

# Internet and Intranet Security: a Case Study of the World's First Internet Bank



“Because your business is Your Business”

David Luther - President, S1 Network Security Division

[info@s-1.com](mailto:info@s-1.com)

<http://www.s-1.com>

- Security First Network Bank Introduction
- Security threats to Electronic Commerce
- Security Solutions used by SFNB
- So, is the Internet safe for commerce?

# What Were Our Objectives?

- Had to be safe
- Had to be first
- Had to be approved by federal regulators





# SECURITY FIRST

## NETWORK BANK, FSB

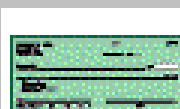
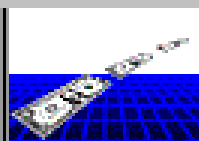
FDIC Insured

*We're Open! Try Out A [Demo](#) or [Open Your Account](#) With SFNB Today!*



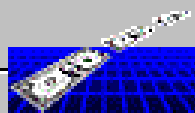
<http://www.sfnb.com/sfnb.map>

Select the section of the statement you want to view.

**Checks****E-Pays****Deposits****ATM****Debits****FDC**

## Checks

Number	Date	Payee	Category	Amount
<a href="#">885</a>	<a href="#">09/21/95</a>	<a href="#">Jeanne Ruegess</a>	<a href="#">Entertainment</a>	<a href="#">20.00</a>
886	09/21/95	Honda Finance Corp.	Auto: Honda Lease Payment	350.00



## E-Pays

Number	Date	Payee	Category	Amount
EFT1009	09/01/95	Forest Green Apartments	Rent	600.00
EFT1010	09/01/95	Midland Bank Visa	Credit Card	200.00
<a href="#">EFT1011</a>	<a href="#">09/01/95</a>	<a href="#">Georgia Power</a>	<a href="#">Utilities: Electric</a>	<a href="#">70.00</a>
EFT1012	09/01/95	Southern Bell	Telephone	135.00





# S1 Network Security Division - formerly SecureWare, Inc. -



## Military Grade Security

# Aspects of Commerce Security (Traditional or Electronic)



- Authentication of participants
- Authorization for requested transaction
- Authenticity of transaction request
- Integrity of transaction request
- Confidentiality of transaction
- Accountability (auditing)
- Non-repudiation



# Five Aspects for Secure Electronic Commerce

1. Client Security
2. Transaction Security
3. Server Security
4. Application Security
5. Protection against Insider Attacks

The diagram illustrates a network architecture on a blue background. On the left, a **Bank Customer** (a woman in a blue suit) and a **Computer Hacker** (a white figure) are shown at their computers. Both have arrows pointing to a central white cloud labeled **Internet**. From the **Internet** cloud, a double-headed arrow connects to a purple circle labeled **Web Server Platform**. To the right of the **Web Server Platform** is a vertical line representing a network backbone. Four horizontal lines connect this backbone to four purple circles, labeled from top to bottom: **Application Server**, **Administrator Workstation**, **Other Internal Hosts**, and **Other Internal Hosts**.

## Threats: Virus and Trojan Horse Attacks

The diagram illustrates a network architecture on a blue background. On the left, a **Bank Customer** (woman at a computer) and a **Computer Hacker** (man at a computer) are shown. The **Bank Customer** has a white arrow pointing to a cloud labeled **Internet**. The **Computer Hacker** has a blue arrow pointing to the same **Internet** cloud. To the right of the **Internet** cloud is a purple circle labeled **Web Server Platform**, connected to the cloud by a double-headed white arrow. To the right of the **Web Server Platform** is a vertical line with four horizontal branches, each ending in a purple circle. These are labeled from top to bottom: **Application Server**, **Administrator Workstation**, **Other Internal Hosts**, and **Other Internal Hosts**.

Threats: Weak encryption, weak protocol, server spoof, man-in-the-middle attacks

The diagram illustrates a Web Server Platform architecture. On the left, a cloud labeled "Internet" is connected to a central purple circle labeled "Web Server Platform". From the "Web Server Platform", a line extends to the right, passing through a vertical line that separates it from the internal hosts. This line then branches out to connect to four distinct internal hosts, each represented by a purple circle. The hosts are labeled from top to bottom: "Application Server", "Administrator Workstation", "Other Internal Hosts", and another unlabeled host. The entire diagram is set against a dark blue background.

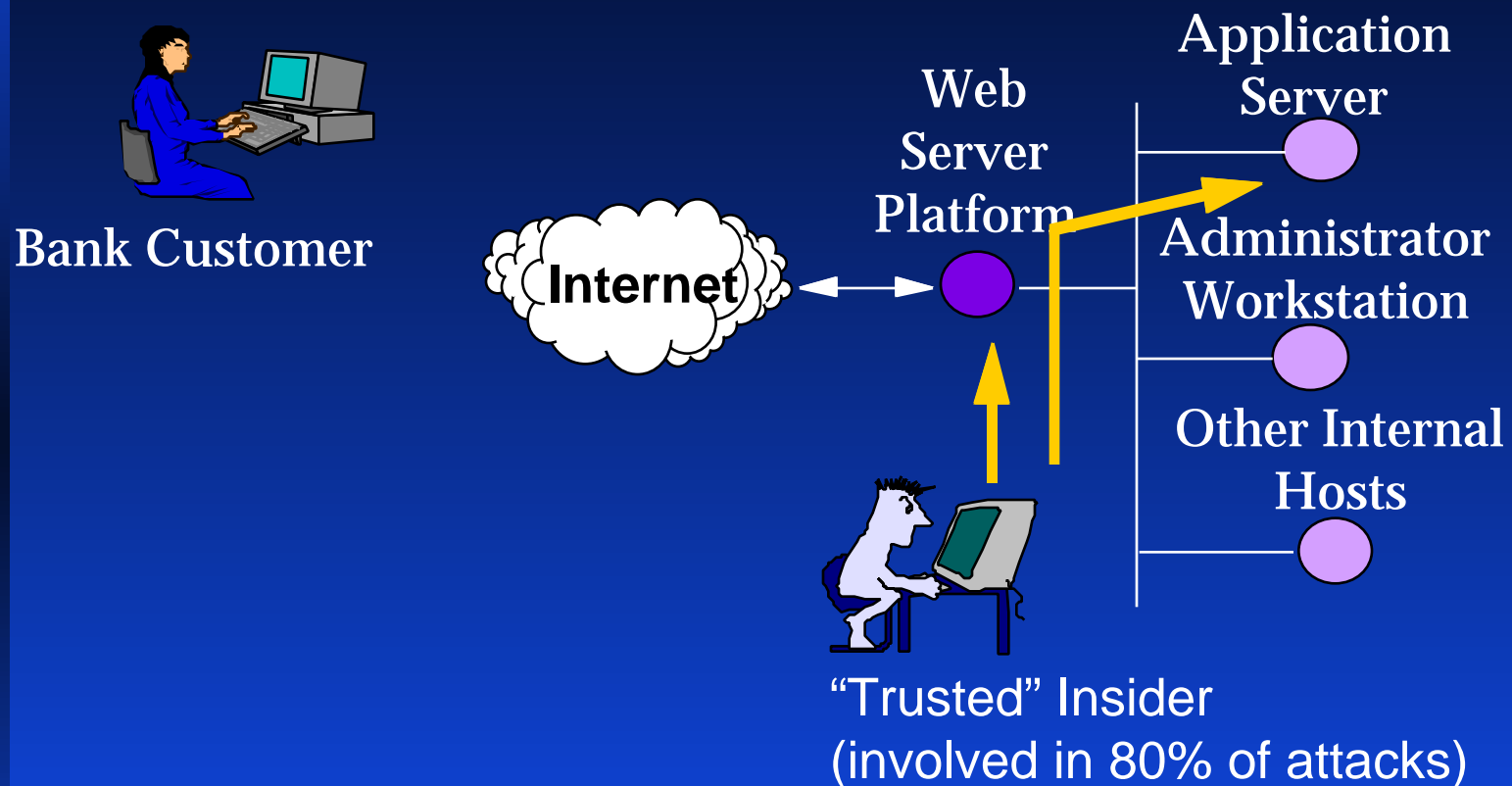
Threats: Unix/NT security holes, improper administration

The diagram illustrates a Web Server Platform architecture. On the left, a cloud labeled "Internet" is connected by a red line to a central purple circle labeled "Web Server Platform". To the right of the "Web Server Platform" is a vertical line representing the internal network. Four components are connected to this vertical line by horizontal red lines: "Application Server" (top), "Administrator Workstation", "Other Internal Hosts", and another unlabeled purple circle at the bottom. A red arrow points from the "Web Server Platform" to the "Application Server".

A cartoon illustration of a man with spiky black hair, wearing a white shirt and blue pants, sitting on a blue chair at a desk. He is looking at a computer monitor which displays a green screen. The background is a solid blue color.

Threats: Poor programming, stack overflow, shell escapes, improper enforcement of authorizations, weak authentication, poor session tracking

# Insider Attacks

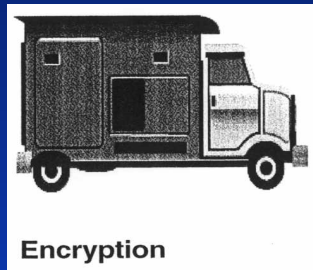


Threats: “Trusted insider”, improper administration, physical attacks, insider knowledge

# End-to-End Security is Critical



**Client Endpoint Security**



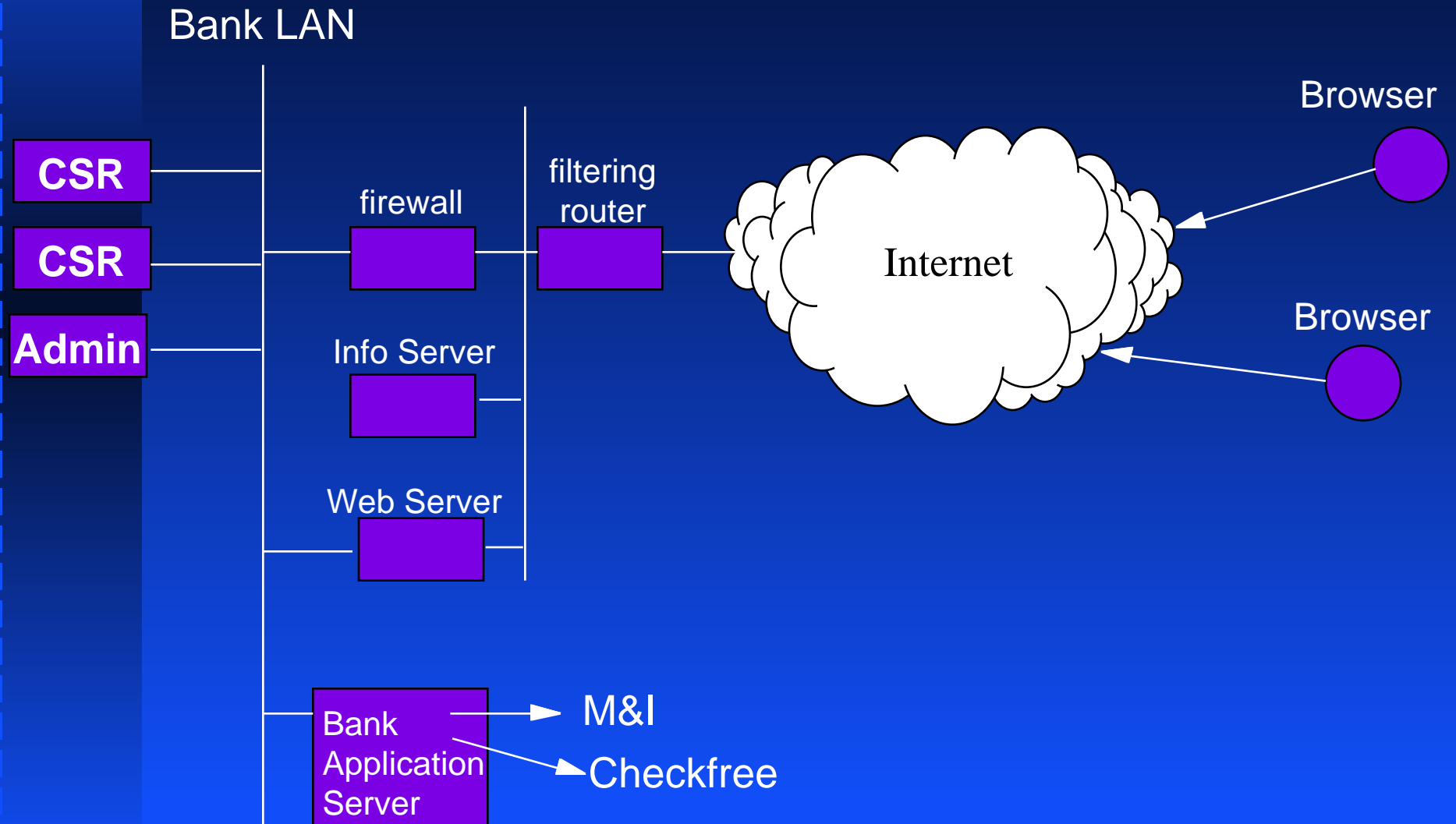
**Over-the-Wire Security**



**Server Endpoint Security**



# Security First Network Bank Architecture



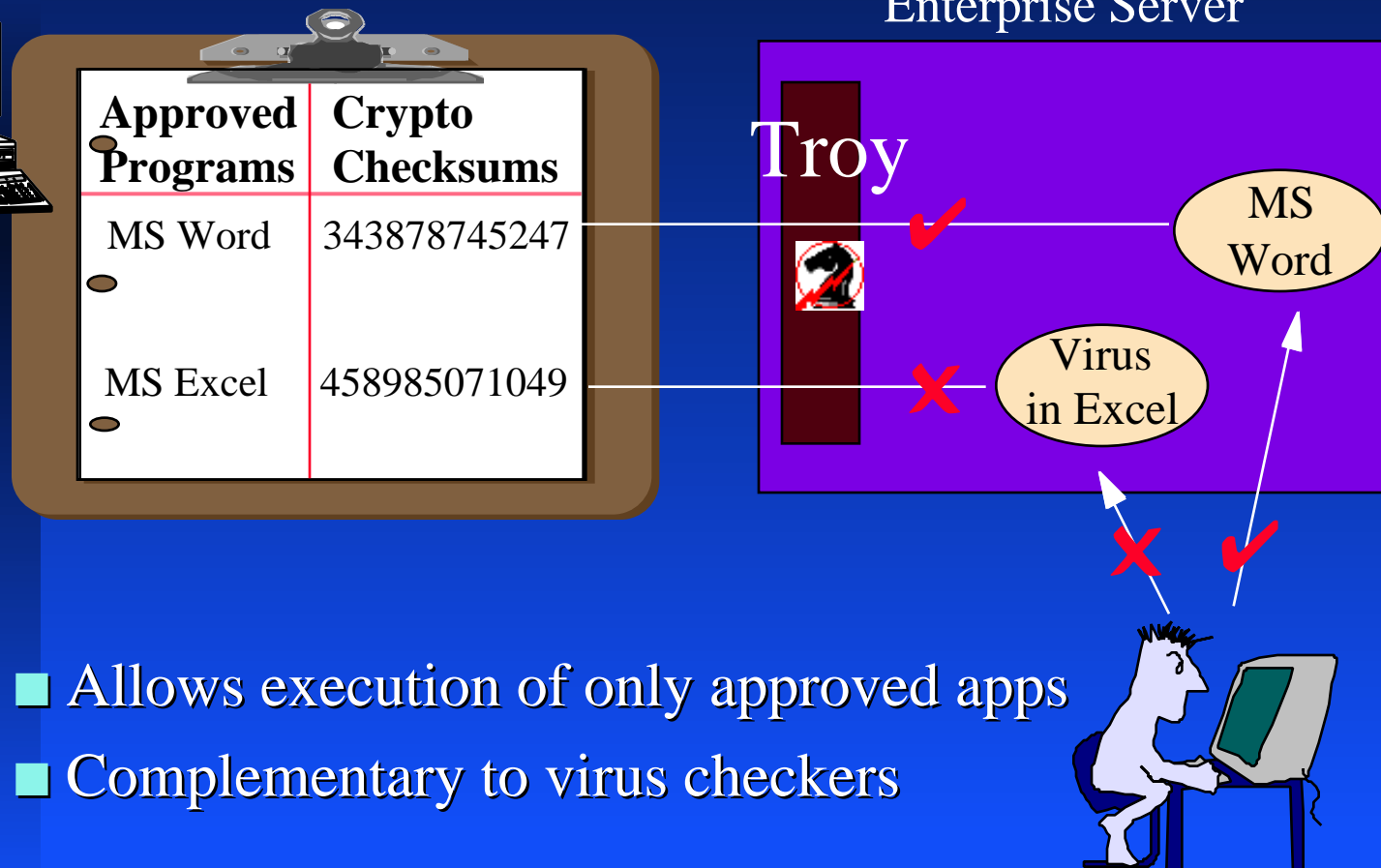


# Client & Server Integrity

(From Unapproved Applications & Viruses)

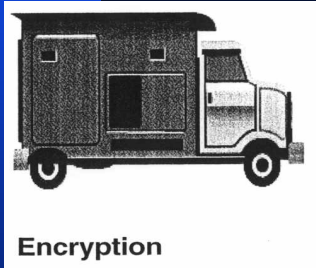


Enterprise Server



# Bank LAN

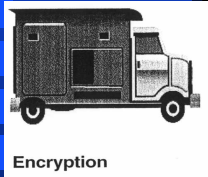




# Transaction Security: Security Over-the-Wire (Cryptography)



- *Encryption* - for confidentiality
  - ◆ DES, DES3, RC4, IDEA, ...
- *Authentication* - for access control
  - ◆ ID/Password, Digital Signature, Smart Cards
- *Integrity* - to ensure data is unchanged
  - ◆ MD5, SHA, MD2, ...

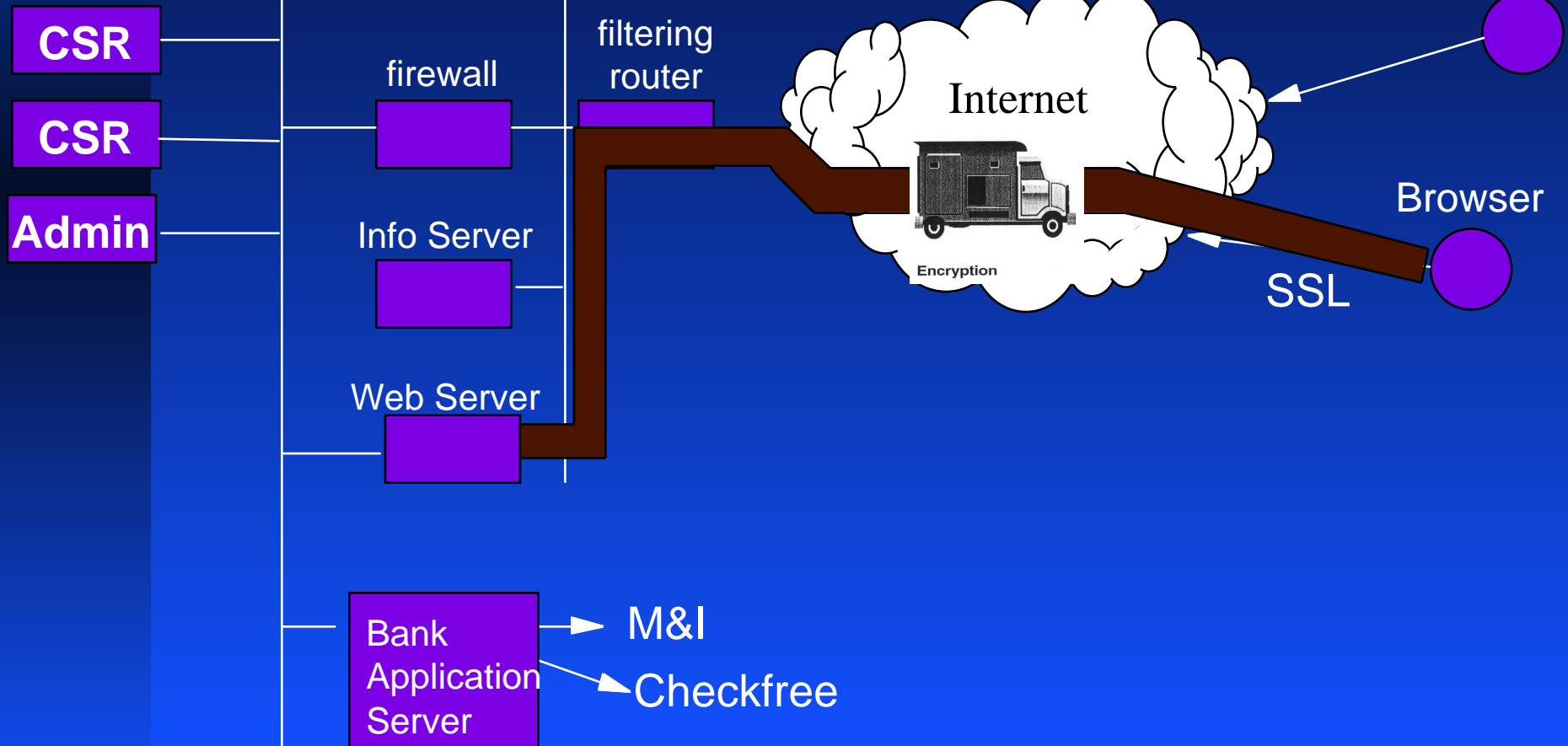


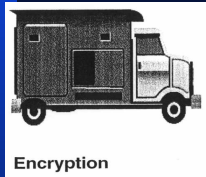
# Protecting Web Network Transactions: Netscape's Secure Sockets Layer (SSL)

- Widely deployed on OS platforms
- Cryptographic authentication today
- Encrypted path between browser and server
- Cryptographic network data integrity
- SST in future (higher level payment protocol)

# Security First Network Bank: Netscape's SSL - Secure Sockets Layer

Bank LAN





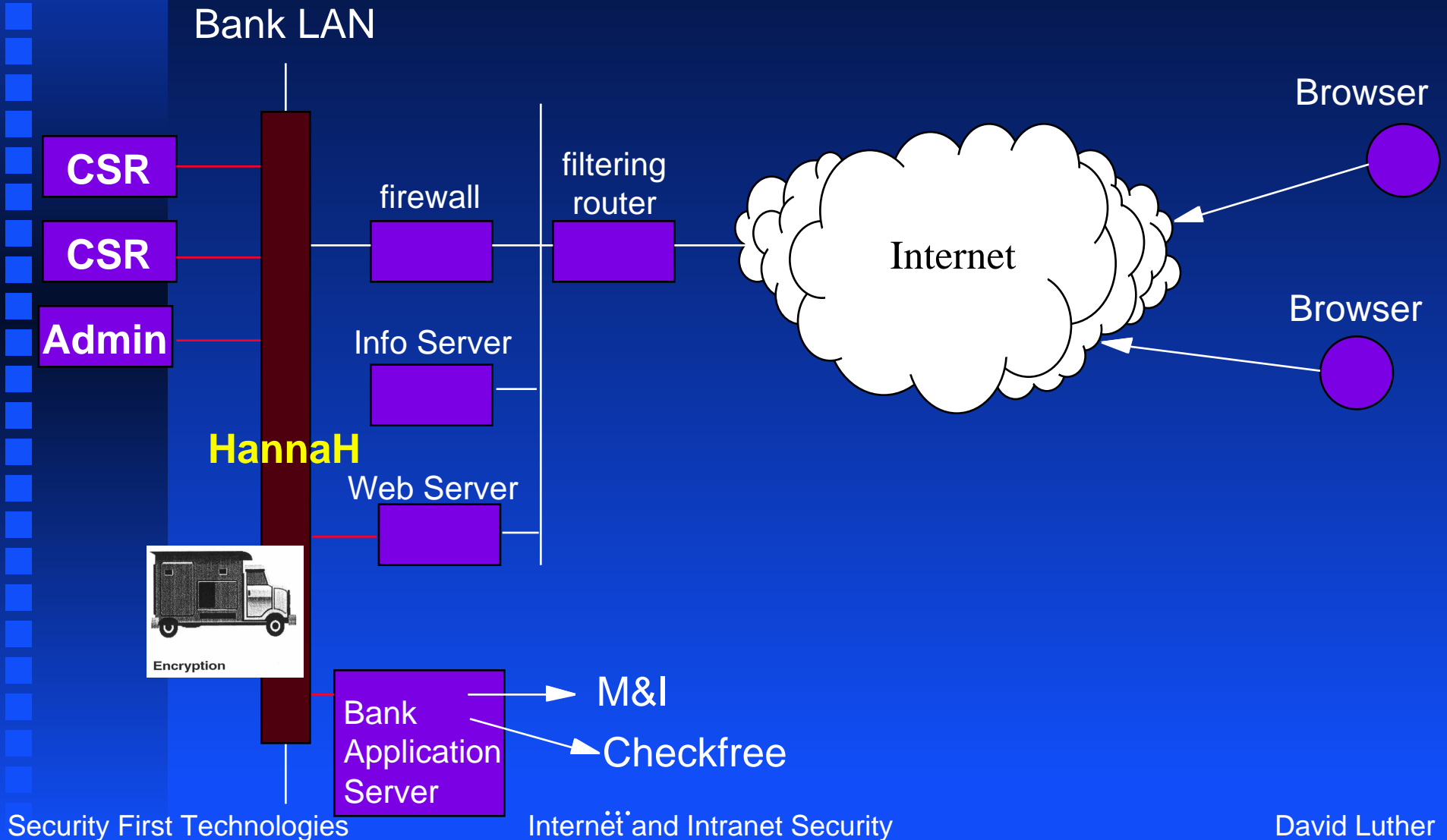
# Protection for ALL Over-the-Wire Network Transactions: HannaH - Network Security



- Access control using authenticated identity
- Data integrity and encryption
- No application modification
- Centrally administered, audited

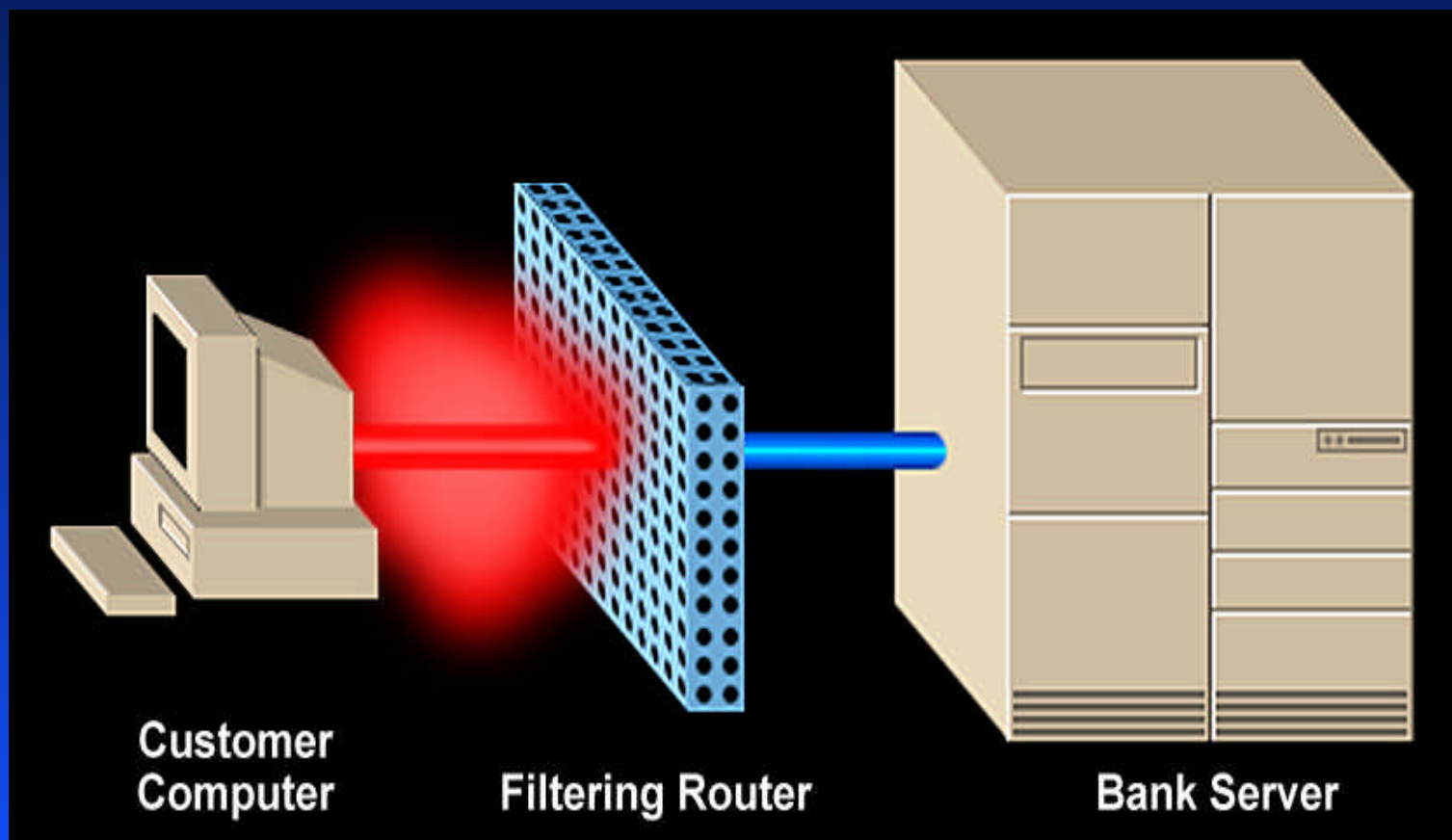


# Security First Network Bank: Security from Insiders - S1's HannaH - Network Security





# Server Security - Filtering Routers: Block Attacks from Outsiders

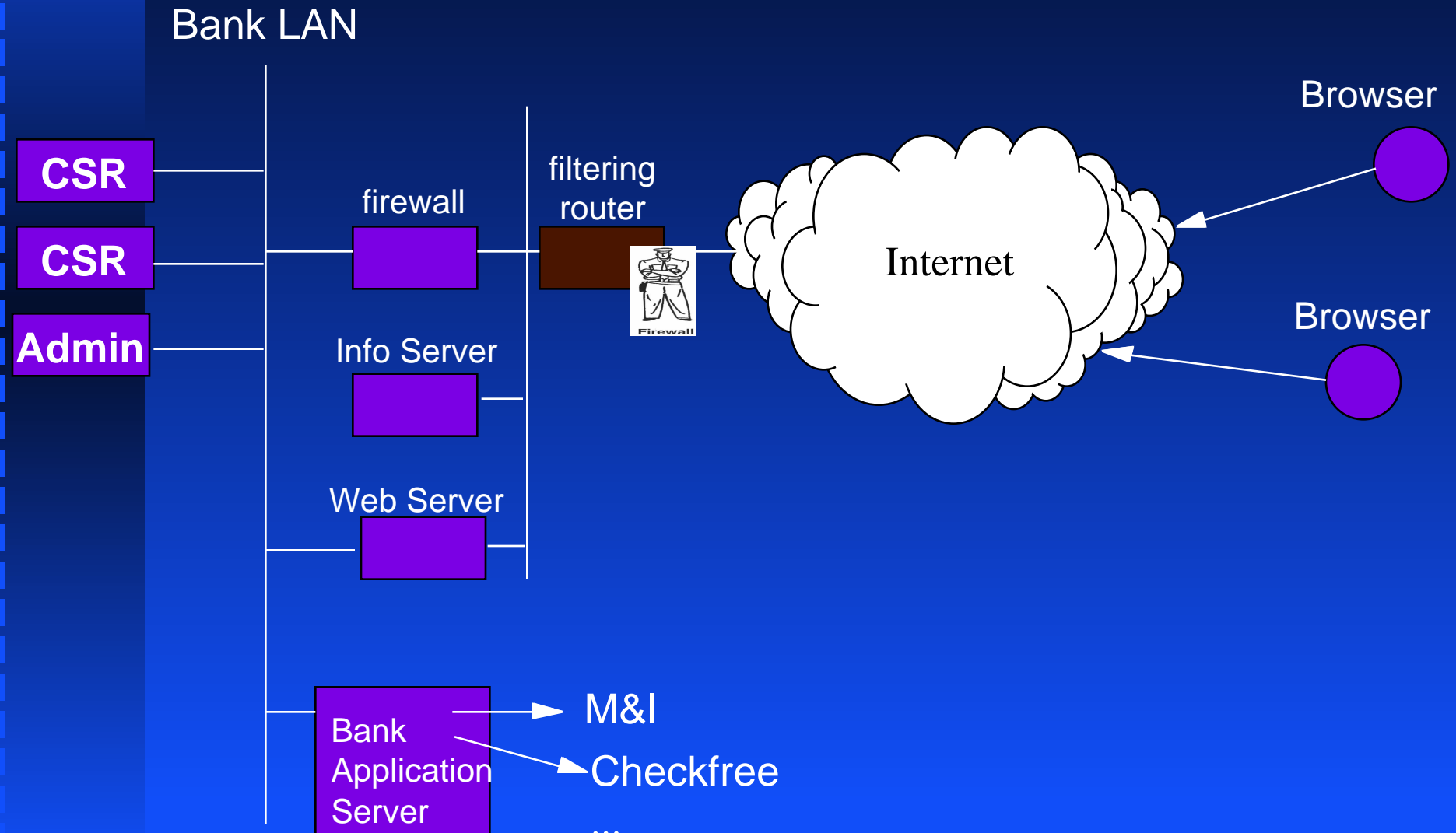




# Providing Server Access Control: Filtering Router

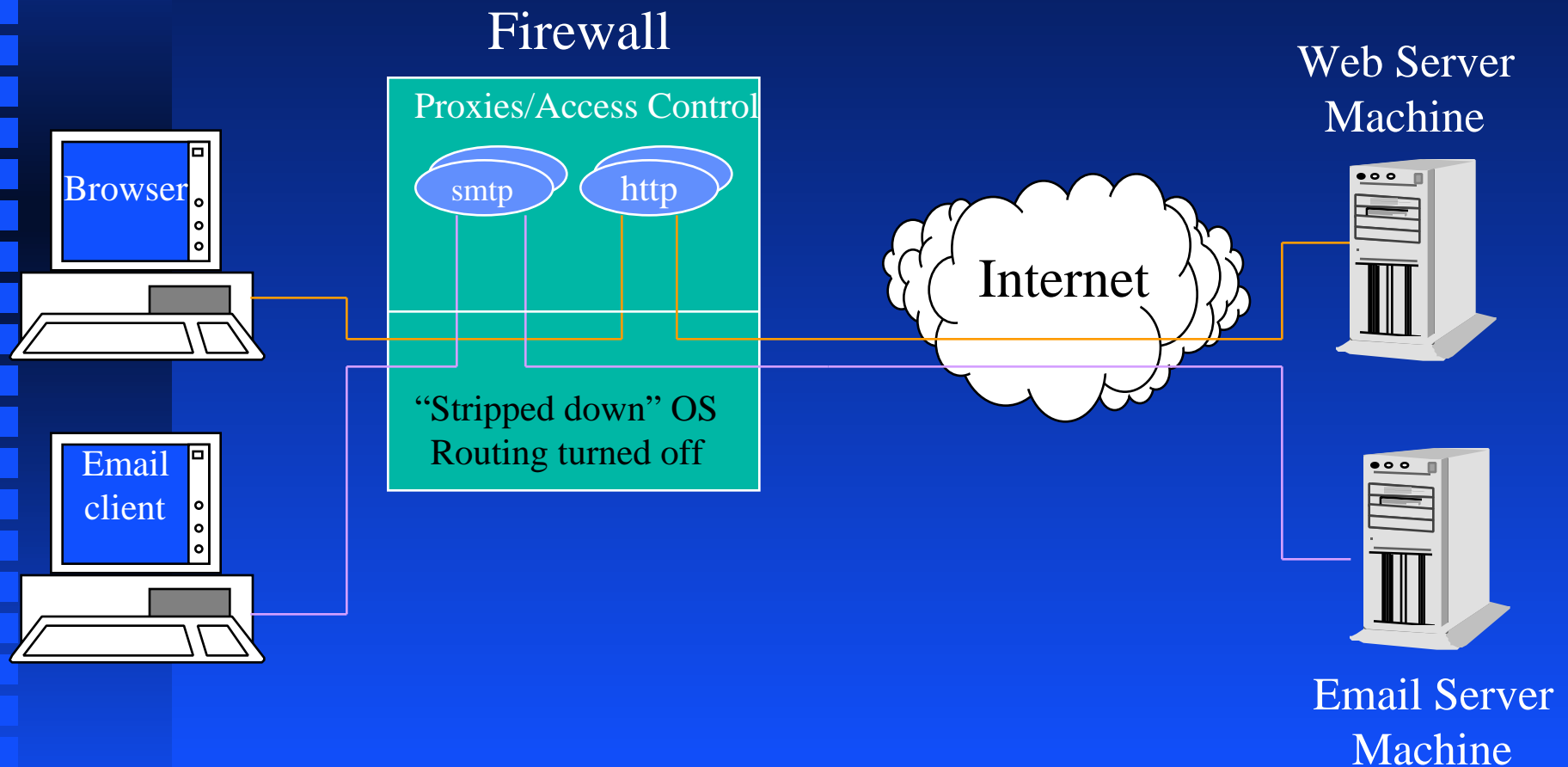
- Prevents unauthorized entry by filtering incoming traffic
  - Prevents attacker from masquerading as an internal machine
  - Checks incoming data against known attacks (source routing)
  - Restricts access to machines/services

# Security First Network Bank: Filtering Router





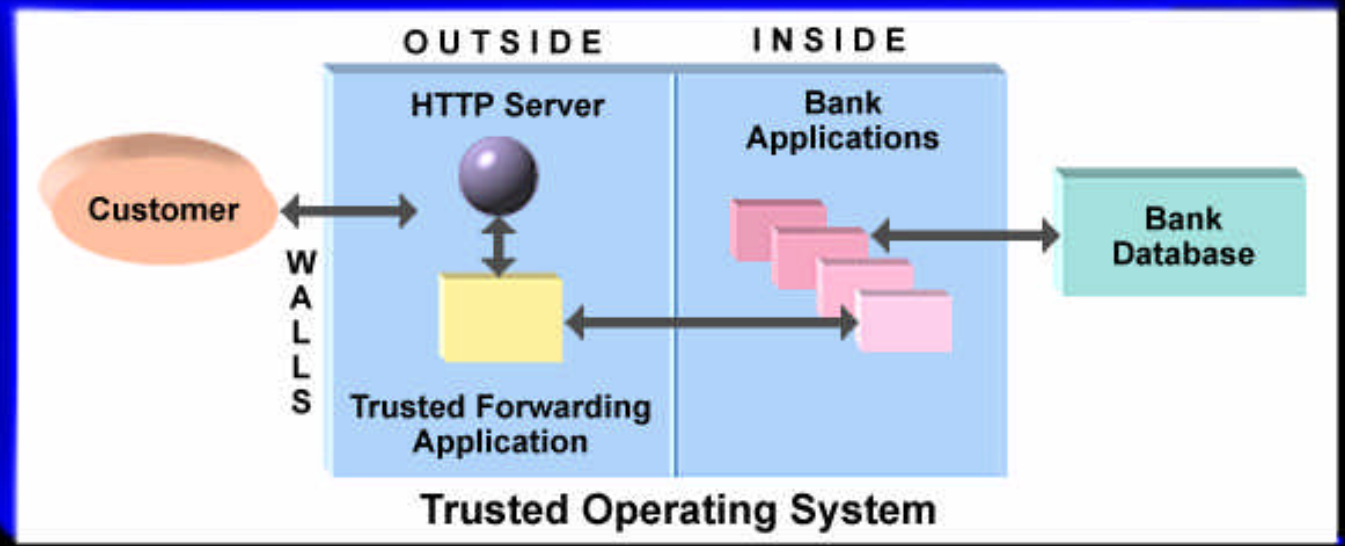
# Server Security - Firewall: Mediates Access to the Intranet



# Bank LAN



# Server Security: Trusted Operating System guards against internal and external threats to Intranet Servers



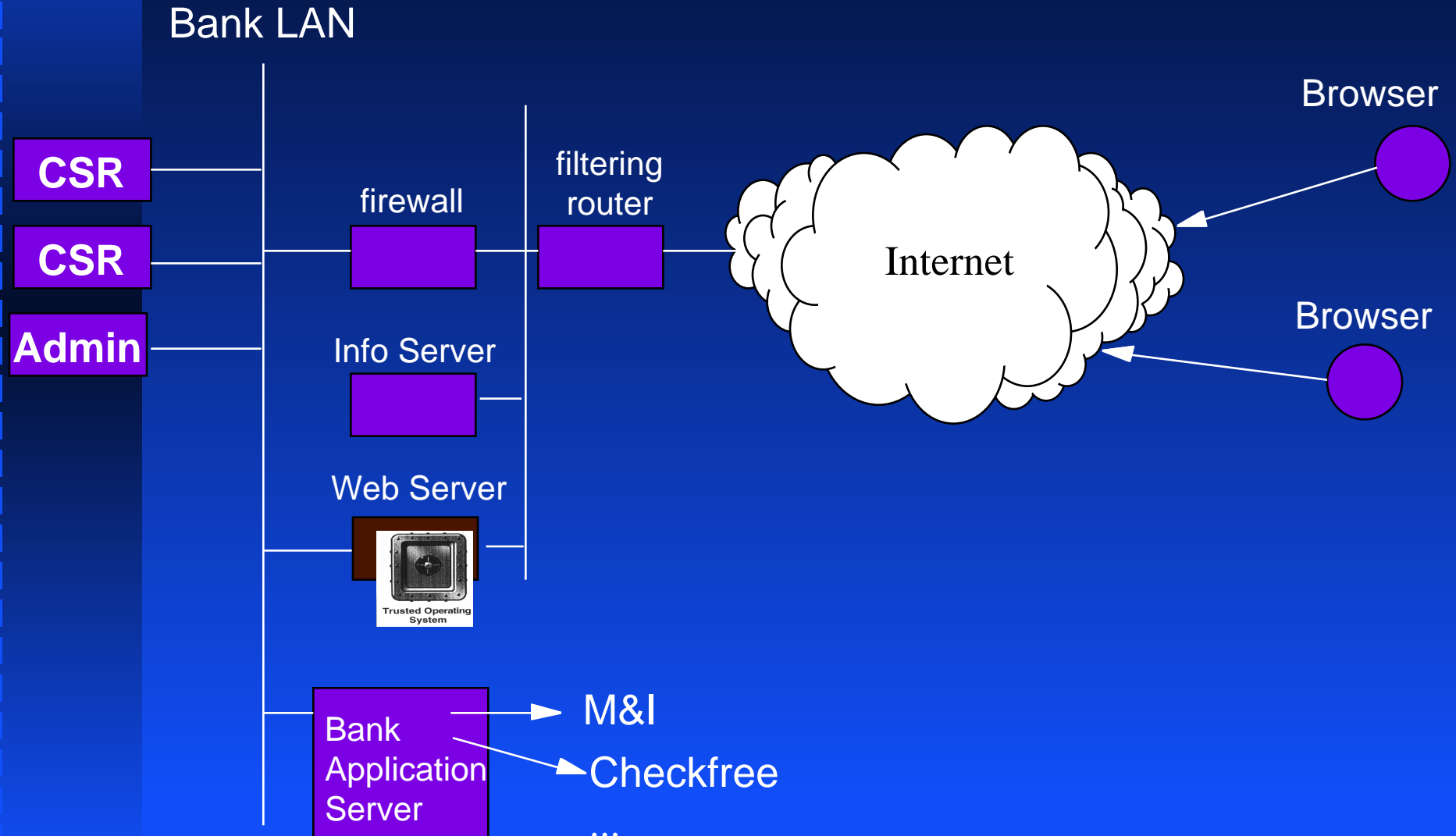




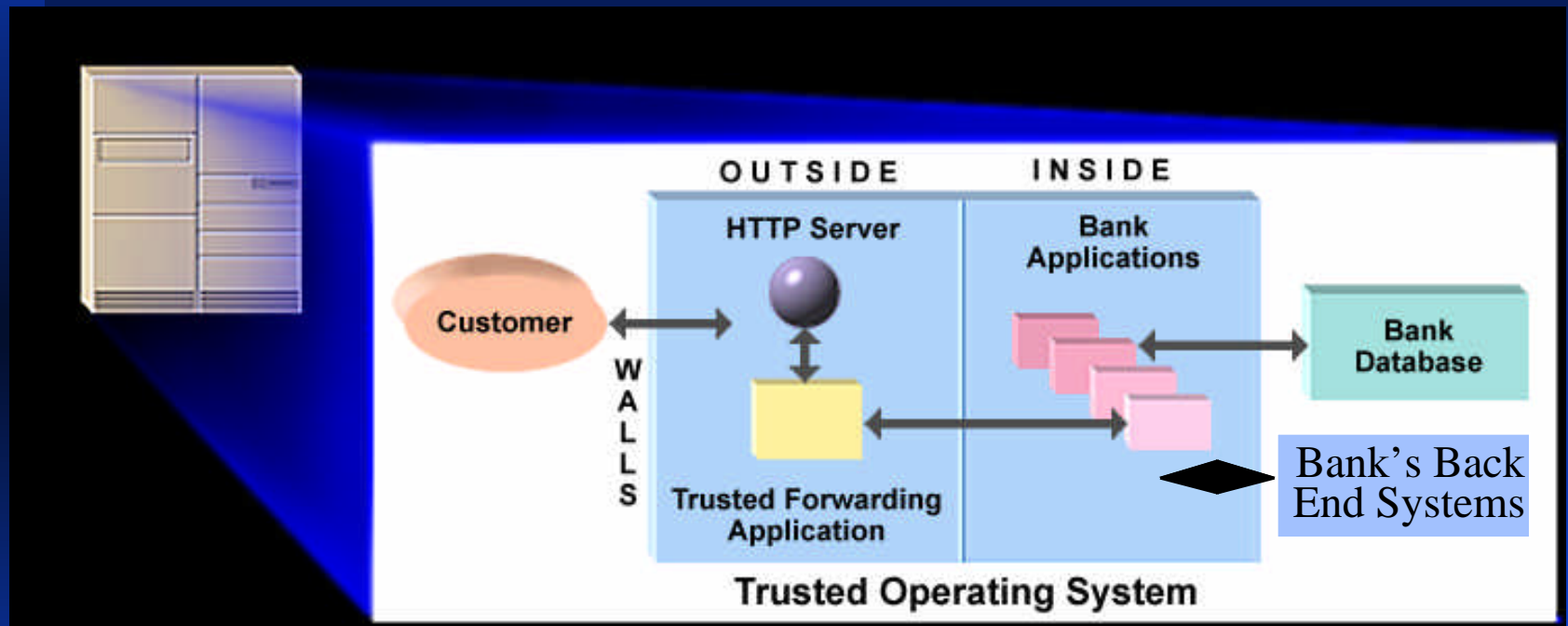
# A Bullet Proof Vault for the Server: Secure Web Platform

- Military Grade Security - Acquired by HP from SecureWare
- Prevents entry by internal and external unauthorized users
  - Compartmentalization of data
  - Administration accounts with limited powers
  - Strong authentication to prevent login break-in
  - Accountability of all significant system actions

# Security First Network Bank: HP's Virtual Vault

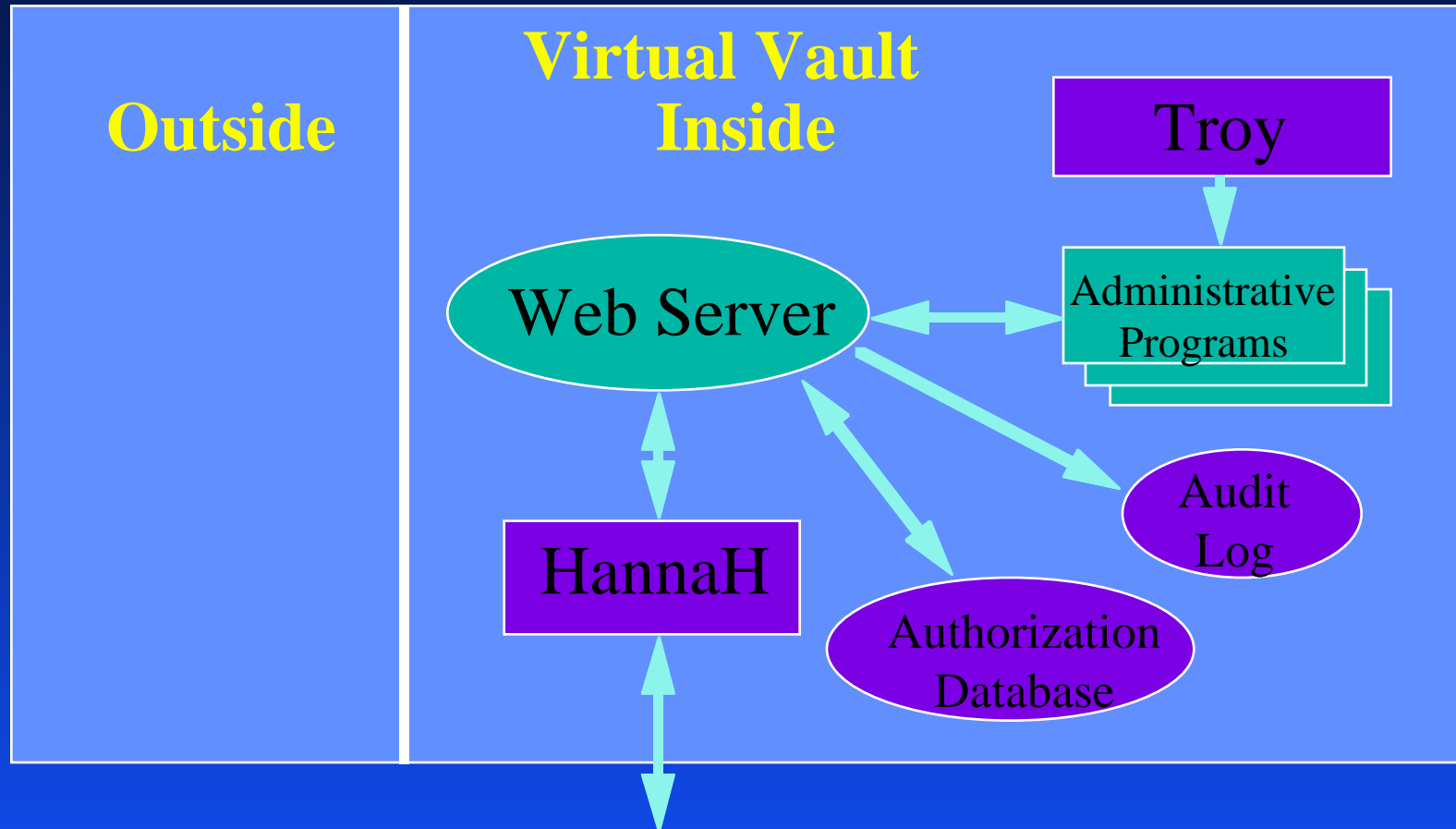


# Application Security - Must be Designed for Security



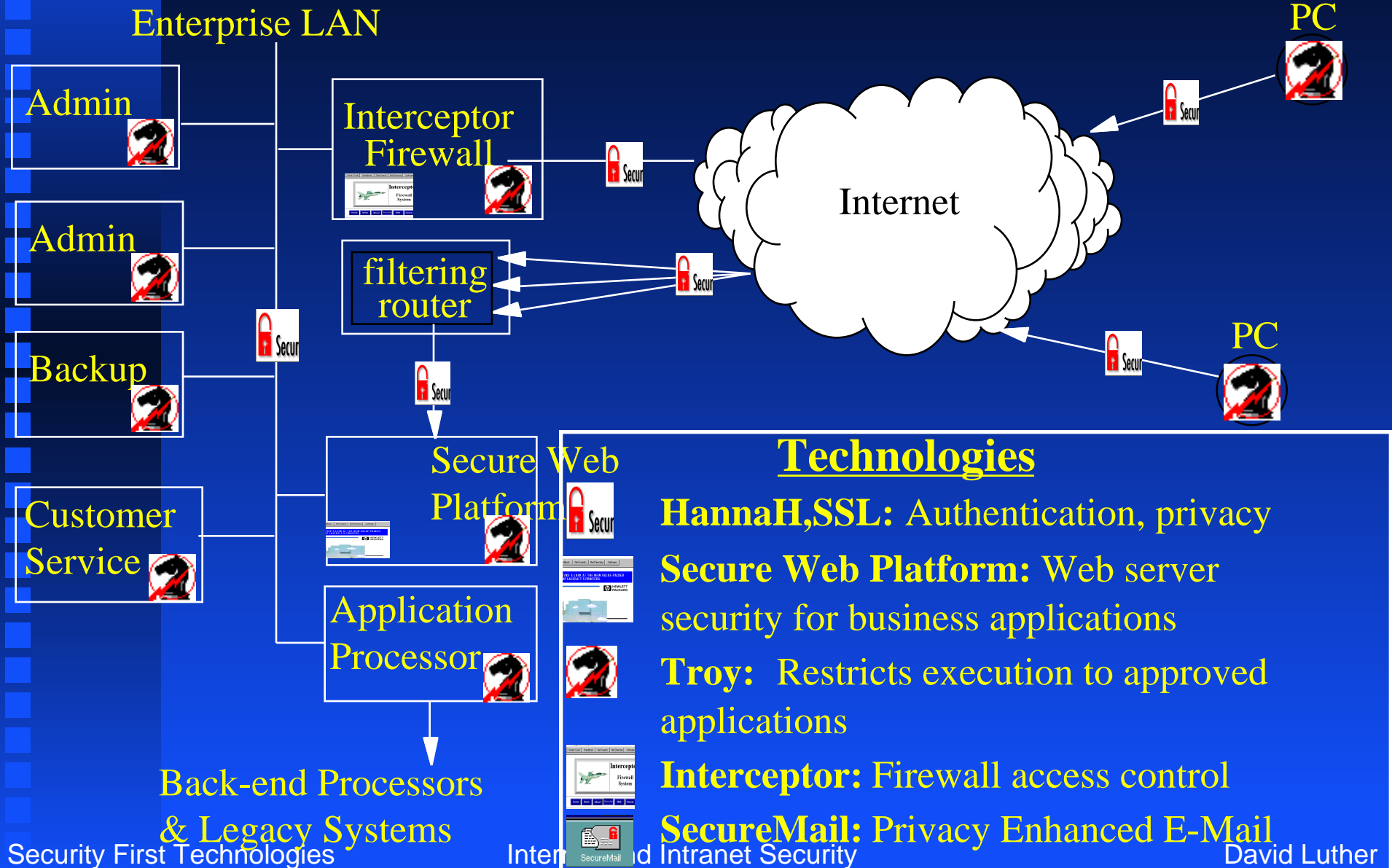
The application has access to the bank database and back-end systems. If it can be subverted, so can the database and back-end systems.

# Secure Against Insider attacks - Authentication, Authorization, Audit



**All Administrative Access**

# Complete Security Solution



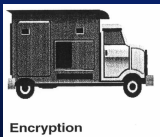
# Electronic Commerce

## What are your risks? What can you do?



- Your personal safe (your computer)

- ◆ Authentication, Platform integrity



Encryption

- Armored truck (over the wire security)

- ◆ Cryptographic strength for data integrity and encryption



Firewall

- Bank guard (filtering router, firewall)

- ◆ Access control, reduce denial of service



Trusted Operating System

- Vault (Virtual)

- ◆ Strong access control and accountability to prevent external & internal attacks

- ◆ Platform Integrity

# Electronic Commerce

## Is it going to happen?

Absolutely!!

But only if you solve the whole problem,  
“all the way to the bank”.