



Joe Basirico

Director, Technology & Security Services



Anatomy of an Attack

Learning Testing Techniques to Help Secure Your
Applications Against Hacker Attacks



Introduction

- About Security Innovation
 - Who we are
 - Where we came from
 - Why we're here
- The Anatomy of an Attack
 - How a hacker thinks
 - How you can beat them to it



About Security Innovation

Highly skilled software quality experts

- Specialization in security
- Over 70% of our staff hold advanced degrees in CS; 33% at the Ph.D. level
- Founded by Dr. James A. Whittaker, Dr. Herbert H. Thompson, Jason Taylor, and key FIT “Jedis”
- Managed by CEO Ed Adams and other software industry veterans
- Spun off company (SI Govs) in Jan. '05 that focuses exclusively on classified US Gov't app sec projects



About Security Innovation

Help companies build, assess, and deploy reliable, secure applications

- Security Assessment & Testing
- Security Education & Training
- Research & Consulting
- Tools



About Security Innovation

Methods and tools based on research

- Years of research: *practical* application analysis & decomposition
- Research center complemented by professional internal R&D teams

Integrity: we *never* go public with vulnerabilities



Cost of Application Security Rising ...

THE WALL STREET JOURNAL.

Stores Blame Checkout Software For Security Breach

April 27, 2005 -- The recently revealed security breach at Polo Ralph Lauren Corp. is a case in point. Banking giant HSBC PLC notified the clothier last fall that credit-card data from some of its customers may have been compromised.

A Polo s

COMPUTERWORLD

BJ's Settles Case with FTC over Customer Data

FTC alleges weak security at wholesale club led to fraudulent sales valued in th

JUNE 17, 2005 -- After credit card data for thousands of customers was used to make frau other stores, BJ's Wholesale Club Inc. has agreed

448%



**Increased cost of
unauthorized access
2005 CSI/FBI Security Survey**

Ap Associated Press

Visa, Amex Cut Ties With Card Processor

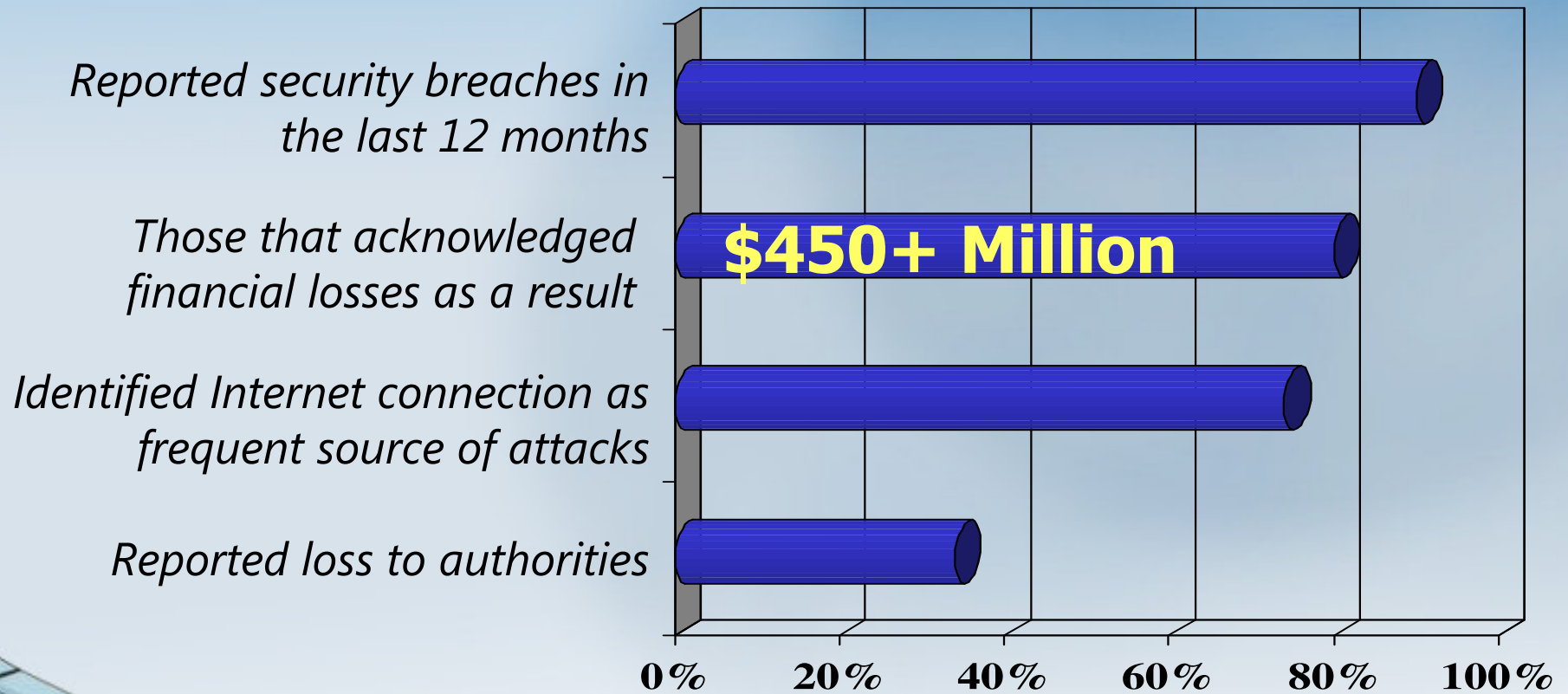
July 19, 2005 -- Visa USA Inc. and American Express Co. are cutting ties with the payment-processing company that left 40 million credit and debit card accounts vulnerable to hackers in one of the biggest breaches of consumer data

SECURITY INNOVATION[®]
THE APPLICATION SECURITY COMPANY



... And Everybody Gets Hit

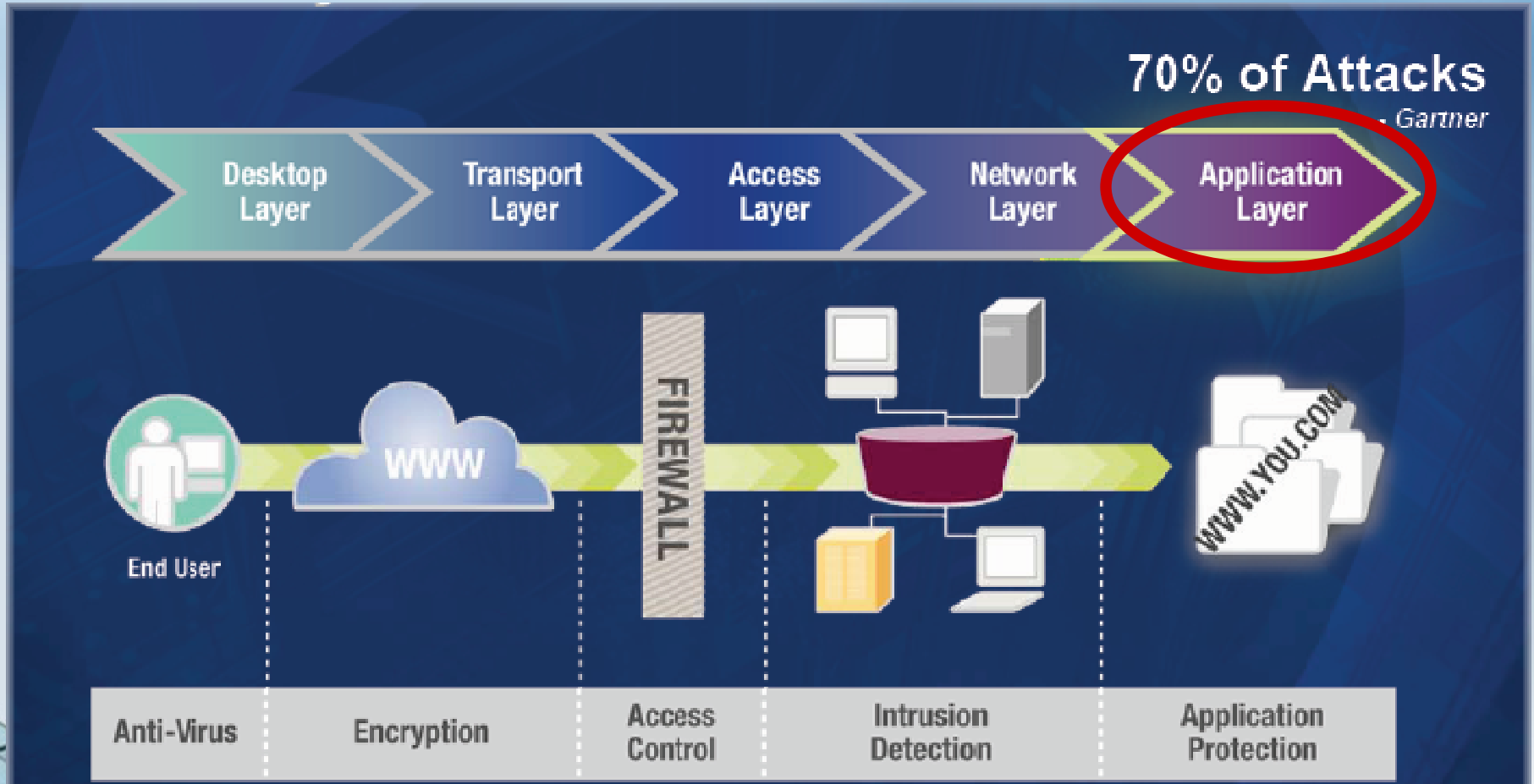
Computer Crime and Security Survey:
Percentages of companies that participated in the survey



SOURCE: FBI/CSI Computer Crime Study, <http://www.gocsi.com>



The Importance of Application Security





Vulnerabilities get expensive quickly

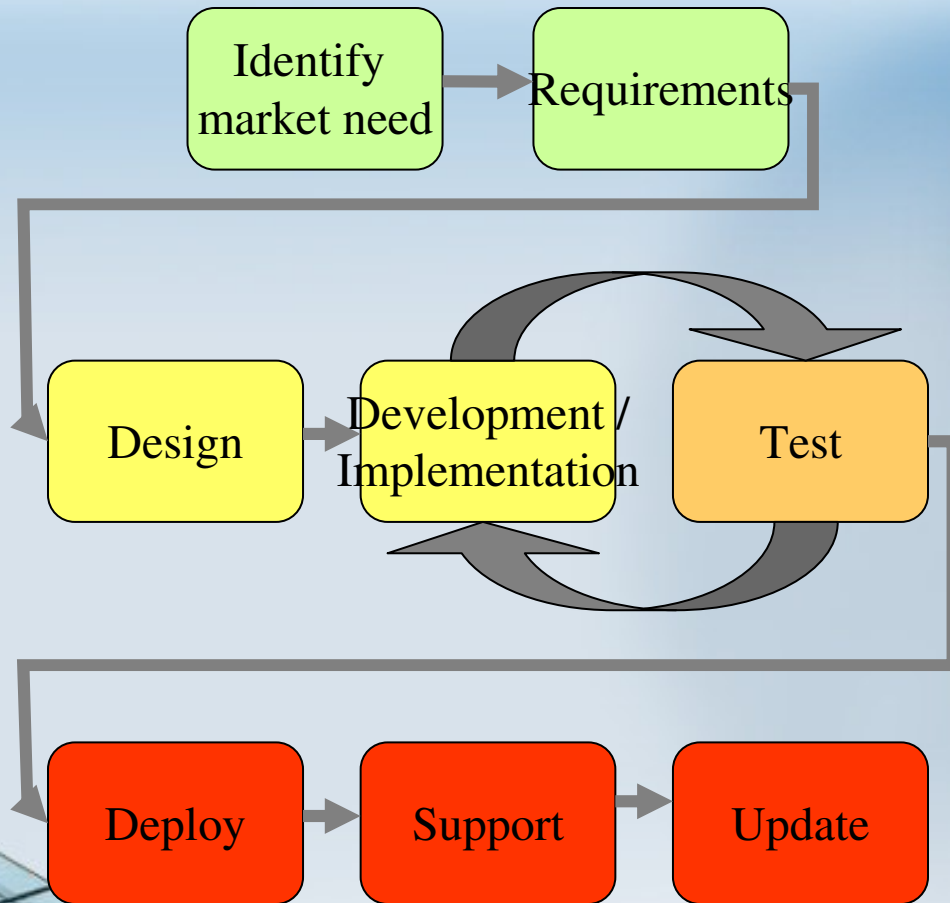
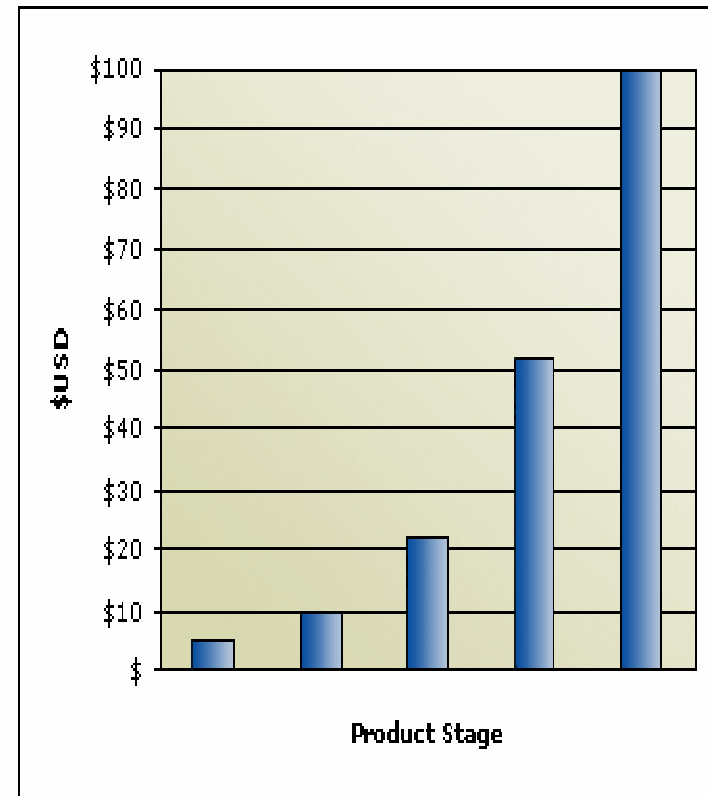


Fig. 1: Cost of Remediation



Source: Boehm et al, COCOMO II, Center for Software Engineering



Overall course objective

- Technology is always evolving and new types of errors will occur
- Learn from mistakes.
- Understand secure design techniques
- Understand/use security tools



Anatomy of an Attack

- Data Gathering
 - Business Information
 - Ping, Port and Service Scanning
 - Manual Discovery of Vulnerabilities
 - Known Vulnerability Scanning
- Exploitation
- Escalate Privileges
- Cover Tracks and Install Tools
- Gather Sensitive Information
- Recovery



What You Will Learn

- Attack/Step overview
- Hacker's motivation
- Testing for this threat
- Tools to use
- Staying safe



Data Gathering

Overview

- Find information about the company or machine
- Business information
- Background information



Data Gathering

Hacker Motivation

Business Information

- Mergers/Acquisitions - careless security configuration, easy entrance into the company
- Hardware purchases - New hardware is difficult to secure, new training.
- Website - Username/Password, other secrets. Configuration information
- Whois - IT contact, Administrative Contact

Ping, Port & Service Scanning

- Ping Sweep
- TCP/UDP/Stealth port scanning
- OS Detection

Known Vulnerability Scanners

- Web Application
- Server Vulnerability Scanners



Data Gathering

Testing for this threat

- Scan your application for sensitive information
- Surf IRC, USEnet for information on your company
- Do research on your own company to know what information is out there
- Routine port & service scans



Data Gathering

Tools to use

- **Wget**
- **Sam Spade**
- **IRC**
- **Whois**
- **Dig**
- **Fping**
- **Nmap**
- **SuperScan**
- **Queso**
- **Nessus**
- **AppScan Audit Edition**
- **Saint5**
- **GFI LANguard**
- **WebInspect**
- **Retina**
- **Scando**



Data Gathering

- Staying Safe
- Do regular scans
- Know what's exposed
- Minimize information passed to the outside
- Stealth all ports
- Learn as much about your company...
....from the outside, as possible



Exploitation

Overview

- Check each door and window for an exploit
- Can range from very easy to very difficult
- Take into consideration
 - Exploitability
 - Damage Potential
 - Difficulty
 - Traceability



Exploitation

Hacker's Motivation

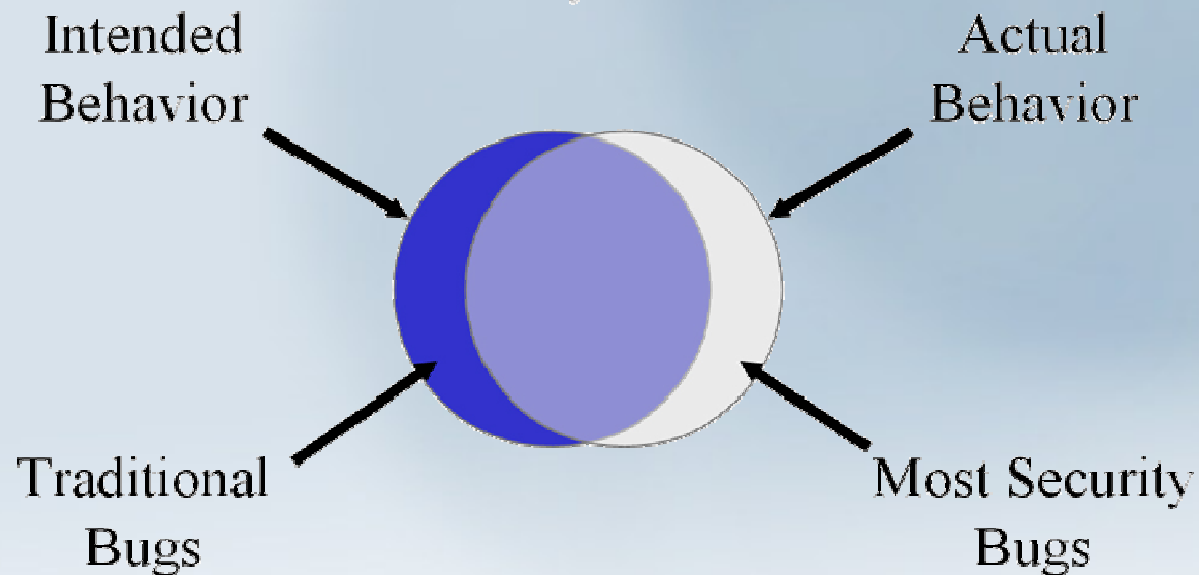
- Exploit Applications
- Proof of Concept (PoC) Code
- Exploit another computer on the network



Exploitation

Testing for this threat

- Check the web for vulnerabilities and exploits
- Application Security Testing!





Exploitation

Tools to use

- BugTraq
- Hacker/Security websites
 - www.securityinnovation.com
 - www.securityfocus.com
 - www.packetstormsecurity.com
- Various PoC Code
- Various Exploit Tools



Exploitation

Staying Safe

- Incorporate Security into the SLDC
- Test for Security Early and Often!
- Don't forget the Developers
- Code Reviews
- Static Analysis Tools
- App Pen Testing



Escalate Privileges

- Sometimes the exploit will only provide the attacker with user level privileges
- Root/Administrator access must be gained to complete the attack
 - Cover Tracks
 - Install Tools
 - Gather Sensitive Information



Escalate Privileges

Hacker's Motivation

- Gain access to all files and resources
- Gather username/password pairs
- Find vulnerabilities in internal apps
- Install password crackers
- Install keystroke loggers



Escalate Privileges

Testing for this threat

- Run a password cracker
- Run a password/packet sniffer
- Test/research your 3rd party apps for exploits
- Know about all trusted relationships



Escalate Privilege

Tools to use

- **John the Ripper**
- **L0phtcrack**
- **Pwddump**
- **Getadmin**
- **Ethereal**
- **Cain/Abel**



Escalate Privilege

Staying Safe

- Keep passwords secure
 - Never embedded in source/executables
- Use strong encryption
- Use strong passwords
- Run Rootkit/keystroke recorder revealers



Cover Tracks and Install Tools

Overview

- Install tools and rootkits to help access the server later
- Backdoors
- Hide/Unhide files tools
- Add Users



Cover Tracks and Install Tools

Hacker's Motivation

- Hide nefarious files
- Remove evidence of an intrusion
- Open (back)doors for future attacks
- Add User
- Install remote control services



Cover Tracks and Install Tools

Testing for this Threat

- RootKit Revealers
- Check Timestamp/checksum/application footprint
- Ensure all assemblies are signed
- Port scan from outside for newly opened ports



Cover Tracks and Install Tools

Tools to Use

- HackerDefender
- RootKit revealer



Cover Tracks and Install Tools

Staying Safe

- Everything before this!
- Run a Rootkit detection program
- Sign assemblies



Gather Sensitive Information

Overview

It's all over...

At this point the Hacker has complete control over the system, and they will discover any sensitive information on the machine



Gather Sensitive Information

Staying Safe

- Encrypt your sensitive information
- Use security best practices
- Keep your data on different machines



Course Summary and Take Aways



Secure Coding

- Security cannot be added by flipping a switch
 - “We used cryptography, it must be secure!”
 - “.NET/Java framework makes our apps secure by default”
- Even with the best technologies in place, creating secure applications requires careful planning, implementation, and thorough testing.
 - Design for security
 - Understand common vulnerabilities
 - Think like an attacker



Design for Security



- Remember the castle!
- Any single security measure can be overcome with enough effort
- Placing security measures at all layers of the product is the best defense.



Understand common vulnerabilities

- **Never** trust user input
 - The most common managed code vulnerabilities come from using unvalidated user input
- Know how to use the technology
 - Cryptography for sensitive data
 - Security libraries
 - Security Tools
- Even the best technology won't help if you don't know how to use it properly.



Next Steps

- Consider the “How to Break Security Software course”
- Stay up to date with security
 - Microsoft security sites
 - <http://www.microsoft.com/security>
 - <http://msdn.microsoft.com/security>
 - External sites
 - <http://www.securityfocus.com>
 - <http://www.windowssecurity.com>
 - <http://www.rootkit.com>
 - <http://www.packetstormsecurity.com>



Free Whitepaper!

See me after the talk, give me a business card and I'll send you a free Whitepaper

Anatomy of an Attack

Author:

Joe Basirico



Thanks for Joining Me!

Joe Basirico

Snail Mail

Security Innovation

701 5th Ave.

Suite 4200

Seattle, WA 98104

E-mail & Web

jbasirico@securityinnovation.com

<http://www.securityinnovation.com>

Cell (206) 227-6458

Work (206) 262-7401

Fax (206) 262-8001

SECURITY INNOVATION[®]

THE APPLICATION SECURITY COMPANY