

Hackernomics

Herbert H. Thompson, Ph.D.
Chief Security Strategist
People Security

The Shifting IT Environment

(...or why security is becoming one of the most important issues in software development)

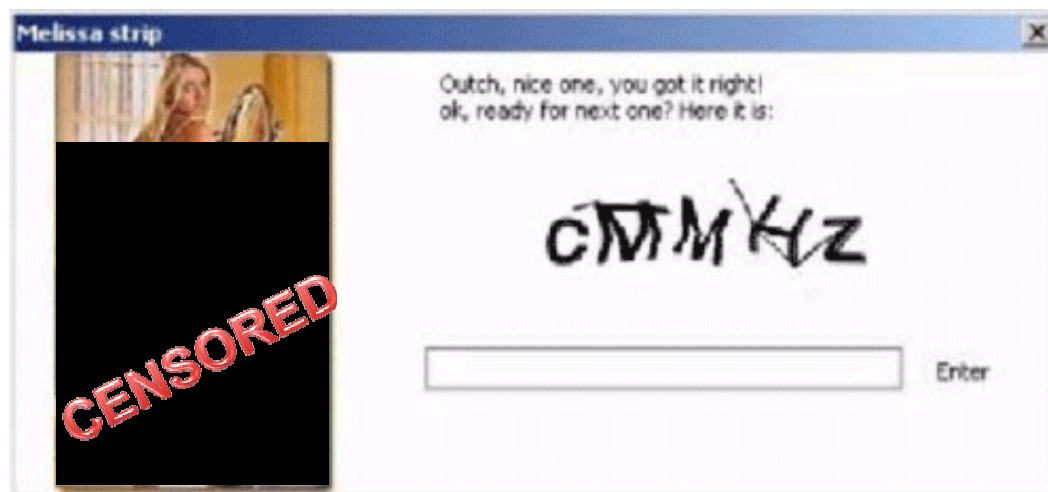
Shift: Technology

- **Software communications is fundamentally changing – many transaction occur over the web:**
 - Service Oriented Architecture (SOA), AJAX, ...
- **Network defenses are covering a shrinking portion of the attack surface**
- **Legacy code is being exposed widely**
- **The security model has changed from good guys vs. bad guys to enabling partial trust**
 - There are more “levels” of access: Extranets, partner access, customer access, identity management, ...
- **Social networking gives attackers access to much more personal and product information**

Shift: Attackers

- **Attackers are becoming organized and profit-driven**
- **An entire underground economy has been created:**
 - Meeting place for buyers and sellers (chat rooms, auction sites, etc.)
 - What they are trading: vulnerabilities, botnet time, credit card numbers, PII, ...
 - New ways to exchange of “value” anonymously and in non-sovereign currency

Example: The CAPTCHA Dilemma



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

Automated Exploitation



TROJ_CAPTCHAR.A disguises itself as a strip-tease game enticing the user to input correctly a given CAPTCHA code



Trojan sends the correct codes to a remote server



Remote malicious user acquires and matches the correct code for a given CAPTCHA on a Web site (ex. Yahoo!)

Shift: Compliance and Consequences

- **The business has to adhere to regulations, guidelines, standards,...**
 - SOX and SAS 112 – have upped the ante on financial audits (and supporting IT systems)
 - PCI DSS – Requirements on companies that process payment cards
 - HIPAA, GLBA, BASEL II, ..., many more
- **Audits are changing the economics of risk and create an “impending event”**

Hackers may attack you but auditors will show up
- **Disclosure laws mean that the consequences of failure have increased**
 - Waves of disclosure legislation

Shift: Customer expectations

- Customers , especially businesses, are starting to use security as a discriminator
- In many ways security has become a non-negotiable expectation of business software
- Banks, photocopiers, pens, etc. are being sold based on security...
- Security starting to be woven into service level agreements (SLAs)

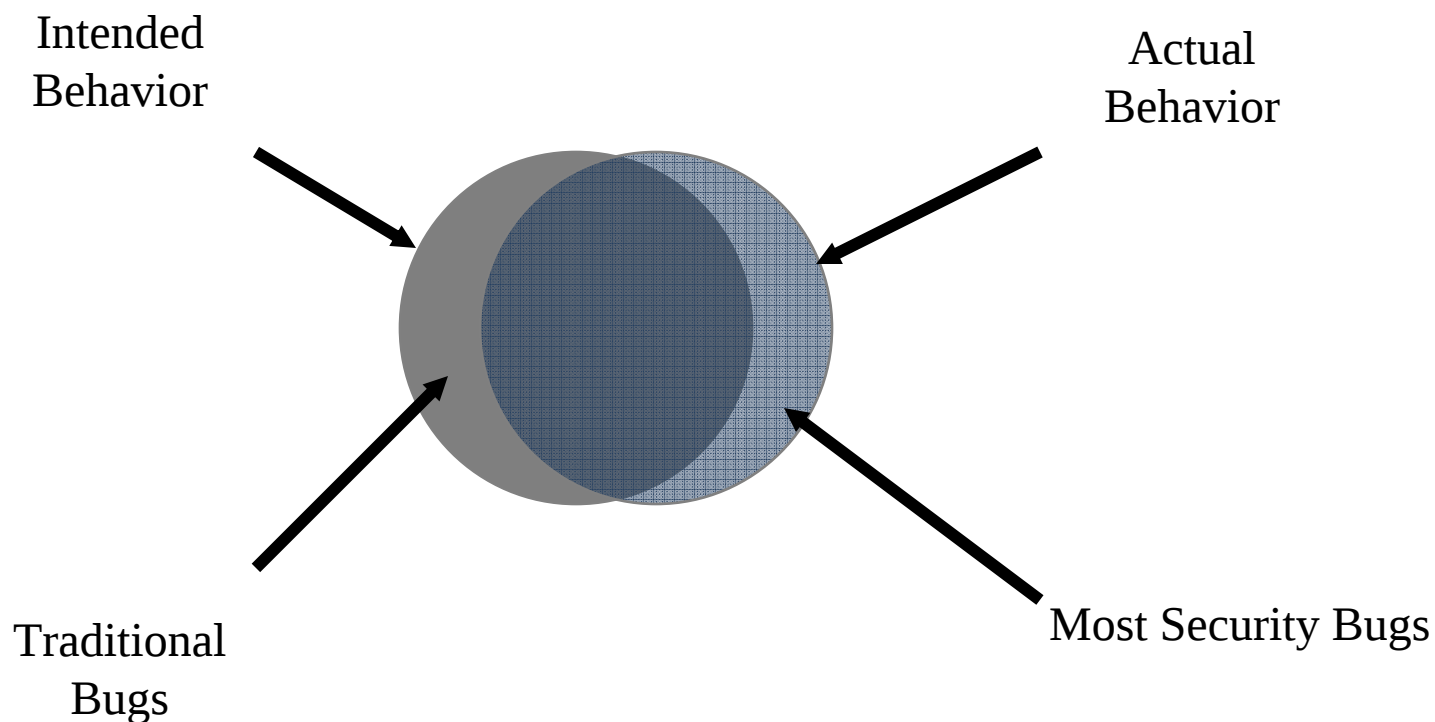
Hackernomics (*noun*)

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

Why *security* bugs are different*



© People Security 2008

* Source: *How to Break Software Security* by J. Whittaker and H. Thompson. Addison Wesley, 2003.

Law 1

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

Corollary 1.a.:

We 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 1: Implications

- Need to value corporate assets smarter (i.e. what are they worth to an attacker?)
- Need to adopt risk management approaches that identify high-value targets and then do threat modeling to determine how those targets can be reached
- Need to make sure that systems are strong and *appear strong* when viewed by an attacker.

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 2: Implications

- Need to value customer data beyond what is currently legally protected
- Need to plan for changes in privacy requirements and legislation that address stored data like “pet’s name”
- Need to plan for new requirements on data disposal

Law 3

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

Law 3: Implications

- **Decisions (including budget allocation decisions) need to be made based on comprehensive risk assessments as opposed to recent incidents**
- **Be open to new technologies and methods but carefully map their benefit to your risks**

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 4: Implications

- Need to ingrain security awareness into the culture
- Need to also assume that people will continue to make poor security decisions and make it easier to make correct ones by baking it into system design

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.

Law 5: Implications

- Need to reverse engineer the assumptions that went into building legacy systems and ensure that they still hold in the current climate
- Need to do “low hanging fruit” risk analysis in addition to looking through the weeds
- Need to spend more time investigating procedures than technology

Summary

- **Software security is about ensuring that security code/features are present and implemented properly and that functional features are implemented securely**
- **Embrace the attacker and think like him/her to succeed – become a hackernomist**

Questions?

Presented by:

Herbert H. Thompson, Ph.D.

Chief Security Strategist

People Security

11 Penn Plaza, 5th Floor
New York, New York 10001

Cell: +1.321.795.4531

www.peoplesecurity.com

hthompson@peoplesecurity.com

People Security is the leading provider of enterprise software security education. To find out about our courses on software security, security testing, secure requirements and more visit:

www.peoplesecurity.com