Hackernomics

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

Hacking a soda machine…

Bahamas 10¢

US 25¢

23.5mm	**Size**	24.26mm
5.7 g	**Weight**	5.67 g
	Composition	
	Value	

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 guys vs. bad guys to enabling partial trust
  - There are more “levels” of access: Extranets, partner access, customer access, identity

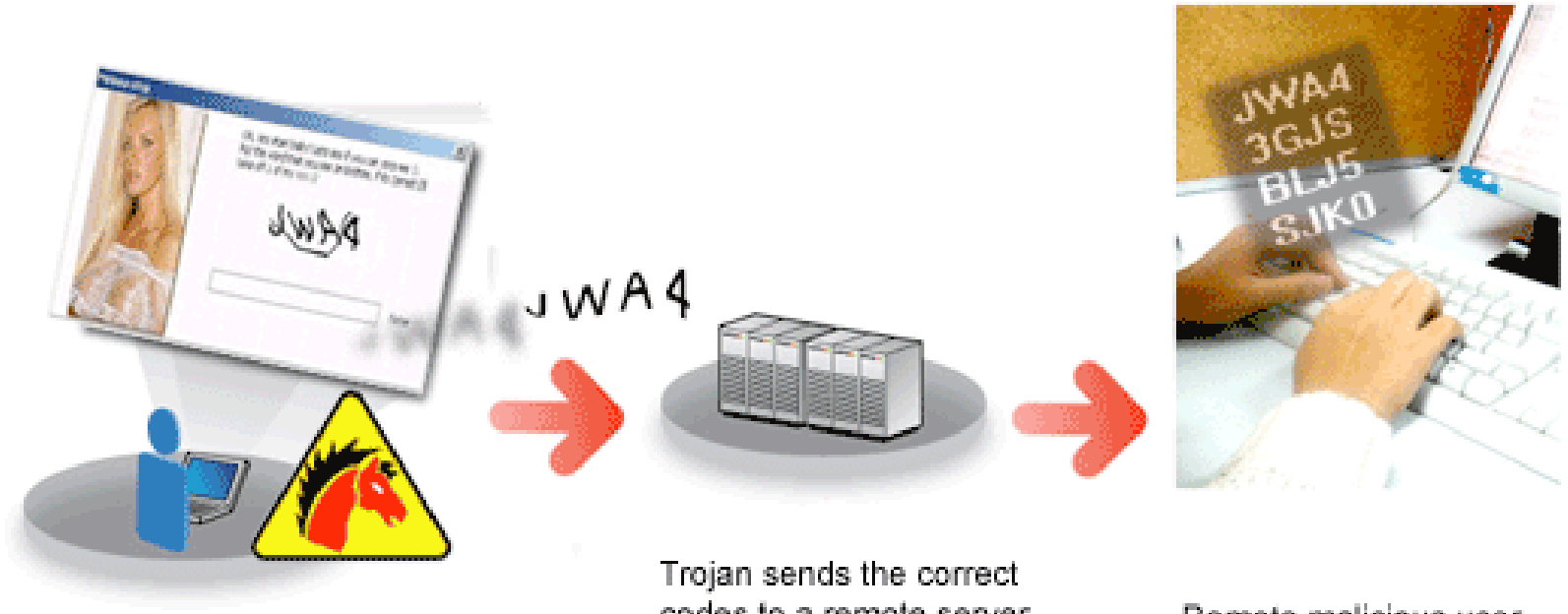
Shift: Attackers

- 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

Example: The CAPTCHA Dilemma

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!*)

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

Shift: Compliance and Consequences

- The business has to adhere to regulations, guidelines, standards,…
  - SOX and SAS 112 – has upped the ante on financial audits (and supporting IT systems) for not-for-profit organizations and for publicly traded companies
  - 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

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

Law 1

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

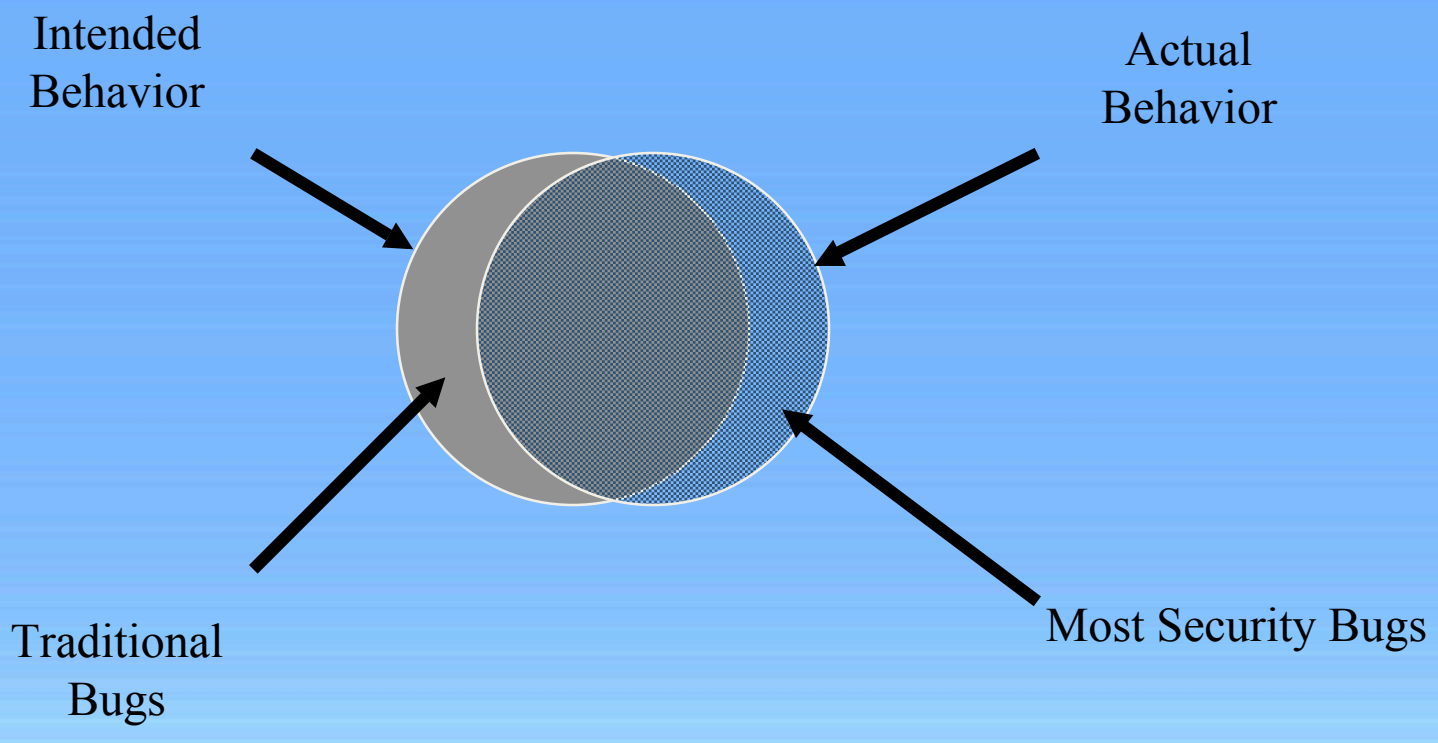
Corollary 1.a.:

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

Why *security* bugs are different*



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 (developers, users, 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**

Corollary 4.b:

Developers are smart people that want to do the right thing. Incomplete requirements, undocumented assumptions, lack of security knowledge, and bad metrics can push them to do the wrong thing.

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.

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
- Software security is everyone's responsibility in the software development life cycle

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