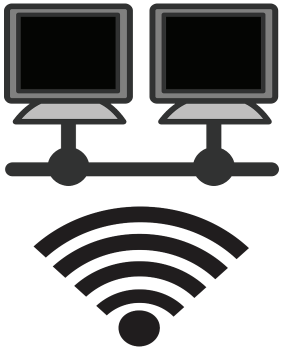
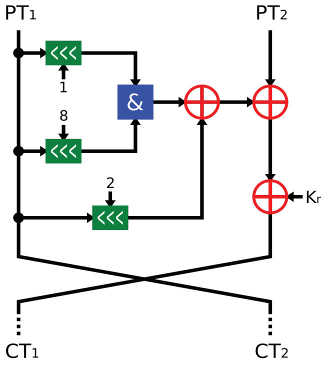
CSE 40567 / 60567: Computer Security





Security Basics 2

State of the Security Landscape

Social Engineering

Low-hanging fruit

A dialogue:

sysadmin: “Yeah, this is systems engineering.”

caller: “Hi, this is Bob Wells from the sales team, I’m trying to log into our portal from a customer’s site, and I left my dang credentials back at the office.”

sysadmin: “OK. To verify your identity, I’ll need your UID, social security num…”

caller: “Look buddy, I don’t have time for all of that, you want to explain to corporate how you blew a $10M deal by making my customer walk out while I play 20 questions?”

sysadmin: *sigh* “Here’s your password…”

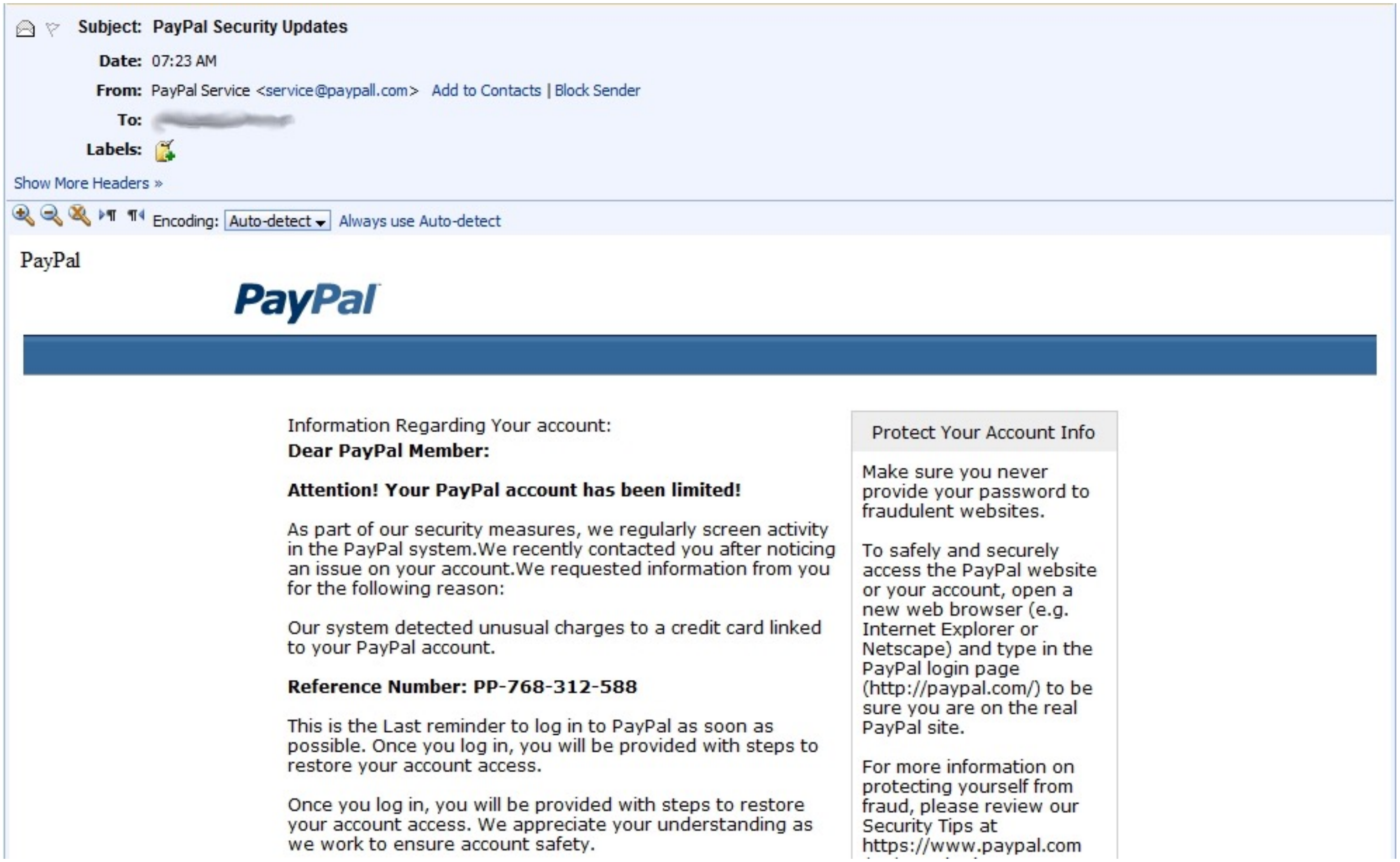
A little reconnaissance improves the execution

- Need info on your mark? The BMV is your best friend
  - Old PI trick
  - Address, Phone Number, Date of Birth, Make and Model of Car

Get hired as a janitor

- Physical access to target facility
  - Access to computers
  - Handwritten passwords in vicinity of workstations
  - You’re handling the trash — a trove of useful information
  - Plant thumb-drives with malware

Software can be an effective social engineer



Subject: **PayPal Security Updates**
Date: 07:23 AM
From: PayPal Service <service@paypall.com>
To: [redacted]
Labels:

PayPal

PayPal

Information Regarding Your account:
Dear PayPal Member:

Attention! Your PayPal account has been limited!

As part of our security measures, we regularly screen activity in the PayPal system.We recently contacted you after noticing an issue on your account.We requested information from you for the following reason:

Our system detected unusual charges to a credit card linked to your PayPal account.

Reference Number: PP-768-312-588

This is the Last reminder to log in to PayPal as soon as possible. Once you log in, you will be provided with steps to restore your account access.

Once you log in, you will be provided with steps to restore your account access. We appreciate your understanding as we work to ensure account safety.

Protect Your Account Info

Make sure you never provide your password to fraudulent websites.

To safely and securely access the PayPal website or your account, open a new web browser (e.g. Internet Explorer or Netscape) and type in the PayPal login page (http://paypal.com/) to be sure you are on the real PayPal site.

For more information on protecting yourself from fraud, please review our Security Tips at https://www.paypal.com

paypal-phishing-scam-email-2 🅭 BY 2.0 Saidul A Shaari

Why are attacks that target the user so hard to defend against?

Human errors made while considering a security regime fall into three categories:

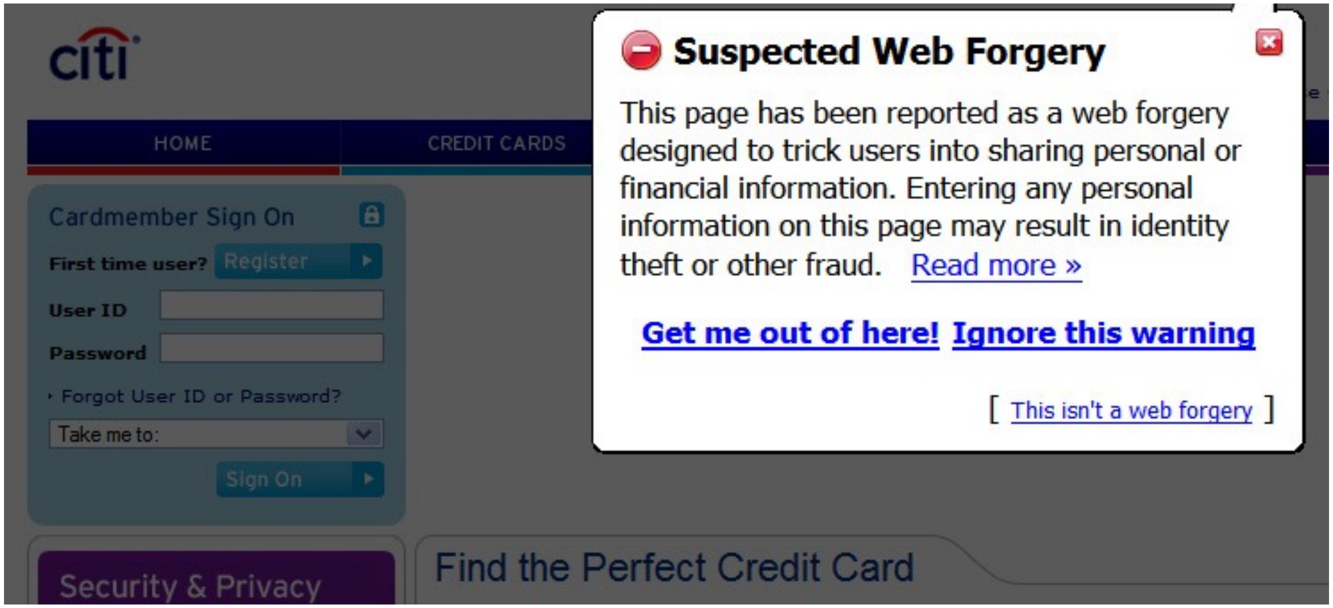
1. Slips and lapses at the level of skill
2. Mistakes at the level of rules
3. Mistakes at the cognitive level

R. Anderson, Chpt. 2

Slips and lapses at the level of skill

Inattention can cause a practiced action to be caused instead of an intended one.

Example:



Suspected Web Forgery

This page has been reported as a web forgery 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.

Danny Sullivan 🅭 BY 2.0 Google/Firefox Phishing Warning

Mistakes at the level of rules

Actions people take by following rules are open to errors when they follow the wrong rule

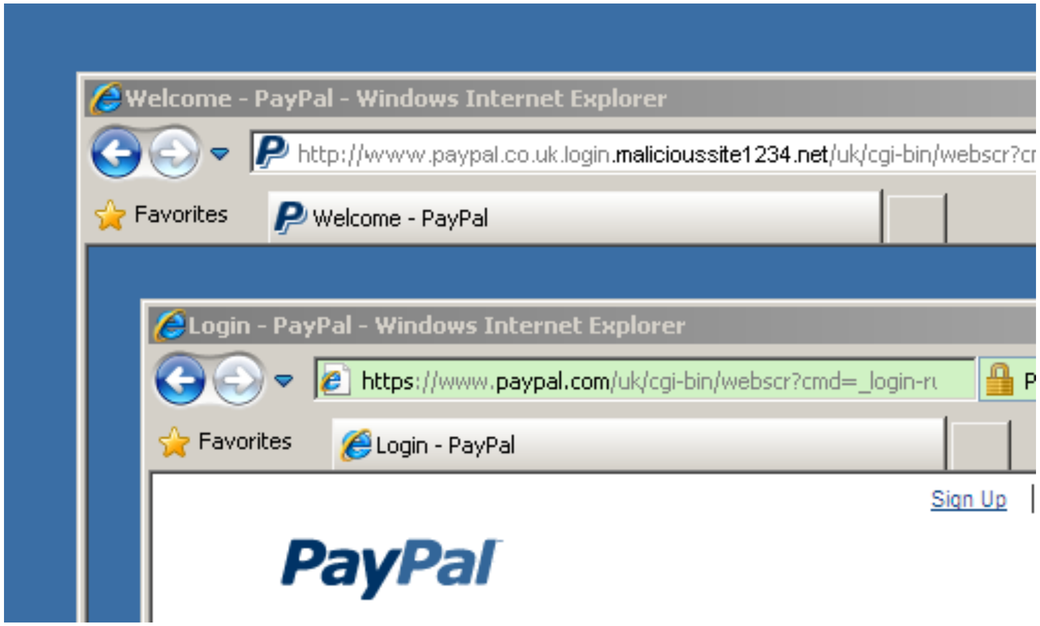
Example: tricky URL

https://www.citibank.secureauthentiction.com

Mistakes at the cognitive level

Many of us simply don’t understand the problem

Example: picture-in-picture attack



Welcome - PayPal - Windows Internet Explorer

http://www.paypal.co.uk.login.malicioussite1234.net/uk/cgi-bin/webscr?cr

Login - PayPal - Windows Internet Explorer

https://www.paypal.com/uk/cgi-bin/webscr?cmd=_login-ru

Image Credit:
https://www.clerkendweller.uk/2009/9/15/Picture-in-Picture-Phishing-Attacks-and-Operating-System-Styles

Our Guiding Philosophy of Security

Fundamentally, computer hacking is a social problem that cannot be addressed entirely by technology

Risk Mitigation

Assume that any system can be compromised

Security systems have many components and connections

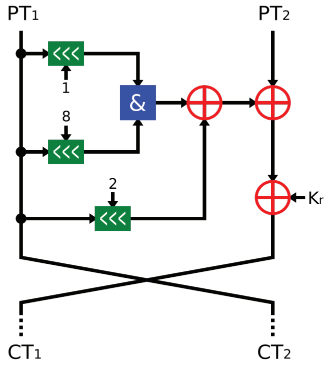
Some of these are unknown to the designers, implementors and users

Our best strategy: **lessen** the risk of attack

B. Schneier, Secrets & Lies, Digital Security in a Networked World, Wiley 2000

Risk Mitigation

Security involves processes:



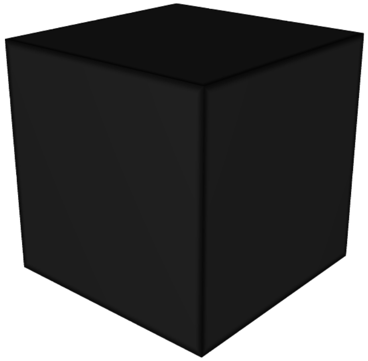
Preventative technologies

Detection and Reaction

Forensic Systems

Security through obscurity is not good security

- Many people think that a security system becomes more secure if its internal structure is secret
    - Example: A secret encryption algorithm



BUT: The exact opposite is the case

Kerckhoffs’ principle

“The security of a cryptographic system shall always and only depend on the secrecy of the key. Everything about the algorithm except for the keys shall be open.”

Kerckhoffs' principle

- Open and standardized systems are subject to constant analysis by the international research community
- Secret systems can only be analyzed by internal specialists
    - Unless an agency or company has a huge budget, severe and constant analysis of internal security systems is not easy

Edward Snowden 🅭
BY 3.0 Hic et nunc

Extending Kerckhoffs' principle

Bruce Schneier: "Kerckhoffs' principle applies beyond codes and ciphers to security systems in general: every secret creates a potential failure point. Secrecy, in other words, is a prime cause of brittleness—and therefore something likely to make a system prone to catastrophic collapse. Conversely, openness provides ductility."

Extending Kerckhoffs’ principle

- Any system whose security depends on keeping the details of the system secret is not secure in the long run.
- **Defense in depth** suggests layers, some of which may contain secrets, but the core must be secure without them.
- Keeping the “algorithm” and key concepts secret increases the asymmetric information, potentially keeping even experts from evaluating the system without significant effort.

Vulnerability Disclosure

What do we do if we find a bug that leads to system compromise?

➡ Ethical Dilemma

The controversy is not new: locksmiths worried about the same thing in the 19th century

Hobbs, Alfred (1853). Locks and Safes: The Construction of Locks. London: Virtue & Co.

Non-disclosure

- Premise: vulnerability information helps attackers, and shouldn’t be shared
- Situation in computer security up to the mid-1990s
    - Enforced via vendor legal intimidation and censorship

⬇

http://attrition.org/errata/legal_threats/

Coordinated Disclosure

Microsoft's position: software vendors have right to control product vulnerability information

- Risk of sharing vulnerability with malicious parties is too high
- Vulnerability is disclosed after the patch is released

Culp, Scott. "It's Time to End Information Anarchy". Technet Security. Microsoft TechNet, 2001.

Full disclosure

"We don't believe in security by obscurity, and as far as we know, full disclosure is the only way to ensure that everyone, not just the insiders, have access to the information we need."

- Leonard Rose (aka Terminus)

Without full disclosure:

- Vendors have no incentive to release patches if there is no customer demand for them
- Sysadmins can't make informed decisions about risks to their systems
- Malicious individuals have a longer window to exploit a flaw