ECE 547/647: Security Engineering

Lesson 5: Human Behavior

Rationale

- Many vulnerabilities are due to human behavior
- Deception is widespread and always evolving

Prior Learning

- Let’s Review from Lesson 4: Case Study: Automotive Security
  - Rise in technologically-advanced automobiles
  - Vulnerabilities
  - Solutions

© 2018 UMass Amherst Global. All rights reserved

Outline of Course – Where We Are

- Part 1
  - Introduction and Objectives
  - Motivations
  - Foundations of Security
  - Case Study: SSD Encryption
  - Case Study: Automotive Security

- **Part 2**
  - **Human Behavior**
  - **Case Study: Password Modeling**
  - **Case Study: Two Factor Token**
  - **Software Security**
  - **Case Study: Voting Systems**
  - **Case Study: Smart Grids**

- Part 3
  - Ciphers and Cryptanalysis

© 2018 UMass Amherst Global. All rights reserved

Security Properties

- Confidentiality
- Integrity
- Authentication

Availability, Accountability

…

© 2018 UMass Amherst Global. All rights reserved

Variants of Confidentiality

Data protection/Personal data privacy

- Fair collection and use of personal data,

Anonymity/Untraceability

- Ability to use a resource without disclosing identity/location

Unlinkability

- Ability to use a resource multiple times without others being able to link these uses together

Pseudonymity

- Anonymity with accountability for actions

Unobservability

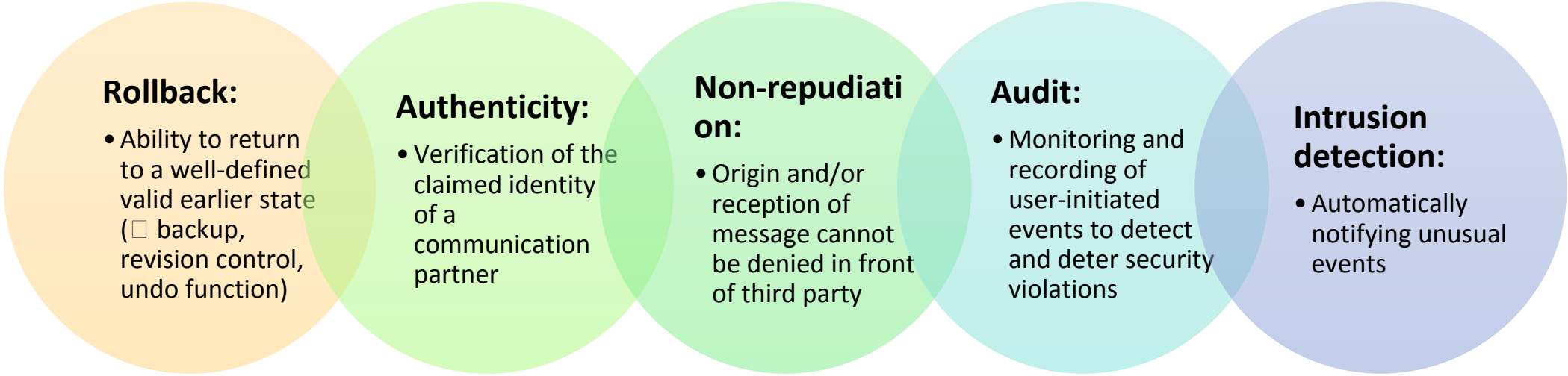
- Ability to use a resource without revealing this activity to third parties

Copy protection, Information flow control

- Ability to control the use and flow of information

© 2018 UMass Amherst Global. All rights reserved

Aspects of Integrity and Availability Protection



"Optimistic Security": Temporary violations of security policy are tolerated where correcting the situation is easy and the violator is accountable.

© 2018 UMass Amherst Global. All rights reserved

Discussion: Identification and Authentication

- Humans can be identified by:

Something they **are**	Something they **do**	Something they **have**	Something they **know**	**Where** they are
Biometric identification: retina pattern, face or fingerprint recognition, etc.	Handwritten signature dynamics, voice, lip motion, etc.	Access tokens: physical key, ID card, smartcard, mobile phone, etc.	Memorized secrets: password, personal identification number (PIN), etc.	Location information:, telephone caller ID, Internet address, GPS, etc.

- For high security, several identification techniques need to be combined to reduce the risks of false- accept/false-reject rates, token theft, carelessness, relaying and impersonation.
- Show one example of two-factor and one of three-factor authentication

© 2018 UMass Amherst Global. All rights reserved

Passwords

- Randomly picked single words have low entropy, dictionaries have less than 2^{18} entries.
- Common improvements:
  - restrict rate at which passwords can be tried (reject delay) and monitor failed logins
  - require minimum length and inclusion of digits, punctuation, and mixed case letters
  - suggest recipes for difficult to guess choices (entire phrase, initials of a phrase related to personal history, etc.)
  - compare passwords with directories and published lists of popular passwords (person's names, pet names, brand names, celebrity names, patterns of initials and birthdays in various arrangements, etc.)
  - issue randomly generated PINs or passwords, preferably pronounceable ones

© 2018 UMass Amherst Global. All rights reserved

Password-Related Problems and Security Measures:

- Trusted path – user must be sure that entered password reaches the correct software (→ Ctrl+Alt+Del on Windows aborts any GUI application and activates proper login prompt)
- Confidentiality of password database – instead of saving password directly or encrypted, store only h(P), where h is a one-way hash function → no secret stored on host
- Brute-force attacks against stolen password database – store (S, hn(SkP)), where a hash function h is iterated n times to make the password comparison inefficient, and S is a nonce ("salt value", like IV) that is concatenated with P to prevent comparison with precalculated hashed dictionaries.
- Eavesdropping – one-time passwords, authentication protocols.
- Inconvenience of multiple password entries – single sign-on.

© 2018 UMass Amherst Global. All rights reserved

Password statistics…

Property	Values	% of PWs
Length	$3-5$	2
	$6-8$	48
	$9-12$	40
	$13-50$	10
Composition	Lower case only	80
	Upper case only	3
	Letters only	38
	Digits only	8
	Special characters only	< 0.1
	Letters & digits only	55
	Containing at least one letter, one digit and one special char	5

Fig. 1: The distribution of password length and composition in the data after cleaning.

Activity: Passwords

- Discuss your own password strategies with your group.
- Without revealing any passwords!

ie “no security through obscurity”

- How does the password space increase from all LOWER CASE to requiring at least one UPPER CASE and one of these special characters: !@#$%^&*(

© 2018 UMass Amherst Global. All rights reserved

Passwords

- Difficulties with password entry
  - Length? U.S. Nuclear Weapons fixing codes: 12 decimal digits
  - Error rate?
  - Password retry limits

- Difficulties remembering passwords
  - Naïve password choices
  - Requirements for changing passwords
  - Your ideas?

© 2018 UMass Amherst Global. All rights reserved

Improving Passwords

- Microsoft Passport
- E-Wallets (Google Wallet, ..)
- Password manglers
- Passwords stored in browsers

© 2018 UMass Amherst Global. All rights reserved

Password Similarity Models using Neural Networks, Cornell Tech and Technion

Key ideas:

- "a compilation of 1.4 billion leaked email, password pairs"!
- Cornell ITSO cooperation
- Learning a model for password similarity
  - a generative model based on sequence-to-sequence style learning as used previously for language translation, and
  - a discriminative model based on word embedding techniques.
- Showed serious vulnerability. 16% accounts broken in <1000 guesses
- Proposed a personalized password strength meter (PPSM) as a countermeasure to detect weak passwords (using same technology as attack!)
- Your ideas?

© 2018 UMass Amherst Global. All rights reserved

Metrics!

- Figures in paper

© 2018 UMass Amherst Global. All rights reserved

Review paper. Display PDF.

Show how to read a technical paper.

Survey
Question
Read
Recite
Review

© 2018 UMass Amherst Global. All rights reserved

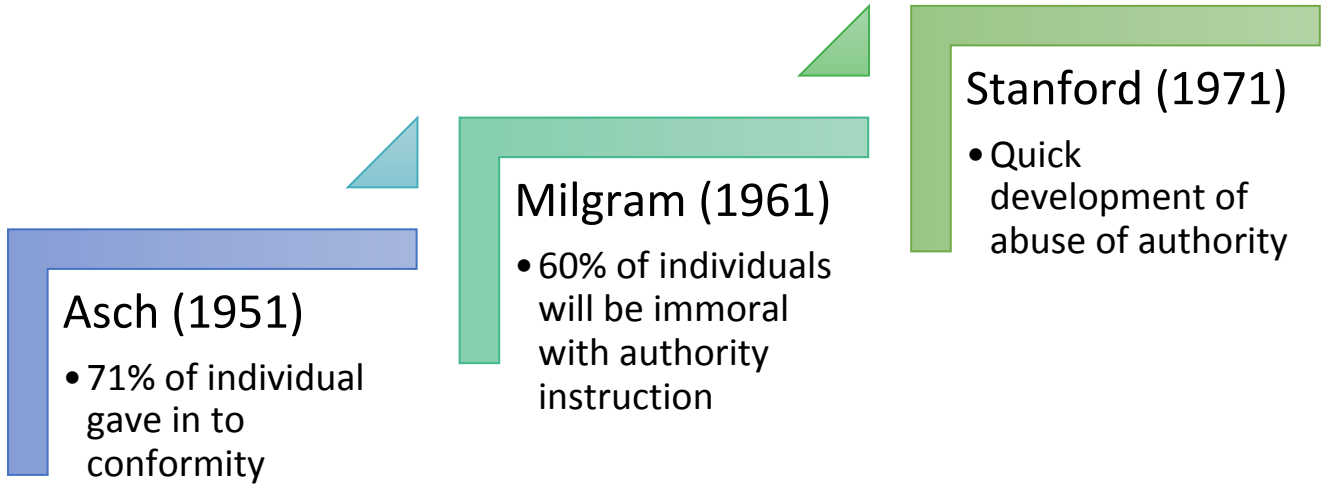
The Human Factor

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.)

— Kaufmann, Perlman and Speciner

© 2018 UMass Amherst Global. All rights reserved

Discussion: Social Psychology



- More modern examples?
  - Abu Ghraib, 2004…
- Conclusion: Can't rely on integrity of humans.
  - Some people are BAD much of the time!
  - Most are BAD at least some of the time?
  - And probably always will be…

© 2018 UMass Amherst Global. All rights reserved

Deception and Hoaxes

- **Deception:** The greatest threat to online security
  - Used to get passwords
  - Compromise confidential information
  - Manipulate financial transactions directly

- **Pretexting:** Most common way for private investigators to steal personal information
  - Phoning someone who has the information under a false pretext
  - Sometimes known collectively as social engineering

© 2018 UMass Amherst Global. All rights reserved

Deception and Hoaxes (cont'd)

Only amateurs attack machines; professionals target people.
— Bruce Schneier

- This quote refers to a notorious stock scam
  - A bogus press release said that a company's CEO had resigned and its earnings would be restated.
  - Several wire services passed this on, and the stock dropped 61% until the hoax was exposed

- Hoaxes and frauds have always happened, but the Internet makes some of them easier
  - Lets others be repackaged in ways that may bypass our existing controls

© 2018 UMass Amherst Global. All rights reserved

Deception Close to Home

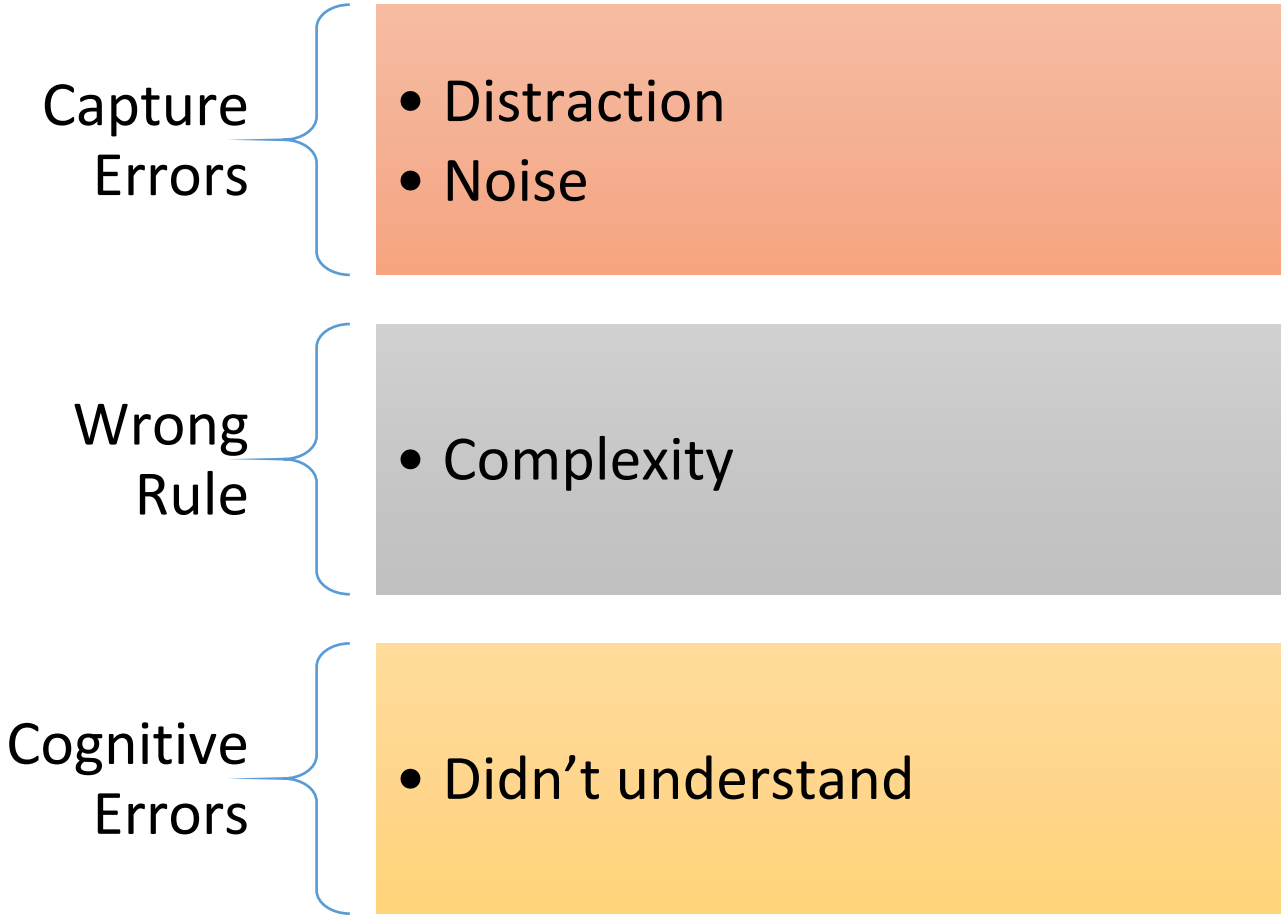
- Audit of IRS in 2007 by the U.S. Treasury Inspector General for Tax Administration
  - Asked for user IDs of 102 IRS employees at all levels
  - Told them to change their passwords to a known value
  - 62 did so

- Result: Many U.S. government departments, including Homeland Security, launch phishing attacks on their own staff in order to gauge the effectiveness of security education.

© 2018 UMass Amherst Global. All rights reserved

To Err is Human

- Misfeasance vs. Malfeasance
- Helpful resource: James Reason's 'Human Error'
  - Explains what the safety-critical systems community has learned from many years studying the cognate problems in their field



© 2018 UMass Amherst Global. All rights reserved

[Activity:]

- Think of an example where your mistake has resulted in a security weakness.

© 2018 UMass Amherst Global. All rights reserved

An example from Tuesday…

From Maciej J. Ciesielski <newsgood858@gmail.com>

Subject **Are You In The Office ?**

To burleson@ecs.umass.edu

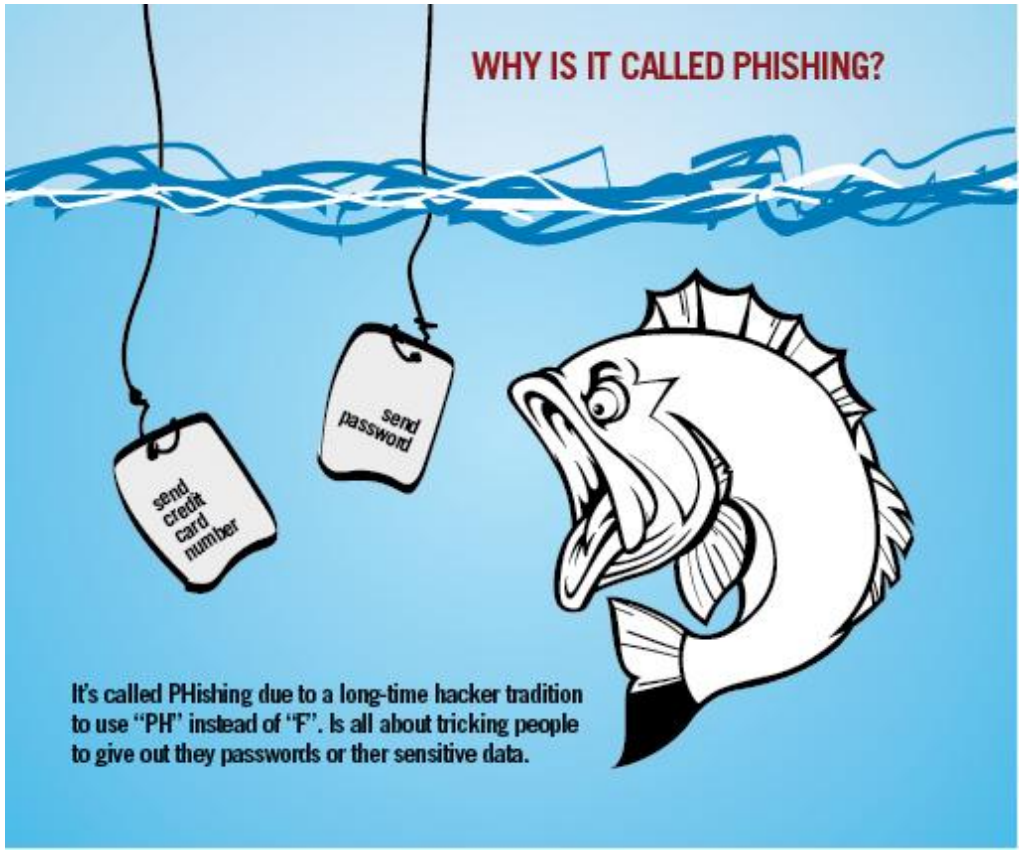
```
--
Good morning,


I have an assignment i will need you to do for me. I'm in a meeting ,i
will not be able to explain on phone.

Thanks
```


© 2018 UMass Amherst Global. All rights reserved

Phishing



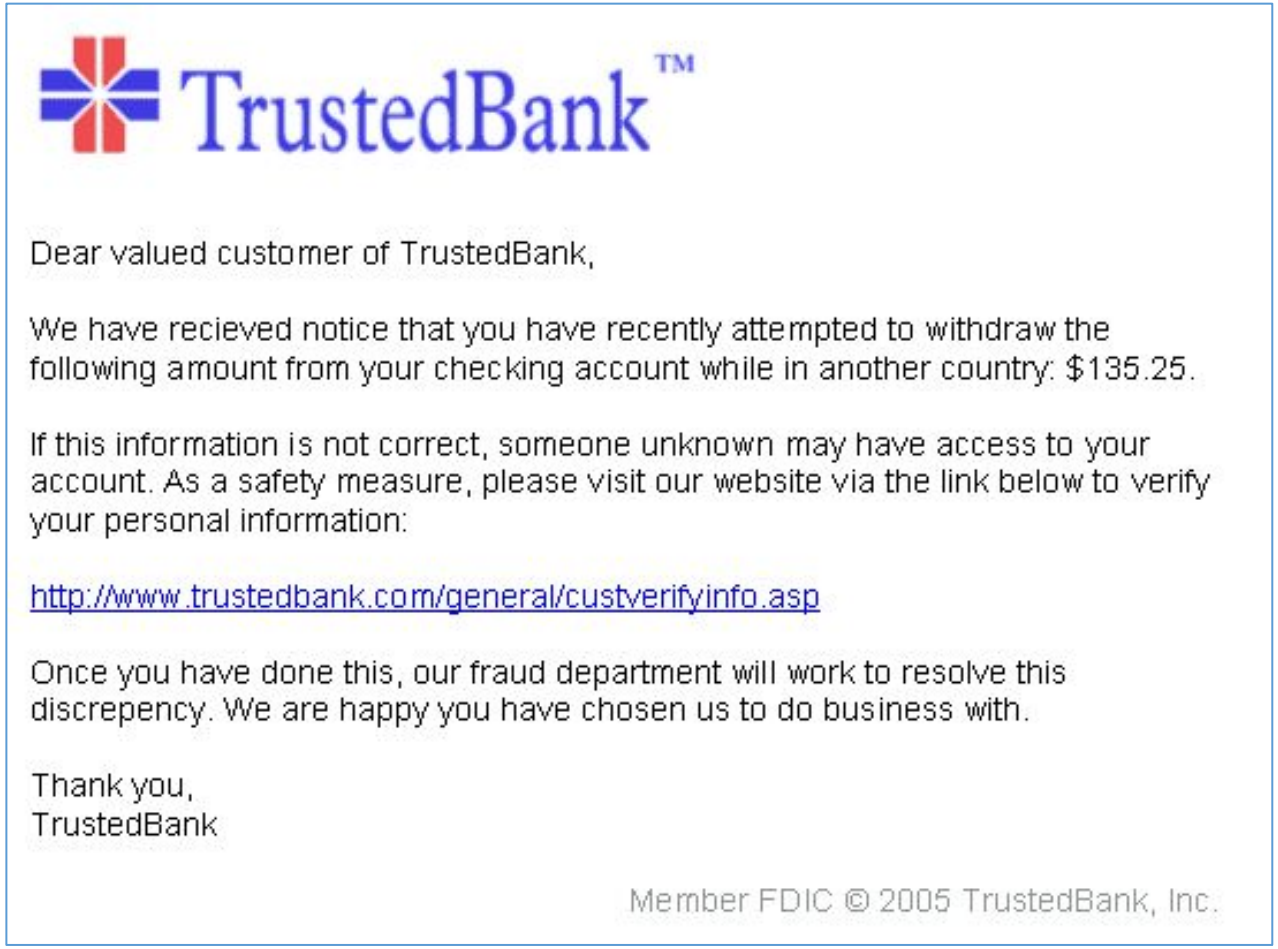
- In computer security:
  - Criminally fraudulent process of attempting to acquire sensitive information by masquerading as a trustworthy entity in an electronic communication
    - Ex. usernames, passwords and credit card details

© 2018 UMass Amherst Global. All rights reserved

Phishing (cont'd)

- Typically carried out using email or instant messaging programs
  - Directs users to enter details in fake websites designed to look identical to legitimate ones

- Common communication sources: social media, auction sites, online banking/payment, and IT Administrators



TrustedBank™

Dear valued customer of TrustedBank,

We have recieved notice that you have recently attempted to withdraw the following amount from your checking account while in another country: $135.25.

If this information is not correct, someone unknown may have access to your account. As a safety measure, please visit our website via the link below to verify your personal information:

http://www.trustedbank.com/general/custverifyinfo.asp

Once you have done this, our fraud department will work to resolve this discrepency. We are happy you have chosen us to do business with.

Thank you,
TrustedBank

Member FDIC © 2005 TrustedBank, Inc.

© 2018 UMass Amherst Global. All rights reserved

Phishing (cont'd)

- Phishing 2019
  - https://www.vadesecure.com/en/top-6-phishing-trends-of-2019/
- The Future
  - Beyond banking
  - Targeting based on social networks
  - Less distinguishable from ads
    - 2.7% of top-ranked companies in web search were BAD,
    - 4.44% of companies who bought ads on the search engine were BAD!
  - Golden client hardware as a solution for high-end market
  - Identity tools: biometrics, ID cards

© 2018 UMass Amherst Global. All rights reserved

True2F: Backdoor-resistant authentication tokens, Stanford and Google

Key Ideas

- New key generation and protocols ECDSA
- new privacy defenses to prevent cross-origin token fingerprinting attacks
- Backwards compatibility with existing tokens
- Performance overhead: A True2F-protected authentication takes just 57ms to complete on the token, compared with 23ms for unprotected U2F.
- Deployment at Google

© 2018 UMass Amherst Global. All rights reserved

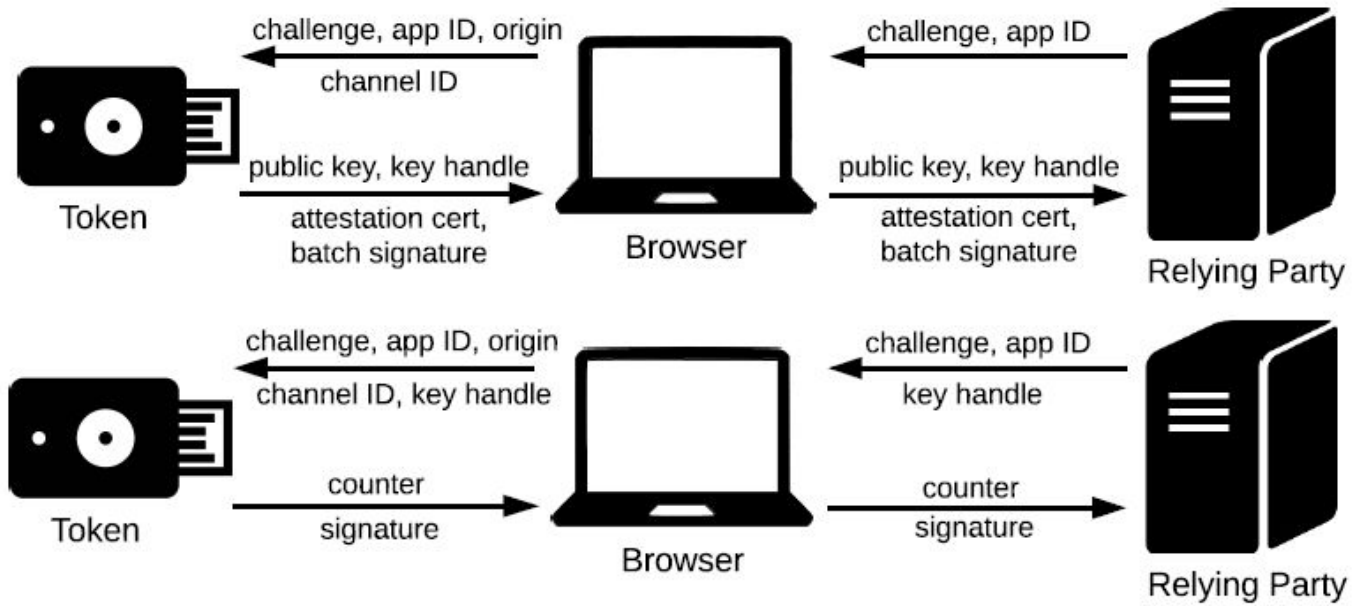


Figure 2: U2F registration (top) and authentication (bottom).

More on T2F

- With True2F, to compromise the cryptographic keys on the token, an attacker has to compromise both the user's machine and the hardware token itself. In this way, True2F provides **"strongest link"** security, while standard U2F provides security that is only as good as the hardware token itself.

© 2018 UMass Amherst Global. All rights reserved

Brain vs. Computer

Computer

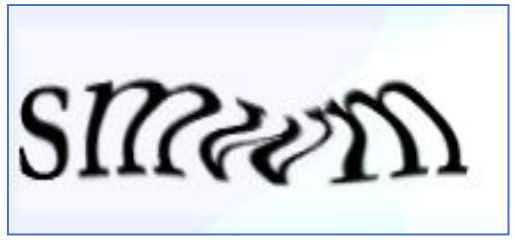
- Fast
- Large memory
- Reliable
- Low-cost
- Small
- Manageable

Brain

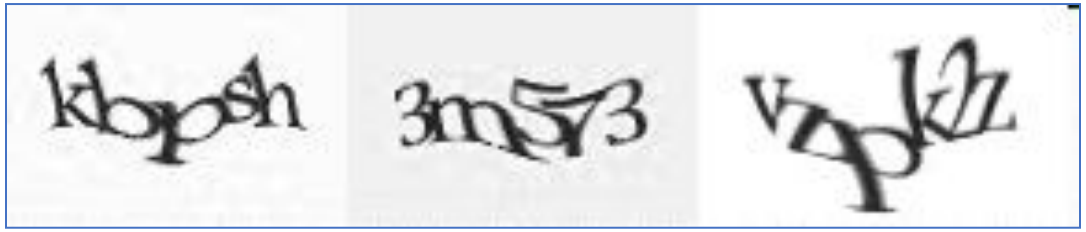
- Face recognition
- Image recognition
- Speech
- Games
- Noisy text: CAPTCHA
- Completely automated public Turing Test to tell computers and humans apart

© 2018 UMass Amherst Global. All rights reserved

CAPTCHAs



Early CAPTCHAs were used on Yahoo!, but technology caught up quickly

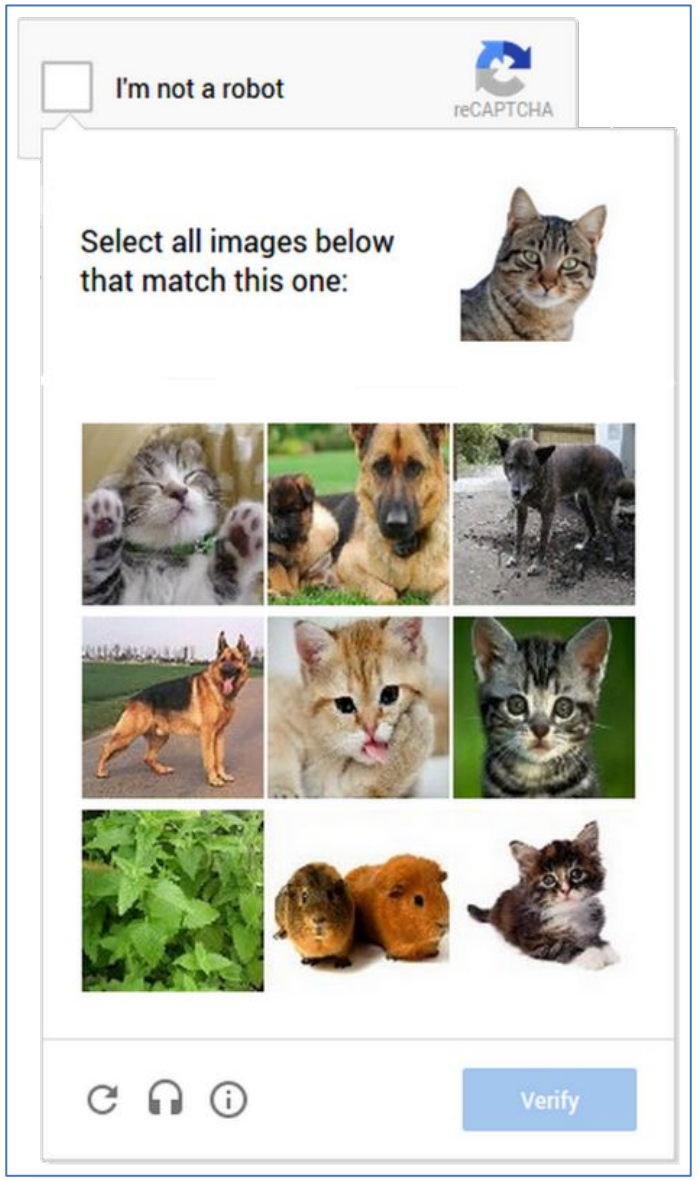


Later CAPTCHAs use angled lines or crowded symbols to deter segmentation

© 2018 UMass Amherst Global. All rights reserved

CAPTCHAs (cont'd)

- reCAPTCHA by Google uses images like street signs and image labeling to increase website security



© 2018 UMass Amherst Global. All rights reserved

Discussion: The Future of CAPTCHAS

- Speech?
- Video?
- Games?
- What about accessibility? See: *https://www.usenix.org/conference/soups2017*
- User-specific knowledge?
- Your ideas?

© 2018 UMass Amherst Global. All rights reserved

Some Meta-Conclusions

- Human factors are probably the largest existing vulnerabilities in secure systems.
- Some vulnerabilities can be fixed with education and engineering, however much is probably innate
- On the bright side, there is much research to be done in this area!

© 2018 UMass Amherst Global. All rights reserved

Recent Events

- **Workshop on Security and Human Behaviour**, brought together psychologists with economists and security engineers,

- ***SOUPS* - Symposium On *Usable* Privacy and *Security***

© 2018 UMass Amherst Global. All rights reserved

Assignment (to be finalized on Moodle)

- Read Voting paper for next Lecture. (2-3 hours)

© 2018 UMass Amherst Global. All rights reserved