Design Category:
Favor Simplicity

Favor Simplicity

- Keep it **so simple** it is **obviously correct**
  - Applies to the external interface, the internal design, and the implementation
    - Classically referred to as **economy of mechanism**
  - **Category**: Prevention

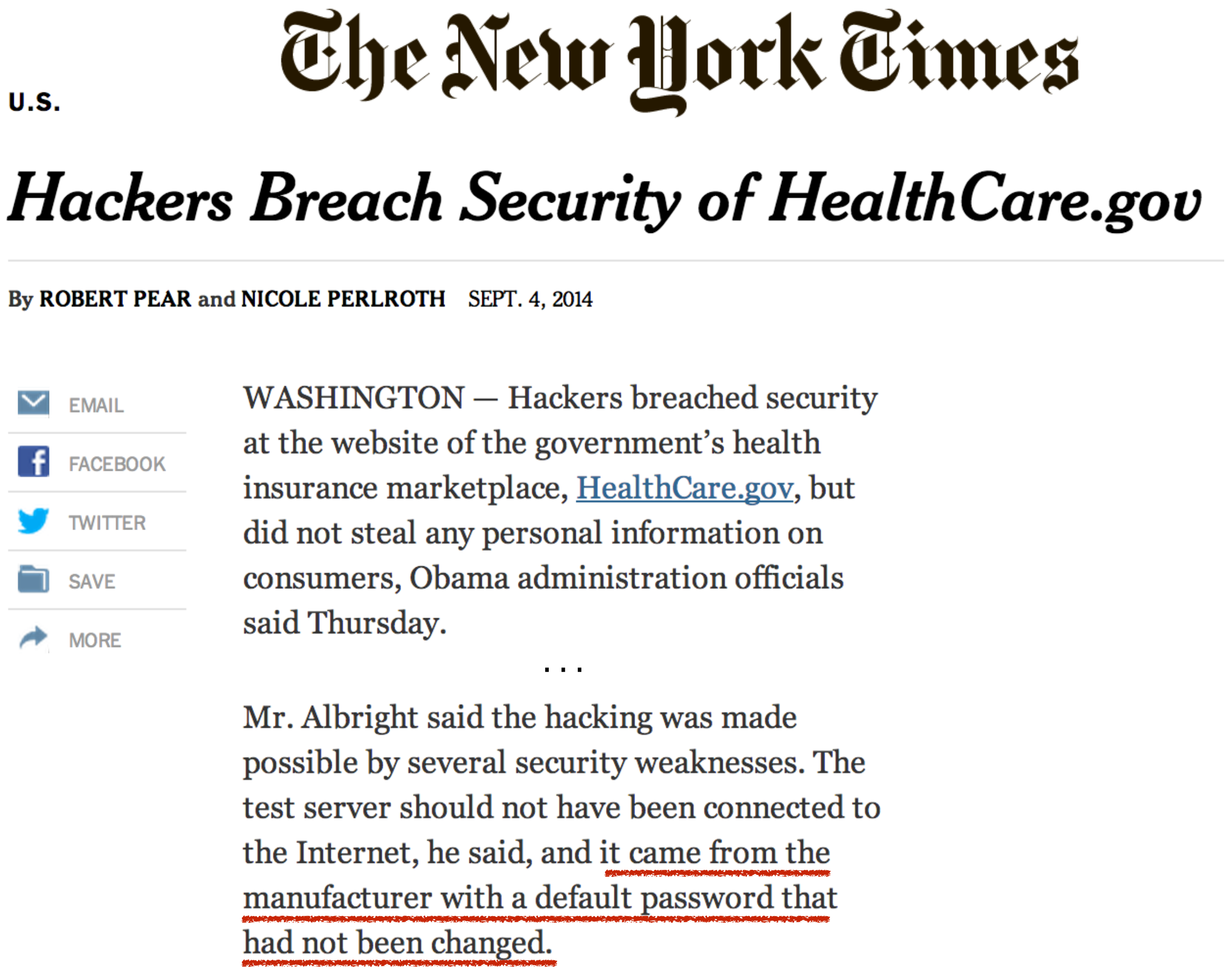
"We've seen **security bugs in almost everything**: operating systems, applications programs, network hardware and software, and security products themselves. **This is a direct result of the complexity of these systems.** The more complex a system is--the more options it has, the more functionality it has, the more interfaces it has, the more interactions it has--the harder it is to analyze [its security]". —*Bruce Schneier*

https://www.schneier.com/essays/archives/1999/11/a_plea_for_simplicit.html

FS: Use fail-safe defaults

- Some **configuration** or **usage choices affect** a system's **security**
  - The length of cryptographic keys
  - The choice of a password
  - Which inputs are deemed valid

- **The default choice should be a secure one**
  - **Default key length is secure** (e.g., 2048-bit RSA keys)
  - **No default password**: cannot run the system without picking one
  - **Whitelist** valid objects, rather than blacklist invalid ones
    - E.g., don't render images from unknown sources



U.S.

The New York Times

Hackers Breach Security of HealthCare.gov

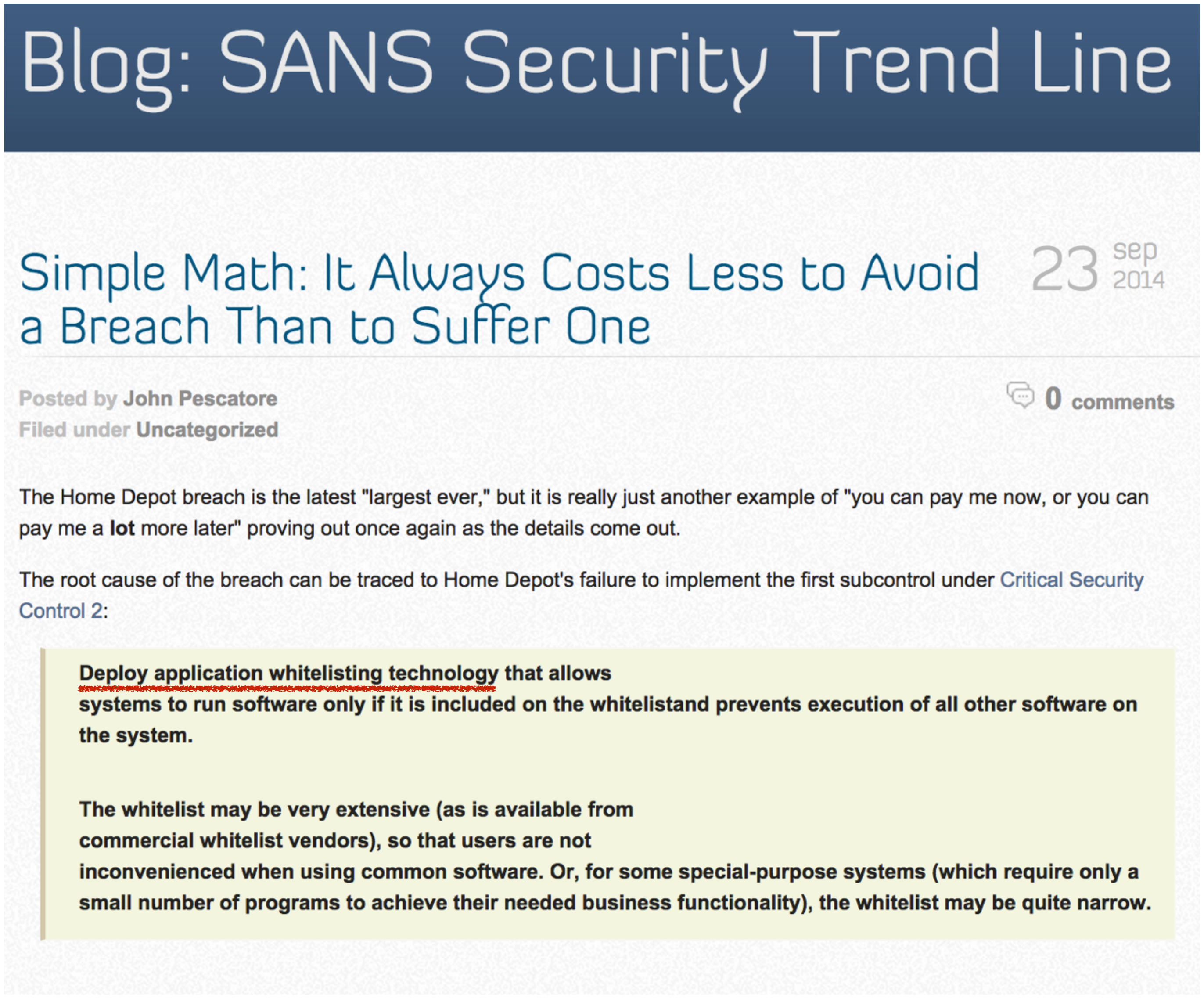
By ROBERT PEAR and NICOLE PERLROTH SEPT. 4, 2014

EMAIL
FACEBOOK
TWITTER
SAVE
MORE

WASHINGTON — Hackers breached security at the website of the government's health insurance marketplace, HealthCare.gov, but did not steal any personal information on consumers, Obama administration officials said Thursday.

. . .

Mr. Albright said the hacking was made possible by several security weaknesses. The test server should not have been connected to the Internet, he said, and it came from the manufacturer with a default password that had not been changed.



Blog: SANS Security Trend Line

Simple Math: It Always Costs Less to Avoid a Breach Than to Suffer One

23 sep 2014

Posted by John Pescatore
Filed under Uncategorized

0 comments

The Home Depot breach is the latest "largest ever," but it is really just another example of "you can pay me now, or you can pay me a **lot** more later" proving out once again as the details come out.

The root cause of the breach can be traced to Home Depot's failure to implement the first subcontrol under Critical Security Control 2:

> **Deploy application whitelisting technology that allows systems to run software only if it is included on the whitelistand prevents execution of all other software on the system.**
>
> **The whitelist may be very extensive (as is available from commercial whitelist vendors), so that users are not inconvenienced when using common software. Or, for some special-purpose systems (which require only a small number of programs to achieve their needed business functionality), the whitelist may be quite narrow.**

"… whitelisting on servers and single function servers or appliances has proven to cause near zero business or IT administration disruption"

FS: Do not expect expert users

[Only] Computer scientists and drug dealers have users
—R. David Lankes

- Software designers should consider how the **mindset and abilities** of (the least sophisticated of) a system's **users** will **affect security**

- **Favor simple user interfaces**
  - **Natural or obvious choice is the secure choice**
    - Or avoid choices at all, if possible, when it comes to security
  - **Don't have users make frequent security decisions**
    - Want to avoid user fatigue
  - **Help users explore ramifications of choices**
    - E.g., allow admin to explore user view of set access control policy

Passwords

- **Goal: easy to remember but hard to guess**
  - Turns out to be **wrong** in many cases!
    - **Hard to guess = Hard to remember!**
  - **Compounding problem: repeated password use**

- **Password cracking tools** train on released data to quickly guess common passwords
  - John the Ripper, http://www.openwall.com/john/
  - Project Rainbow, http://project-rainbowcrack.com/
  - many more …
  - **Top 10 worst passwords of 2013**:123456, password, 12345678, qwerty, abc123, 123456789, 111111, 1234567, iloveyou, adobe123 [from SplashData]

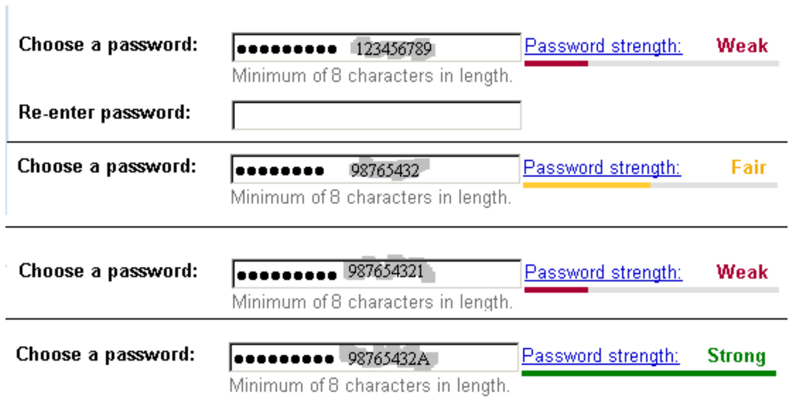
Password Manager

- A password manager (PM) stores a **database of passwords, indexed by site**
  - Encrypted by a **single, master password** chosen (and remembered) by the user, used as a key
  - **PM generates complicated per-site passwords**
    - Hard to guess, hard to remember, but the latter doesn't matter!

- **Benefits**
  - Only a single password for user to remember
  - User's password at any given site is hard to guess
  - Compromise of password at one site does not permit immediate compromise at other sites
- **But**:
  - Must still **protect** and **remember** strong **master password**

Password Strength Meter

- **Gives user feedback on the strength of the password**
  - Intended to **measure guessability**
  - Research shows that these **can work**, but the design must be **stringent** (e.g., forcing unusual characters)
    - Ur et al, "How does your password measure up? The effect of strength meters on password creation", Proc. USENIX Security Symposium, 2012.



Choose a password: ●●●●●●●●●● 123456789 Password strength: Weak
Minimum of 8 characters in length.
Re-enter password:

Choose a password: ●●●●●●●● 98765432 Password strength: Fair
Minimum of 8 characters in length.

Choose a password: ●●●●●●●●● 987654321 Password strength: Weak
Minimum of 8 characters in length.

Choose a password: ●●●●●●●●●● 98765432A Password strength: Strong
Minimum of 8 characters in length.

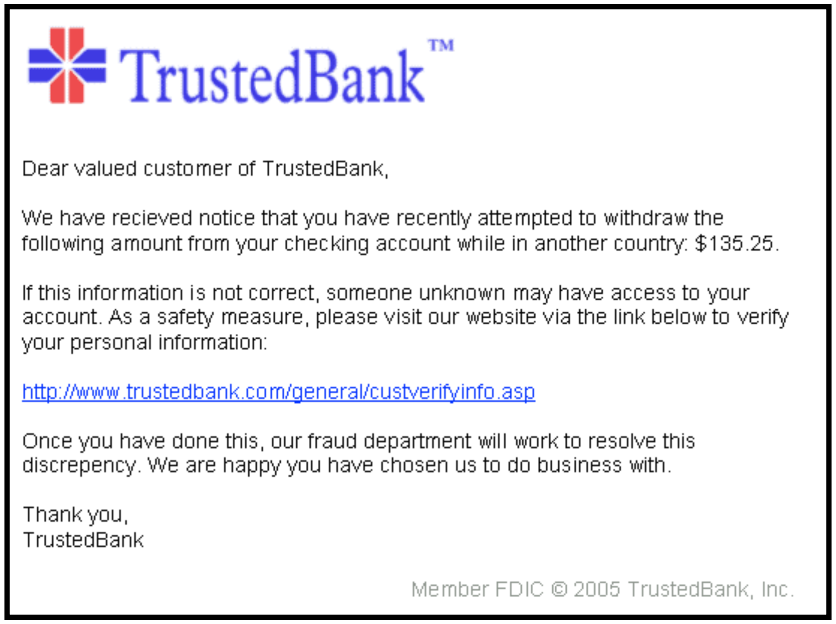
Better together

- **Password manager**
  - **One security decision**, not many

- **Password meter**
  - Users can **explore ramifications of various choices** by visualizing quality and reasoning of password
  - **Do not permit poor choices** (or reduce the chances of them) by enforcing a minimum score

Phishing

- **User is tricked** into thinking that a **site** or **e-mail** **is legitimate**, rather than a scam
  - And is then tricked into installing malware or performing other harmful actions



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

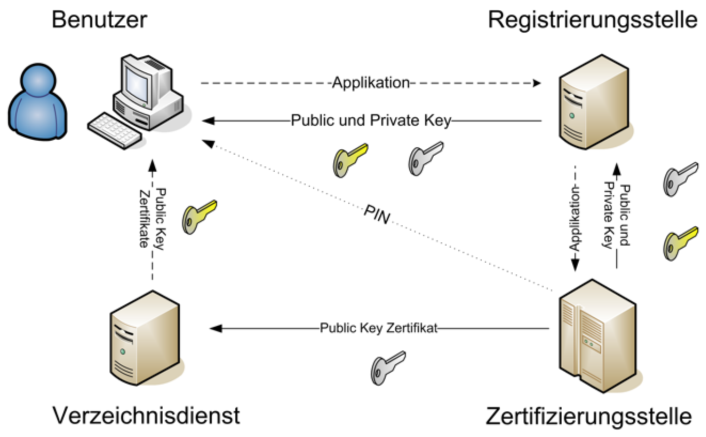
Member FDIC © 2005 TrustedBank, Inc.

Phishing

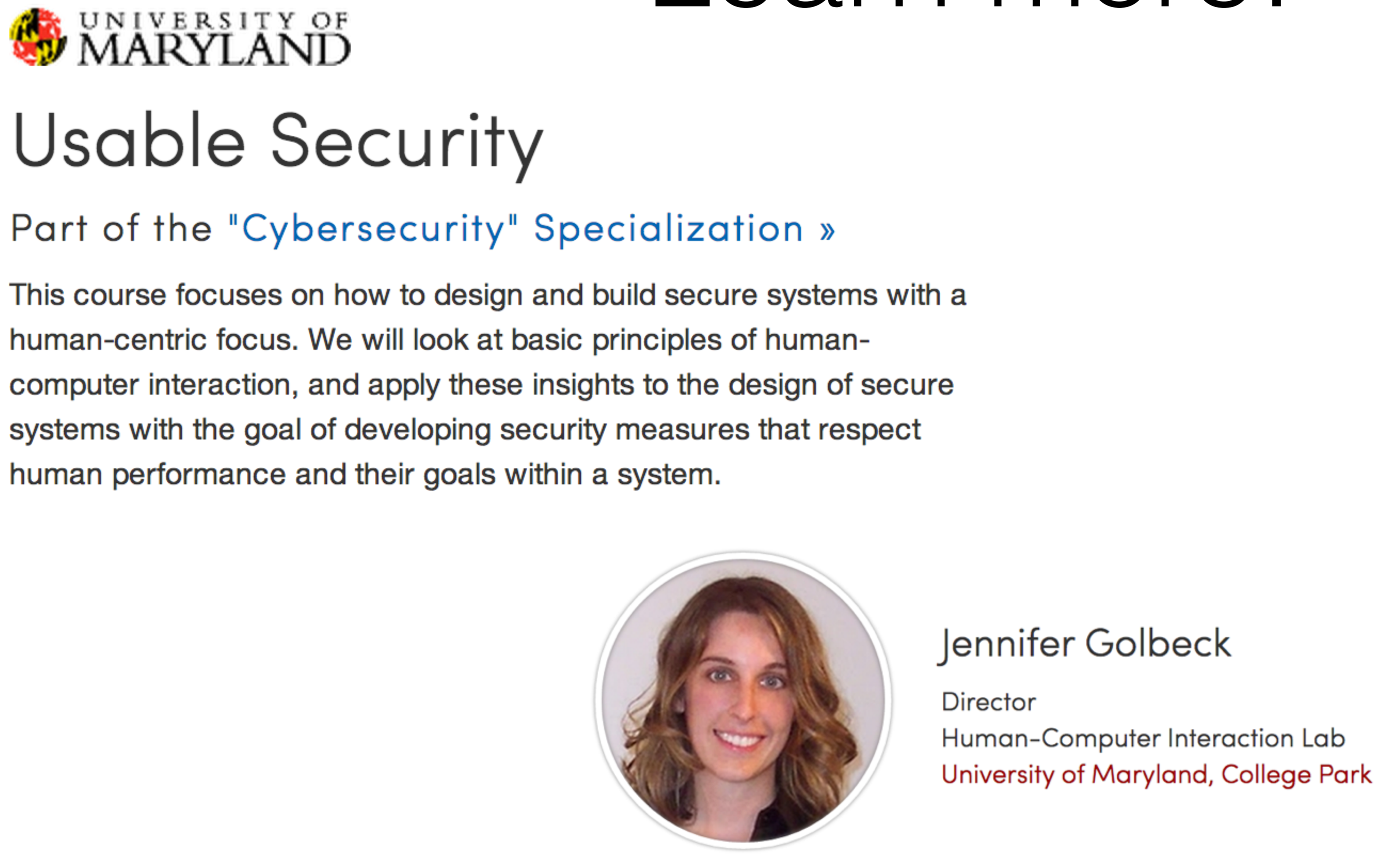
- **Failure: Site or e-mail not (really) authenticated**
  - Internet e-mail and web protocols **not originally designed for remote authentication**
  - Solution is **hard to deploy**
    - Use hard-to-fake notions of identity, like **public key cryptography.** But which system? How to upgrade gradually?

GPGTOOLS

THE ENIGMAIL PROJECT
OPENPGP EMAIL SECURITY FOR MOZILLA APPLICATIONS



Learn more!



UNIVERSITY OF MARYLAND

Usable Security

Part of the "Cybersecurity" Specialization »

This course focuses on how to design and build secure systems with a human-centric focus. We will look at basic principles of human-computer interaction, and apply these insights to the design of secure systems with the goal of developing security measures that respect human performance and their goals within a system.

Jennifer Golbeck

Director
Human-Computer Interaction Lab
University of Maryland, College Park