

COMS E6998-9:
Software Security and
Exploitation

Lecture 2: Hackernomics and Design

Hugh Thompson, Ph.D.
hthompson@cs.columbia.edu

Hackernomics (*noun*)

A social science concerned chiefly with description and analysis of attacker motivations, economics, and business risk. Characterized by

5 fundamental immutable laws and 6 corollaries

Law 1

Most attackers aren't evil or insane; they just want something

Corollary 1.a.:

Companies don't have the budget to protect against evil people but we *can* protect against people that will look for weaker targets

Corollary 1.b.:

Security Theatre can sometimes be good...assuming that the cost to test it does not approach \$0

Law 2

The type of data that attackers care about is changing

Corollary 2.a.:

When new data suddenly becomes important we have a big archival problem

Law 3

In the absence of metrics, we tend to over focus on risks that are either familiar or recent.

Law 4

In the absence of security education or experience, people (customers, managers, developers, testers, designers) naturally make poor security decisions with technology

Corollary 4.a.:

Software needs to be **easy to use securely and difficult to use insecurely**

Law 5

Most costly breaches come from simple failures, not from attacker ingenuity

Corollary 5.a.:

Bad guys can, however, be VERY creative if properly incentivized.

The CAPTCHA Dilemma

Completely

Automated

Public

Turing test to tell

Computers and

Humans

Apart

following

finding

smmm

Melissa strip



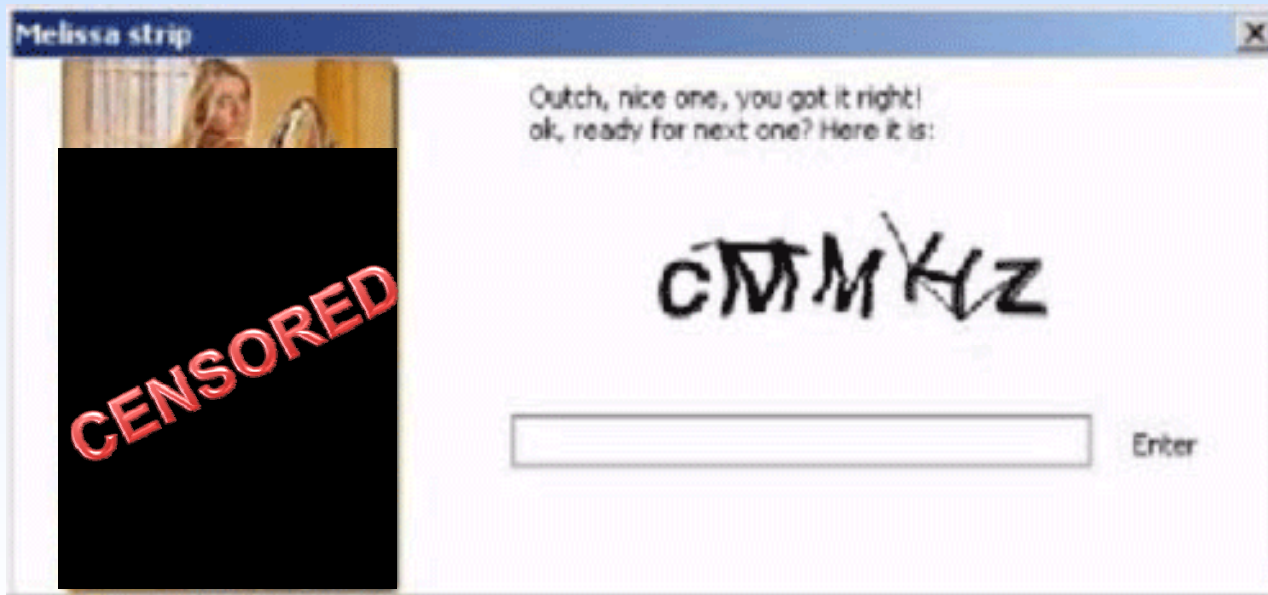
Ok, lets start baby! Lets see if you can strip me :). Put the word that you see on bottom, if its correct I'll take off 1 of my xxx :)

JWSA

Enter

CENSORED

Melissa strip



Cutch, nice one, you got it right! ok, ready for next one? Here it is:

CTM KZ

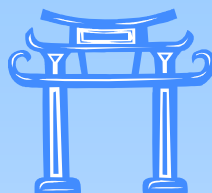
Enter

CENSORED

Source: Trend Micro <http://blog.trendmicro.com/captcha-wish-your-girlfriend-was-hot-like-me/>

© Hugh Thompson 2009

Software Security in an Evolving Environment



Gateway Data (*noun*) – *Data that seems harmless but, when used properly, can facilitate access to highly sensitive information.*



Direct Use

Conversion of public data to access through defined rules

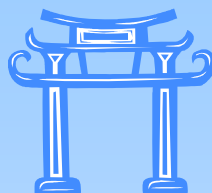
Amplification

Conversion of public data to private data by bouncing it off a person

Collective Intelligence

Correlating employee behavior to uncover sensitive corporate information

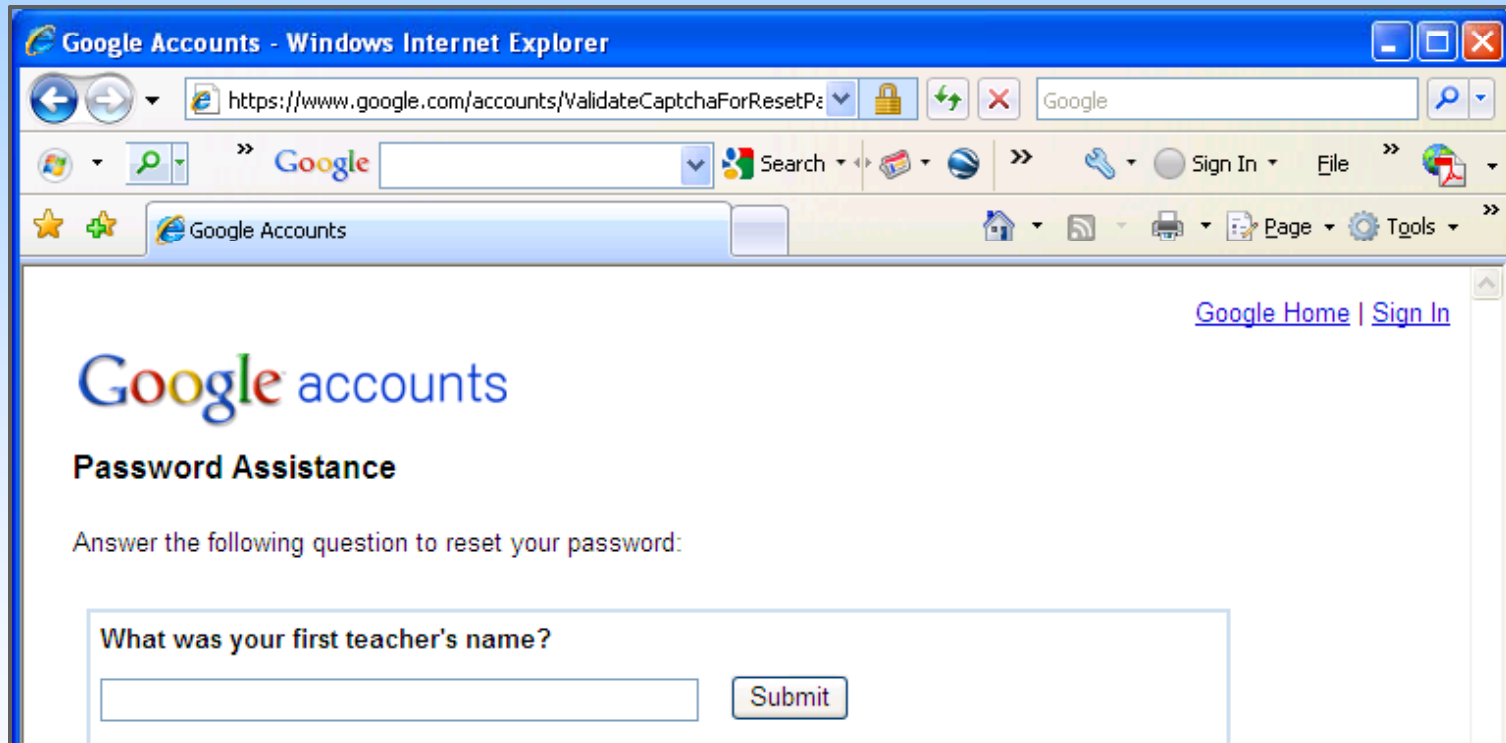




Direct Use Gateway Data: Data directly convertible into access through rules



What is your pet's name?
Where were you born?
What was your first teacher's name?
What is the mascot of your favorite team?
What was your first phone number?
What is your favorite restaurant?
Who is your favorite singer?
Where was your first job?



Step 1:
Reconnaissance

Old resumes, LinkedIn, Twitter, Facebook, blogs, friends/family blogs, public online records, etc.

Step 2:
Attempt Resets

Click on “Forgot your password?” or similar links. What do they ask for? What do they reveal?

Step 3:
Identify
Dependencies

Most people’s online identities have a common root. Is it one email address? A mobile phone?

Step 4:
Secure the Root

Once you’ve identified core dependencies, do what you can to strengthen the common root.

Sarah Palin

From Wikipedia, the free encyclopedia
(Redirected from Sara palin)

Sarah Louise Palin (pronounced *PAH-lin*; born February 11, 1964) is an American politician, author, and television personality. She served as the 11th Governor of Alaska from 2006 to 2009. She was the first female governor of Alaska and the youngest person ever elected governor of that state.

The family moved to Alaska when she was an infant. She attended Wasilla High School,^[10] where she was the head of the Fellowship of Christian Athletes, a

Palin was a member of the Wasilla, Alaska, city council from 1992 to 1996 and the city's mayor from 1996 to 2002. After an unsuccessful campaign for Lieutenant Governor of Alaska in 2002, she chaired the Alaska Oil and Gas Conservation Commission from 2003 until her resignation in 2004. She was elected Governor of Alaska in November 2006. Palin was the first female governor of Alaska and the youngest person ever elected governor of that state.

In 2008, Republican presidential candidate John McCain chose Palin as his running mate in that year's presidential election, making her the second female candidate and the first Alaskan candidate of either major party on a national ticket, as well as the first female vice-presidential pick for a Republican.

sports reporter for the *Mat-Su Valley Frontiersman*.^{[21][22]} In 1988, she eloped with her childhood sweetheart Todd Palin, believing that her parents "couldn't afford a big

Palin resigned as Governor on July 26, 2009, two and a half years into her four-year term.^{[7][8][9]}

Contents [hide]

- 1 Early life and career

11th Governor of Alaska
In office



Wednesday, Sep. 17, 2008

Sarah Palin's E-Mail Hacked

By M.J. Stephey

The cryptic Internet posse
target in Republican vice-p
members of Anonymous, a
4Chan, apparently breache
(gov.palin@yahoo.com) la

Mail Contacts Calendar Notepad What's New? - Mobile Mail - Mail Options Go

Check Mail Compose Search Mail Search the Web

Free phones at AT&T

Folders [Add - Edit]
 Inbox (84)
 Drafts
 Sent
 Spam (9) [Empty]
 Trash [Empty]
 My Folders [Hide]
 Emails for Arc...

Search Shortcuts
 My Photos
 My Attachments

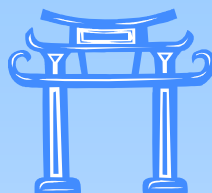
ADVERTISEMENT
FREE* Dinner for two at

Inbox
 View: All Messages Go Messages 1-100 of 174 First Previous Next Last

Delete Spam Mark as Unread Go Move... Go

	From	Subject	Date	Size
<input type="checkbox"/>	yahoo-account-services-us	Your Yahoo! password was changed	4:23 AM	5KB
<input type="checkbox"/>	19079829061@mms.dobson.	LOOK AT TRIG!!!!	12:36 AM	52KB
<input type="checkbox"/>	Amy McCorkell	HI SARAH	Sun, 9/14/08	4KB
<input type="checkbox"/>	Ivy Frye	Delivered: Re:	Sat, 9/13/08	3KB
<input type="checkbox"/>	Ivy Frye	Delivered: Re:	Sat, 9/13/08	3KB
<input type="checkbox"/>	Ivy Frye	Delivered: Re:	Sat, 9/13/08	3KB
<input type="checkbox"/>	Candy Sunderland	Welcome Home!	Wed, 9/10/08	17KB
<input type="checkbox"/>	Juanita	Re: Hello!	Mon, 9/8/08	3KB
<input type="checkbox"/>	Fatkidron@aol.com	Fwd: Fw: A story you will never read anywhere else.	Mon, 9/8/08	20KB
<input type="checkbox"/>	Remus	Read: Hello!	Mon, 9/8/08	3KB
<input type="checkbox"/>	JD & Trish	cousin jason	Sat, 9/6/08	6KB
<input type="checkbox"/>	Amy McCorkell	Read: Hello!	Fri, 9/5/08	3KB
<input type="checkbox"/>	Juanita	Read: Hello!	Fri, 9/5/08	3KB

Done



Amplification Gateway Data: data that can be amplified when bounced off a person.



From: Citi Cards [citicards@info2.citibank.com]

Sent: Wed 7/22/2009 9:51 AM

To: [REDACTED]

Cc:

Subject: Reminder: You Still Have until 8/14/09 to Save with a Balance Transfer Offer



[Email Security Zone](#)

For your account ending in: [REDACTED]

YOUR ACCOUNT: BALANCE TRANSFER

Add citicards@info2.citibank.com to your address book to ensure delivery.

A simple card
A smart financial

[Email Security Zone](#)

For your account ending in: [REDACTED]

[» Transfer Now](#)

[» Learn More](#)

Save now with
**2.99% APR on
transferred
balances until
07/01/10***

Act now to transfer balances to your Citi® Card and you can save money on interest.

We're offering you a special rate:

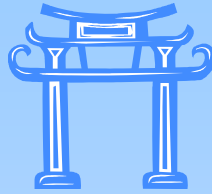
2.99% APR on transferred balances until 07/01/10*

You can transfer any amount, including balance transfer fees, up to your available credit line which is \$17,720 as of 06/25/09 on your Citi® account.**

We're all looking for intelligent ways to manage our finances and Citi has a great solution. With a special rate on **balance transfers**, you can save money on interest. Plus, you can consolidate all of your balances into one easy monthly payment.

[Transfer your balances to Citi today to:](#)

Credit Card	First 4 Digits	Total Digits
American Express	34xx or 37xx	15
VISA	4xxx	13 or 16
MasterCard	51xx-55xx	16
Discover	6011	16



Collective Intelligence Gateway Data:
Seemingly innocuous data that can be combined with other data across time, a company, or a group to reveal something sensitive.



Some Potential Direct Disclosures

- Information about customers or sales
- Information about the health of a company
- New policies or policy changes
- Ethics issues internally
- Hiring or firing
- Company violated a law
- Disclosure of legally protected data
- Creation of a legally protected “record” in a public place
- Mergers and acquisitions
- Potential strikes
- Trade secrets disclosed
- New features in a product or product changes

Company Name: We're losing customers, so we're reduced to having to screw employees. That's how we roll. Apparently.

10:17 AM Oct 3rd from Twiterrific

Telegraphed Information

- Location – services like Loopt append location information
- Job seeking behavior – LinkedIn recommendation requests, resume distribution, etc.
- Linkages/Relationships – new contacts or friends added to social networks

Flying to bentonville arkansas for a quick trip and meetings straight through the day friday.

7:39 PM Aug 20th from TinyTwitter

Holiday Ro-o-o-o-o-o-o-o-o-o-o-o-o-o-ad, Holiday Ro-o-o-o-o-o-o-o-o-ad! in
Bentonville, AR <http://loopt.us/> [REDACTED]

2:43 PM Apr 1st from Loopt

LinkedIn Recommendations

John Smith is requesting an endorsement for work

LinkedIn® Invitation Accepted

Congratulations! You and Mike are now connected.



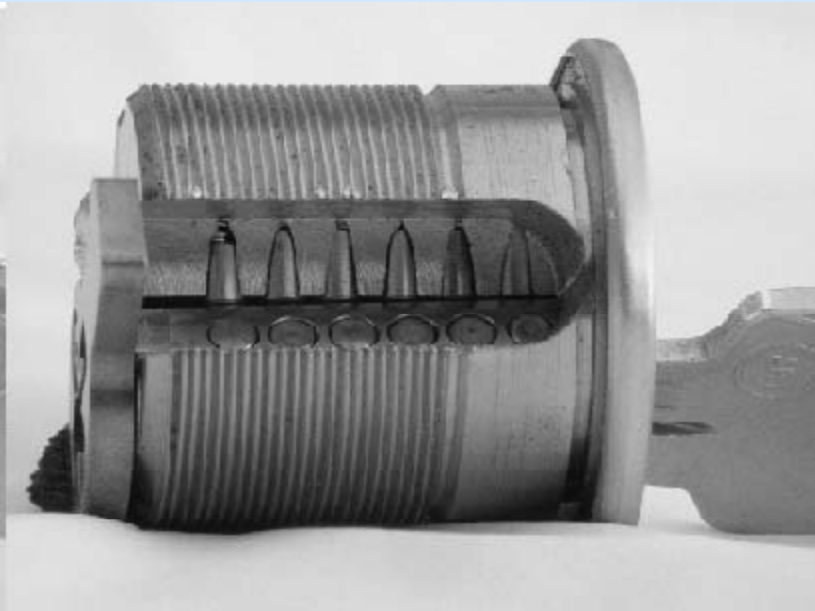
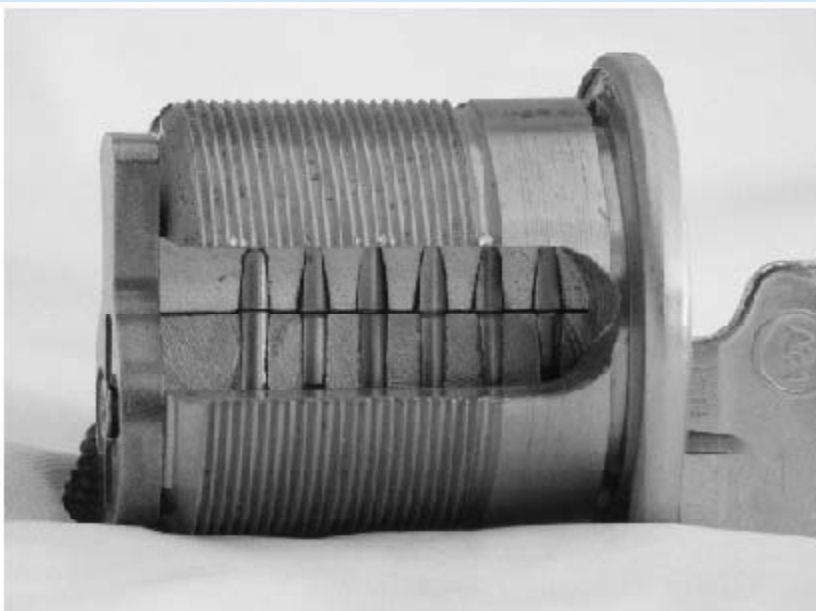
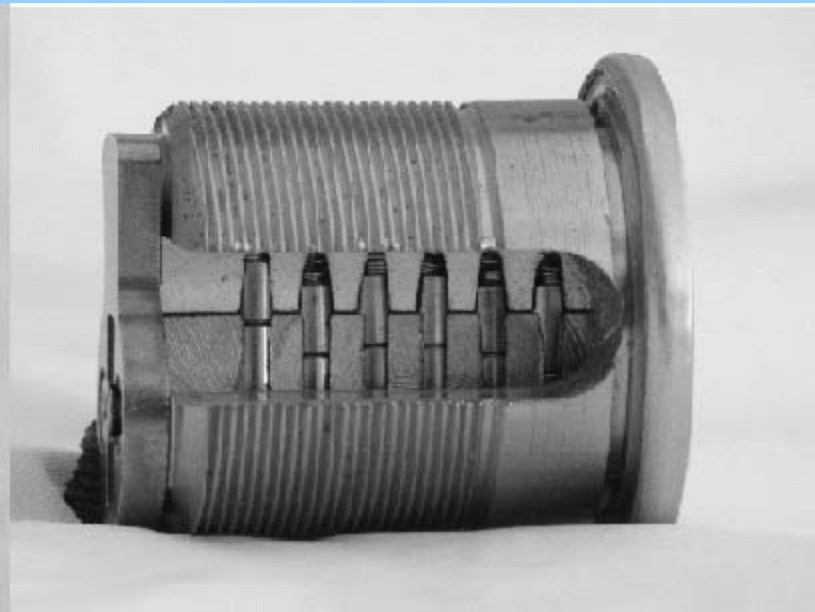
View [Mike's profile](#) to:

- Download Mike's current contact information
 - Write a recommendation for Mike
 - Find opportunities through Mike's network
 - See who you know in common
-

Overview of Security Design Principles

Design Principles

1. **Defense in depth** – Always set up multiple lines of defense for high value assets.
2. **Least privilege** – Software should only operate with the privileges it needs to get a task done, no more and no less.
3. **Input validation** – We need to make sure that assumptions about user input are also enforced in code.
4. **Compartmentalization** – Need to ensure that if an attacker compromises one system they can't compromise them all.



Class Break: “Bump Key”



BUG OF ZEN