



SSH | Original Secure Shell
10 Years 1995 – 2005

Managing Internal Security Risks

June 7th, 2005

Timo J. Rinne

Chief Technology Officer

SSH Communications Security Corp.



SSH Communications Security

- Founded 1995
- Original developer of the Secure Shell
- Public company since 2000 (Helsinki Stock Exchange)
- Global presence through sales offices and channel partners; R&D in Finland
- Complete focus on SSH Tectia providing security for business applications and system administration for
 - Large enterprises
 - Financial institutions
 - Government agencies
- Values (Select, Solve, Honor)



Agenda

- Identifying relevant security risks
- Deperimeterization
- Risk management and compliance approaches to IT security
- Managed security middleware – cost-effective protection
- Conclusions



Relevant Security Risks

- Business continuity
- Loss of reputation
- Breaches in regulation compliance
- Immediate loss of money
- Susceptibility to external interference and pressure (even blackmail)
- Internal security breaches and “social engineering”

More than 70% of unauthorized access to information systems is committed by employees, as are more than 95% of intrusions that result in significant financial losses.

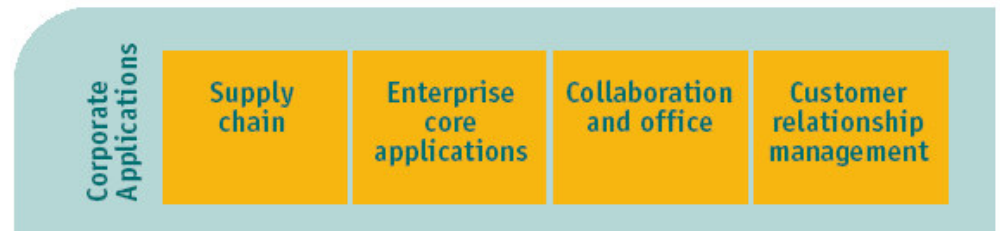
[Source: Gartner, 2003]

Deperimeterization

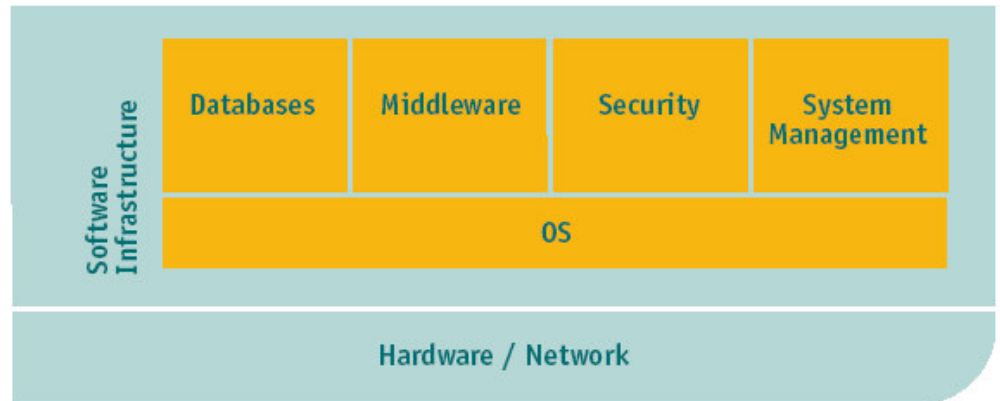
- Border between the internal and external network is disappearing
 - Access to internal systems is provided for partners and customers
 - Accelerated adoption of wireless LAN
- Network worms are becoming more sophisticated
 - Quick propagation to internal network once infected
 - Can combine various attack techniques such as password collection
- Insider risks
 - Often more relevant than external ones
 - Regulations require protection also against these

Corporate IT Architecture

- Corporate applications help you to run business effectively



- Infrastructure exists to support efficient use of corporate applications



Common Application Security Vulnerabilities

- Critical business data travels as plain-text in the corporate network
 - Standard sniffer tools can be used for data eavesdropping
- Passwords are sent as plain-text during application login
 - During the application login, plain-text password is sent to the server
 - Stealing password is trivial with tools that are readily available
- Access rights are not properly defined
- Weak password policies or no policy at all
 - Easy-to-remember passwords are also easy-to-crack
- Buffer overflows and other programming errors in applications
 - Exploiting the vulnerability may offer even a administrator level access to the server

Need for Risk Management

Copyright 2003 by Randy Glasbergen.
www.glasbergen.com



“We don’t need to worry about information security or message encryption. Most of our communications are impossible to understand in the first place.”



Business Risks

- Threat + IT vulnerability = Business risk
 - Loss of reputation and brand erosion
 - Business interruption
 - Exploitation of confidential business information by competitors
- Risk management requires a holistic approach
 - Combination of people, policies, processes, and technical methods
 - Protecting applications is only one part of the whole but it is an area that *can be solved in a cost-effective way*

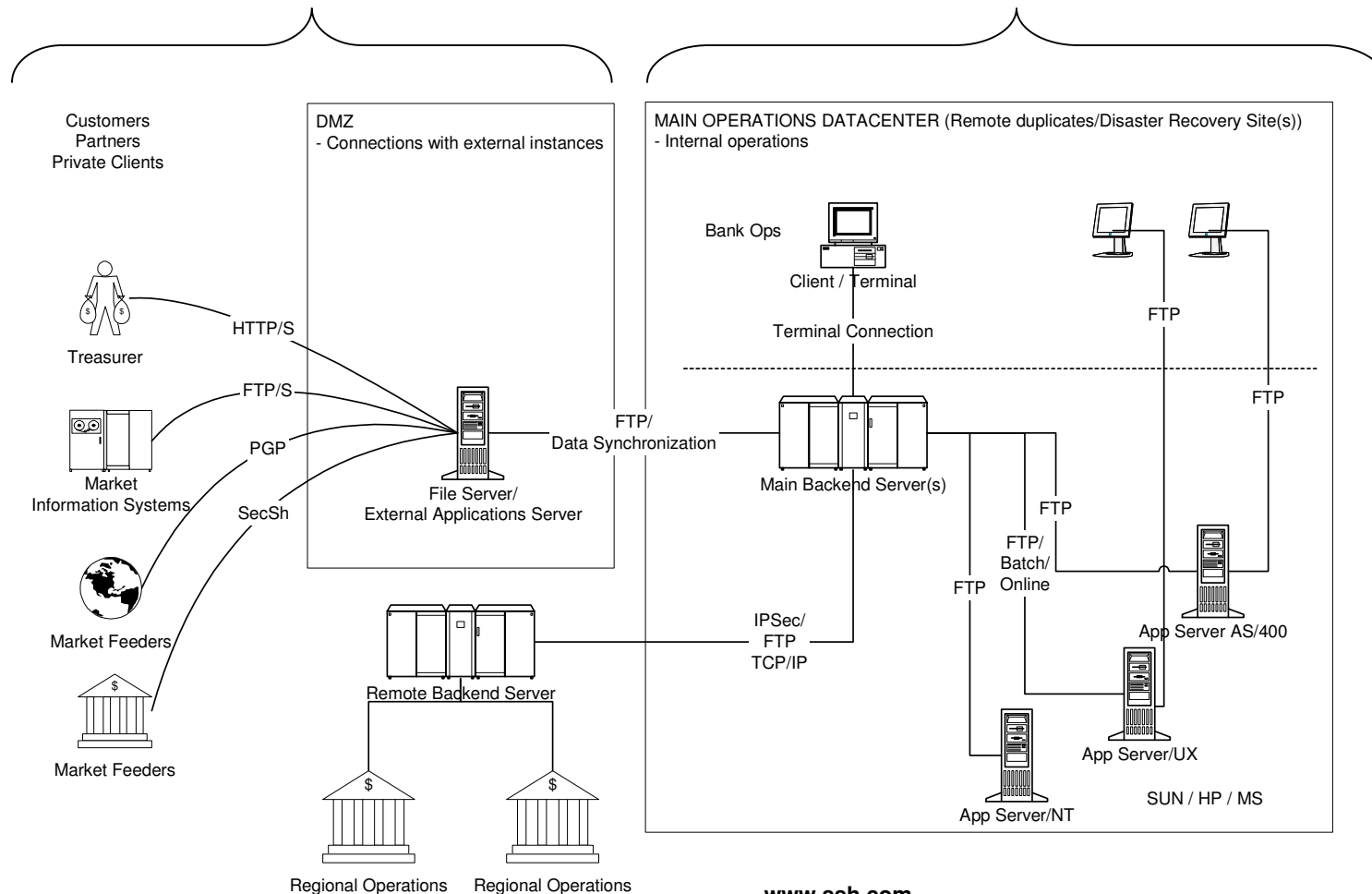
Regulatory Compliance and Security

- New regulations with security implications are emerging globally
 - How to ensure health-care data privacy (HIPAA)
 - How to ensure confidentiality of consumer financial data (GLBA)
 - How to ensure validity of financial reporting information (SOX)
- Increasing adoption of critical business applications is the driver
 - Old methods and practices cannot be applied to electronic data
- Increasing awareness of operational risk management
 - For example, Basel II defines capital allocation also for operational risks
- Most of the legislation in place is currently from US, but has already a strong implications to European business too
 - SOX compliance already needed if relevant presence in the US
 - Other national and EU legislation will follow

Case Example – Need for End-to-end Security

External access secured

Internal access unsecured



Application Security Requirements

- Reliable authentication of users accessing business applications
 - Establishing the identity of the remote and local users
- Authorization of users once they have been authenticated
 - Preventing illegitimate access to critical data stored in the servers
 - Ensuring that users cannot see or do more than they need to
- Confidentiality and integrity for application communications
 - Encrypting data in transit prevents eavesdropping
 - Preventing data modification while in transit
 - **Not addressed by most organizations, except for remote access and even then only up to the perimeter!**
- Traceability
 - All transactions need to leave forensic trace
 - Auditing & logging is mandatory in regulated environment



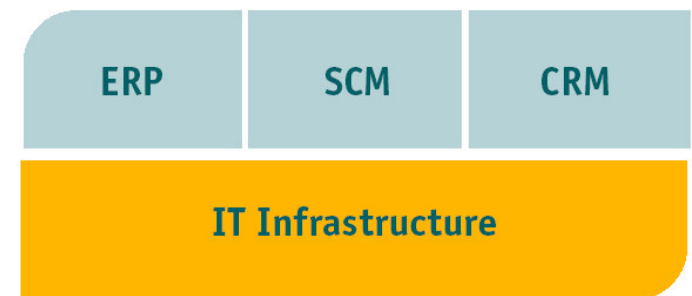
Key Design Principles for Cost-effective Operation

- Centralized management and automation of repetitive tasks
 - Reduced administration burden
- Security policies enforceable in real-time
 - Users can not override security policies
 - Fast reaction to new threats and changes in policies
- End-user transparency
 - To eliminate end-user training and helpdesk costs
- Adaptability in heterogeneous, multi-platform IT environments
 - Possibility to leverage existing IT systems with minimum integration
- Seamless integration to user management processes
 - No need to change the way how identity information is managed
- Connection level auditing can be provided

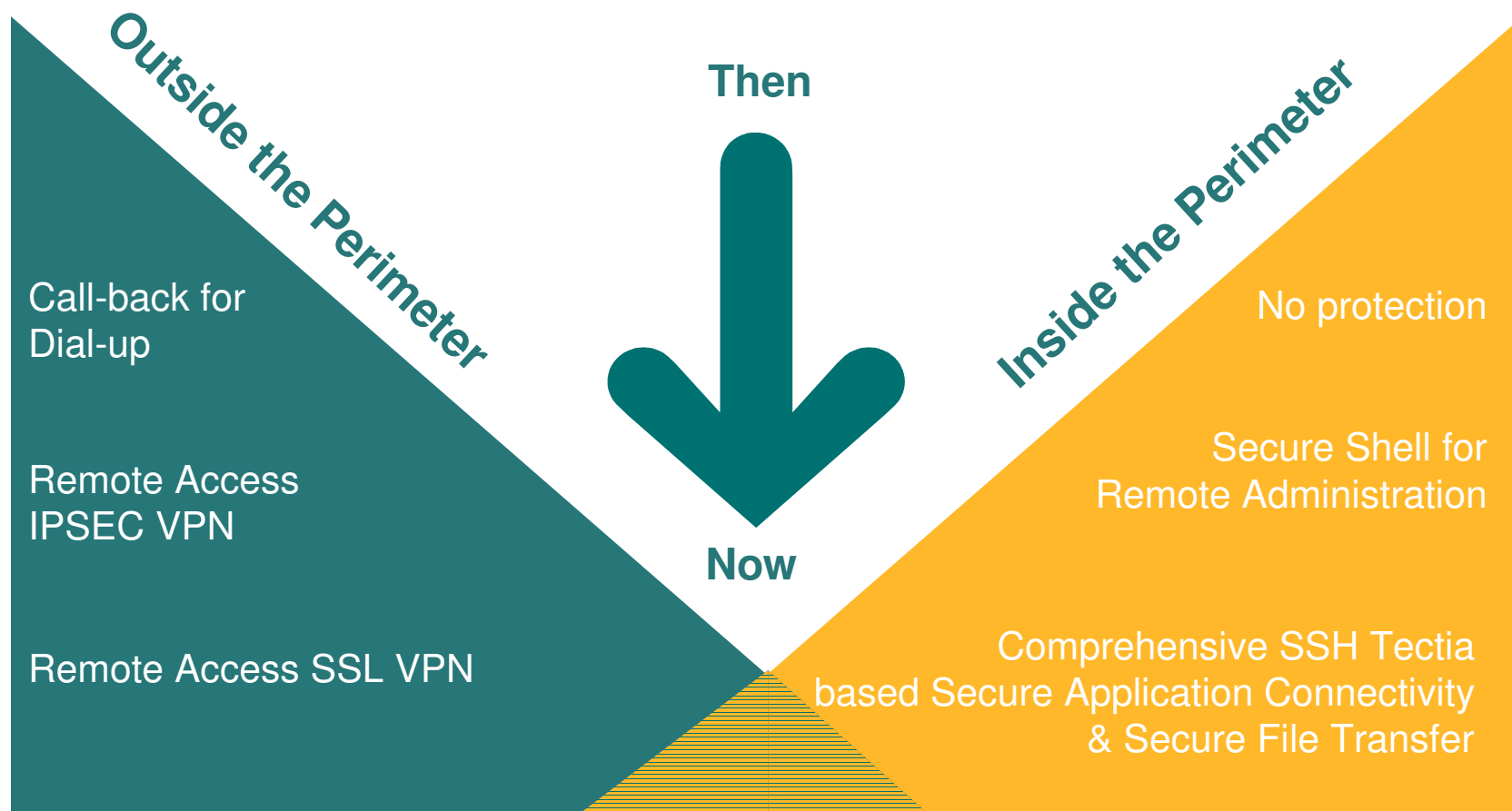


Communications Security – Traditional Approaches

- Communications security can be implemented in different layers in the IT architecture
- The traditional approaches are not well suited for end-to-end application protection
 - Network security (IPSec VPN) is hardware dependent and does not work in heterogeneous environments
 - Application integrated security requires code-level changes for each application and is not centrally manageable

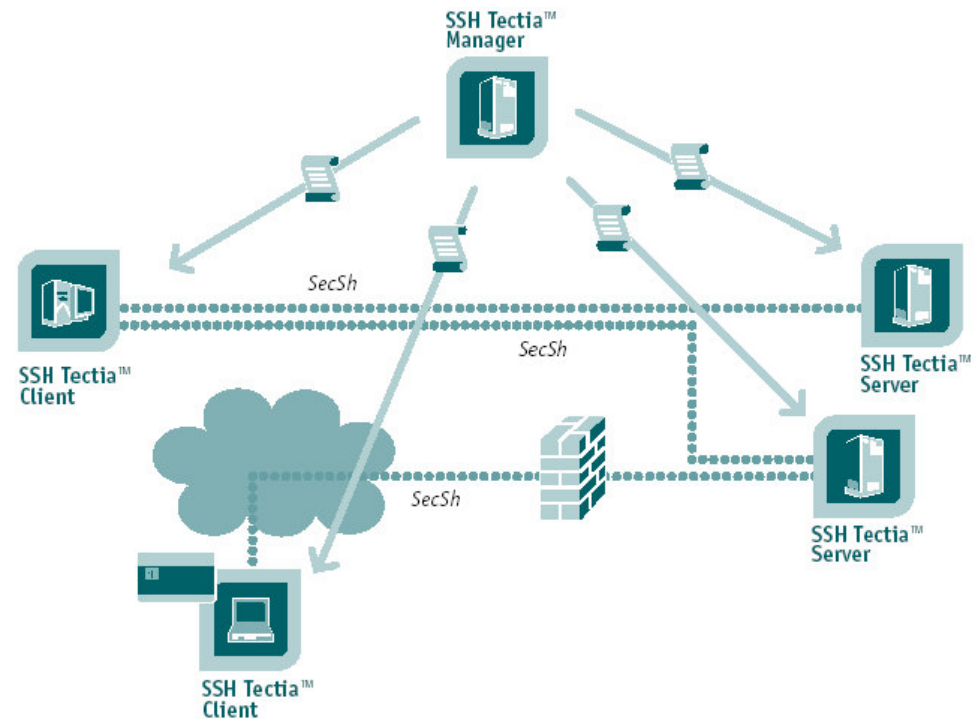


Evolution of Security Models



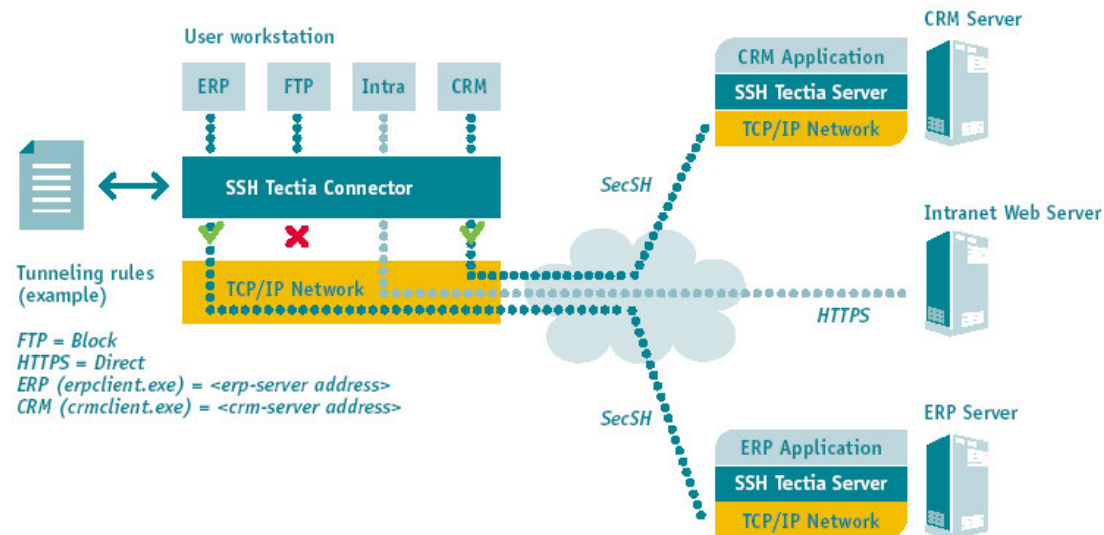
Secure Shell for System Administration

- Typical system administration operations require high admin privileges
 - Remote command execution, installation, etc
- Use of legacy tools like telnet and rlogin is a major risk
 - Passwords are sent as plain-text
- As a result, Secure Shell has become the de-facto standard for end-to-end secure system administration



Evolution towards Business Application Protection

- Once system administration is secured, new security needs arise
 - How to ensure confidentiality of personal health data, consumers' financial data, insider information etc
 - Due to deperimeterization strong end-to-end protection is needed
- SSH Tectia Secure Application Connectivity provides transparent security for applications
 - Supports legacy client/server applications, commercial applications
- SSH Tectia Secure File Transfer provides security for file transfer applications



Secure Application Connectivity

- Overcomes the limitations of other communications security approaches
 - Adaptability, no need to re-engineer business applications or IT infrastructure
 - Invisible to the users
 - Enables centralized management, policy enforcement and monitoring
 - Can be implemented across the enterprise also in heterogeneous client/server application environments using Secure Shell
 - Wide platform support from Windows workstations to Unix servers and IBM zSeries mainframes



Secure File Transfer

- Can be applied to an existing file transfer system
- Can be used as a building block for a completely new system
- Command line tools can be used from scripts
- Programming API is provided for implementation of secure plug-in replacements of legacy tools
- Wide platform support
- High performance



Summary

- In order to deliver security, relevant risks need to be charted first
 - Security can only be implemented after the security policy exists
- Perimeter is disappearing
 - Internal network cannot be trusted any more
 - Perimeter security alone is not enough, end-to-end security needed
- Lack of communications security in LAN creates business risks
 - Deperimeterization puts internal network at risk
 - Easy to eavesdrop application data, hijack connections, collect passwords, etc
 - Regulation compliance doesn't allow unrestricted access even for "trusted insiders"
- SSH Tectia – cost-effective security
 - Centrally managed end-to-end protection for system administration, application connectivity, and file transfer





SSH | Original Secure Shell
10 Years 1995 – 2005

Questions?



SSH | Original Secure Shell
10 Years 1995 – 2005

Thank You

timo.rinne@ssh.com