What is the key to successful Application Security?

Chris Peterson
Senior Director of Application Security
Zynga, Inc.

Introduction

- Chris Peterson

zynga

security

Key to our success

- The key to AppSec is Developers!
- What Developers Hate
  - Entire days spent chasing bugs
  - Short deadlines
  - Constantly having skillsets superseded by new technology
  - No appreciation for the work it takes outside other developers
  - The elitist nature of many in the developer community
  - Moronic clients
  - Late nights, long hours in front of a computer screen
  - The constant inkling that some 14 year old Japanese kid already did this better than you
  - The lottery-esque likelihood of independent success
  - Silly checklists, policies and procedures they are required to follow
- What Developers Love
  - **Solving hard problems and writing good code**

zynga®
security

Challenging Engineering Problem

- Application Security is one of the most challenging engineering problems a developer will encounter
  - Active adversary
  - Complexity of modern code lends itself to exploitable errors
  - Many difficult security problems are fundamental design issues that are difficult to identify and difficult to fix
- Developers often discount security as a challenge
  - Lack of adversarial mind-set
  - Humans are generally bad at risk analysis
  - Security is seen as a “trivial” issue

Results in a number of misconceptions regarding security.

Consequently, not perceived as an interesting engineering challenge.

How to build "grass roots" awareness

- Training is key to dispel the common "myths"
  - Myth 1: Vulnerabilities are difficult to find
    - Hands-on training with real-world vulnerability detection techniques, including bot-based scans
  - Myth 2: Vulnerabilities are difficult to exploit
    - Hands-on training with real-world exploit tools
  - Myth 3: "Hacking" is just a hobby of bored kids
    - In-depth threat education, clearly showing the economics and prevalence of attacks
  - Myth 4: Vulnerabilities are just simple code bugs and are uncommon
    - Demonstrate the impact of fundamental design issues and demonstrate how common the issues are within our own code
  - Myth 5: "Encryption", "Firewalls", "Intrusion Detection", etc. protects us from attack
    - Hands-on demonstrations of end-to-end attack scenarios, clearly showing how all of these technologies are irrelevant
  - Myth 6: We just make games, no one will hack a game
    - Real-world examples of e-crime scenarios on our own games and applications

zynga®

security

Outcome

- Obviously a fully featured Application Security program is important
- Developer awareness and more importantly PASSION is essential

- Recommended references:
  - Cenzic's Application Security Mythbusters Series (www.cenzic.com)
  - The "Rugged Code Manifesto" (www.ruggedsoftware.org)
  - Hacking Exposed – Web Applications 3 (www.webhackingexposed.com)

zynga® security

Chris Peterson
Senior Director of Application Security

cpeterson@zynga.com
@ZyngaAppSec