Authentication and Human Aspects to Computer Security

Tadayoshi Kohno

Some slides derived from Vitaly Shmatikov's and Dan Simon's

PBKDF

- Problem:
  - Wish to encrypt file on local system using a password
  - User remembers password (e.g., a 16 character passphrase)
  - File encrypted with a symmetric cryptographic key (e.g., a 128 bit random key)
- Solution: Password-based key derivation

SKeys

- One time “passwords”
  - Easy for server to check
  - Hard for adversary who captures token to figure out the next one
  - User keeps list of passwords
- Problems?

Lamport’s Hash

- Main idea: "hash stalk"
  - Moving up the stalk (computing the next hash) is easy, moving down the stalk (inverting the hash) is hard
  - n should be large (can only use it for n authentications)
- For verification, only need the tip of the stalk

“Small n” Attack

- First message from Bob is not authenticated!
- Alice should remember current value of n

Two-factor authentication

- Authentication
  - What you know
  - Who you are
  - What you are
- Idea: More is better
  - Authenticate with two factors
  - ATM cards
    - Physical card - something you have
    - PIN - something you know
Authentication Adversaries

- Eavesdropper
- Pretend to be Bob and accept connections from Alice
- Initiate conversation pretending to be Alice
- Read Alice’s database
- Read Bob’s database
- Modify messages in transit between Alice and Bob
- Any combination of the above

Poor Usability Causes Problems

- Mismatch between perception of technology and what really happens

Importance

- Why is usability important?
  - People are the critical element of any computer system
    - People are the real reason computers exist in the first place
  - Even if it is possible for a system to protect against an adversary, people may use the system in other, less secure ways
- Today
  - Challenges with security and usability
  - Key design principles
  - New trends and directions

Issue #1: Complexities, Lack of Intuition

Real World

Electronic World

- SSL/TLS
- XSS
- RSA
- Buffer overflows
- Phishing
- Spyware

We can see, understand, relate to.

Too complex, hidden, no intuition.

Issue #1: Complexities, Lack of Intuition

We can see, understand, relate to.

Too complex, hidden, no intuition.

- Mismatch between perception of technology and what really happens
  - Public keys?
  - Signatures?
  - Encryption?
  - Message integrity?
  - Chosen-plaintext attacks?
  - Chosen-ciphertext attacks?
  - Password management?
  - ...
Issue #2: Who’s in Charge?

- Complex, hidden, but doctors manage
- Complex, hidden, and users manage

Real World
Electronic World

Adversaries in the electronic world can be intelligent, sneaky, and malicious.

Users want to feel like they’re in control.

- Systems developers should help protect users
  - Usable authentication systems
  - Red/green lights
- Software applications help users manage their applications
  - P3P for privacy control
  - PwdHash, Keychain for password management
  - Some say: Can we trust software for these tasks?

Issue #3: Hard to Gage Risks
Issue #3: Hard to Gage Risks

“It won’t happen to me!” (Sometimes a reasonable assumption, sometimes not.)

"I remembered hearing about it and thinking that people that click on those links are stupid,” she says. “Then it happened to me.” Ms. Miller says she now changes her password regularly and avoids clicking on strange links. (Open Doors, by V. Vara, The Wall Street Journal, Jan 29, 2007)

Social Network Users Have Ruined Their Privacy

<table>
<thead>
<tr>
<th>Schneier on Security</th>
<th>Users Disabling Security</th>
</tr>
</thead>
<tbody>
<tr>
<td>A New Threat: A World Without Privacy</td>
<td>It’s an old story: users disable a security measure because it’s annoying, allowing an attacker to bypass the measure.</td>
</tr>
<tr>
<td>May 02, 2005</td>
<td>May 02, 2005</td>
</tr>
<tr>
<td>Users Disabling Security</td>
<td>A rape defendant accused of a deadly courthouse rampage was able to enter the chambers of the judge, skin in the attacker and hold the occupants hostage because the door was unlocked and a buzzer entry system was not activated, a sheriff’s report says.</td>
</tr>
<tr>
<td>Security doesn’t work unless the user wants it to work. This is true on the personal and national scale, with or without technology.</td>
<td></td>
</tr>
</tbody>
</table>
**Issue #3: Hard to Gage Risks**

"It won't happen to me!" (Sometimes a reasonable assumption, sometimes not.)

<table>
<thead>
<tr>
<th>Social Network Users Have Ruined Their Privacy</th>
</tr>
</thead>
<tbody>
<tr>
<td><strong>Schenler on Security</strong></td>
</tr>
<tr>
<td>A working covering security and security technology.</td>
</tr>
<tr>
<td><em>&quot;There’s a Time to Pave The Road for a Shared Solution&quot;</em></td>
</tr>
<tr>
<td>May 02, 2005</td>
</tr>
<tr>
<td>Users Disabling Security</td>
</tr>
<tr>
<td>It’s not effective to disable a security measure because it’s annoying, allowing an attacker to bypass the measure.</td>
</tr>
<tr>
<td>A parolee accused in a deadly courthouse rampage was able to enter the chambers of the judge-bane in the attack and hold the occupants hostage because the door was unlocked and a buzzer entry system was not activated. A sheriff’s report says:</td>
</tr>
<tr>
<td>Security doesn’t work unless the users want it to work. This is true on the personal and national scale, with or without technology.</td>
</tr>
</tbody>
</table>

**Issue #4: No Accountability**

- Issue #3 is amplified when users are not held accountable for their actions
  - E.g., from employers, service providers, etc.
  - (Not all parties will perceive risks the same way)

**Issue #5: Awkward, Annoying, or Difficult**

- **Difficult**
  - Remembering 50 different, "random" passwords
- **Awkward**
  - Lock computer screen every time leave the room
- **Annoying**
  - Browser warnings, virus alerts, forgotten passwords, firewalls

**Issue #6: Social Issues**

- **Public opinion, self-image**
  - Only “nerds” or the “super paranoid” follow security guidelines
- **Unfriendly**
  - Locking computers suggests distrust of co-workers
- **Annoying**
  - Sending encrypted emails that say, “what would you like for lunch?”

**Issue #7: Usability Promotes Trust**

- **Well known by con artists, medicine men**
- **Phishing**
  - More likely to trust professional-looking websites than non-professional-looking ones

**Response #1: Education and Training**

- **Education:**
  - Teaching technical concepts, risks
- **Training**
  - Change behavior through
    - Drill
    - Monitoring
    - Feedback
    - Reinforcement
    - Punishment

- May be part of the solution - but not the solution
**Response #2: Security Should Be Invisible**

- Security should happen
  - Naturally
  - By Default
  - Without user input or understanding
- Recognize and stop bad actions
- Starting to see some invisibility
  - SSL/TLS
  - VPNs
  - Automatic Security Updates

See Dan Simon's slides: [http://research.microsoft.com/projects/SWSecInstitute/slides/simon.ppt](http://research.microsoft.com/projects/SWSecInstitute/slides/simon.ppt)

**Response #3: “Three-word UI:” “Are You Sure?”**

- Security should be transparent
  - Except when the user tries something dangerous
  - In which case a warning is given
- But how do users evaluate the warning? Two realistic cases:
  - Always heed warning. But see problems / commonality with Response #2
  - Always ignore the warning. If so, what's the point?

See Dan Simon's slides: [http://research.microsoft.com/projects/SWSecInstitute/slides/simon.ppt](http://research.microsoft.com/projects/SWSecInstitute/slides/simon.ppt)

**Response #4: Use Metaphors, Focus on Users**

- Clear, understandable metaphors:
  - Physical analogs; e.g., red-green lights
- User-centered design: Start with user model
- Unified security model across applications
  - User doesn't need to learn many models, one for each application
- Meaningful, intuitive user input
  - Don't assume things on user's behalf
  - Figure out how to ask so that user can answer intelligently

See Dan Simon's slides: [http://research.microsoft.com/projects/SWSecInstitute/slides/simon.ppt](http://research.microsoft.com/projects/SWSecInstitute/slides/simon.ppt)

**Response #5: Least Resistance**

- “Match the most comfortable way to do tasks with the least granting of authority”
  - Ka-Ping Yee, Security and Usability
- Should be “easy” to comply with security policy
- “Users value and want security and privacy, but they regard them only as secondary to completing the primary tasks”
  - Karat et al, Security and Usability

**Human Verification**

- Problem:
  - Want to make it hard for spammers to automatically create many free email accounts
  - Want to make it difficult for computers to automatically crawl some data repository
- Need a method for servers to distinguish between
  - Human users
  - Machine users
- Approach: CAPTCHA
  - Completely Automated Public Turing Test to Tell Computers and Humans Apart
CAPTCHAs

Idea: “easy” for humans to read words in this picture, but “hard” for computers

Caveats

- Usability challenges with visual impairments
- Researchers studying how to break CAPTCHAs
- Some attackers don’t break CAPTCHAs; they hire or trick others

Caveats

- Usability challenges with visual impairments
- Researchers studying how to break CAPTCHAs
- Some attackers don’t break CAPTCHAs; they hire or trick others

Phishing: A Few Headlines

- “11.9 million Americans clicked on a phishing e-mail in 2005”
- “Gartner estimates that the total financial losses attributable to phishing will total $2.8 bln in 2006”
- “Phishing and key-logging Trojans cost UK banks £12m”
- “Swedish bank hit by ‘biggest ever’ online heist”
  “Swedish Bank loses $1 Million through Russian hacker”

Caveats

The following article describes an attack against the web images (so-called “CAPTCHA”) that are used to prevent robots from causing problems with websites. The images are a form of “detective task”, easy for a human user of normal ability to process, but difficult for a piece of software. The attack involves routing the CAPTCHA images to a page that advertises fake porn. Users have to decode the CAPTCHA to get the advertised image and in doing so, unwittingly assist spammers in creating bogus e-mail addresses.

But at least one potential spammer managed to crack the CAPTCHA test. Someone designed a software robot that would fill out a registration form and, when confronted with a CAPTCHA test, would post it on a free porn site. Visitors to the porn site would be asked to complete the test before they could view more pornography, and the software robot would use their answer to complete the e-mail registration.

MillerSmiles.co.uk

Welcome to MillerSmiles.co.uk! We are one of the Internet’s leading anti-phishing sites, maintaining a massive archive of phishing and identity theft emails and scams.

We are currently storing all scam reports with our MoneyFy ‘scam database which is now available for commercial license. This database currently holds 172095 reports.

We also run a news service (headlines below) which brings you all the latest headlines from the world of fraudulent emails and phishing.

Latest Phishing News Headlines:
- Anti-Phishing Browsers Not Working
- Keylogging Worsens Trend
- Facebook Phishing
- Phishing Trend Continues
- Phishing in Email
- Christmas phishing threat looms
- Phishing: A Tougher Act
- Google Faxes ‘suspicious’ flow
- Phishing Protection in Office 2003

eBay: 14th April 2007
- eBay Limited Account Access Details

Fishtank: 14th April 2007
- Phishing Warning: Citibank Identity Protection

HSBC: 24th April 2007
- Internet Security (HSBC Bank Ownership Verification Alert)

PayPal: 24th April 2007
- Receipt of your last transaction

5th Third: 24th April 2007
- The 3rd Bank USA Commercial Banking: Please Update Your Banking Data

PayPlus: 24th April 2007
- New email address added to your account!

PayPro: 23rd April 2007
- Verify Your Account!
New Phishing Sites by Month (Oct 2005 to Oct 2006)


Typical Phishing Page
• Weird URL
• http instead of https

Or Even Like This

Or Even Like This
A Closer Look

From: "Wells Fargo" <aw-updateWells.Fargo.com@abm-tech.com>

What you'll see on the page

And You End Up Here

Where the link actually goes
And You End Up Here

Phishing Techniques
- Use confusing URLs
- Use URL with multiple redirection
- Host phishing sites on botnet zombies
  - Move from bot to bot using dynamic DNS
- Pharming
  - Poison DNS tables so that victim’s address (e.g., www.paypal.com) points to the phishing site
  - URL checking doesn’t help!

Why Phishing Works
- Experiment
  - 22 participants
  - 20 websites
  - Asked to determine whether fraudulent
- Results
  - Successful phishing sites fooled 90% of participants
  - 23% of participants did not look at address bar, status bar, or other security indicators
  - 15 of 22 participants ignored popup warnings

Social Engineering Tricks
- Create a bank page advertising an interest rate slightly higher than any real bank; ask users for their credentials to initiate money transfer
  - Some victims provided their bank account numbers to “Flintstone National Bank” of “Bedrock, Colorado”
- Exploit social network
  - Spoof an email from a Facebook or MySpace friend
    - Jan 29 WSJ article about MySpace hack
  - In a West Point experiment, 80% of cadets were deceived into following an embedded link regarding their grade report from a fictitious colonel

Experiments at Indiana University
- Reconstructed the social network by crawling sites like Facebook, MySpace, LinkedIn and Friendster
Seven Stages of Grief
(according to Elizabeth Kübler-Ross)

- Shock or disbelief
- Denial
- Bargaining
- Guilt
- Anger
- Depression
- Acceptance

Experiments at Indiana University

Reconstructed the social network by crawling sites like Facebook, MySpace, LinkedIn and Friendster
Sent 921 Indiana University students a spoofed email that appeared to come from their friend
Email redirected to a spoofed site inviting the user to enter his/her secure university credentials
  - Domain name clearly distinct from indiana.edu

Victims’ Reactions (1)

- Anger
  - Subjects called the experiment unethical, inappropriate, illegal, unprofessional, fraudulent, self-serving, useless
  - They called for the researchers conducting the study to be fired, prosecuted, expelled, or reprimanded

- Denial
  - No posted comments included an admission that the writer had fallen victim to the attack
  - Many posts stated that the poster did not and would never fall for such an attack, and they were speaking on behalf of friends who had been phished

Seven Stages of Grief

Reconstructed the social network by crawling sites like Facebook, MySpace, LinkedIn and Friendster
Sent 921 Indiana University students a spoofed email that appeared to come from their friend
Email redirected to a spoofed site inviting the user to enter his/her secure university credentials
  - Domain name clearly distinct from indiana.edu

72% of students entered their real credentials into the spoofed site
  - Males more likely to do this if email is from a female
Victims’ Reactions (2)

- Misunderstanding
  - Many subjects were convinced that the experimenters hacked into their email accounts. They believed it was the only possible explanation for the spoofed messages.

- Underestimation of privacy risks
  - Many subjects didn’t understand how the researchers obtained information about their friends, and assumed that the researchers accessed their address books.
  - Others, understanding that the information was mined from social network sites, objected that their privacy had been violated by the researchers who accessed the information that they had posted online.

More Details

- Control group: 15 of 94 (16%) entered personal information
- Social group: 349 of 487 (72%) entered personal information
- 70% of responses within first 12 hours
- Adversary wins by gaining users’ trust

More Details

<table>
<thead>
<tr>
<th>To Male</th>
<th>To Female</th>
<th>To Any</th>
</tr>
</thead>
<tbody>
<tr>
<td>From Male</td>
<td>53%</td>
<td>78%</td>
</tr>
<tr>
<td>From Female</td>
<td>68%</td>
<td>76%</td>
</tr>
<tr>
<td>From Any</td>
<td>65%</td>
<td>77%</td>
</tr>
</tbody>
</table>

More Details

- Confidentiality and Integrity are related
  - But different!
  - Confidentiality problems can lead to integrity problems, and vice versa
- Bank example
**Vulnerabilities**

- Weaknesses of a system that could be exploited to cause damage
  - Accounts with system privileges where the default password has not been changed (Diebold: 1111)
  - Programs with unnecessary privileges
  - Programs with known flaws
  - Known problems with cryptography
  - Weak firewall configurations that allow access to vulnerable services
- Sources for vulnerability updates: CERT, SANS, Bugtraq, the news(?)

**Adversaries**

- National governments
- Terrorists
- Thieves
- Business competitors
- Your supplier
- Your consumer
- New York Times
- Your family members (parents, children)
- Your friends
- Your ex-friends

**Threats**

- Threats are actions by adversaries who try to exploit vulnerabilities to damage assets
  - Spoofing identities: Attacker pretends to be someone else
  - Tampering with data: Change outcome of election
  - Denial of service: Attacker makes voting machines unavailable on election day
  - Elevation of privilege: Regular voter becomes admin
- Specific threats depend on environmental conditions, enforcement mechanisms, etc
  - You must have a clear, simple, accurate understanding of how the system works!

**Risks**

- Quantitative risk management
  - Example: Risk = Asset × Threat × Vulnerability
- Monetary value to assets
- Threats and vulnerabilities are probabilities
  - (Yes: Difficult to assign these costs and probabilities)
- Qualitative risk management
  - Assets: Critical, very important, important, not important
  - Vulnerabilities: Has to be fixed soon, should be fixed, fix if convenient
  - Threats: Very likely, likely, unlikely, very unlikely

**Assets**

- Need to know what you are protecting!
  - Hardware: Laptops, servers, routers, PDAs, phones, ...
  - Software: Applications, operating systems, database systems, source code, object code, ...
  - Data and information: Data for running and planning your business, design documents, data about your customers, data about your identity
  - Reputation, brand name
  - Responsiveness
- Assets should have an associated value (e.g., cost to replace hardware, cost to reputation, how important to business operation)
CTR and CBC homework problems