



IBM Systems and Technology Group University 2005

IBM Systems and Technology Group University 2005

San Diego, California
January 16 - 19, 2005





IBM Systems and Technology Group University 2005

Security: The Technology

Course #: CB33

Steven Bade
STG Security Architect



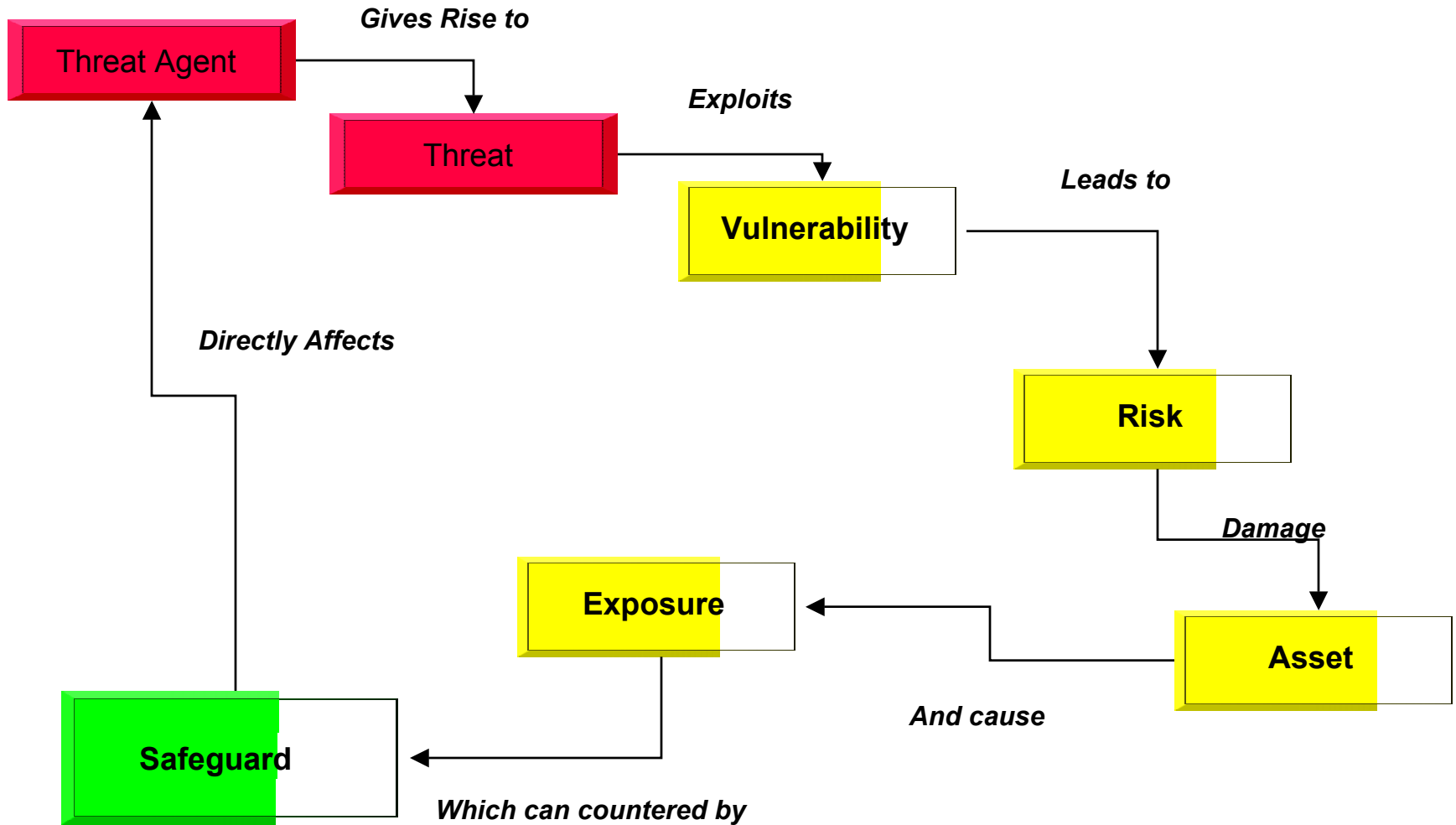
Section Goals

- **Provide primer on Security**
 - Enable you to understand basic security principles in a non-technological view.
- **Review IBM technologies that support security principles**
- **Solicit field feedback**

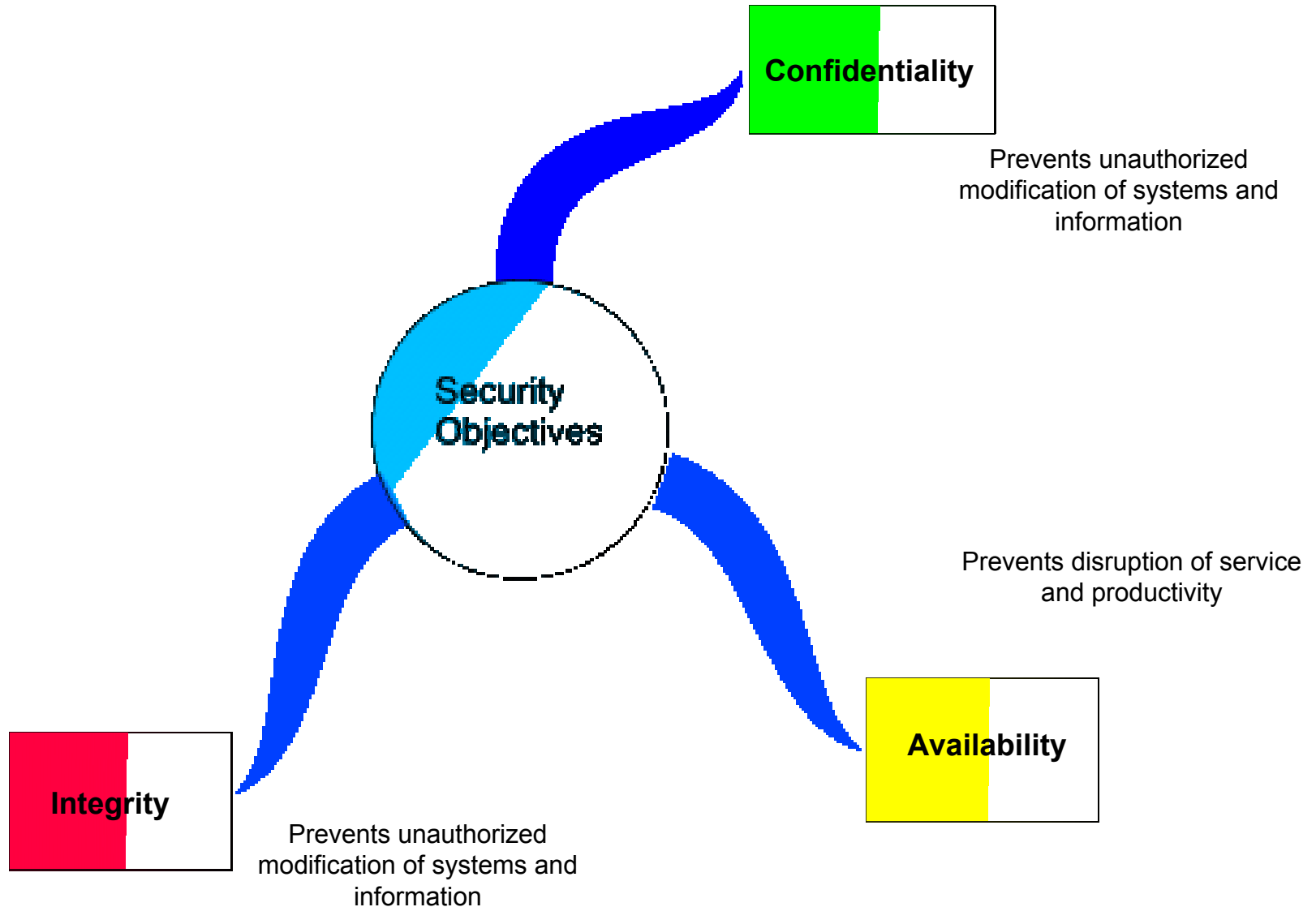
Common Terms Used

- **Vulnerability**
 - Absence or weakness of a safeguard that could be exploited
- **Threat**
 - Any potential danger to a computer, network or data
- **Risk**
 - Probability of a threat agent exploiting a vulnerability and the potential loss from that action
- **Exposure**
 - Instance of being exposed to losses from a thread
- **Countermeasure/Safeguard**
 - Mechanisms used to mitigate the potential risk
- **Assurance**
 - Confidence that a computer system meets its security requirements

Security is a Process



Security Objectives



Confidentiality



- **Supported through**
 - Access Controls
 - Authentication/Authorization
 - Encryption
 - Network segmentation
 - Firewalls, packet filters

Integrity



- **Supported through**
 - Digital Signatures
 - Network Security Protocols
 - Auditing
 - Intrusion Defense

Availability

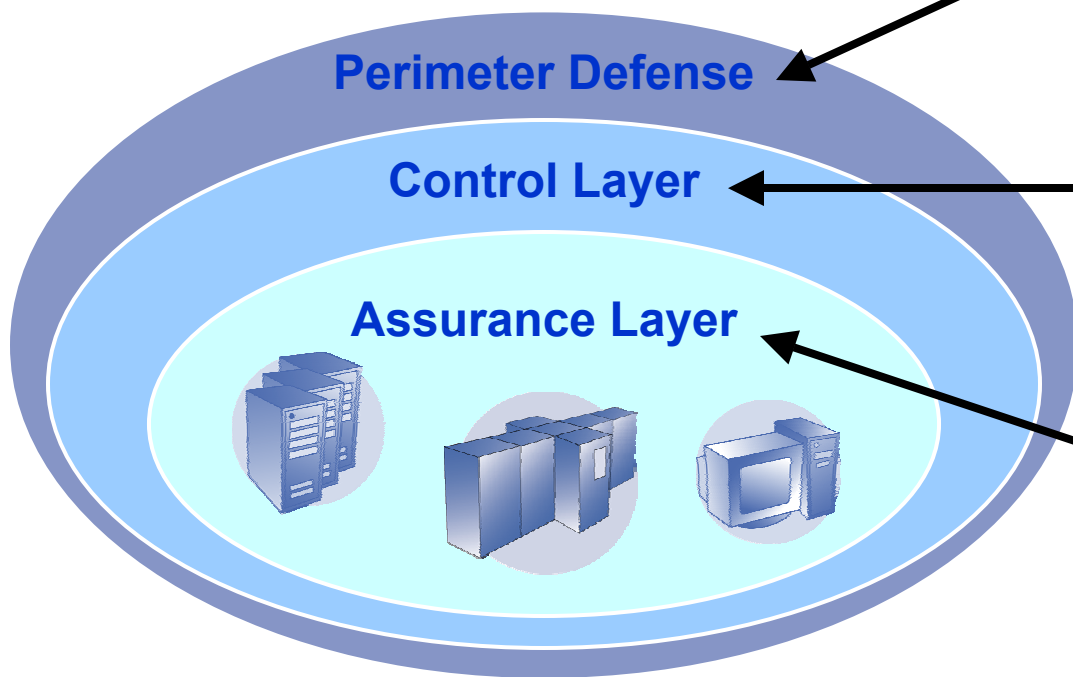


Availability

- **Supported Through**
 - Intrusion Defense
 - Auditing
 - LPAR
 - Firewalls, Routers, Packet filtering

Organizations Need More Than Just Perimeter Defense

IBM solutions provide management for all three layers



Perimeter Defense

Keep out unwanted with

- Firewalls
- Anti-Virus
- Intrusion Detection, etc.

Control Layer

- Which users can come in?
- What can users see and do?
- Are user preferences supported?
- Can user privacy be protected?

Assurance Layer

- Can I comply with regulations?
- Can I deliver audit reports?
- Am I at risk?
- Can I respond to security events?

Security Principles

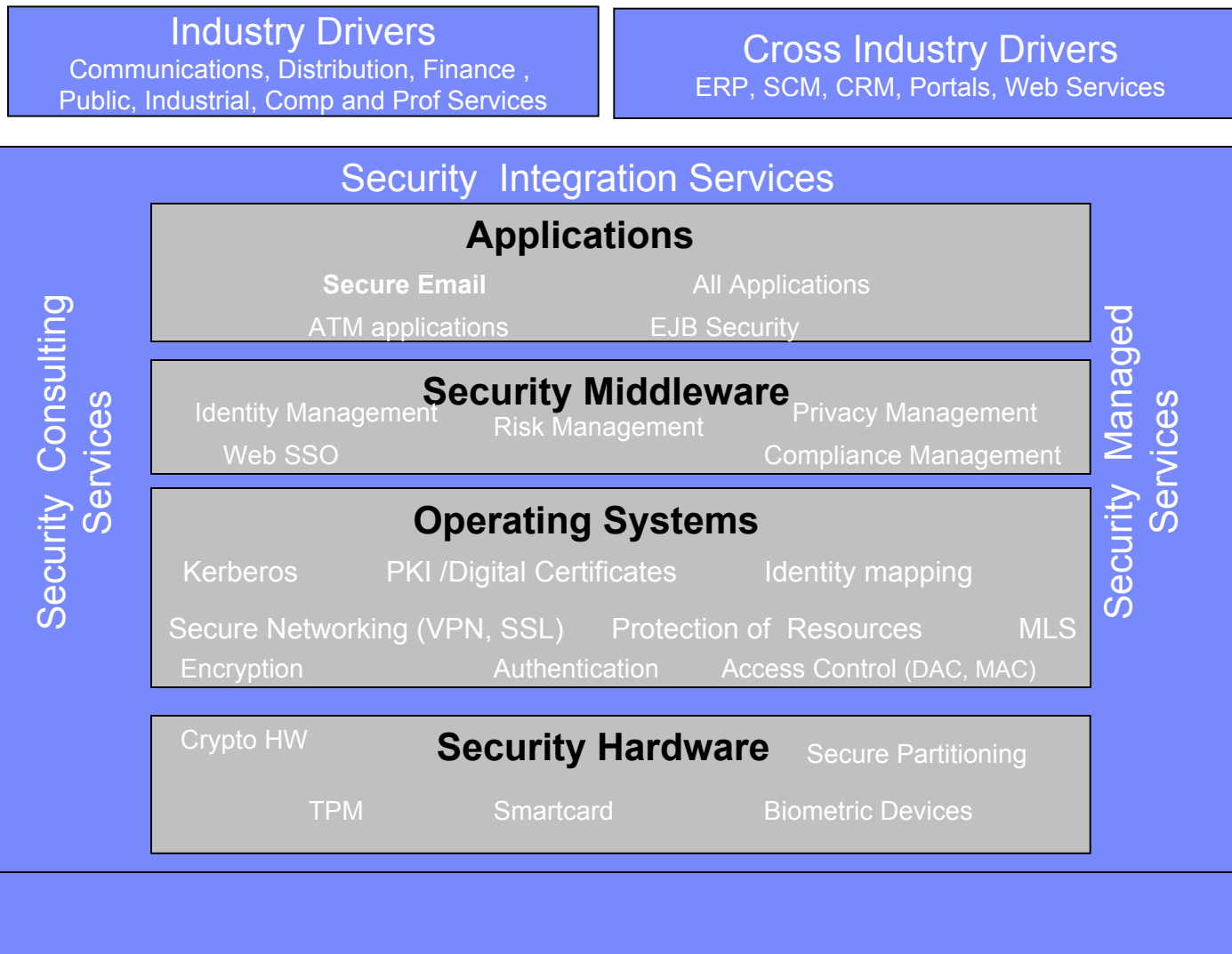
■ **Defense in Depth**

- Physical Security
- Systems Security
- Operating Systems Security
- Middleware Security
- Application Security
- Layering of Networks (multiple Zones)

■ **Least Privilege**

- Separation of Duties
- No single point of control

Common Architecture of Security Landscape



Security elements for the on demand business

Business Controls, Risk Management & Security Governance

Security Management

Identity & Access Control

Data Protection & Disclosure Control

Secure Transactions

Secure Systems & Networks

“In security, the best defense is a good offense, and the more proactive you can be, the more secure you will be,” *Vic Wheatman, Gartner*

Source: Gartner, Inc., The Future of Enterprise Security September 2004

Securing Systems

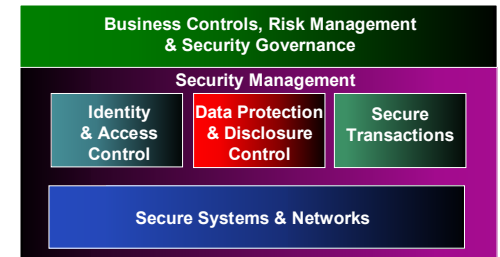
■ Isolation

– LPAR

- zSeries
 - PR/SM – Common Criteria Evaluated EAL5+
 - zVM -
- p/i Series – pHype

■ Data Protection

- Hardware Cryptography support
 - zSeries, iSeries – Common Cryptographic Architecture (CCA)
 - pSeries - (CCA and PKCS#11)
- Trusted Platform Module
 - xSeries – 2005 Statement of Direction
 - Thinkpads and Desktops
- Biometric Devices
 - Integrated Fingerprint Reader – Think Pad



Integrity Based Platforms

Kerberos

Integrated H/W Crypto

- DES, TDES, RSA and more
- FIPS 140-1 Level 4 certified
- Tamper Resistant
- TPM on X- Series

WEB Security

- SSL
- Digital Certificates

Tivoli Security Management

Local Security

- Access Control - RACF
- Auditing

SSL API's

Virtual Private Network

- IKE support



Linux

- Common Criteria – EAL4
- Trusted Computing
- Encryption
- More . . .

Enterprise Identity mapping

Embedded Directory - LDAP

Storage

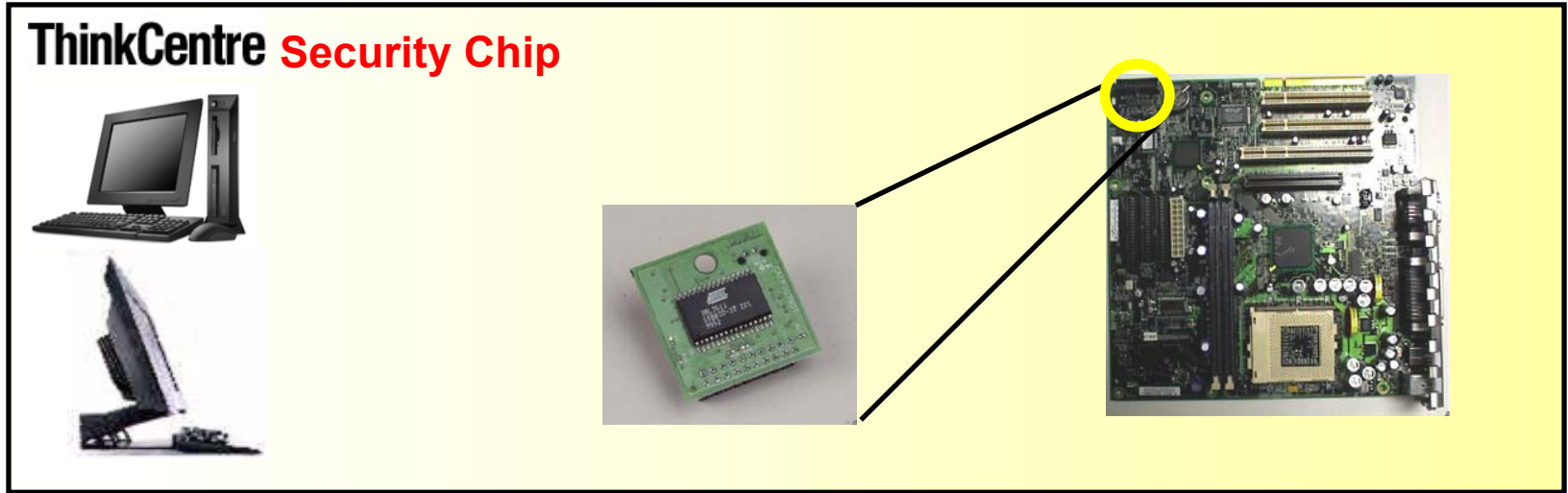
LUN Masking

Server Intrusion Detection

- TCP/IP (z)
- Signed O/S (p, i)
- Connect to Tivoli's Risk Manager (future - z, i)

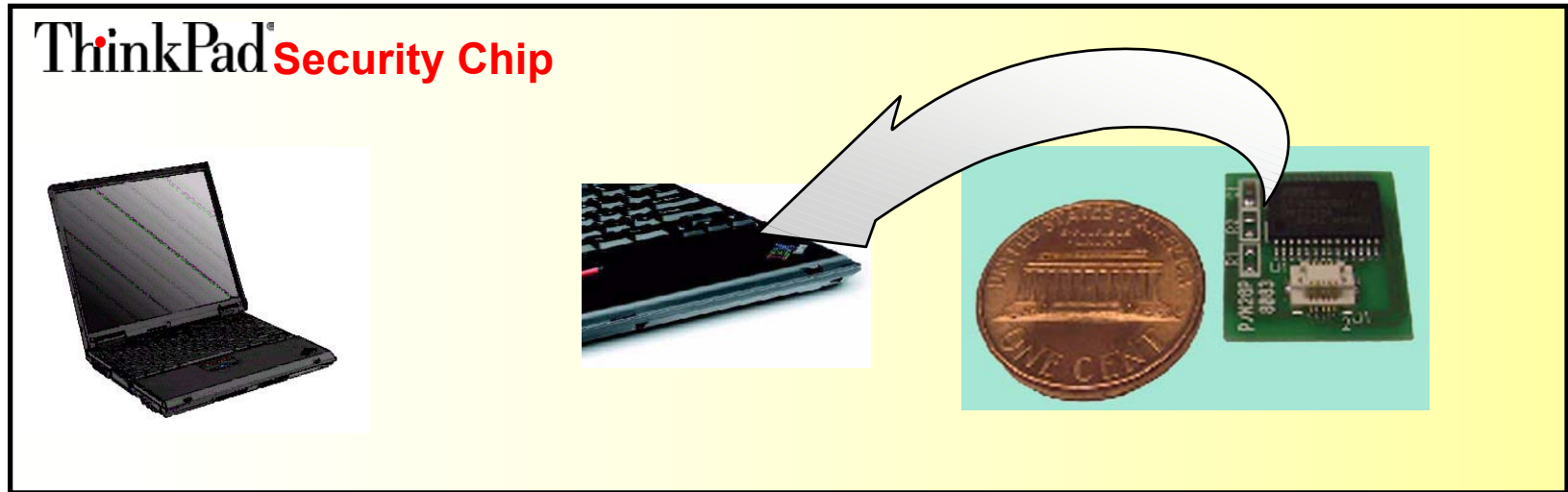
The Embedded Security Subsystem – First shipped Sep. 1999

ThinkCentre Security Chip



This section illustrates the ThinkCentre Security Chip. On the left, there are two images of a desktop computer system: a monitor, keyboard, and tower unit, and a laptop. In the center, a green printed circuit board (PCB) is shown with a black security chip mounted on it. On the right, a larger image of a computer motherboard is shown, with a yellow circle highlighting the location of the security chip. Two black lines connect the corners of the green PCB to the highlighted area on the motherboard.

ThinkPad Security Chip



This section illustrates the ThinkPad Security Chip. On the left, there is an image of an open ThinkPad laptop. In the center, there is an image of the laptop's keyboard area with a small security chip located near the bottom right corner. A large, white, curved arrow points from the keyboard area towards the right. On the right, there is a close-up image of the security chip next to a US quarter coin for scale. The chip is green and has a black square chip mounted on it. The coin is a US quarter, showing the Lincoln Memorial on the reverse side.

IBM ThinkPad with Biometric Security

Secure Systems & Networks

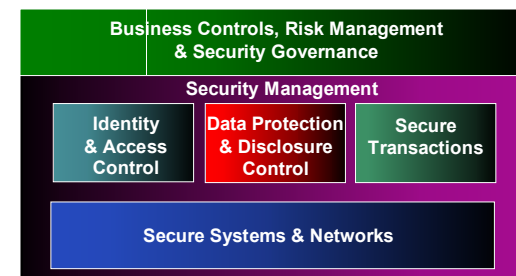
- Fingerprint Reader
 - replace typing in all your passwords.
- Password Manager
 - banks all your passwords.
- Security Chip
 - stores the passwords and encrypts VPN communication
- Cisco and Tivoli support
 - Integration with Enterprise management systems



All these security features on the award-winning ThinkPad T42 notebook computer

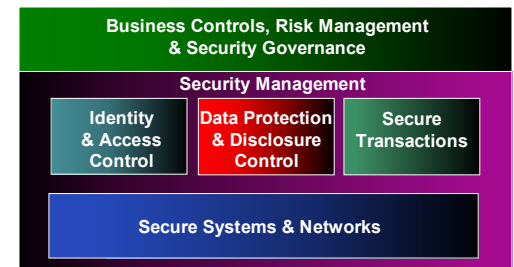
Securing Networks

- **VPN**
 - IP Security (ipsec) – AIX, Linux, zOS, i5OS – NATIVE
- **Kerberos**
 - Native – AIX, Linux, zOS, i5OS
- **SSL**
 - Applications enabled through toolkits
 - zOS, i5OS – Native APIs
 - AIX GSKIT (SWG Products)
 - Linux – openSSL
- **NFS v4 Security**
 - AIX – First operating system to support NFS v4 ACL's
- **Firewall**
 - All OS's provide integrated firewall capabilities
- **Network Intrusion Defense**
 - zOS Communications Manager ID
 - AIX pattern matching ID engine
 - Linux – SNORT leading ID technology
- **Web Services**
 - WS-Security -



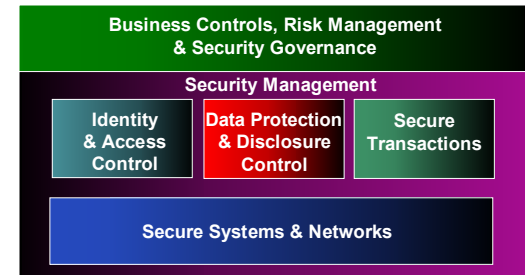
Identity Authentication and Access Control

- **PKI/Digital Certificates**
 - Supported for Identity on AIX, i5OS and zOS
- **Centralized Identity**
 - RACF – zOS
 - LDAP based ID management – AIX, i5OS, Linux
 - Tivoli Identity Manager – All platforms
 - Radius – AIX, Linux – distributed Authentication
- **Access Control Lists**
 - RACF – zOS
 - AIX – AIXC and NFSv4 types
 - Tivoli Access Manager – Cross Platform Centralized Access Control
 - Linux - Supported on All common file systems



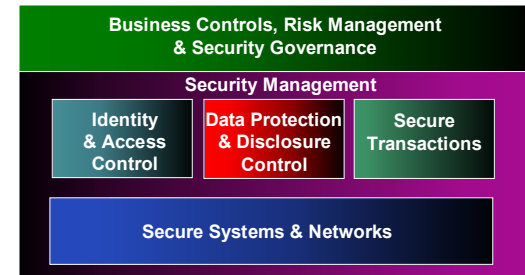
Secure Transactions

- **MQ Series**
- **Service Oriented Architectures**
 - WS-Security, VPN, SSL all enable security in SOA's



Data Protection and Disclosure Control

- **Labeled Security**
 - zOS and DB2
 - AIX
 - Linux – SE Linux LSM
- **Privacy Manager**
- **Monitoring and Reporting tools (what to say here)**
- **Tivoli Security Compliance Manager**
 - Enables cross platform policy conformance
 - Integration with business processes
- **Sentry**
 - Joint effort with CISCO
- **Cryptography**
 - Hardware Crypto capabilities
 - Software Cryptographic libraries on all platforms
 - Java Cryptographic



STG Security Features – Across Servers

- Enterprise Identity Mapping:
 - Associate single system user with many system registries
 - Available across platforms: z/OS, AIX, Linux, OS/400
- PKI Authentication
 - foundation for secure electronic commerce
 - Available across platforms: z/OS, AIX, Linux, OS/400
- Kerberos Network Authentication
 - client/server network authentication
 - Available across platforms
- Pluggable Authentication
- LPAR – Separation of function
- VPN

STG Security Features – Across Our Servers

- Common Criteria – provides assurance level for security
 - International common criteria for IT security
 - Third part evaluation of security against a protection profile
 - Controlled Access Protection Profile (CAPP)
 - Labeled Security Protection Profile (LSPP)
 - Multi-Level Security (MLS)
- Common Criteria is a government requirement; other industries are looking to adopt

| Operating Environment | 2004 Evaluation | 2005 Planned Evaluation |
|-------------------------|------------------------|-------------------------|
| AIX 5.2 AIX 5.2B | CAPP/EAL4 | LSPP/EAL4 with Argus |
| Linux on x, i, p, and z | CAPP/EAL3+ | LSPP/EAL4 |
| i5OS | | CAPP/EAL4+ |
| z/OS 1.6 | CAPP/EAL3 LSPP/EAL3 | CAPP/EAL4 LSPP/EAL4 |
| zVM | CAPP/EAL3+ | |
| pSeries LPAR | EAL4+ | |
| zSeries LPAR/PRSM | EAL5 | EAL5 |

STG Security -- zSeries

- Multi-level security (MLS)
 - on z/OS with DB2
 - labeled security allows sharing of resources with mixed level of security in single image
- Discretionary Access Control
 - Restricting access to objects based on identity of users or groups
 - RACF – over 25 years of providing system integrity
- Public Key Infrastructure (PKI) Services
 - z/OS can issue and manage their own digital certificates
- Cryptography through tamper resistant hardware encryption
- Secure Sockets Layer (SSL)
- Embedded self-healing and self-protecting system security:
 - Real time diagnostics
 - EAL5 secure system partitioning
 - Intrusion detection
 - Dedicated cryptographic processors

STG Security -- pSeries

- Tivoli security-ready client and agent software pre-installed on POWER
- AIXL security:
 - Network Intrusion detection
 - Secure Shell
- Advanced Access controls
 - Local and Distributed User management
 - LDAP, NIS, NIS+
- Radius
- LPAR – Secure virtualization

STG Security -- iSeries

- Single sign-on with i5OS via EIM and Kerberos
- Integrated user and password management between Windows and i5OS
- Built-in operating system security:
 - Integrated files systems promotes virus resistance
- Cryptography through tamper resistant hardware
- Monitoring of entire operating system to detect unauthorized changes; also provides host base firewall and IP filtering

STG Security -- xSeries

- Enhanced authentication with Trusted Platform Module
 - ***Statement of Direction – this may change at any time.***
 - Planned on 4-way xSeries systems
 - Data protection to protect documents, files, applications
- Secure Remote Administration
 - Manage servers from any place at any time over secure link
 - Monitoring of servers across secure link
 - Automated and policy driven via IBM Director
- Enhanced System Health:
 - Dynamically measure, store and report system health

STG Security – Linux on all Servers

- Open standards based security
 - LDAP, Secure Shell, ...
 - openSSL
 - Intrusion Detection: Network Intrusion Detection Systems, Host Intrusion Detection Systems, Remote Scan, System Hardening
- Network Packet Filtering
- IPSEcurity
- IBM Business Partners offer security solutions for anti-virus and firewall protection

STG Security – Storage

- Security features:
 - LUN Masking
 - Automatic administrator notifications to unauthorized changes
 - No switch software/firmware
 - Switch Zoning
- IBM TotalStorage Resiliency Family
 - high performance data sharing accessing SAN-attached storage
 - common file system with single global namespace
 - embedded capabilities to protect unauthorized access
 - Password protection
 - Privileged service access
- Tape:
 - Write Once Read Many (Worm) cannot be altered

- Data Retention 450
 - Enable management of data that has no explicit retention period
 - Multiple tiers of storage
 - Protect explicit data deletion before retention criteria expiration
- Enterprise Storage Server (Shark)
 - Password protection
 - All unnecessary software daemons disabled
 - Hardened against customer data transmitted over service channels
 - No web servers run on root
 - Non-authenticated access using expiring account

Reference Links

- **RACF** <http://www-1.ibm.com/servers/eserver/zseries/zos/racf/>
- **AIX** <http://webevents.broadcast.com/ibm/developer/120204/index.asp?loc=100>
- **I5os** <http://publib.boulder.ibm.com/infocenter/iserics/v5r3/ic2924/index.htm>
- **Tivoli Identity Manager** <http://www-3.ibm.com/software/tivoli/products/identity-mgr/>
- **Tivoli Access Manager** <http://www-3.ibm.com/software/tivoli/products/access-mgr-e-bus/>
 - <http://www-3.ibm.com/software/tivoli/products/access-mgr-bus-integration/>
 - <http://www-306.ibm.com/software/tivoli/products/access-mgr-operating-sys/>
- **Tivoli Privacy Manager** <http://www-3.ibm.com/software/tivoli/products/privacy-mgr-e-bus/>
- **Tivoli Security Compliance Manager**
 - <http://www-3.ibm.com/software/tivoli/products/security-compliance-mgr/>
- **Tivoli Risk Manager** <http://www-3.ibm.com/software/tivoli/products/risk-mgr/>
- **IBM Tivoli Directory Server**
 - <http://www-3.ibm.com/software/tivoli/products/directory-server/>
- **IBM Tivoli Directory Integrator**
 - <http://www-3.ibm.com/software/tivoli/products/directory-integrator/>

Open Forum

- **What HOLES do you feel exist?**
- **What technically would you like for us to be doing to HELP you?**

Trademarks

The following are trademarks of the International Business Machines Corporation in the United States and/or other countries. For a complete list of IBM Trademarks, see www.ibm.com/legal/copytrade.shtml: AS/400, DBE, e-business logo, ESCO, eServer, FICON, IBM, IBM Logo, iSeries, MVS, OS/390, pSeries, RS/6000, S/30, VM/ESA, VSE/ESA, Websphere, xSeries, z/OS, zSeries, z/VM

The following are trademarks or registered trademarks of other companies

Lotus, Notes, and Domino are trademarks or registered trademarks of Lotus Development Corporation

Java and all Java-related trademarks and logos are trademarks of Sun Microsystems, Inc., in the United States and other countries

LINUX is a registered trademark of Linux Torvalds

UNIX is a registered trademark of The Open Group in the United States and other countries.

Microsoft, Windows and Windows NT are registered trademarks of Microsoft Corporation.

SET and Secure Electronic Transaction are trademarks owned by SET Secure Electronic Transaction LLC.

Intel is a registered trademark of Intel Corporation

* All other products may be trademarks or registered trademarks of their respective companies.

NOTES:

Performance is in Internal Throughput Rate (ITR) ratio based on measurements and projections using standard IBM benchmarks in a controlled environment. The actual throughput that any user will experience will vary depending upon considerations such as the amount of multiprogramming in the user's job stream, the I/O configuration, the storage configuration, and the workload processed. Therefore, no assurance can be given that an individual user will achieve throughput improvements equivalent to the performance ratios stated here.

IBM hardware products are manufactured from new parts, or new and serviceable used parts. Regardless, our warranty terms apply.

All customer examples cited or described in this presentation are presented as illustrations of the manner in which some customers have used IBM products and the results they may have achieved. Actual environmental costs and performance characteristics will vary depending on individual customer configurations and conditions.

This publication was produced in the United States. IBM may not offer the products, services or features discussed in this document in other countries, and the information may be subject to change without notice. Consult your local IBM business contact for information on the product or services available in your area.

All statements regarding IBM's future direction and intent are subject to change or withdrawal without notice, and represent goals and objectives only.

Information about non-IBM products is obtained from the manufacturers of those products or their published announcements. IBM has not tested those products and cannot confirm the performance, compatibility, or any other claims related to non-IBM products. Questions on the capabilities of non-IBM products should be addressed to the suppliers of those products.

Prices subject to change without notice. Contact your IBM representative or Business Partner for the most current pricing in your geography.

References in this document to IBM products or services do not imply that IBM intends to make them available in every country.

Any proposed use of claims in this presentation outside of the United States must be reviewed by local IBM country counsel prior to such use.

The information could include technical inaccuracies or typographical errors. Changes are periodically made to the information herein; these changes will be incorporated in new editions of the publication. IBM may make improvements and/or changes in the product(s) and/or the program(s) described in this publication at any time without notice.

Any references in this information to non-IBM Web sites are provided for convenience only and do not in any manner serve as an endorsement of those Web sites. The materials at those Web sites are not part of the materials for this IBM product and use of those Web sites is at your own risk.