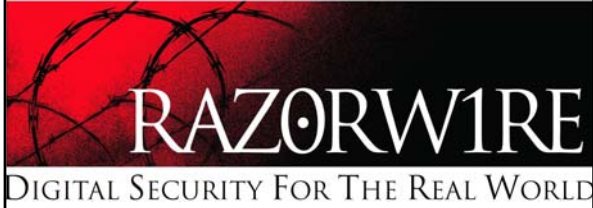


Nebraska Cert 2003



Application Security

Copyright July 2003 All Rights Reserved



Who am I?

S. Ramesh – CEO and Chief Security Architect

- **Sprint's**
 - Integrated On-demand Network (ION);
 - Interfaces Subsystem on Connection Manager (Billing, Traffic Management, Connectivity to All Other Systems)
- **IBM's** Visual Banker - #1 Banking Solution in '90s
- **Goldman Sachs'** Strategic Stream Initiative ; PIASys
- **Chubb Insurance's** Underwriter Workstation
- **ClearStream Bank's** Global Corporate Actions (24/7 Global Securities Trading and Settlement Platform)
- **Standard Chartered Bank, CIBC, Toronto-Dominion Bank's** Branch Sales Platform

<http://www.rzwire.com>
info@rzwire.com
Copyright July 2003 All Rights Reserved



Agenda

- Introduction to Application Security
- Securing Your Custom Applications
- Common Application Exploits
- Classic Ways to Protect Your Application Layer
- New Products to Protect Your Application Layer
- Top 10 List to improve your application security
- Information on Razorwire Security

<http://www.rzwire.com>
info@rzwire.com
Copyright July 2003 All Rights Reserved




How Big Are The Problems In IT Security?

DIGITAL SECURITY FOR THE REAL WORLD

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

¹ American Society for Industrial Security (ASIS), Price Waterhouse Coopers, and the U.S. Chamber of Commerce
² Oregon Bankers' Association

<http://www.rzwire.com>
info@rzwire.com
Copyright July 2003 All Rights Reserved




Who Would Want to Attack You?

DIGITAL SECURITY FOR THE REAL WORLD

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.

<http://www.rzwire.com>
info@rzwire.com
Copyright July 2003 All Rights Reserved




Why Do People Want to Break In?

DIGITAL SECURITY FOR THE REAL WORLD

- 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

<http://www.rzwire.com>
info@rzwire.com
Copyright July 2003 All Rights Reserved




RAZORWIRE
DIGITAL SECURITY FOR THE REAL WORLD

Laws and Liability

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

<http://www.rzwire.com>
info@rzwire.com
Copyright July 2003 All Rights Reserved




RAZORWIRE
DIGITAL SECURITY FOR THE REAL WORLD

You and IT Security

- 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

<http://www.rzwire.com>
info@rzwire.com
Copyright July 2003 All Rights Reserved




RAZORWIRE
DIGITAL SECURITY FOR THE REAL WORLD

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

<http://www.rzwire.com>
info@rzwire.com
Copyright July 2003 All Rights Reserved



Layers of Security

DIGITAL SECURITY FOR THE REAL WORLD

- Physical Security
- Network Perimeter Security
- Application Security

<http://www.rzwire.com>
info@rzwire.com
Copyright July 2003 All Rights Reserved




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

<http://www.rzwire.com>
info@rzwire.com
Copyright July 2003 All Rights Reserved




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

<http://www.rzwire.com>
info@rzwire.com
Copyright July 2003 All Rights Reserved




Firewalls are Not Enough

DIGITAL SECURITY FOR THE REAL WORLD

- Most dangerous attacks are at the application level
 - SANS top ten vulnerability list (Web, SMTP, SQL)
 - Microsoft RPC buffer overflow vulnerability
 - SQL Slammer (MS SQL Server) 1-25-2003
- Firewalls are not enough
 - Firewalls were invented 10 years ago
 - Control where people can go in your systems
 - Not what they do once they get there

<http://www.rzwire.com>
info@rzwire.com
Copyright July 2003 All Rights Reserved



Application Security

DIGITAL SECURITY FOR THE REAL WORLD

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

<http://www.rzwire.com>
info@rzwire.com
Copyright July 2003 All Rights Reserved



Aspects to Application Security

DIGITAL SECURITY FOR THE REAL WORLD

- Ensure that all your custom software is secure
- Ensure your vendors take steps to ensure their applications are secure and conduct and show you the results of 3rd party security audits
- Create additional layers of security to protect you in case a you miss a vulnerability

<http://www.rzwire.com>
info@rzwire.com
Copyright July 2003 All Rights Reserved



Securing your Custom Software – Design

DIGITAL SECURITY FOR THE REAL WORLD

- Architect and Design your application, considering security from the beginning
- Conduct Security Reviews throughout the software development lifecycle
- Create test cases from your software design
- Include security test cases in your test suite

<http://www.rzwire.com>
info@rzwire.com
Copyright July 2003 All Rights Reserved



Securing your Custom Software – Best Practices

DIGITAL SECURITY FOR THE REAL WORLD

- Version Management and Release Management
- Deployment Plans
- Limit developer access to production systems and production data – create test environments and test data
- Backup and Disaster Recovery Plans

<http://www.rzwire.com>
info@rzwire.com
Copyright July 2003 All Rights Reserved



Securing your Custom Software – Databases

DIGITAL SECURITY FOR THE REAL WORLD

- Access control and user lists
- Database level encryption
- Disabling ad hoc access
- Database segmentation

<http://www.rzwire.com>
info@rzwire.com
Copyright July 2003 All Rights Reserved




Securing your Custom Software – Middleware

DIGITAL SECURITY FOR THE REAL WORLD

- Authentication and Authorization Services
- Directory Services (LDAP) and Single Sign-On
- Audit trails
- Transaction monitors

<http://www.rzwire.com>
info@rzwire.com
Copyright July 2003 All Rights Reserved




Securing your Software – Legacy Interfaces

DIGITAL SECURITY FOR THE REAL WORLD

- Legacy applications were built for a different world, when networks weren't interconnected
- Legacy applications require specialized security procedures
- Interfaces to legacy applications should always be considered high risk

<http://www.rzwire.com>
info@rzwire.com
Copyright July 2003 All Rights Reserved




Common Application Exploits

DIGITAL SECURITY FOR THE REAL WORLD

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

<http://www.rzwire.com>
info@rzwire.com
Copyright July 2003 All Rights Reserved




Common Application Exploits

DIGITAL SECURITY FOR THE REAL WORLD

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

<http://www.rzwire.com>
info@rzwire.com
Copyright July 2003 All Rights Reserved




Techniques to Protect Your Application Layer

DIGITAL SECURITY FOR THE REAL WORLD

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

<http://www.rzwire.com>
info@rzwire.com
Copyright July 2003 All Rights Reserved



New Products to Protect Your Application Layer

DIGITAL SECURITY FOR THE REAL WORLD

Inline Proxy Type Products

- Like a Video Teller, the intruder can't get in
- Only works on known vulnerability types (signatures), 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

<http://www.rzwire.com>
info@rzwire.com
Copyright July 2003 All Rights Reserved



**New Products to Protect
Your Application Layer**

DIGITAL SECURITY FOR THE REAL WORLD

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

<http://www.rzwire.com>
info@rzwire.com
Copyright July 2003 All Rights Reserved



**New Products to Protect
Your Application Layer**

DIGITAL SECURITY FOR THE REAL WORLD

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

<http://www.rzwire.com>
info@rzwire.com
Copyright July 2003 All Rights Reserved



**Top 10 List to Avoid IT
Security Breaches**

DIGITAL SECURITY FOR THE REAL WORLD

- 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

<http://www.rzwire.com>
info@rzwire.com
Copyright July 2003 All Rights Reserved



Top 10 List to Avoid IT Security Breaches

DIGITAL SECURITY FOR THE REAL WORLD

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

<http://www.rzwire.com>
info@rzwire.com
Copyright July 2003 All Rights Reserved



Top 10 List to Avoid IT Security Breaches

DIGITAL SECURITY FOR THE REAL WORLD

4) Be very careful of remote access. Products like PCAnywhere and GoToMyPC do not belong on a corporate 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 to follow it

<http://www.rzwire.com>
info@rzwire.com
Copyright July 2003 All Rights Reserved



Top 10 List to Avoid IT Security Breaches

DIGITAL SECURITY FOR THE REAL WORLD

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

<http://www.rzwire.com>
info@rzwire.com
Copyright July 2003 All Rights Reserved



Razorwire Security

DIGITAL SECURITY FOR THE REAL WORLD

- Focused in Network and Application Security
- Recognized Experts in the Industry
- Experienced in Helping Our Clients Secure Their Systems, and Pass Mandatory Audits
- Tailored Services for All Sizes of Clients
- Work With Clients Across the Country
- Offices in Los Angeles and Ottawa, Canada

<http://www.rzwire.com>
info@rzwire.com
Copyright July 2003 All Rights Reserved



Who Are Razorwire's Customers?

DIGITAL SECURITY FOR THE REAL WORLD

- Very Active in the Financial Industry
 - Credit Unions, Banks, Insurance
- Funded Startups
 - Our Parent Company is a Venture Company, so we understand the concerns of startups
- Hospitals and Medical Centers
- Local Governments
- Universities

<http://www.rzwire.com>
info@rzwire.com
Copyright July 2003 All Rights Reserved



RippleImpact Software – Razorwire's Sister Company

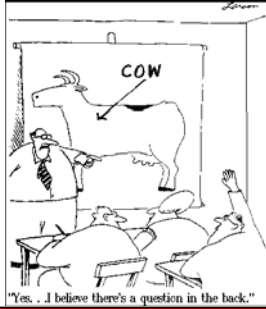
PROVEN TECHNOLOGY SOLUTIONS

- 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
- IBM Premier Partner
- Custom Security Software Development
- Secure Software Design and Development

<http://www.rzwire.com>
info@rzwire.com
Copyright July 2003 All Rights Reserved



Questions?



Razorwire Security

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

Cost Effective
Real World
Security Solutions

Serving Clients Across the Country

Offices in
Los Angeles, California
and Ottawa, Canada

<http://www.rzwire.com>
info@rzwire.com

Copyright July 2003 All Rights Reserved
