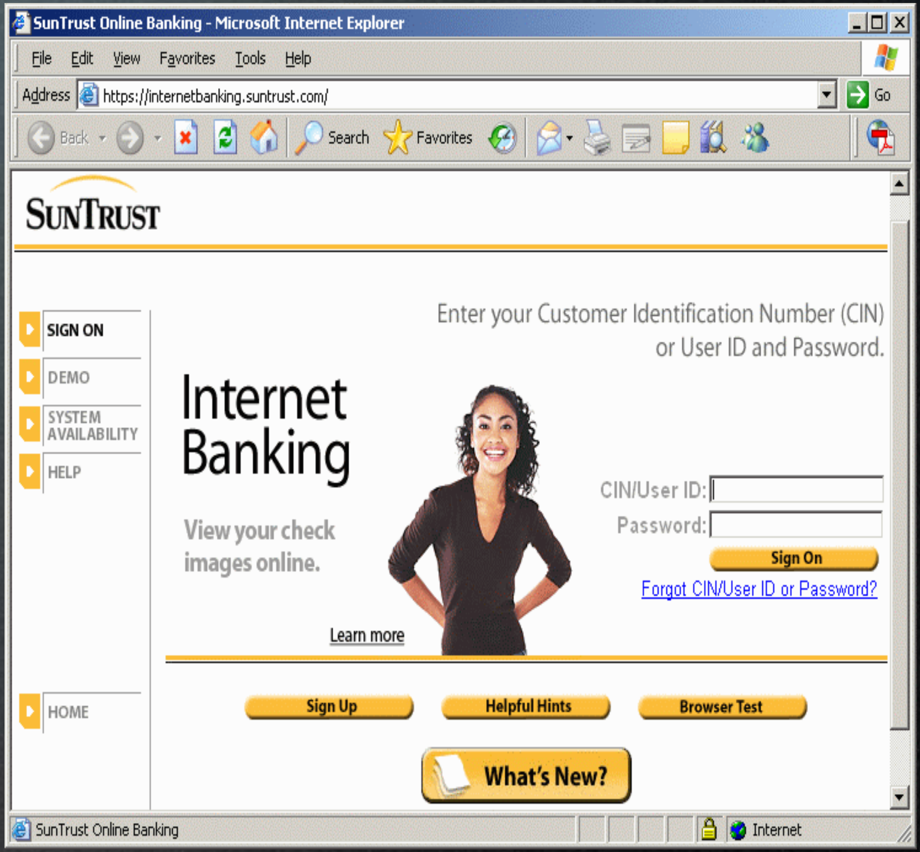
Internet Banking

View your check images online.

CIN/User ID:

Password:

SunTrust Online Banking



SunTrust Online Banking - Microsoft Internet Explorer

Address: https://internetbanking.suntrust.com/

Enter your Customer Identification Number (CIN) or User ID and Password.

Internet Banking

View your check images online.

CIN/User ID:

Password:

SunTrust Online Banking

Good Luck!!

Trust and Context

vs.

Resource Verification

Which merchant is more established?

Trust and Context

vs.

Resource Verification
With whom will you bank?

One Story

- Instead of a plethora of add-ins, add-ons, and ever expanding vocabulary
- A single story with one metaphor about the context, and a path to mitigation
- Translucent security

Two Examples

- Certificates
  - Work in progress
- Risks at work
  - communicating risks in decision-making

Perspectives

- public “network notary” servers
  - monitor the SSL certificates
  - Advantage: covers100,000s+ websites, text
  - Disadvantages: privacy, personalized coverage, notary incentives (all liability, no profit)

No One Is Here

We can figure this out. We have never been there. No one else is there either

You’ve Never Been Here

- Simple communication
- Single narrative
- Make their risks clear
  - You have never been here before, yet you are entering a password
  - Your friends have not been here
  - 95% are repeat clicks; 99% with n=10
- Individuals have incentives to protect themselves

History is Powerful

- Align with their mental models
- Integrate socially available information into the browsing or email experience
    - You don’t know this site.
    - That’s your bank password!
    - Perhaps you should call your bank first?

Other Options

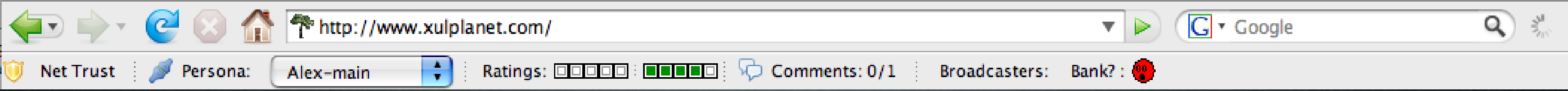
- Enable them to utilize their social networks
  - None of your friends have been here
  - No one knows this site
- Use patterns and heuristics
  - Certificate chain
  - Rank date; level; signing party
    - Compare with trusted/ untrusted

Other Rating Options

- Those that have been previously visited are trusted
- Those that have not been previously visited are considered untrusted
- The ratings of an untrusted website comes from McAfee SiteAdvisor
- The workplace provides a list of trusted certificates

Do Not Assume, but Enable

- Use what we know
  - Where you have been
  - Identify & protect critical authenticating info
  - Identify context
    - Explicit (work, banking)
    - Implicit (play, family)
    - Minimize explicit user-rating actions



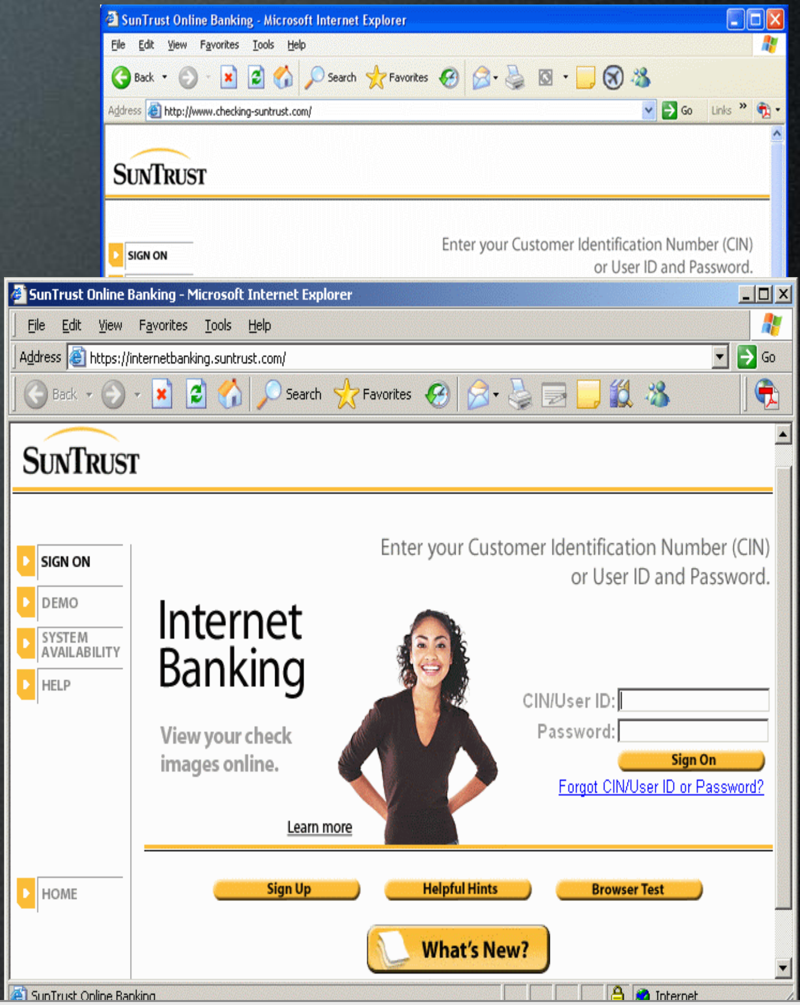
http://www.xulplanet.com/

Net Trust | Persona: Alex-main | Ratings: □□□□□ ■■■■□ | Comments: 0/1 | Broadcasters: | Bank? :

User- Centered Security

This is not a bank. If you enter this password, your money can be stolen.

This is a bank. Would you like assistance with your security settings?



SunTrust Online Banking - Microsoft Internet Explorer

Address http://www.checking-suntrust.com/

SunTrust Online Banking - Microsoft Internet Explorer

Address https://internetbanking.suntrust.com/

SunTrust

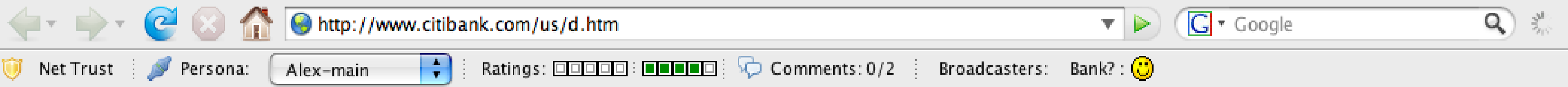
Enter your Customer Identification Number (CIN) or User ID and Password.

Internet Banking

View your check images online.

CIN/User ID:

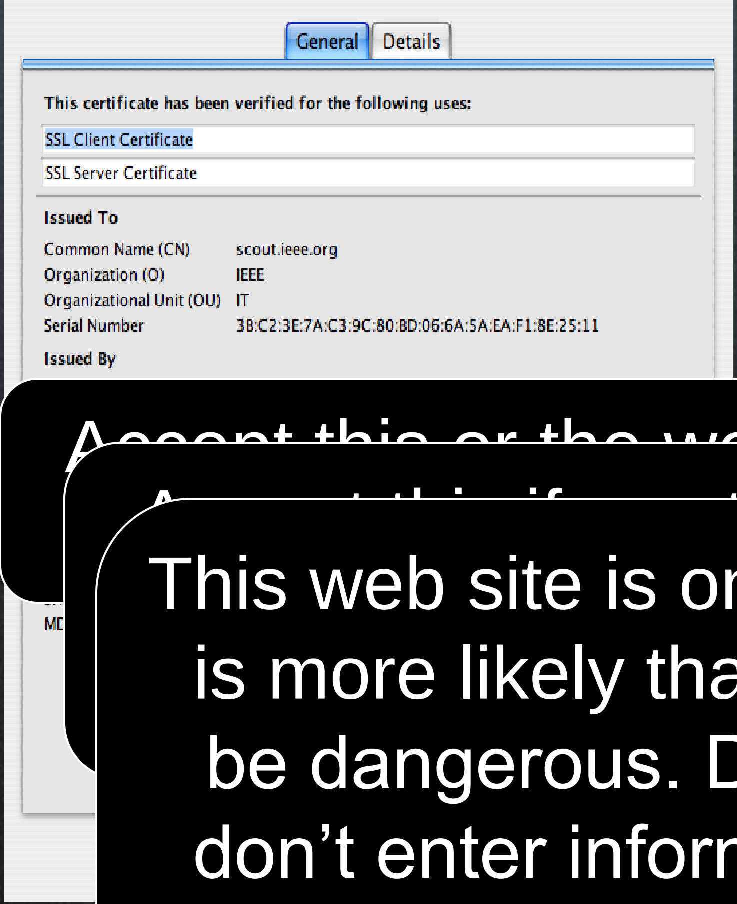
Password:



http://www.citibank.com/us/d.htm

Net Trust | Persona: Alex-main | Ratings: □□□□□ ■■■■□ | Comments: 0/2 | Broadcasters: | Bank? :

Actionable & Nontechnical?



This certificate has been verified for the following uses:

SSL Client Certificate

SSL Server Certificate

Issued To

Common Name (CN)	scout.ieee.org
Organization (O)	IEEE
Organizational Unit (OU)	IT
Serial Number	3B:C2:3E:7A:C3:9C:80:BD:06:6A:5A:EA:F1:8E:25:11

Issued By

Accept this or the web

This web site is one day old. It is more likely than others to be dangerous. Don’t go, or don’t enter information, and don’t download anything.

Do not accept any images or download anything from this site

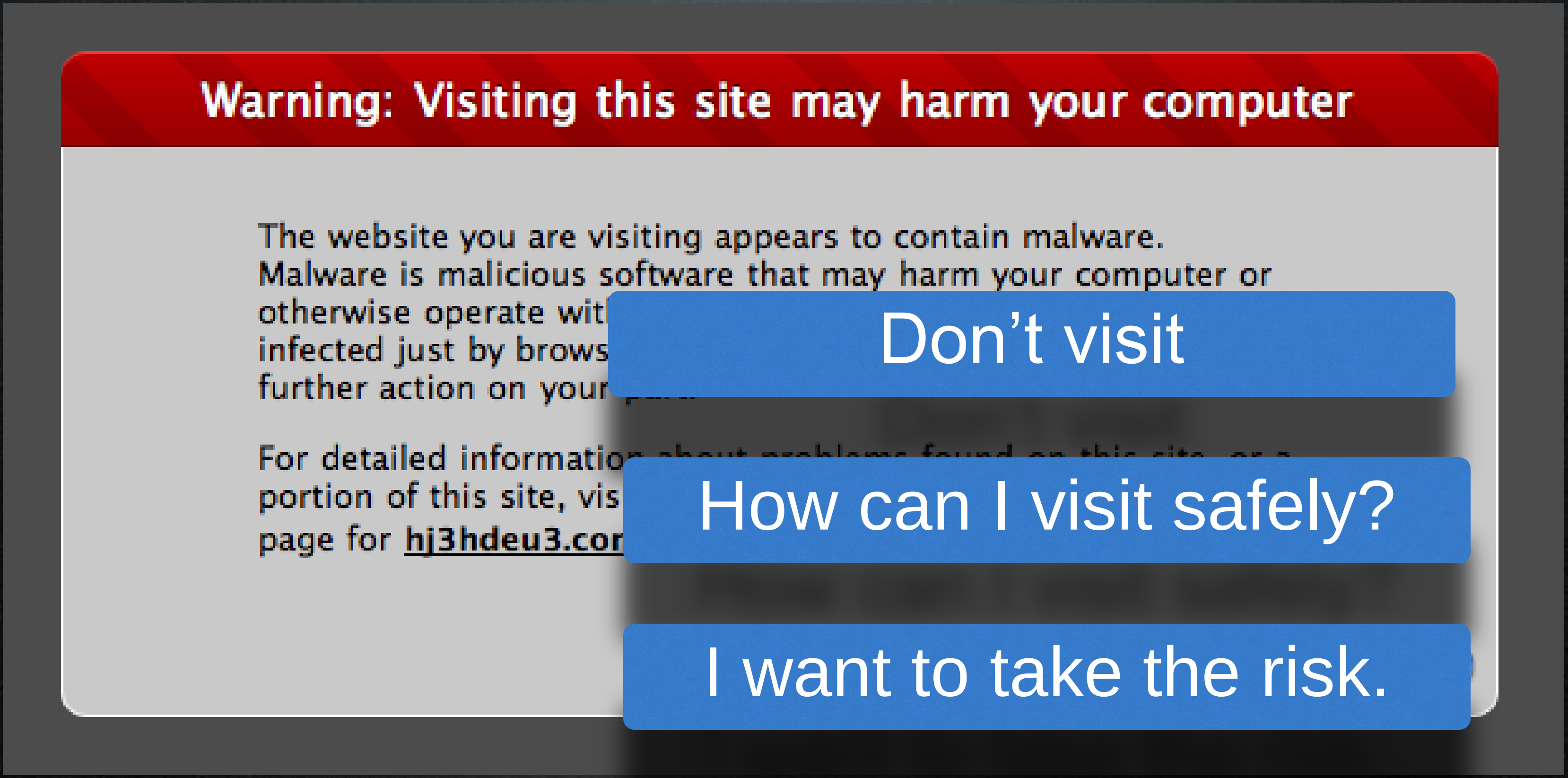
- The organization knows why this site can offer risk

Your plug-ins are still on, you are accepting serious risks to your machine and data

Don’t enter any information in this site!

Disable all plug-ins. Click **here**.

Details, details



Warning: Visiting this site may harm your computer

The website you are visiting appears to contain malware.
Malware is malicious software that may harm your computer or
otherwise operate wit
infected just by brows
further action on your part.

For detailed information about problems found on this site, or a
portion of this site, vis
page for hj3hdeu3.cor

Don’t visit

How can I visit safely?

I want to take the risk.

Define Contexts

- Network
  - Known machines? Security level? Hostile behaviors?
- Client
  - Known behaviors? Connection patterns?
- Limit data portability
  - Each device learns either on its own or from a location-authenticated and shared-credential small set

Shared Histories

- Perfect forward secrecy
  - Shared key efficient, deniable
  - Device vs person
    - authentication vs invitation
- Cloud-stored encrypted
- Traffic and timing attacks possible
  - Enables identification of social networks

Coordinate Human/Technical/Organizational

- Three contexts: Banking, working, playing
  - Participant override with risk communication
  - Security settings, isolated memory spaces, limit/prevent credential reuse
  - Privacy settings
  - Workplace compliance?
    - Work because they fail

Example 2: Risk @Work

- The Insider is mostly benign
- Inadvertent creation of risk
- Complete the task at hand
- Security is someone else’s problem

Risk Alignment

- Design a risk management mechanism
  - **inform** employees about organizational risk
  - **align** incentives between employees and organization
  - **identify** changes in status and risk behavior
  - **encourage** the users to self-manage their risks
  - **enable** them to get the job done

Risk Mitigation

- Provide each employee with a risk budget
    - access is priced
        - 1, 10, 100, break glass
    - create a long term record of aggregate risks
    - periodic review of employee risk behaviors

Budget as Risk Limit

- By the organization
- Based on
    - organizational preference
    - employee access rights
    - employee security preference
    - machine state
    - peer history
    - employee history

Simple Budget

- Risks are order of magnitude
- Risk points expire, no hoarding

Punishments?

- Translate exhausted budget into a cost
- An incentive against risk-seeking behaviors
  - enforced by the organization?
  - enforced by employee concern?
  - options
    - audit, training, limited access, verbal reminder, security review

Rewards

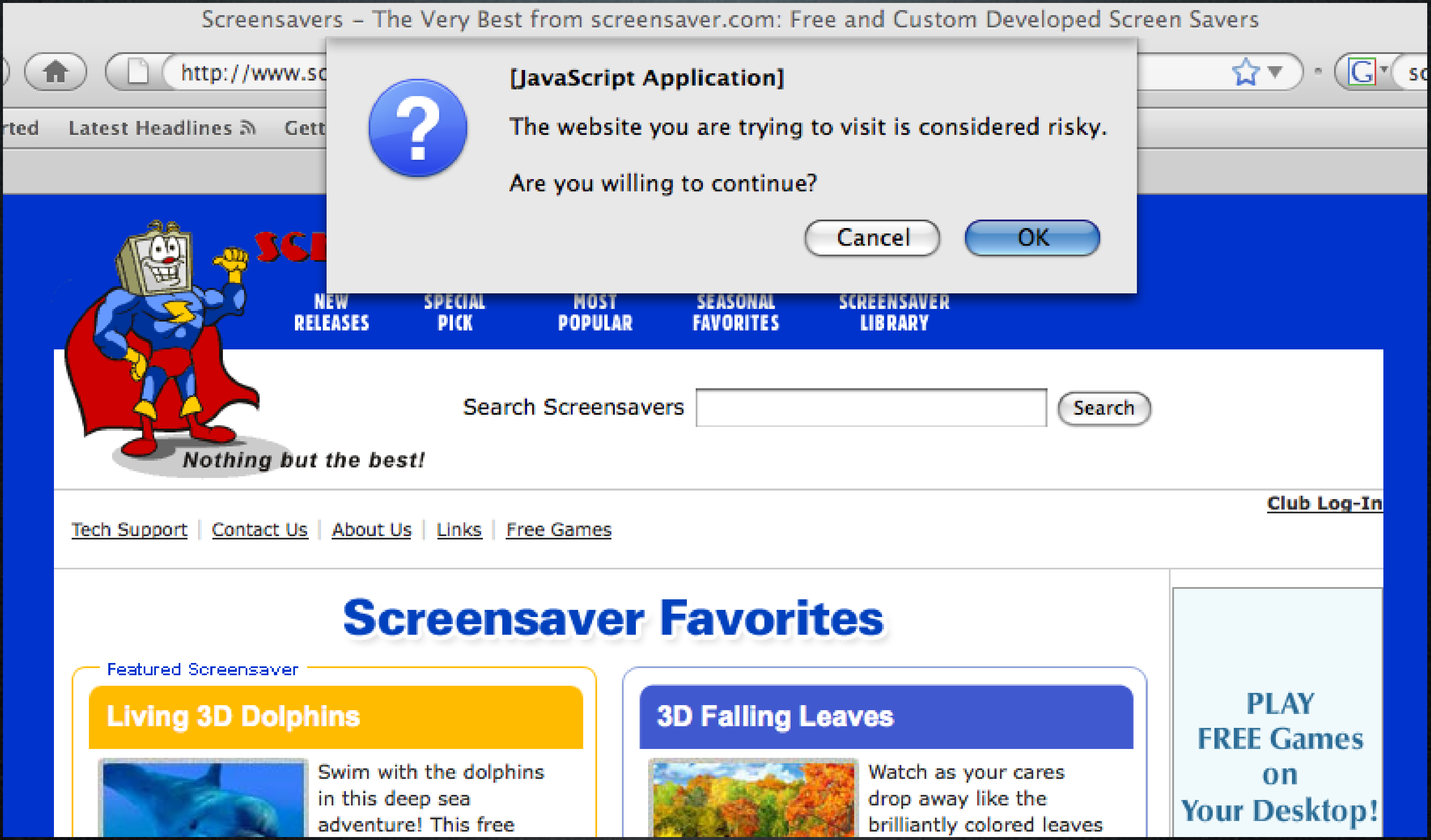
- A measure to reward the careful employee
- In the form of
  - more access
  - monetary award
  - opt-out of otherwise mandatory training
  - group competition
  - symbolic, e.g. atta-girl
    - accumulated
    - redeem

Experimental Configuration

- Two human-subject experiments
  - based on a firefox browser extension

- The 1st experiment
  - as benchmark
  - to understand users' risk behaviors
- The 2nd experiment
  - to study the change of risk behaviors

Experiment One



Screensavers – The Very Best from screensaver.com: Free and Custom Developed Screen Savers

[JavaScript Application]

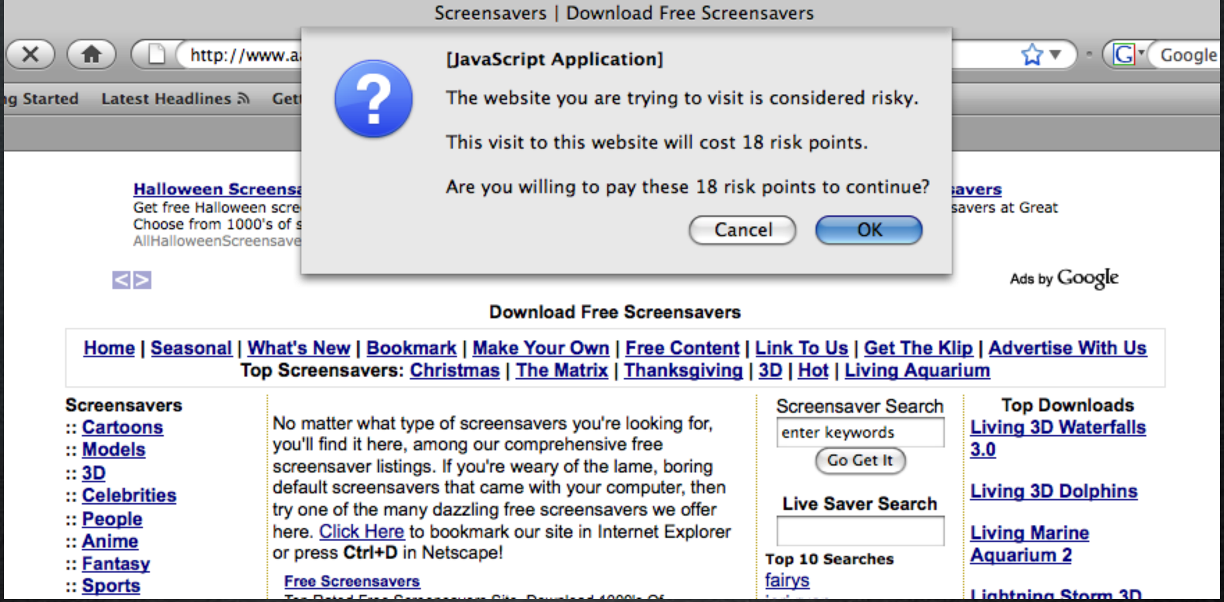
The website you are trying to visit is considered risky.

Are you willing to continue?

Swim with the dolphins in this deep sea adventure! This free

Watch as your cares drop away like the brilliantly colored leaves

Inclusion of Budget



[JavaScript Application]

The website you are trying to visit is considered risky.

This visit to this website will cost 18 risk points.

Are you willing to pay these 18 risk points to continue?

Halloween Screens
Get free Halloween scre
Choose from 1000's of s
AllHalloweenScreensave

avers
savers at Great

Ads by Google

Download Free Screensavers

Home | Seasonal | What's New | Bookmark | Make Your Own | Free Content | Link To Us | Get The Klip | Advertise With Us
Top Screensavers: Christmas | The Matrix | Thanksgiving | 3D | Hot | Living Aquarium

Screensavers
:: Cartoons
:: Models
:: 3D
:: Celebrities
:: People
:: Anime
:: Fantasy
:: Sports

No matter what type of screensavers you're looking for, you'll find it here, among our comprehensive free screensaver listings. If you're weary of the lame, boring default screensavers that came with your computer, then try one of the many dazzling free screensavers we offer here. Click Here to bookmark our site in Internet Explorer or press **Ctrl+D** in Netscape!

Free Screensavers

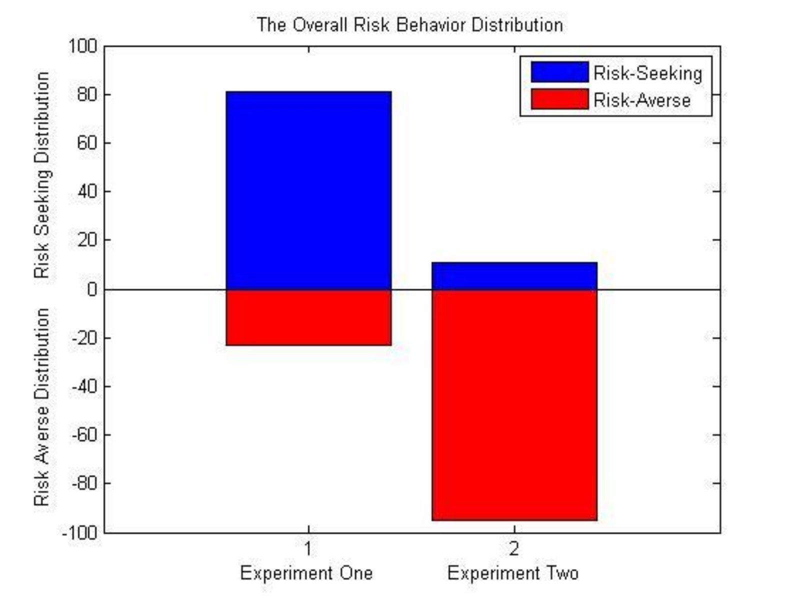
Screensaver Search
enter keywords
Go Get It

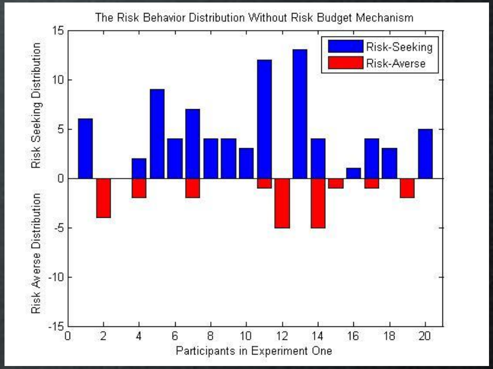
Live Saver Search

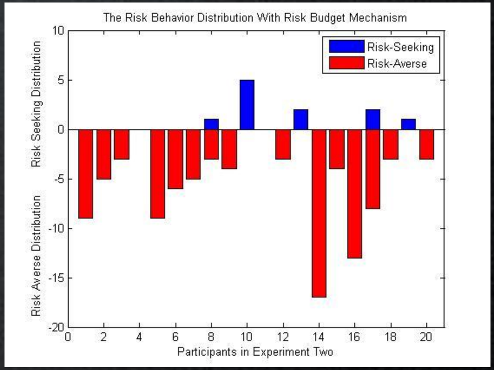
Top 10 Searches
fairys

Top Downloads
Living 3D Waterfalls 3.0
Living 3D Dolphins
Living Marine Aquarium 2

Response to Risk Budget







Regulatory Friction

- The efforts made by the users to adopt a risk-averse strategy instead of a risk-seeking strategy
- Measured friction using time interval for completing the task
- 1st experiment 5:45
- 2nd experiment 6:00
- Regulatory friction of 4.3% of the time committed in experiment one

Security Behaviors Embed Trust and Risk

- Incentives must be
  - correctly aligned
  - clearly communicated
  - to change behavior
- Design path
  - mechanism design
  - simulations
  - human experimentation

Translucent Security

- Is not usable security
- Is not default security
- Is cooperative security based on risk communication
    - Computer and human as partners

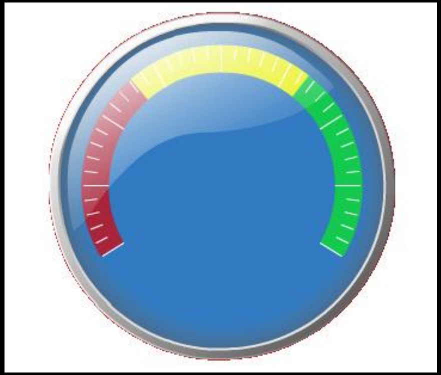
A Safe Place: Clear, Actionable, Personalized

This web site steals information. Don’t share it.

-Or –

Reset and configure

-Or-



Provide mostly useless information

Thanks!

Browsing data structure?

What to ask?

Questions?

Note

- IEEE S&PW
    - Needed:
        - Site chair
            - Handle onsite issues, interact with chairs and S&P committee
            - 3rd yr; be on market soon; give people a face to match the name
        - Publications chair
            - After event, harass authors and chairs for camera-ready papers
            - Connect with senior people from a place of authority

What to Ask & Ask & Ask

- Get involved!
  - USACM; IEEE-USA
  - Mailing lists matter hcisec@yahoogroups.com, ias-opportunities@googlegroups.com
- Get funded!
    - Who has grants on your campus? In your area?
  - NSF
    - Capacity building, YI
  - DARPA note
    - Mudge’s program?
  - NIH
    - Security & Privacy, YI, FI

Experimental Details

- Warning

- Bad wordy slides ahead
- Will abuse for attention span for funding

In Practice

- An employee
  - Internet surfing
  - documents downloading
    - a daily risk budget B
    - spend p_j to visit a website w_j that costs p_k to perform the downloading
    - spend p'_j to visit another website w'_j that costs p'_k to download
    - p_j , p_k , p'_j and p'_k are set by the organization based on its perception and evaluation of potential risks
    - assuming $B > (p_j + p_k) > (p'_j + p'_k)$
    - we expect she voluntarily chooses the second website, which incurs lower risks, under our risk budget mechanism

Experimental Configuration

- Two human-subject experiments
  - based on a firefox browser extension

- The 1st experiment
  - as benchmark
  - to understand users’ risk behaviors
- The 2nd experiment
  - to study the change of risk behaviors

Recruitment

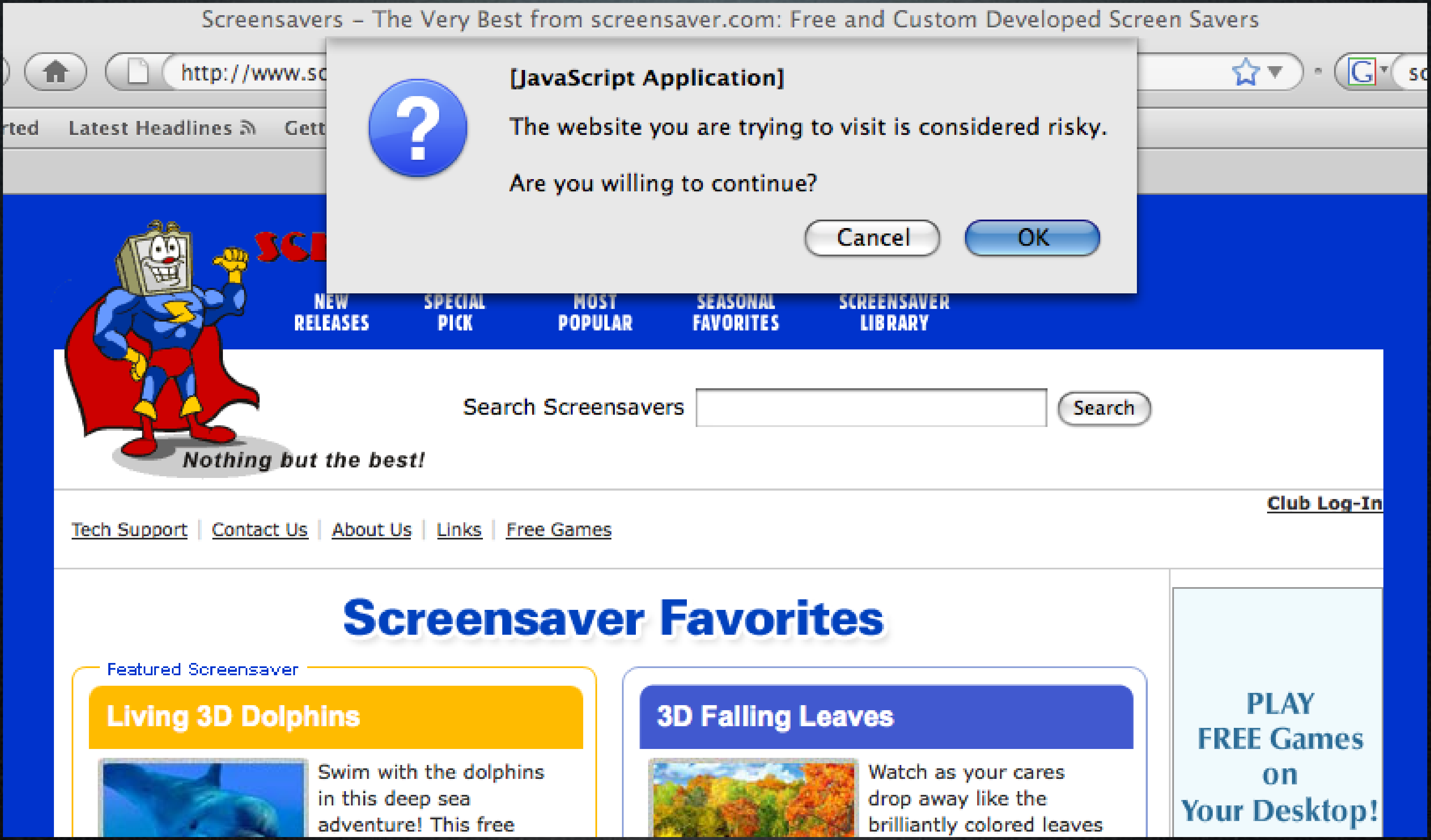
- 40 participants
- Voluntarily recruited from the undergraduates at Indiana University
- Randomly and equally divided into two group
- None of them have majors in computer related fields

Task Descriptions

1. Search for the websites offering free screen savers downloads from the web
2. From the search results, choose five websites: website-1, website-2, website-3, website-4 and website-5
3. From website-1, please take a screenshot of an {Animal, nature, sport, space, flower} screensaver

5. Thank you. You have completed the experiment

Experiment One



Screensavers – The Very Best from screensaver.com: Free and Custom Developed Screen Savers

[JavaScript Application]

The website you are trying to visit is considered risky.

Are you willing to continue?

Screensaver Favorites

Featured Screensaver

Living 3D Dolphins

Swim with the dolphins in this deep sea adventure! This free

3D Falling Leaves

Watch as your cares drop away like the brilliantly colored leaves

PLAY FREE Games on Your Desktop!

Experiment Two

- 20 participants completed the same task under the additional constraint of their risk budgets
- If they successfully accomplished their tasks
  - receive $10 plus a bonus
  - bonus based on the remaining risk points
- If any participant exhausted a risk budget
  - compensation forfeited
- If any participant failed to complete the experiment in time allowed
  - compensation forfeited

Firefox Browser Extension

1. Detect a new page being loaded;
2. Check the domain name of a webpage;
3. Maintain a list of target high risk websites and their reputations;
4. Pop up a warning message when a high risk website was about to be visited;
5. Ask for confirmation or rejection of the visit choice from the participant;
6. Record the experimental results;

(In experiment two, the extension also took the following actions:)

7. Generate a price based on a website's reputation;
8. Track participants risk budgets balance.

Data

- 1st experiment
    - 104 pop-up warning messages
    - 81 risk-seeking decisions
    - 23 risk-averse decisions
- 2nd experiment
    - 106 pop-up warning messages
    - 11 risk-seeking decisions
    - 95 risk-averse decisions

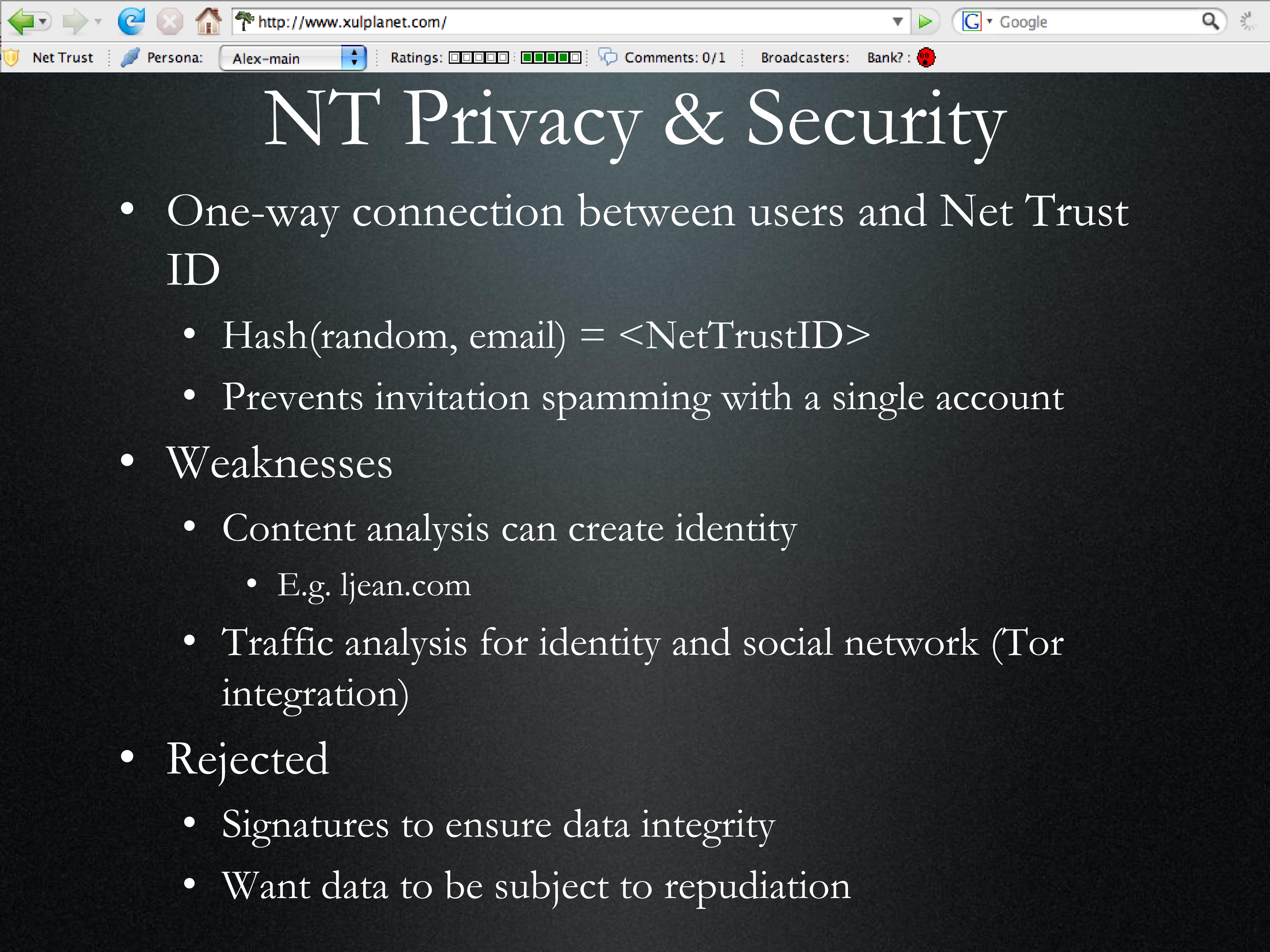
Game Theoretic Perspective

	Risk-Seeking	**Risk-Averse**
No Reward	$(-P_1, 0)$	$(-P_2, -C)$
Reward	$(-P_1-R_1, R_1)$	$(-P_2-R_2, R_2-C)$

- P_1: the cost to the organization when a risk-seeking adopted
- P_2: the cost to the organization when a risk-averse adopted
- $P_1 > P_2$
- R_1: the reward to the user when a risk-seeking strategy is adopted
- R_2: the reward to the user when a risk-averse strategy is adopted
- $R_1 < R_2$
- C: the friction between the risk-seeking and the risk-averse strategy

Game Solution and Application

- $R_1 < R_2 - C$ must hold
- *(reward, risk averse)* as equilibrium strategy in the repeated game
- It’s critical to determine the parameters
  - *C* could be estimated from time difference observation
  - adjust the incentive functions and monitor the risks, until the risk behavior distribution becomes acceptable



http://www.xulplanet.com/

Google

Net Trust

Persona: Alex-main

Ratings: □□□□□ 🟩🟩🟩🟩□

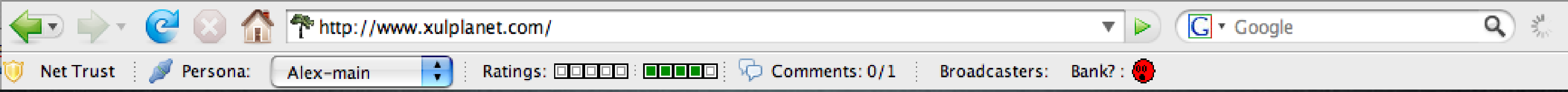
Comments: 0/1

Broadcasters:

Bank? :

NT Privacy & Security

- One-way connection between users and Net Trust ID
  - Hash(random, email) = <NetTrustID>
  - Prevents invitation spamming with a single account
- Weaknesses
  - Content analysis can create identity
    - E.g. ljean.com
  - Traffic analysis for identity and social network (Tor integration)
- Rejected
  - Signatures to ensure data integrity
  - Want data to be subject to repudiation

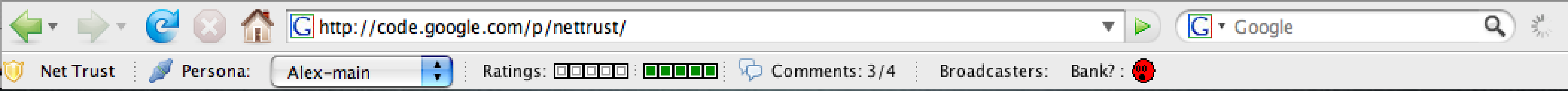


http://www.xulplanet.com/

Net Trust | Persona: Alex-main | Ratings: □□□□□ 🟩🟩🟩🟩□ | Comments: 0/1 | Broadcasters: | Bank? :

Do Not Assume Trust

- Reputation based on
- Implicit based on behavior
  - First visit results in delayed rating
    - Time delay is roughly equivalent to lifetime of phishing sites 72hrs
  - 1-nth visit increased by one
  - Increases up to nth visit, decreases to as low as n/2 after a delay
    - ✓Trust fades over time

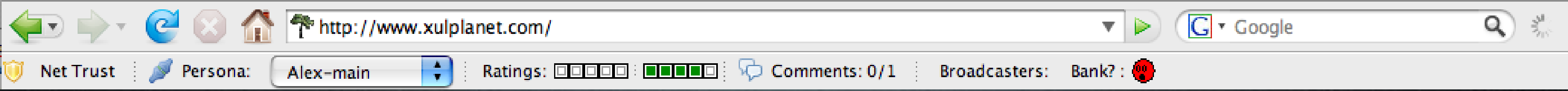


http://code.google.com/p/nettrust/

Net Trust | Persona: Alex-main | Ratings: □□□□□ 🟩🟩🟩🟩🟩 | Comments: 3/4 | Broadcasters: Bank? :

Implementation Status

- Centralized storage and distribution of data
  - Immediate synchronization of peer data
- Social network management
  - Email invitation
  - Manual entry of peer credentials
- Privacy
  - Uncorrelated IDs -- deniable histories
  - History limited to domain+top directory (no CGI)
  - No credentials required for ratings download
  - SN downloads delayed to prevent timing attack



http://www.xulplanet.com/

Net Trust

Persona: Alex-main

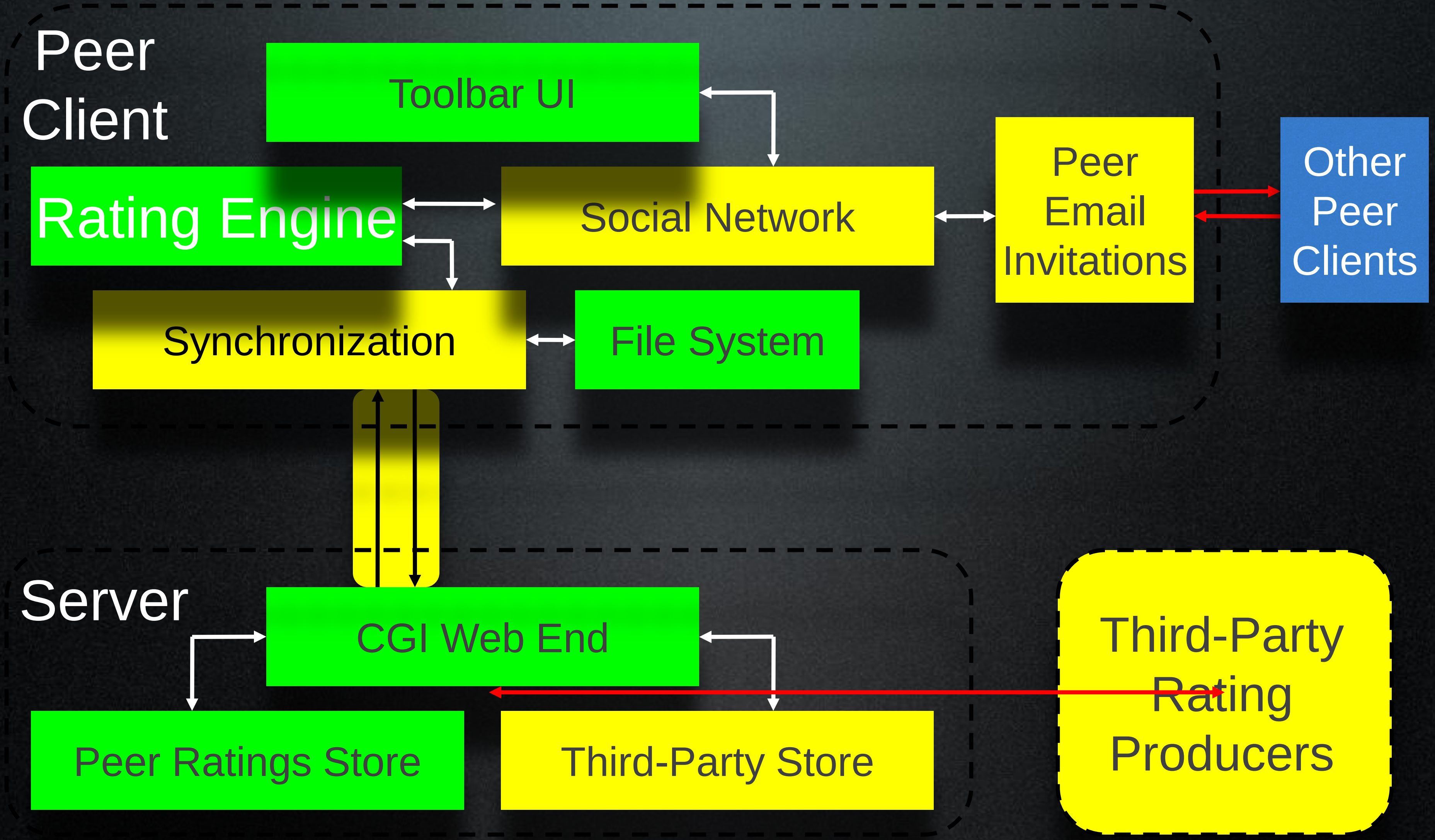
Ratings: □□□□□ ■■■■■

Comments: 0/1

Broadcasters:

Bank? :

Architectural Overview



Peer Client

Toolbar UI

Rating Engine

Social Network

Peer Email Invitations

Other Peer Clients

Synchronization

File System

Server

CGI Web End

Peer Ratings Store

Third-Party Store

Third-Party Rating Producers