Attack Trends 2011
-or-
why software security?

Gary McGraw, Ph.D.
Chief Technology Officer, Cigital
Cigital

- Founded in 1992 to provide software security and software quality professional services
- Recognized experts in software security and software quality
  - Widely published in books, white papers, and articles
  - Industry thought leaders
Pop quiz

- What do wireless devices, cell phones, PDAs, browsers, operating systems, servers, routers, personal computers, public key infrastructure systems, and firewalls have in common?

badness-ometer
Defending castles is passé

Today’s computer and network security mechanisms are like the walls, moats, and drawbridges of medieval times. At one point, effective for defending against isolated attacks, mounted on horseback. Unfortunately, today’s attackers have access to airplanes and laser-guided bombs!
Attaining software security gets harder

The Trinity of Trouble

- **Connectivity**
  - The Internet is everywhere and most software is on it

- **Complexity**
  - Networked, distributed, mobile code is hard

- **Extensibility**
  - Systems evolve in unexpected ways and are changed on the fly
Security and social networking

- Social networking technology
  - Twitter
  - Facebook
  - Myspace
  - AIM
  - Wave/buzz
  - Orkut
  - Tumblr

- Risk tradeoffs are very interesting and often counter-intuitive
  - Spearfishing anyone?

- All 20-somethings expect this stuff---at work!
  - is hacking around controls a "gateway drug"?
  - is there a line between purely social interaction and professional interaction?
  - is there a parallel to the history of phones in the workplace?
  - how about e-mail?
Mobile security

- Think the Internet Is big?
  - There are approximately 1,000,000,000 people on the internet
  - There are approximately 3,000,000,000 mobile handsets in use
- What sort of attack surface, computational power, and force multiplication do cell phones and their apps have?
Mobile risks

- Internet connectivity
- Data convergence
  - Contacts, SMS, Pictures, Location… VPN keys?!
- Location based services
  - A mobile device is a rich target for snoops
  - Attackers know where you are
- Theft or loss
  - How does a user revoke their own phone/pad? Who do they call? HOW do they call them?
Example: Phishing at the app store

- Many publishers have sent in applications purporting to be for mobile banking
- These applications simply prompt for usernames, passwords, PINs, or account numbers...
- This means the user is at the mercy of the application store’s (lame) search function!
Cyberwar rears its head

- Using computer security attacks as weapons of war
  - Reality
    - 1982 pipeline attack
    - 2007 Syrian reactor bombing
    - 2010 Stuxnet
  - Fake
    - Estonia/Georgia DDoS
    - Chinese BGP error
- We all live in glass houses, so building security in is our only recourse
Malware Trends
Modern malicious code

- **Zeus**
  - Banking Trojan toolkit
  - Targets banking info
  - Defeats multi-factor authentication with “attacker in the browser”
  - pdf, and drive by download install using social network G2

- **Persistent web threat**
  - Zeus, Sinowal.CP, MPACK

- **Wrap the browser in a VM**
  - Invincea
Malicious code for the cell phone = not new

- Blue tooth "Blue Snarfling" attack (Nov 2003)
  - Connect and gain access silently w/o pairing
  - Nokia 6310i (firmware 5.50)
  - Sony Ericsson T610 (firmware R1A081)
  - Disrupt a phone call
  - Initiate a voice/data/fax call
  - Hijack a phone call by forwarding speaker and microphone to attacker
  - Read / Write Phonebook entries
  - Read / Write Messages
  - Send SMS to any number
  - Send Fax to any number

- NOKIA Cabir virus (June 2004)
  - Smartphones running on Symbian and Series 60 software
  - Spreads by bluetooth
  - Proof of concept
  - Kills battery
  - PHONE BOTNET?

http://www.thebunker.net/security/bluetooth.htm
Stuxnet

- Very sophisticated, targeted collection of malware
- Delivery
  - 40 days
  - Stolen private keys
  - USB injection
  - Network C&C
- The PAYLOAD matters
  - Inject code into a running control system
  - Siemens SIMATIC PLC (step 7)
- Cyberwar?
  - Natanz in Iran

How to p0wn a Control System with Stuxnet (9/23/10)
The attacker’s toolkit

- The standard attacker’s toolkit has lots of (software analysis) stuff
  - Disassemblers and decompilers
  - Control flow and coverage tools
  - APISPY32
  - Breakpoint setters and monitors
  - Buffer overflow
  - Shell code
  - Rootkits
Attacker’s toolkit: rootkits

- The apex of software exploit...complete control of the machine
- Live in the kernel
  - XP kernel rootkit in Exploiting Software
  - See http://www.rootkit.com
- Hide files and directories by controlling access to process tables
- Provide control and access over the network
- Get into the EEPROM (hardware viruses)
The Future
Online games are a bellwether

- Online games (like World of Warcraft) have up to 900,000 simultaneous users on six continents
  - 10,000,000 people subscribe to WoW
  - 16,000,000+ play MMORPGs
  - Clients and servers are massively distributed
  - Time and state errors are rampant
- MMORPGs push the limits of software technology
- Modern distributed systems in other domains are evolving toward similar models
  - SOA, Web 2.0
- Time and state errors are the XSS of tomorrow
Thread hijacking in online games

- Used in a few WoW botting programs

Loops hundreds of times per second
MAIN THREAD

RenderWorld(..)

HARDWARE BP

super

INJECTED CODE PAGE

uncloak

branch

complete

MAIN THREAD

recloak

restore

CastSpellByID( .. )

ScriptExecute( .. )

ClearTarget( .. )

super
Classic arms race
Software Security
The bugs/flaws continuum

- Customized static rules (Fidelity)
- Commercial SCA tools: Fortify, Ounce Labs, Coverity
- Open source tools: ITS4, RATS, grep()
- Architectural risk analysis
Touchpoints adoption

- Code review
  - Widespread
  - Customized tools
  - Training
- ARA
  - Components help
  - Apprenticeship
  - Training
- Pen testing
  - No longer solo
- Security testing
  - Training
- Abuse cases and security requirements
  - Training
BSIMM: Software Security Measurement

- Real data from (42) real initiatives
- 81 measurements
- 11 over time
- McGraw, Chess, & Migues
Twelve things “everybody” does (well, 66%) 

Core activities
- identify gates
- know PII obligations
- awareness training
- data classification
- identify features
- security standards
- review security features
- static analysis tool
- QA boundary testing
- external pen testers
- good network security
- close ops bugs loop
BSIMM3 as a measuring stick

- Compare a firm with peers using the high water mark view
- Descriptive (not prescriptive)
- Incredible insight for planning
BSIMM2 to BSIMM3

- BSIMM3 released September 2011 under creative commons
  - [http://bsimm.com](http://bsimm.com)
  - Italian and German translations available soon
- BSIMM is a yardstick
  - Use it to see where you stand
  - Use it to figure out what your peers do
- BSIMM3 → BSIMM4
  - BSIMM is growing
  - Target of 50 firms
Where to Learn More
informIT & Justice League

- www.cigital.com/justiceleague
- In-depth thought leadership blog from the Cigital Principals
  - Scott Matsumoto
  - Gary McGraw
  - Sammy Migues
  - John Steven

- www.informIT.com
- No-nonsense monthly security column by Gary McGraw
IEEE Security & Privacy Magazine + Podcast

- Building Security In
- Software Security Best Practices column edited by John Steven
- www.computer.org/security/bsisub/

www.cigital.com/silverbullet
Software Security: the book

- How to DO software security
  - Best practices
  - Tools
  - Knowledge
- Cornerstone of the Addison-Wesley Software Security Series
- www.swsec.com
Cigital’s Software Security Group invents and delivers Software Security

See the Addison-Wesley Software Security series

Send e-mail: gem@cigital.com

“So now, when we face a choice between adding features and resolving security issues, we need to choose security.”
-Bill Gates