



# Information Technology Security 2003

Application Security

<http://www.RzWire.com/>

[Info@RzWire.com](mailto:Info@RzWire.com)

---

---

---

---

---

---

---

---



## How Big a Problem Is IT Security?

- ◆ US Corporations lost at least \$59 Billion in 2001 due to IT Security Breaches <sup>1</sup>.
- ◆ 98% of Theft Losses From Financial Institutions are Caused By IT Security Breaches <sup>2</sup>.

<sup>1</sup> American Society for Industrial Security (ASIS), Price Waterhouse Coopers, and the U.S. Chamber of Commerce

<sup>2</sup> Oregon Bankers' Association

---

---

---

---

---

---

---

---



## Who Would Want to Attack You?

The HoneyPot Project found in 2001:

- ◆ On average, every computer on the internet is scanned for weaknesses 14 times per day.
- ◆ On average, every computer on the internet is subjected to a real attack once every 3 days.

---

---

---

---

---

---

---

---



## Why Do People Want to Break In?

- ◆ Wire and Check Fraud
- ◆ Credit Card Fraud
- ◆ Identity Theft
- ◆ Information Brokering
  - Stalking
  - Terrorism and Organized Crime
  - Murder

“FBI gets involved in a major theft (>\$50,000) or in a threat to electronic infrastructure or sensitive research” – FBI

---

---

---

---

---

---

---

---



## Laws and Liability

- ◆ HIPAA
- ◆ FERPA
- ◆ Gramm-Leach-Bliley Act
- ◆ California Senate Bill 1386

---

---

---

---

---

---

---

---



## You and Data Theft

- ◆ Companies like yours are losing billions to data theft
- ◆ Everyone is being attacked
- ◆ Security Breaches are being used to perpetrate horrible crimes including fraud, terrorism, stalking, and murder
- ◆ The local and federal police forces are unlikely to help, unless the loss is extremely high
- ◆ You may be liable if your customer data is stolen

---

---

---

---

---

---

---

---



## IT Security – Defense in Depth

- ◆ Defense in Depth is the practice of creating multiple layers of security
- ◆ If intruders break through one layer, most of your assets are still secure
- ◆ You can detect and respond while the intruders are trying to breach other layers

---

---

---

---

---

---

---

---



## Layers of Security

- ◆ Physical Security
- ◆ Network Perimeter Security
- ◆ Application Security

---

---

---

---

---

---

---

---



## Physical Security

Like Your Building and Your Vault

- ◆ Is your hardware and communications safe and snoop-proof?
- ◆ The best IT security won't protect you from crooks taking your computers and carting them away
- ◆ Laptops, PDA's and some phones are computers

---

---

---

---

---

---

---

---



## Network Perimeter Security

Like Doors, ID Badges, Surveillance Cameras, and Rules of where clients can go

- ◆ Firewalls, Routers, Intrusion Detection Systems
- ◆ There are always places where the general public can go (like your tellers, ATM's, and web sites)

Network Security can't protect you from intruders who look like your customers, and seem to have legitimate business

---

---

---

---

---

---

---

---



## Application Security

Applications are the Interfaces to your clients, like your tellers, ATM machines, phone banking

- ◆ Determined intruders can get by your perimeter defenses and get to your applications
- ◆ Employees are already inside your perimeter

Application Security can prevent the most dangerous attacks long enough for you to detect and respond to the attack

---

---

---

---

---

---

---

---



## Common Application Exploits

- ◆ Password Cracking
- ◆ Authorization Bypass
- ◆ Directory Traversal
- ◆ Unused Services or Features

---

---

---

---

---

---

---

---



## Common Application Exploits

- ◆ Session Hijacking
- ◆ Cross Site Scripting
- ◆ SQL Injection
- ◆ Buffer Overflow

---

---

---

---

---

---

---

---



## Old Techniques to Protect Your Applications

- ◆ Filter all input data
- ◆ Remove all unused services and features
- ◆ Make sure your authentication and authorization is centralized and enforced through every part of your application
- ◆ Make sure that your application, and all components it uses, including the operating system and databases are not vulnerable to buffer overflow attacks
- ◆ Encrypt all personal information, esp. session info

---

---

---

---

---

---

---

---



## New Techniques to Protect Your Applications

### Inline Proxy Type Products

- ◆ Like a Video Teller, the intruder can't get in
- ◆ Only works on known vulnerability types, so won't help against new threat
- ◆ Works like a proxy server, so it can affect performance and service availability and scalability
- ◆ Works inline, so can immediately drop a known threat

---

---

---

---

---

---

---

---



## New Techniques to Protect Your Applications

### AI Style "Sniffer" Type Products

- ◆ Like a Guard, looks for suspicious behavior and reacts
- ◆ Works like a network traffic sniffer, so has minimal impact on network performance and availability
- ◆ Uses inference techniques to identify suspicious behavior, so it can prevent brand new attacks
- ◆ Not inline, so a well executed attack may be able to get through before it is detected
- ◆ New technology - only as good as its inference engine

---

---

---

---

---

---

---

---



## New Techniques to Protect Your Applications

### Blended Products

- ◆ Uses both known signatures, and looks for suspicious behavior
- ◆ Usually built from a base product which is either an inline or sniffer type product – suffers from the weaknesses of the base product
- ◆ Newest type of product, so still working out the kinks

---

---

---

---

---

---

---

---



## Top 10 List to Avoid Data Theft

- 10) Enforce anti-virus software on all your computers, keep it up to date, and filter email for viruses automatically
- 9) Remove all samples, demos, source code and default users from your applications, and try to change the default path and port
- 8) Filter user input on the server for characters, length, tags

---

---

---

---

---

---

---

---



### Top 10 List to Avoid Data Theft

- 7) Encrypt your cookies, or don't put any identifying information in them, or in URL rewriting, and remember hidden fields aren't
- 6) Don't allow your applications to send ad hoc sql to your database
- 5) Encrypt confidential data on your database

---

---

---

---

---

---

---

---



### Top 10 List to Avoid Data Theft

- 4) Be very careful of remote access, and don't let products like PCAnywhere on your network
- 3) Dedicate some IT staff to only security, or use consultants who work only on security
- 2) Create a comprehensive security policy, and make sure it is followed

---

---

---

---

---

---

---

---



### Top 10 List to Avoid Data Theft

- 1) Get regular third party audits, covering both **Network Security** and **Application Security**, from a qualified vendor, and implement the recommendations

---

---

---

---

---

---

---

---



## Razorwire Security

- ◆ Experts with highly focused backgrounds in Network and Application Security
- ◆ Professionals dedicated to improving your real world security

Reducing your Real World Risks

Working Within Your Real World Budget

---

---

---

---

---

---

---

---

---

---



## RippleImpact – Sister Company of Razorwire

- ◆ OO Software Development in Microsoft .NET, Java, J2EE, C++, MS Sql Server, Oracle, DB/2
- ◆ Reputation for Excellence with Senior Software Architects from IBM, Sun, Sprint, NASA, Visa
- ◆ Symitar Consulting - RepGen, SymForm, SymConnect
- ◆ Cookie Encryption Software – transparent to your application
- ◆ Electronic Signing Product for the Mortgage Industry

---

---

---

---

---

---

---

---

---

---



## The Whole Package

- ◆ Razorwire Security and RippleImpact work together to provide an end-to-end solution
- ◆ A Unique Application Security offering, with dedicated experts from both the security and software worlds
- ◆ Secure Software Development
- ◆ Development of Security Applications, such as Transparent Cookie Encryption, and Electronic Signing for the Mortgage Industry

---

---

---

---

---

---

---

---

---

---



<http://www.RzWire.com>

Cost Effective  
Real World  
Security Solutions

S. Ramesh, CEO and Chief Security Architect  
[SRamesh@RzWire.com](mailto:SRamesh@RzWire.com)

**Corporate Office**  
1611 S. Pacific Coast Highway, Ste. 102  
Los Angeles, CA. 90277  
Phone: 310.316.3100

---

---

---

---

---

---

---

---

---

---