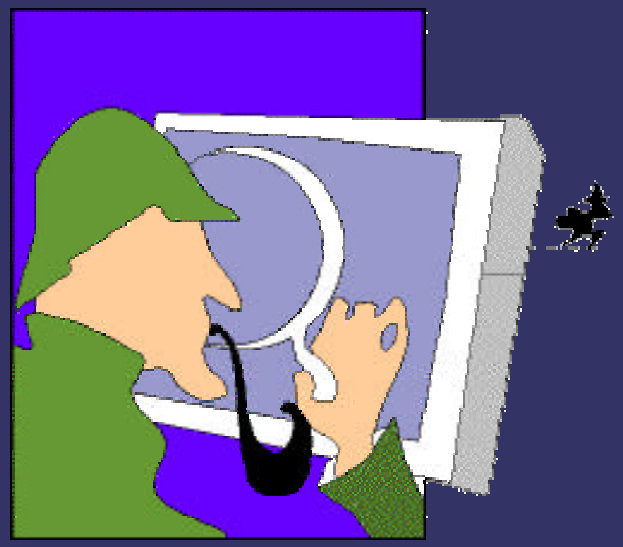


18th Annual Security Applications Conference

"The Big 5 Challenges of Enterprise Network Security"

Rod Murchison
VP Product and Corporate Development
Ingrian Networks Inc.

Thursday, December 12th, 2002

Security Market Analysis

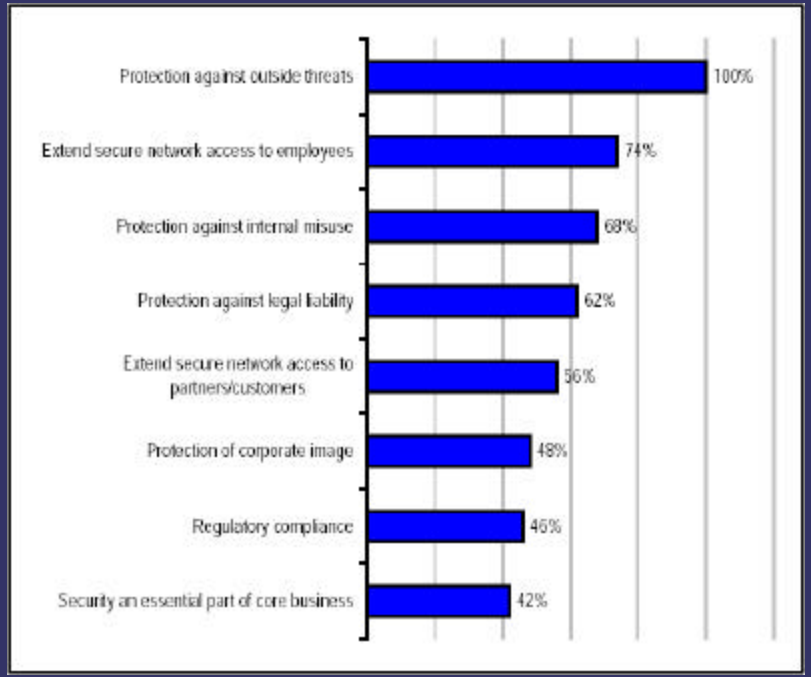
- "Security Software Market"
  - 2002 market size estimate at $9.8 B US [1]
  - Includes software, appliances, some hardware products
  - Expected to grow to $15 B US by 2006 [1]
- Security technology is moving up the stack from network layer to application / data layer
- Increasing concern over malicious activity within the infrastructure rather than the perimeter
- Emergence of a myriad of SSL/TLS-based web applications… and problems deploying them

1 - Source: "Security Software In-Depth Report – Merrill Lynch – Oct. 30th 2002

Security Market Analysis (cont.)

- Merrill Lynch Survey of 50 CIOs
- Showing surprising contradiction… 80% of attacks internal, but key concern is external threats
- Corporate policy changes on internal threats are driving new deployments
- SSL/TLS still one of the fastest growing application data transports

What are the key factors in your decision to purchase security software?



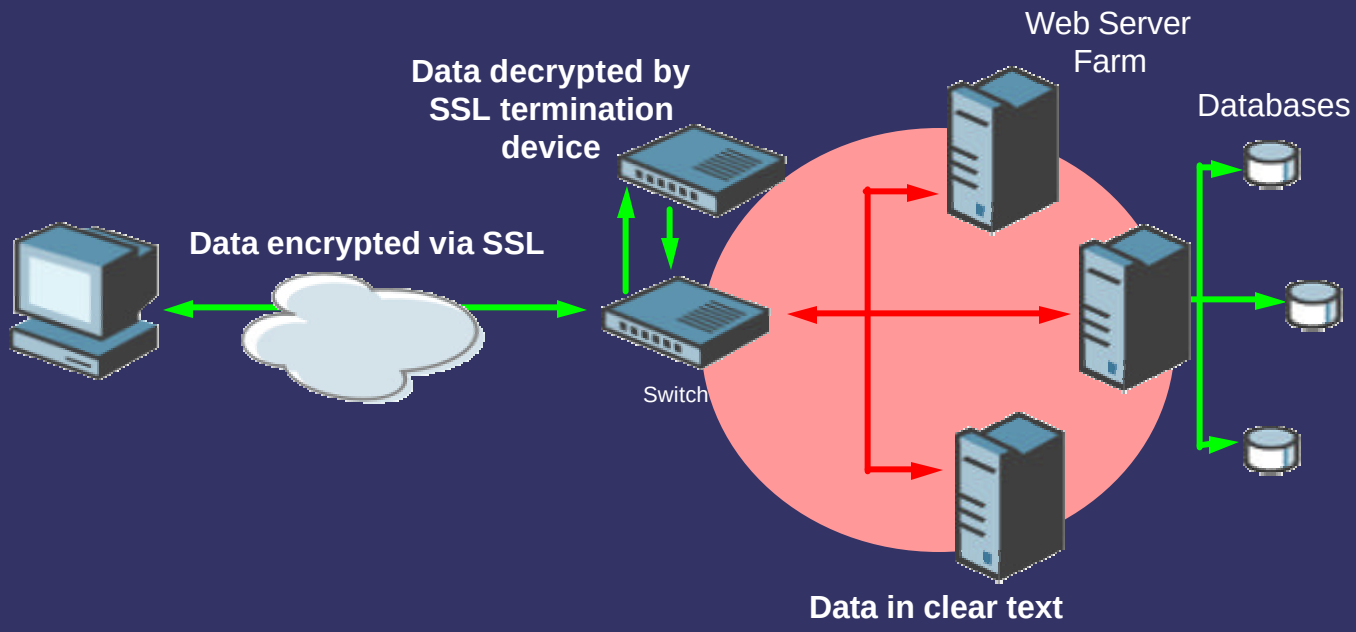
SOURCE: ML Survey of 50 CIOs

The 5 Biggest Threats

- 5 significant threats to network security:

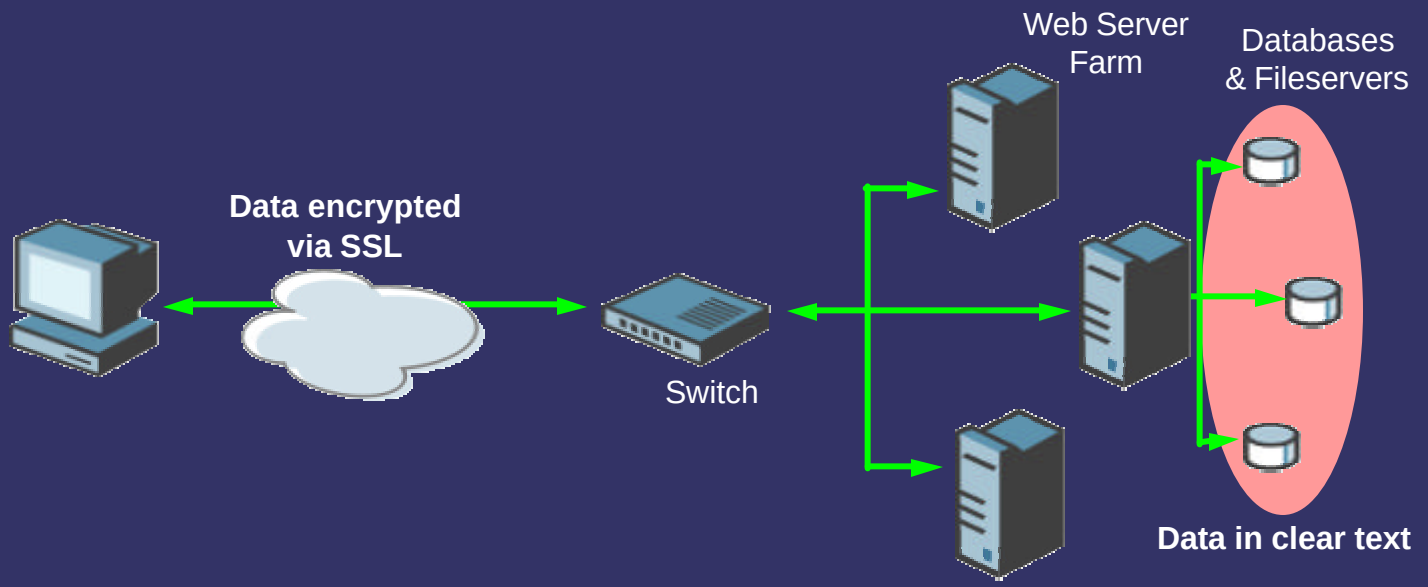
1. Compromise of Unencrypted Data
2. System Intrusion via Application Level Attacks
3. Theft of Private Keys
4. Unauthorized System Access
5. Administrative Errors

Threat 1: Compromise of Unencrypted Data (Transit Vulnerability)



- Encryption stripped off inside network
- Data in clear text – easy to misuse
- Traditional switches, firewalls, intrusion detection products, etc. can't fully process secure data
- Cookie poisoning

Threat 1: Compromise of Unencrypted Data (Storage Vulnerability)



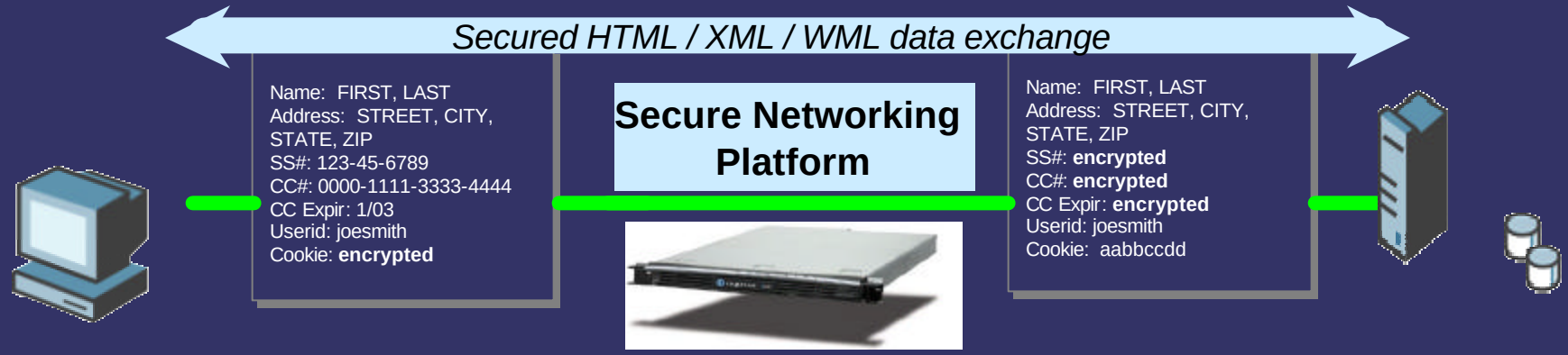
- Data in clear text in database & on fileserver
  - Passwords and cookies
  - Credit card and Social Security numbers
  - Personal data: financial, medical, etc.
  - Corporate data: plans, strategies, price lists, etc.

Data Infrastructure Attacks

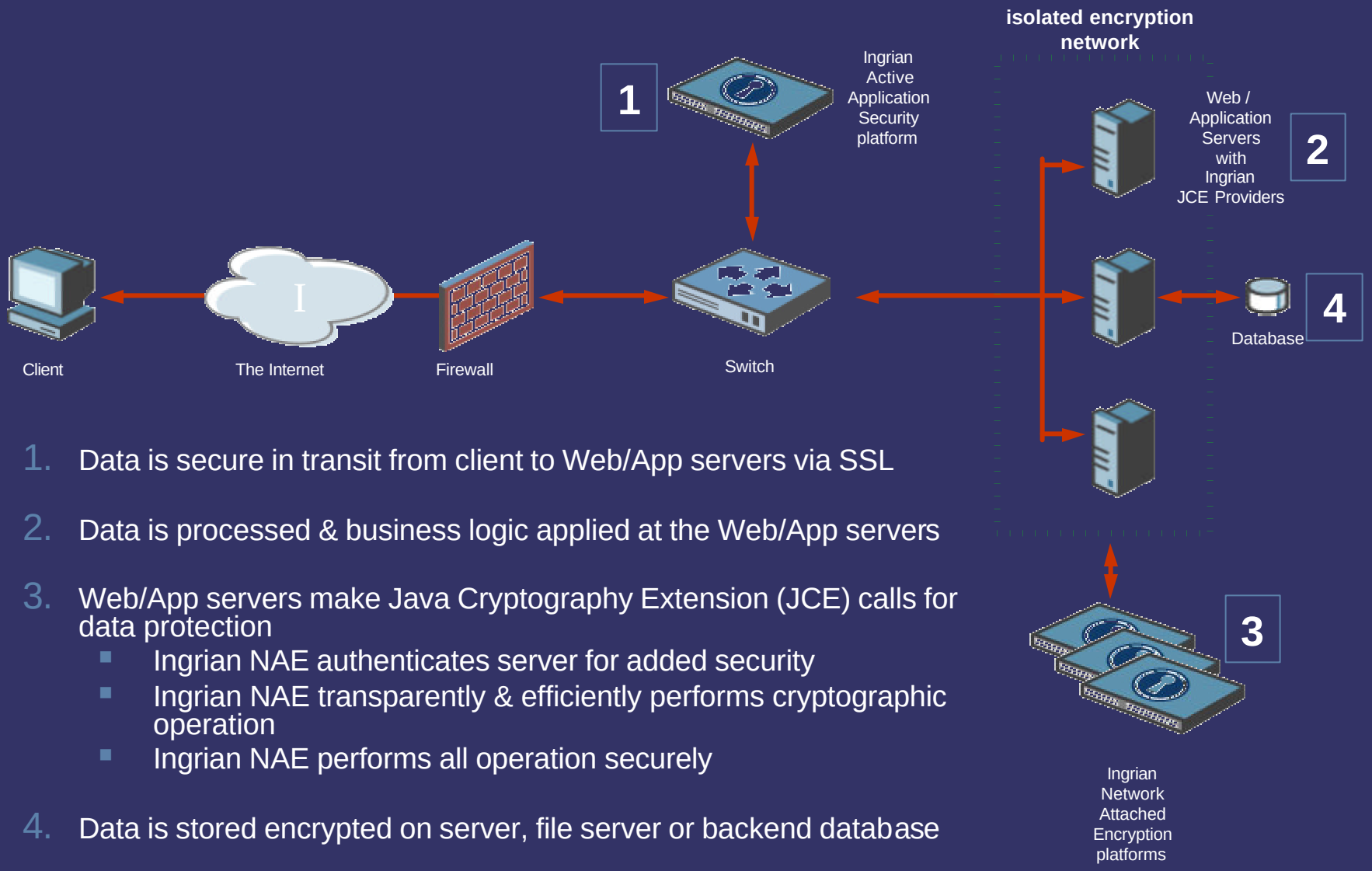
- How is this possible?
  - Latest web and security attacks are designed to get at your core data, and they are working
  - Most breaches are internal, and poor controls are in place for administrative data access
  - Consumers and Administrators believing that SSL = data security
- What can you do
  - Adopt data encryption methods that ensure sensitive data is never used or stored in the clear
  - Employ stringent controls on administrative access to sensitive data
  - Decide how you want to handle data encryption… in the network, at the server, at the database, or at the storage infrastructure

Example 1: Selective Data Encryption in Transit

- Provides on-the-fly HTML/XML/*ML data field encryption for secure storage in back-end databases and Web servers
- Works over HTTP or HTTPS
- Works in “both directions” & enables protection against cookie poisoning
- Sensitive data never exists “in the clear” in back-end databases and Web servers



Example 2 - Network Attached Encryption

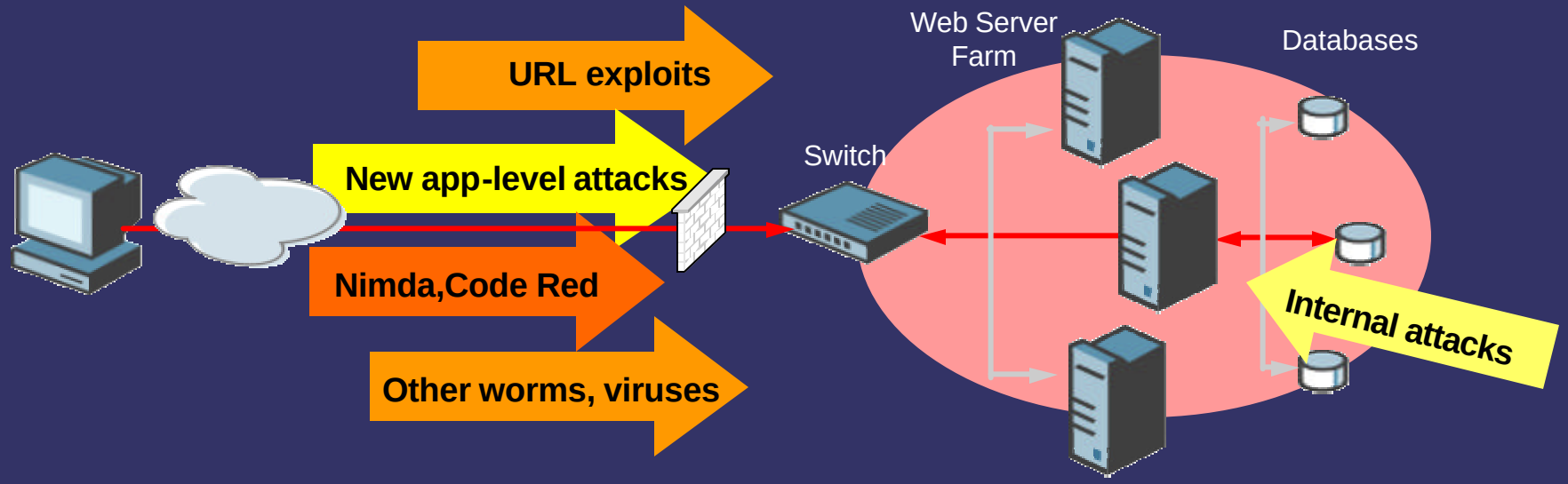


1. Data is secure in transit from client to Web/App servers via SSL
2. Data is processed & business logic applied at the Web/App servers
3. Web/App servers make Java Cryptography Extension (JCE) calls for data protection
   - Ingrian NAE authenticates server for added security
   - Ingrian NAE transparently & efficiently performs cryptographic operation
   - Ingrian NAE performs all operation securely
4. Data is stored encrypted on server, file server or backend database

Advantages Of Network Attached Encryption

Network Attached Encryption		"Per-Server" Based Architecture
❖ Cryptographic keys live on a single, secure platform	vs.	❖ Cryptographic keys reside insecurely on each and every web/app server
❖ Key management (creation, deletion, replication, etc.) performed in one location	vs.	❖ Key management (creation, deletion, replication, etc.) performed laboriously and repetitively on each and every web/app server
❖ Administration and management access is controlled by fine-grained, multi-factor authentication	vs.	❖ Administration and management access is controlled by server-based authentication
❖ Logs, statistics, and crypto information aggregated centrally and stored securely	vs.	❖ Logs, statistics, and crypto information scattered among servers and stored insecurely
❖ Scalability for additional encryption capability is horizontal with one-click replication	vs.	❖ Scalability for additional encryption capability is vertical and labor-intensive

Threat 2: System Intrusions via Application-Level Attacks

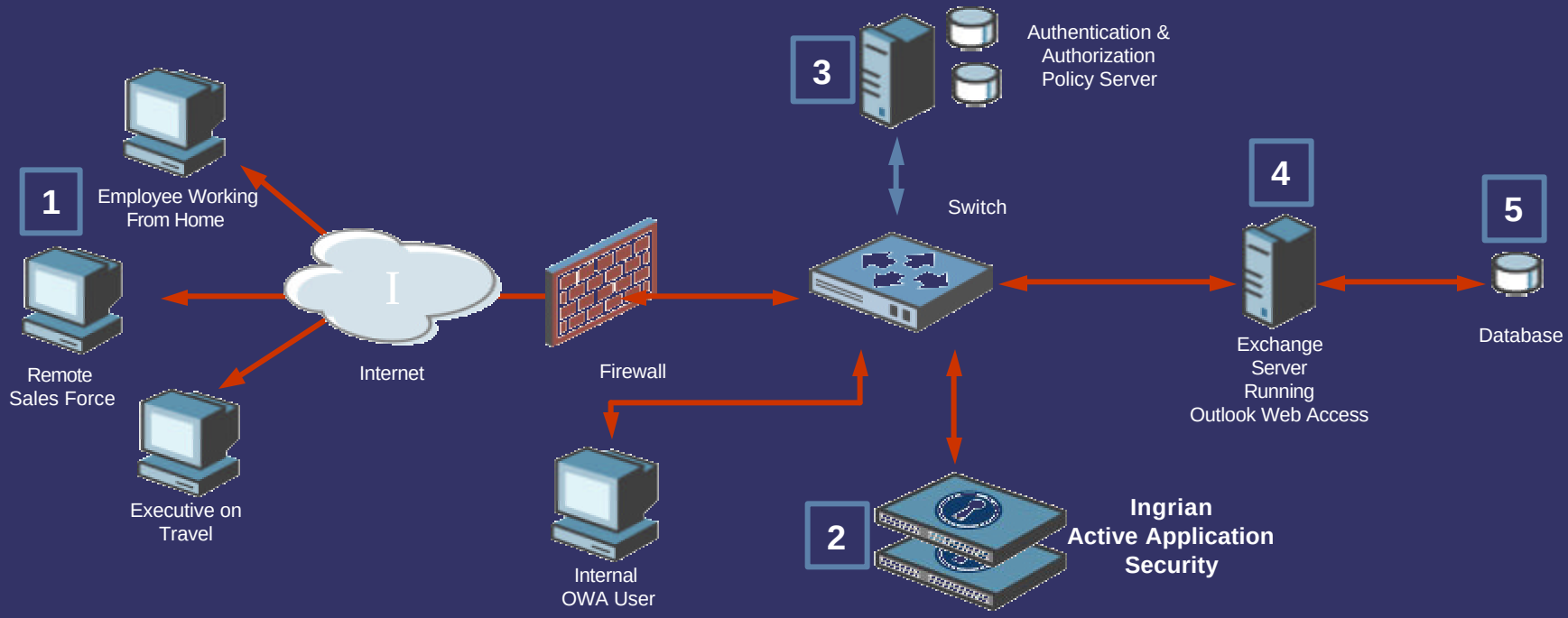


- SSL is a direct tunnel to Web servers
- Firewalls don't stop new threats to Web server-based applications
- Internal and external breaches can access entire network
- Deeper attacks with HTML, XML, SOAP, etc.
- Cookie Poisoning

Web Application Infrastructure Attacks

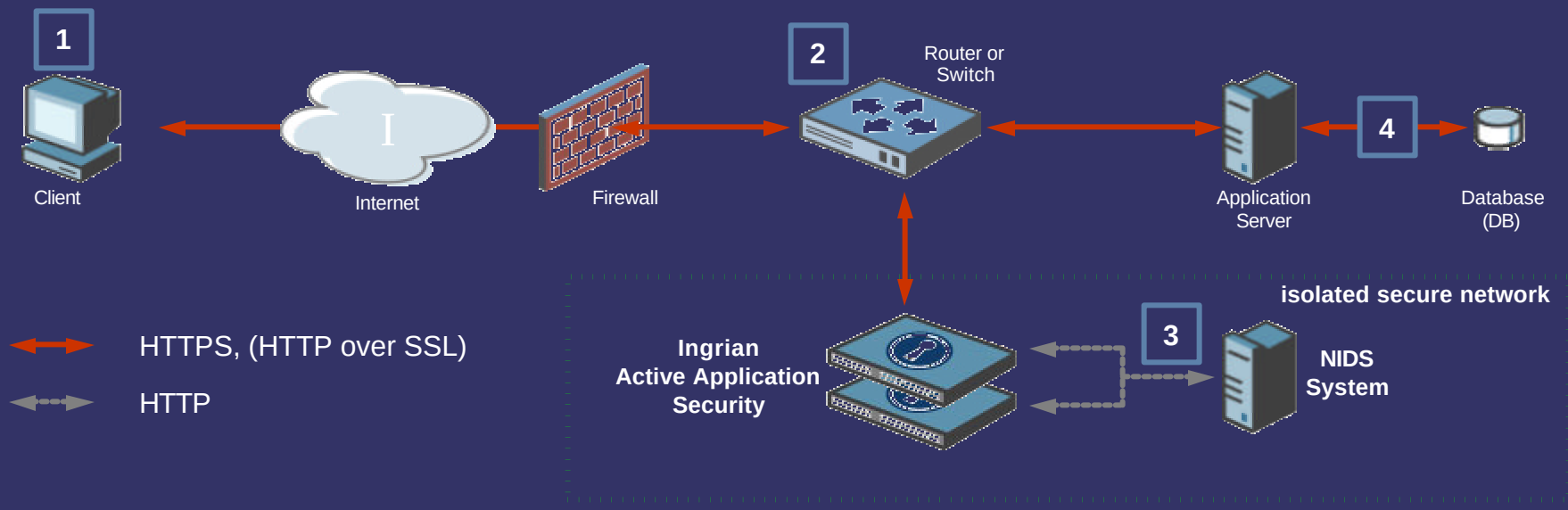
- What is “Code Red” and “Nimda”?
  - Specific attacks that exploit errors in the way URLs are processed on webservers
  - Successful attack opens up your webserver to the possibility of executing code delivered by the hacker
  - Foothold on the webserver can provide the hacker a means to infiltrate backend systems (app servers, databases, etc.)
- What can you do?
  - Ensure that any system that provides web services is fully protected with software / hardware
  - Plan for scalable network performance
  - Prepare for going even deeper in the *ML to find attacks with Intrusion Prevention & Application Protection solutions
  - Don’t forget about SSL…

Example 3 - Microsoft Exchange Outlook Web Access Protection



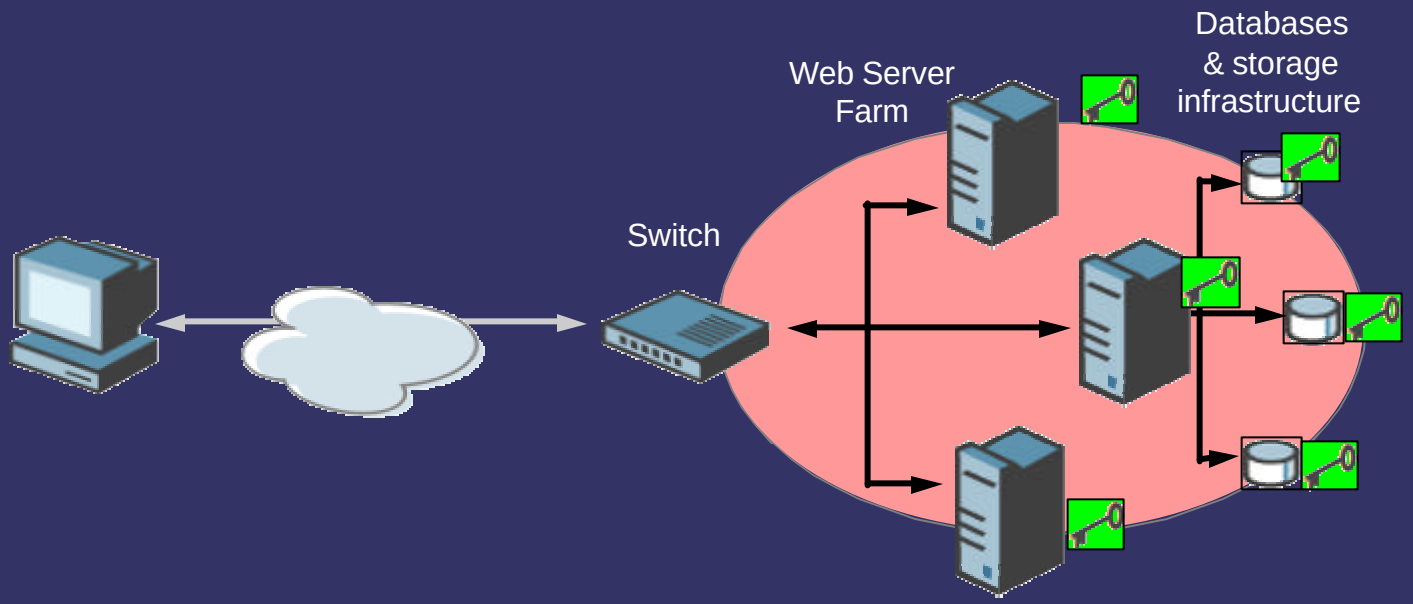
1. Microsoft OWA client launches e-Mail application through the Internet
2. Ingrian Active Application Security platform negotiates secure SSL connection with client
3. Once connection is made, Ingrian Active Application Security platform running Netegrity SiteMinder Service Engine routes connection request to AAA Policy Server for authentication and authorization
4. Once authenticated, client gains access to e-Mail through the Exchange server

Example 4 - IDS Solution for SSL Connections



1. Network traffic originates from the client, traveling through via SSL to the switch.
2. The switch routes the secure traffic to the Ingrian Active Application Security platform to handle the SSL handshake with the client.
3. Data is then routed back to the web/application server over an SSL tunnel **and** mirrored to the IDS system in cleartext on an isolated secure network. Mirroring the traffic allows for end-to-end SSL encryption and IDS application protection to function simultaneously.

Threat 3: Theft of Private Keys

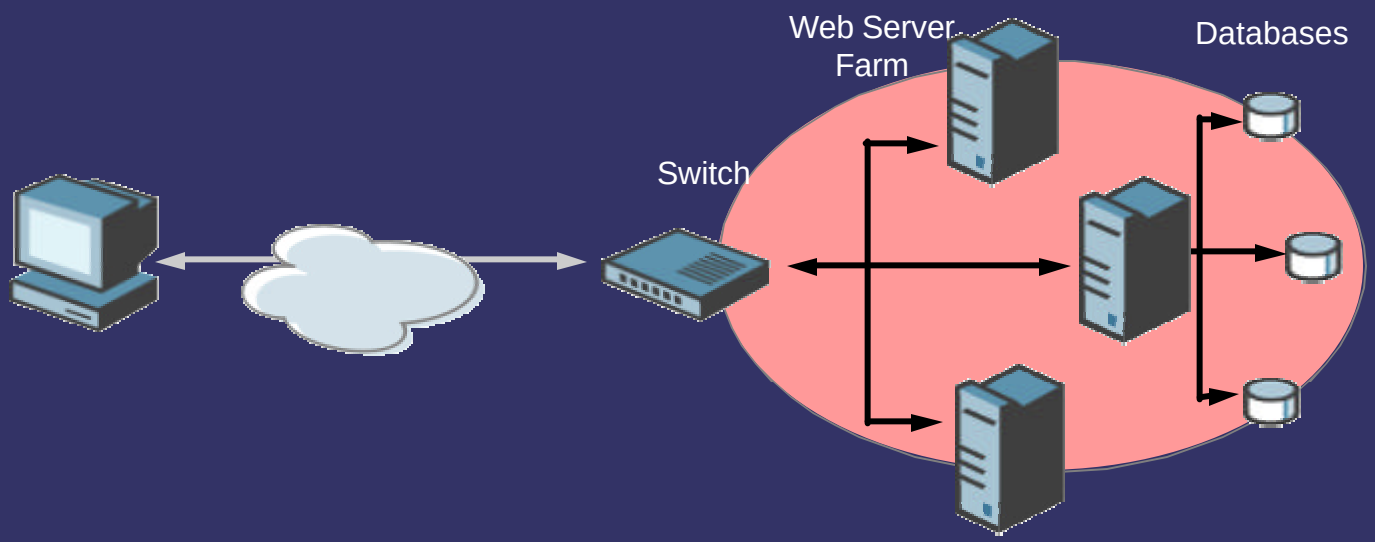


- Private keys kept in clear text
- Keys insecurely stored on Web and Application servers
- Vulnerable to internal and external compromise
- Theft of corporate identity
- Significant upswing in SSL has pushed this problem to the forefront

Security Infrastructure Attacks

- Why is private key theft so damaging?
  - With your private key, a hacker could decrypt your data, transactions, or even spoof your identity
  - Significant liability being associated with key theft
  - Loss of partner / consumer trust can be fatal
- What can you do?
  - Fully assess your security environment, and audit who is capable of what regarding your security context
  - Embrace Federal Information Processing Standard (FIPS) 140-2 Level 3
  - Embrace Single Sign On and other additional authentication and authorization mechanisms

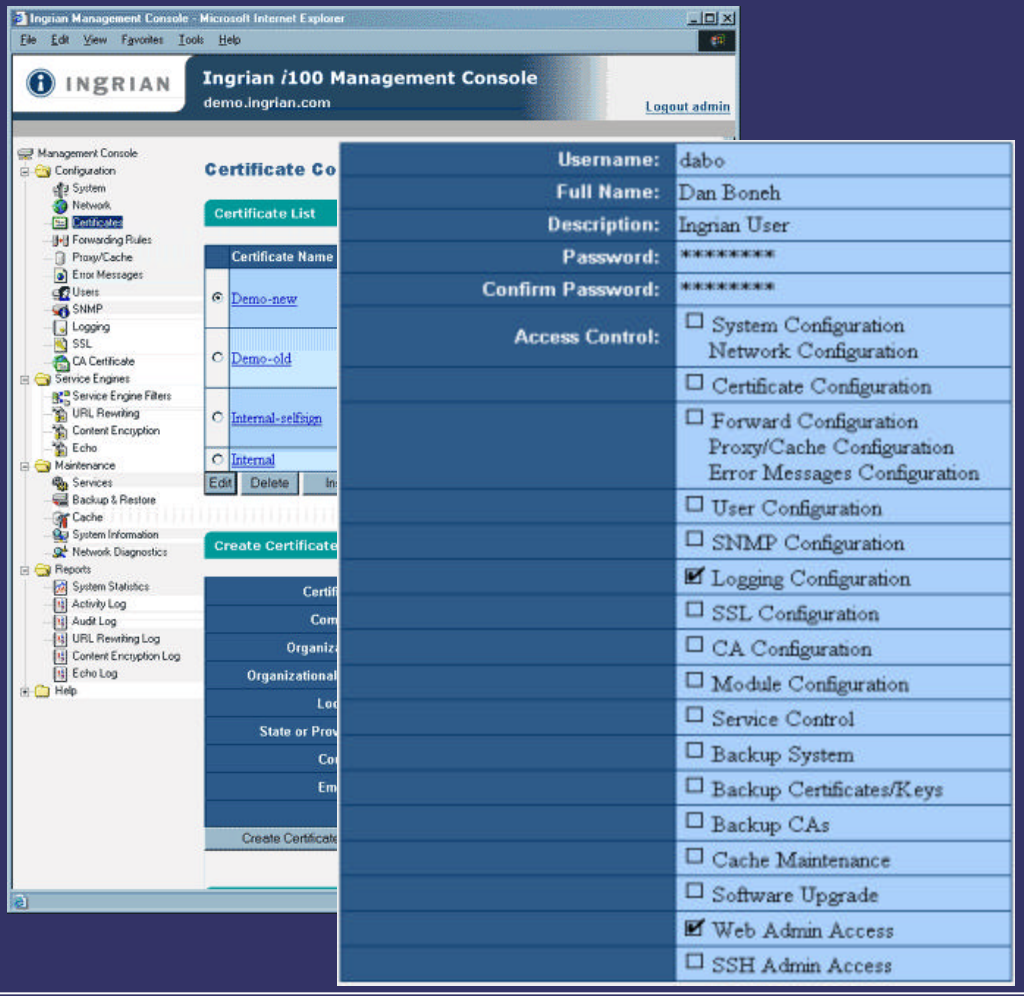
Threat 4: Unauthorized System Access



- Inadequate access controls on sensitive data is big threat.
- Fine-grained policies for administration often not in place
- Inadequate administrative action logging or audits
- Remember… most breaches are internal

Example 5: Detailed Administrative Access and Controls

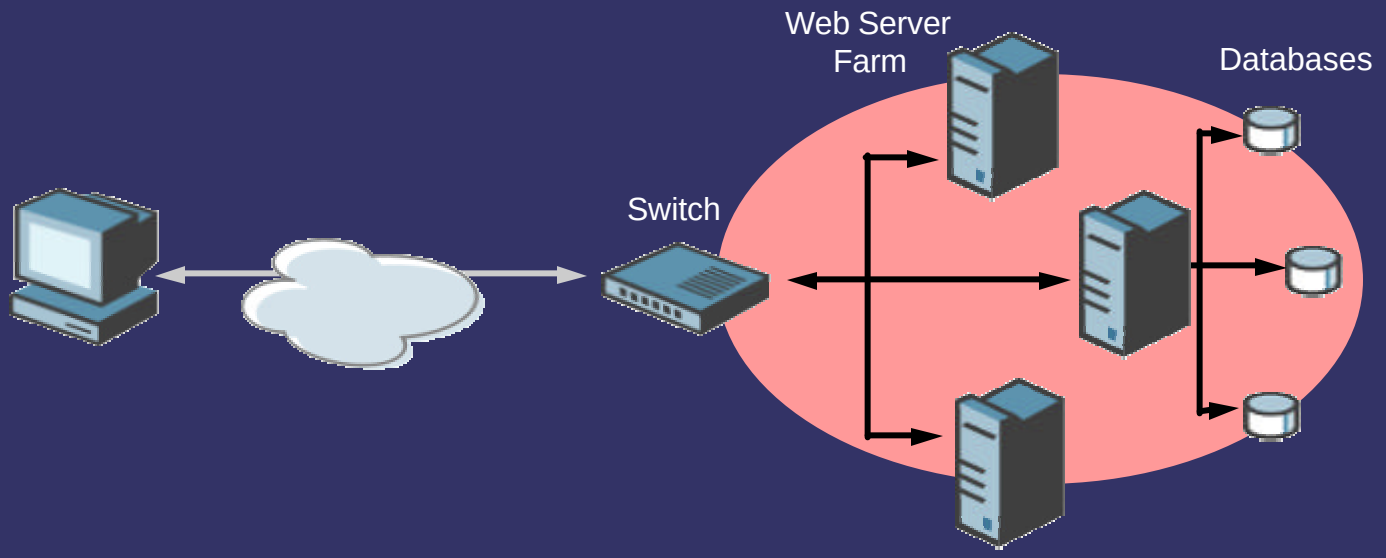
Example: Ingrian Management Console



What to look for:

- Intuitive GUI
- Ease-of-use to reduce configuration errors
- Full audit and activity logs
- Redundancy and Recovery mechanisms
- One-button addition of devices

Threat 5: Administrative Errors



- Mis-configuration of security parameters
- Network-based attacks have blurred the line of control between network and security managers
- Many administrators do not even know they have inadvertently caused a security problem
- Auditing policies and procedures are key

Summary: Selected Best Practices

- Keep security patches / products up to date
- Encrypt stored sensitive data as necessary
  - Products now available to handle higher volumes & performance requirements
- Encrypt data sent across open networks
  - But… SSL/TLS is not a solution by itself
- Assign unique ID to each person with computer access to data
- Track and audit access to data by unique ID
  - Ensure you 100% know and can track customers AND administrators
- Restrict physical access to nonpublic information
  - FIPS 140-2 L3 validation for protection of security context

Questions & Comments Welcome!

Rod Murchison
Ingrian Networks
rod@ingrian.com
Office: 650-261-2476