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
Software Security in an Evolving Environment
**Gateway Data** (noun) – Data that seems harmless but, when used properly, can facilitate access to highly sensitive information.
Collective 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

© Hugh Thompson 2009
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?
Google accounts

Password Assistance

Answer the following question to reset your password:

What was your first teacher's name?

Submit
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.
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 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
Sarah Palin's E-Mail Hacked

By M.J. Stephey

The cryptic Internet posses is the latest target in Republican vice-presidential nominee's campaign. Members of Anonymous, a group of hackers, apparently breached Sarah Palin's email account (gov.palin@yahoo.com) last month.
Amplification Gateway Data: data that can be amplified when bounced off a person.
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:
<table>
<thead>
<tr>
<th>Credit Card</th>
<th>First 4 Digits</th>
<th>Total Digits</th>
</tr>
</thead>
<tbody>
<tr>
<td>American Express</td>
<td>34xx or 37xx</td>
<td>15</td>
</tr>
<tr>
<td>VISA</td>
<td>4xxx</td>
<td>13 or 16</td>
</tr>
<tr>
<td>MasterCard</td>
<td>51xx-55xx</td>
<td>16</td>
</tr>
<tr>
<td>Discover</td>
<td>6011</td>
<td>16</td>
</tr>
</tbody>
</table>
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 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-o-oad, Holiday Ro-o-o-o-o-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
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