COMS E6998-9:

Software Security and Exploitation

Lecture 2: Hackernomics and Design

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

Columbia University

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

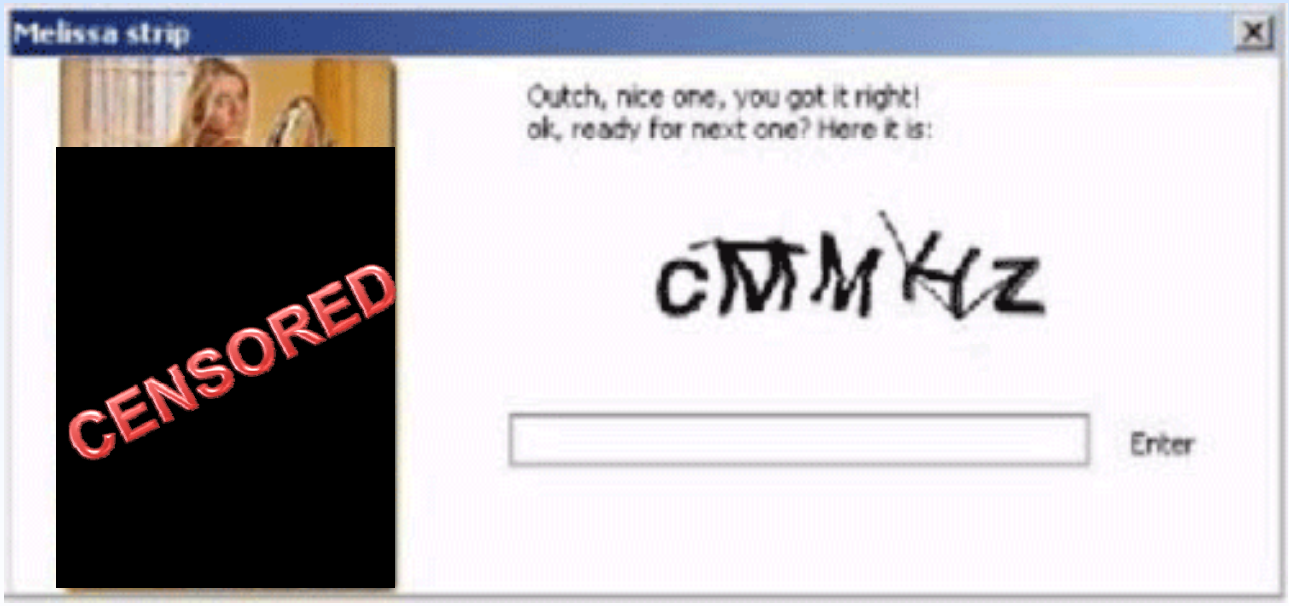
Public

Turing test to tell

Computers and

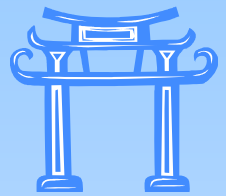
Humans

Apart

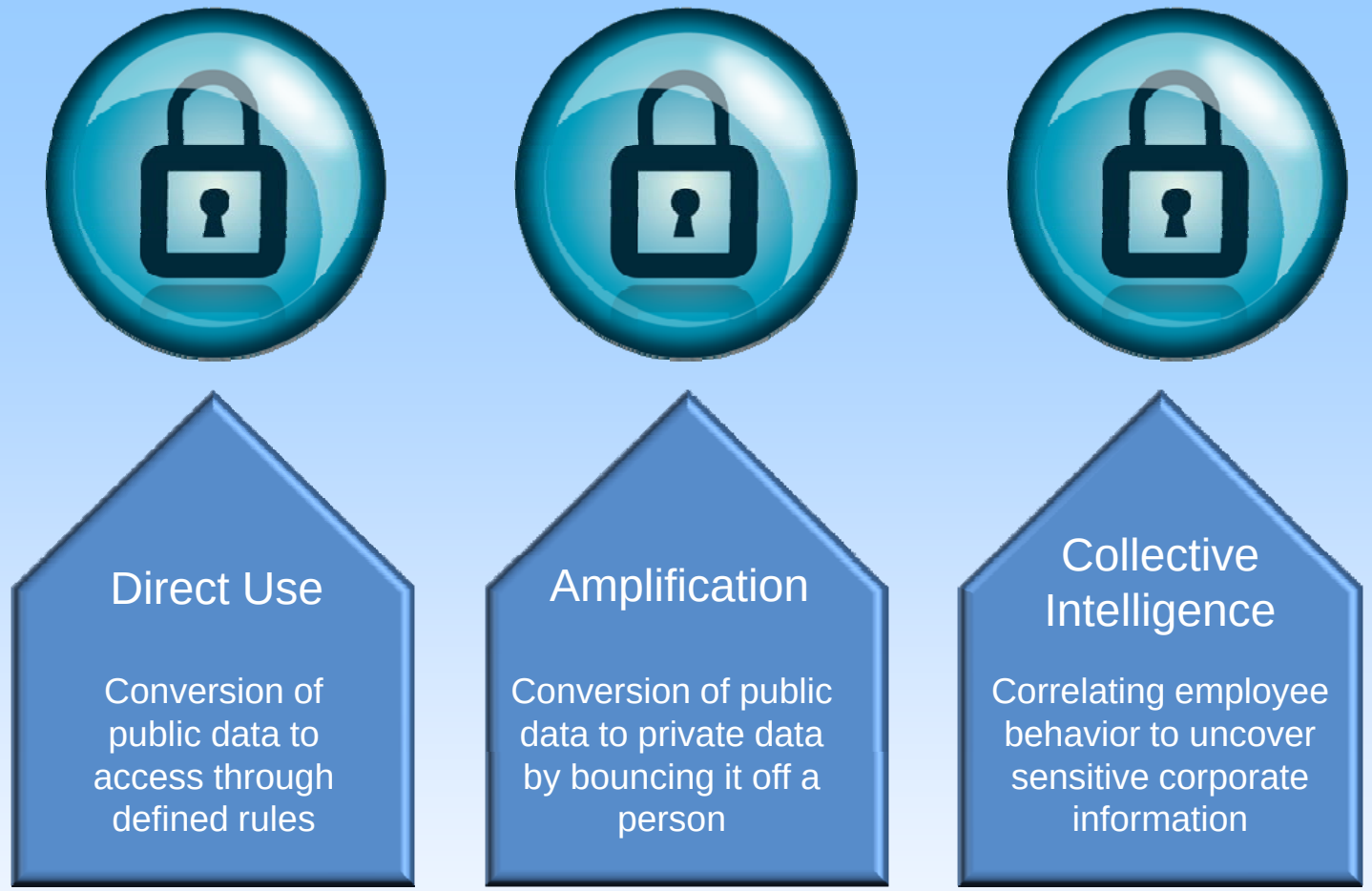


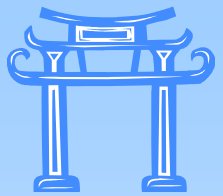
Source: Trend Micro http://blog.trendmicro.com/captcha-wish-your-girlfriend-was-hot-like-me/

Software Security in an Evolving Environment



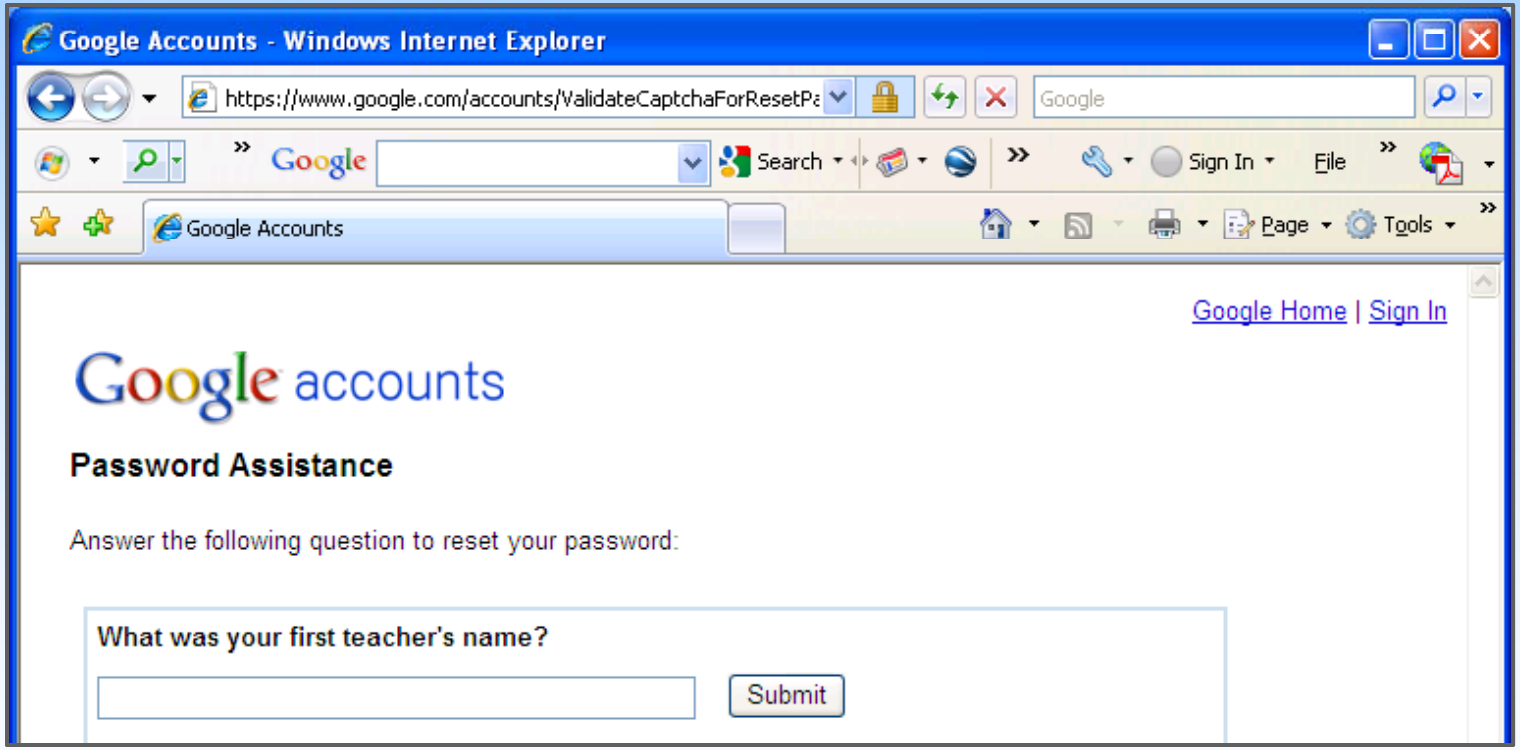
Gateway Data *(noun) – Data that seems harmless but, when used properly, can facilitate access to highly sensitive information.*





Direct Use 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.

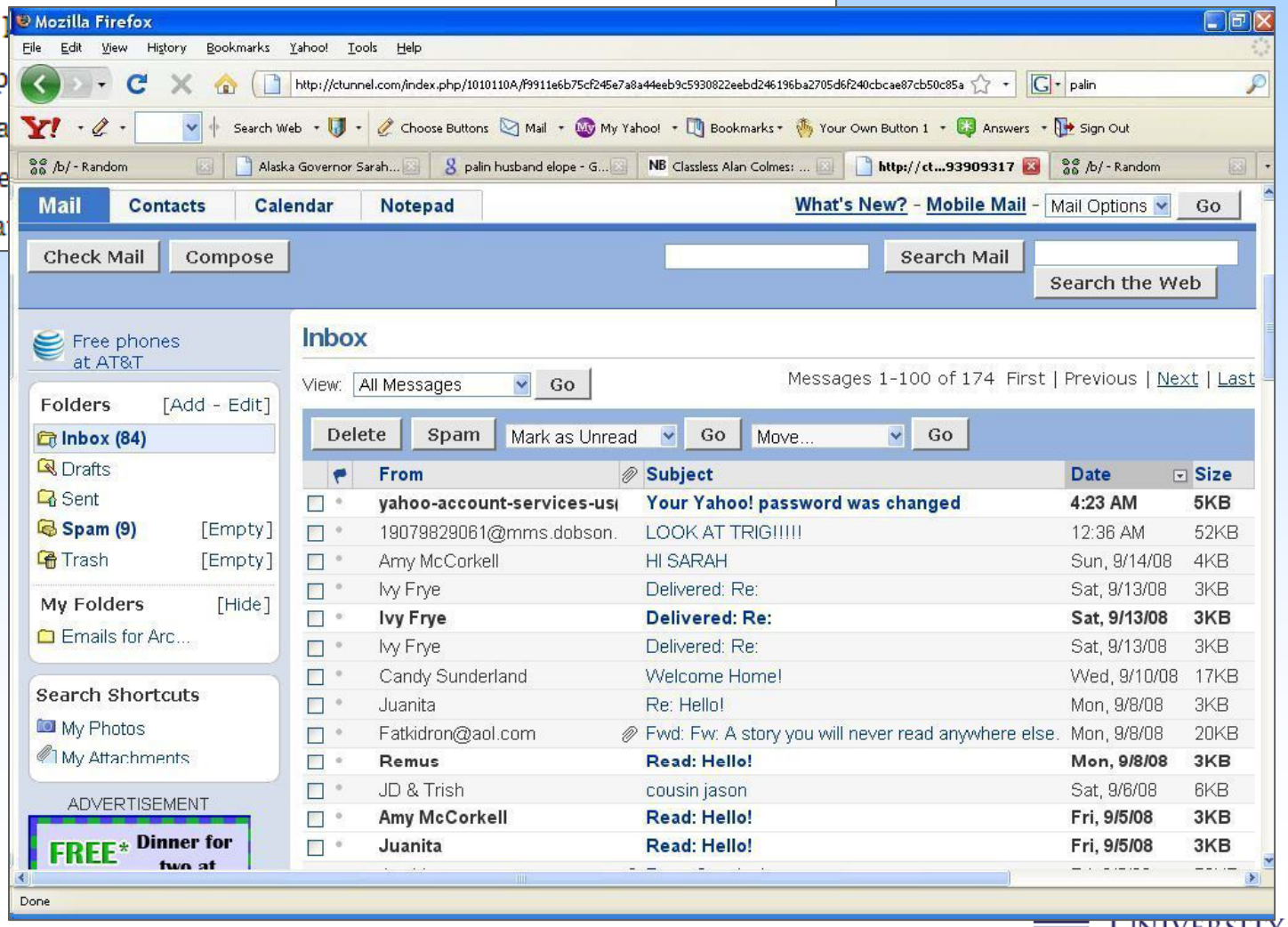
TIME
IN PARTNERSHIP WITH CNN

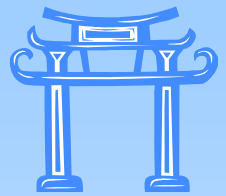
Wednesday, Sep. 17, 2008

Sarah Palin's E-Mail Hacked

By M.J. Stephey

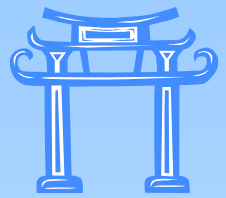
The cryptic Internet posse l
target in Republican vice-p
members of Anonymous, a
4Chan, apparently breache
(gov.palin@yahoo.com) la





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

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

[redacted]: 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 Twitterrific

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.

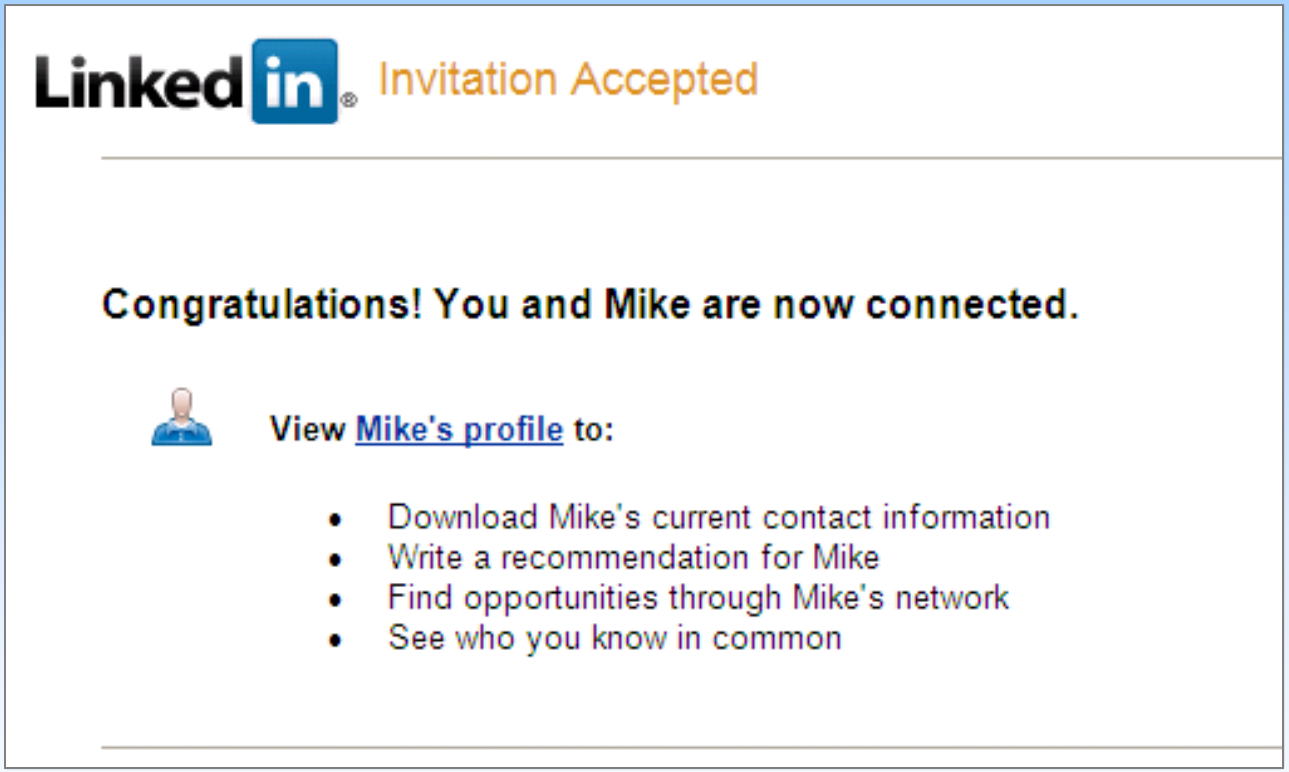
7:39 PM Aug 20th from TinyTwitter

Holiday Ro-o-o-o-o-o-o-o-o-o-oad, Holiday Ro-o-o-o-o-o-o-oad! in Bentonville, AR http://loopt.us/[redacted]

2:43 PM Apr 1st from Loopt

LinkedIn Recommendations

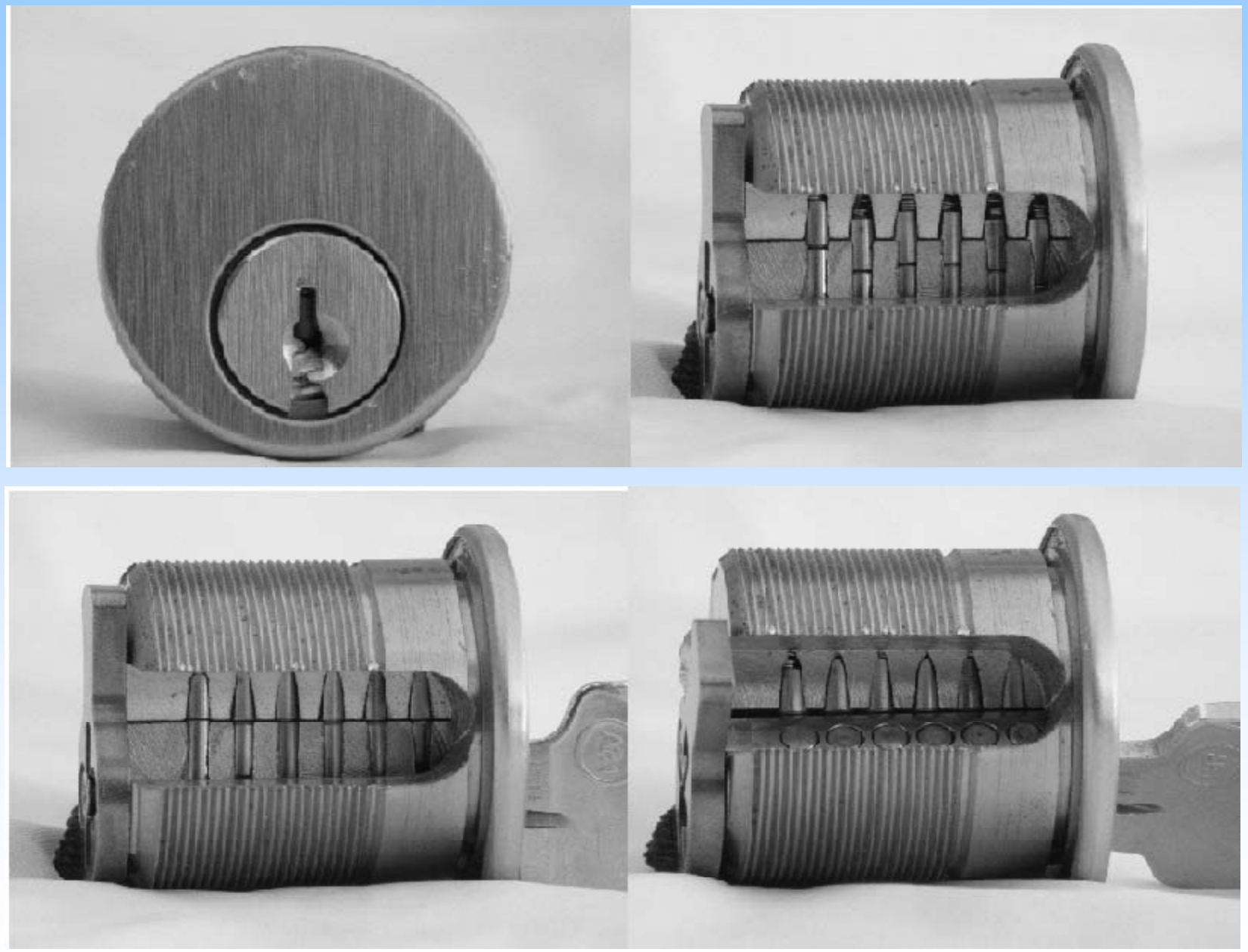
John Smith is requesting an endorsement for work



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.



Photos courtesy of Matt Blaze

Class Break: “Bump Key”

BUG OF ZEN