SYBASE

TECHWAVE

SYMPOSIUM 2009

Security Considerations for Mobile Applications

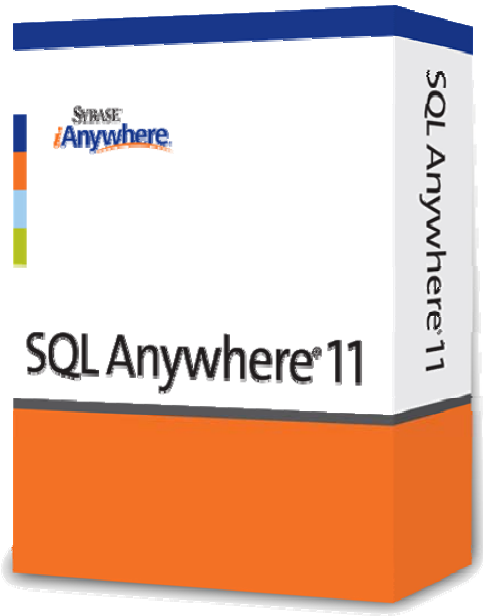
Joshua Savill

Product Manager

August 27th, 2009

AGENDA

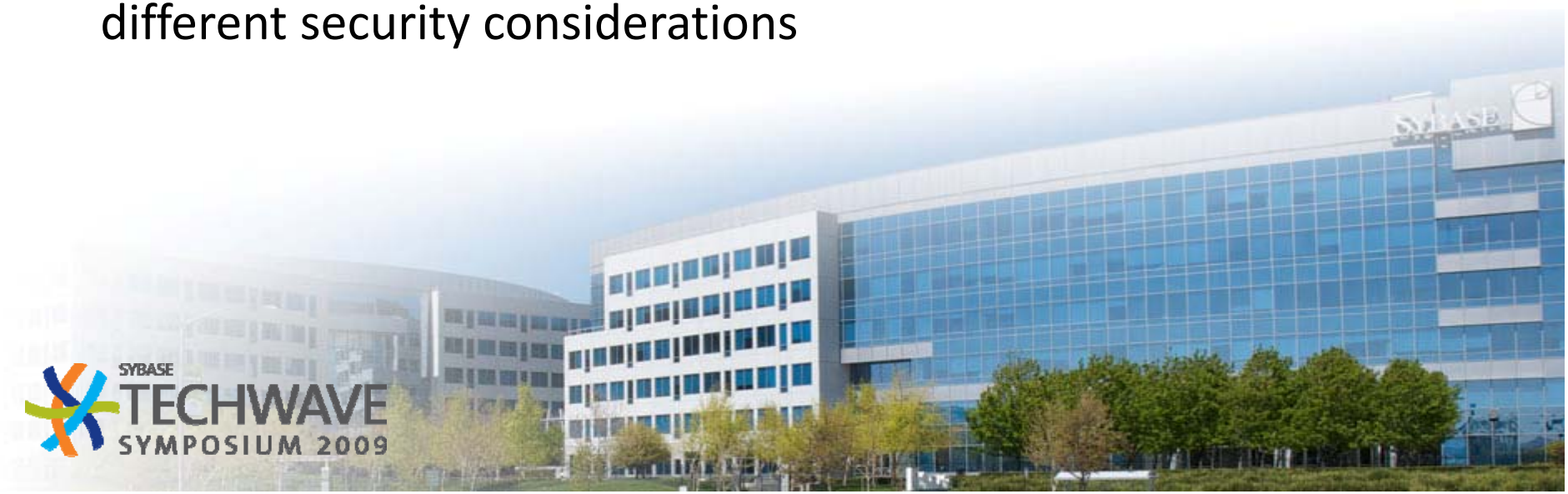
- Introduction to data security
- Consideration for synchronizing data outside the data center
- Steps to implement secure data synchronization environments



SYBASE TECHWAVE SYMPOSIUM 2009

PRESENTATION GOALS

- Provide an understanding of the various types of security options available with SQL Anywhere
- Understanding the considerations for different security options for securing data synchronization
- Gain knowledge of the various moving pieces in a MobiLink synchronization environment and how each piece requires different security considerations



VALUE OF SECURITY

Is there a need to secure a mobile application?

- Information is a key business commodity
  - Lost data = lost productivity = lost revenue
- Risk of data breaches are real
- Not securing and protecting data privacy has consequences
  - Time
  - Legal
  - Opportunities
  - Credibility

VALUE OF SECURITY

US Government and state regulations regarding data security and privacy

- **Federal privacy laws:**
  - HIPAA (health information)
  - Gramm-Leach-Bliley (financial information)
  - Fair Credit Reporting Act
  - Children's Online Privacy Act
  - FERPA (student records)
  - FTC regulations regarding consumer information
  - Additional legislation pending for general protection of private information…
- **State privacy laws include protections for**
  - Breach notification required: 39 states
  - Citizen information, e.g., California, New York
  - Health records
  - Social Security Numbers
  - Genetic information; HIV status
  - Video rentals; library borrowing
  - Bank records
  - Cable viewing
  - Polygraphs
  - Employment records

RECENT SECURITY BREACHES

DATE MADE PUBLIC	NAME	TYPE OF BREACH	RECORDS
06-Jan-2009	CheckFree Corp	Electronic bill payment service taken over by criminals and redirected to a site in the Ukraine.	5 million people
20-Jan-2009	Heartland Payment Systems	Malicious software compromised credit card data that crossed the network (lawsuit pending).	100 million transactions per month
9-Feb-2009	Federal Aviation Administration	Current and former employee names, Social Security numbers and other personal information were stolen.	43,000 people
11-Apr-2009	Peninsula Orthopaedic Associates	Patient information was stolen while being transported to offsite storage.	100,000 people

* Privacy Rights Clearinghouse – privacyrights.org

SECURITY AND PERFORMANCE

Implementing secure adds overhead to application performance

- Benchmark
  - The only true way to determine the affects of security in your environment is to benchmark your application and synchronization
- Determine the level of security required for your business needs
  - Business plan
  - Consult with security experts

SECURITY AND PERFORMANCE

Implementing secure adds overhead to application performance

- Database
  - Time required to encrypt/decrypt data for file I/O
  - Cost of auditing
  - Time required to encrypt/decrypt communication data
- Network
  - Time required to encrypt/decrypt network communication
  - Processing time on intermediaries
  - Network authentication processing time
- Enterprise components
  - Authentication and validation time

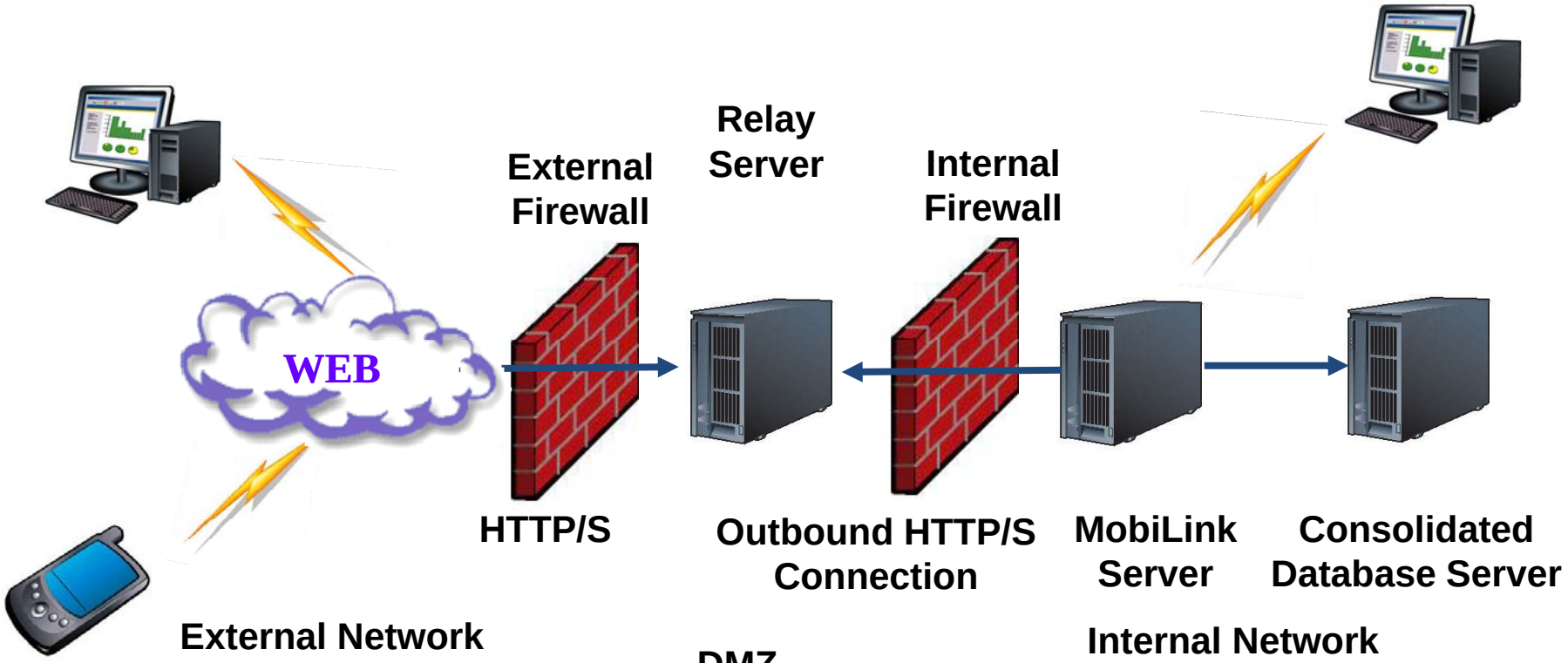
BUILDING SECURITY

How are we going to build secure mobile applications?

- Enterprise data center security
  - Data storage and security
  - IT policies and procedures
- DMZ and internal network security
  - Intermediary security
  - Internal data transfer
- Data transmission from device to middleware
  - Network security
  - Data transfer
- Mobile devices and laptops
  - Security of devices and laptops
  - Security of data
  - IT policies and procedures

MOBILE APPLICATION VULNERABILITY

Where do security risks exist in a MobiLink synchronization environment?



SECURITY RISKS

Enterprise data security risk

- Physical theft of the machine or breach of the data center
- Environmental disasters
  - Floods, fire, earth quakes, explosions
- Security circumvention
  - External drives, USB keys, DVDs, Tapes
  - Social engineering, password hacking
- Unauthorized machine and database access via network
- Unauthorized and insecure access via:
  - Insecure Web service calls
  - Insecure APIs
  - Default User IDs and passwords

SECURITY RISKS

Enterprise data security risk

- Hacking
  - SQL Injections
  - Cross-site scripting (XSS)
  - Cracked passwords
  - Internal access/backdoors
    - Key loggers
  - Malicious software
  - Buffer overflows

SECURING THE DATA CENTER

Physical access to the data center

- Software security is ineffective if access to the physical machine is available
  - Store data center machines in a physically secure location
    - Require specific entry credentials to data center
    - Audit entry to environment
    - Surveillance and security
    - Prohibit food and drinks in the data center
- Protect against environmental conditions
  - Fire detection and suppression systems
  - Geographical data centers
    - Redundancy systems and data transfer

SECURING THE DATA CENTER

Securing the data center machines

- Leverage IT policies and procedures
  - Educate administrators on policies and expectations
  - Provide consequences for failing to abide by policies and procedures
- Ensure all machines in the data center run the latest security patches and software
- Ensure all physical upgrades to data center machines are done based on IT policies and procedures
- Avoid running unnecessary services or daemons on machines in the data center
  - Shutdown ftp, telnet, remote desktop, etc…
- Monitor and control all access and user accounts with access to the data center

SECURING THE DATA CENTER

Securing access to database and data center machines

- Password policies
  - Change the default DBA password
  - No passwords in ODBC Data Source Name
  - Implement password creation policy
    - Minimum password length
      - Controllable via database option min_password_length
    - Password expiration
      - Use the verify_password_function to facilitate
    - Password generation rules
      - No dictionary words
      - Mix of numbers, digits, special characters, etc…
      - Use the verify_password_function to facilitate
- Enforce password policies on machines in the data center

SECURING THE DATA CENTER

Securing the MobiLink server

- Authentication
  - Built-in user authentication
    - User name exists in ml_user table
    - Do not use –zu+ in production
  - Custom authentication
    - authenticate_user script to build custom authentication
      - Authenticate user with external enterprise server
- User ID and password (not the same as database)
  - Ensure each user has a unique MobiLink user ID and password
- No verbose logging
  - Keep logging to a minimal and only when debugging issues

SECURING THE DATA CENTER

Securing the consolidated database

- Database permissions to prevent:
  - Unauthorized user access
  - Accessing system during inactivity
  - Hacking of users and passwords
  - Access to non-authorized objects
  - Viewing of non-encrypted data
- User account and permissions
  - Enforce password policies
  - Create login policies (if supported)
    - E.g. maximum failed login attempts, password life time/expiry
  - Integrated login (if supported)

SECURING THE DATA CENTER

Securing the consolidated database

- User accounts
  - Use groups to consolidate and control permissions
  - Use unique user IDs to control specific user permissions
  - Restrict DBA authority
  - Require permissions to start/stop databases on the server
  - Prevent creation of new databases on a server
  - Limit access to bulk data unload statements
  - Use specific user permissions for specific operations – BACKUP, VALIDATE
  - Make use of the REVOKE statement
  - Disable unnecessary users

SECURING THE DATA CENTER

Securing the consolidated database

- Disable unused database features
  - Some features require access to the network and file system
    - Notifications
    - Data import
    - cmdshell activities
  - Features to be leery of if not required
    - Server-side and client-side backups
    - External stored procedures
    - Remote data access
    - Web services

SECURING THE DATA CENTER

Securing the consolidated database

- Secure users for accessing database utilities
  - Many utilities require elevated permissions to run
  - Make use of user authority when creating users for utilities
    - E.g. VALIDATE authority, BACKUP authority
- Debugging can reveal information
  - Connection IDs, request information may be logged in plain text
  - Logging requires admin permissions, but users may be able to start a server with logging enabled
  - Delete request logs when debugging is finished
  - Limit the size of the request log

SECURING THE DATA CENTER

Securing the consolidated database

- Monitor database and server access
  - Auditing tracks
    - All login attempts (failed and successful)
    - Timestamps for all events
    - All permissions checks (successful and failed) and associated object information
    - All actions that require DBA authority
  - Audit information for SQL Anywhere is stored in the transaction log
    - Encrypt the database

SECURING THE DATA CENTER

Securing the consolidated database

- Secure all Web services
  - Use HTTPS
    - Authentication is required
    - All http requests are sent in the clear
    - Only provide access to required web service resources
  - Strongly type parameters
    - Validate parameters before being used in SQL statements

SECURING THE DATA CENTER

Securing the consolidated database

- SQL Injection attack prevention
  - Detect and reject escape characters
    - E.g. Quotes, wildcards,
  - Use parameterized queries

```
E.g. "SELECT * FROM Customers WHERE Country =
  @CountryName";SqlCommandcmd = new SqlCommand(
  commandText, conn );cmd.Parameters.Add(
  "@CountryName",countryName );
```

  - Use stored procedures
    - Enforce type checking
    - Disguise functionality

SECURING THE DATA CENTER

Database file encryption and backup

- Encrypt entire database
- Encrypt specific tables
  - Only encrypt tables containing sensitive data
  - Minimize any performance implications
- Encrypt specific values
  - Using built in ENCRYPT() and DECRYPT() type functions
- Embed the key in the application
  - Only prevents average user from finding
- Use an algorithm to derive the key at runtime
  - Based on characteristics specific to each install
  - Protect the algorithm
- Hide the key in the registry
  - Relatively simple to snoop, but deters average users
- Each user has knowledge of the key
  - Every user is responsible for security

SECURING THE DATA CENTER

Database file encryption and backup

- Protecting backups is crucial
  - Same considerations for data center need to be made for physically protecting backups, onsite and offsite
  - Use secure transportation
- Network backup
  - Use encrypted communications

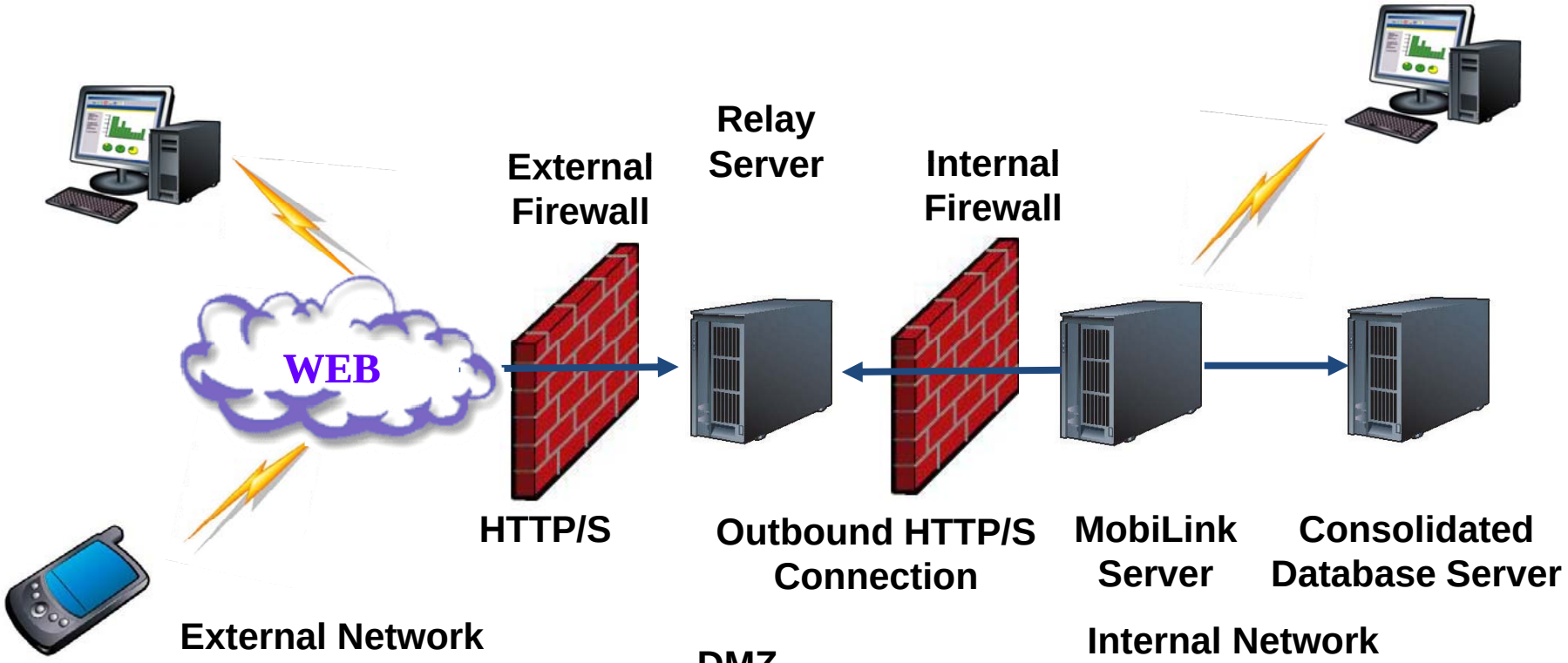
BUILDING SECURITY

How are we going to build secure mobile applications?

- DMZ and internal network security
  - Intermediary security
  - Internal data transfer
- Data transmission from device to middleware
  - Network security
  - Data transfer
- Mobile devices and laptops
  - Security of devices and laptops
  - Security of data
  - IT policies and procedures

MOBILE APPLICATION VULNERABILITY

Where do security risks exist in a MobiLink synchronization environment?



SECURITY RISKS

Intermediary security and internal data transfer

- Database and enterprise application exposure to the Internet
- Unauthorized connections to the internal network
- Internal packet sniffing and interception

SECURING THE DMZ

DMZ security considerations

- Incoming connections should be subject to authentication and validation
  - Any inbound connection should be verified before being allowed to synchronize
- Database server and enterprise applications should not be directly exposed to the Internet
  - Use middleware to force all requests to go through a validation layer
    - Demilitarized zone (DMZ)
- All internal network communications should be secured
  - Internal packet sniffing and interception
    - Transport layer security

SECURING THE DMZ

DMZ security considerations

- Securing the DMZ machines is the same as data center machines
  - Latest security patches
  - Do not run unnecessary services or daemons
  - Monitor and control all access and user accounts
  - Upgrades based on IT policies
  - Enforce password policies

SECURING THE DMZ

DMZ security considerations

- Web server authentication
  - Client-side certificates
    - Use 3rd party management software to ensure all certificates are secure
  - Server-side certificates
    - Use commercial Certificate Authority to issue certificates

SECURING INTERNAL DATA TRANSFER

Internal data transfer security

- Transport layer security
  - RSA, RSA_FIPS 140-2 certified
  - ECC

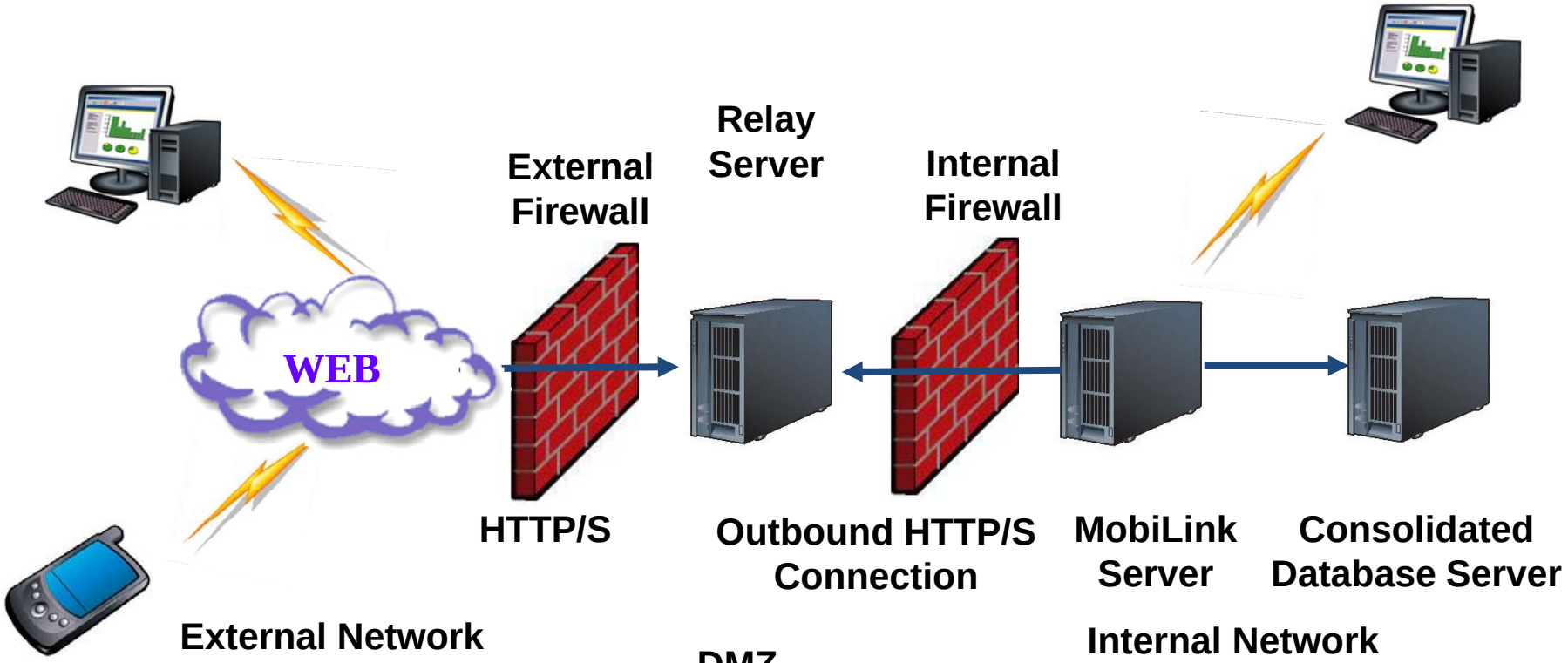
BUILDING SECURITY

How are we going to build secure mobile applications?

- Data transmission from device to middleware
  - Network security
  - Data transfer
- Mobile devices and laptops
  - Security of devices and laptops
  - Security of data
  - IT policies and procedures

MOBILE APPLICATION VULNERABILITY

Where do security risks exist in a MobiLink synchronization environment?



SECURITY RISKS

Data transmission from device to middleware

- Packet sniffing and interception
- Packet and data manipulation

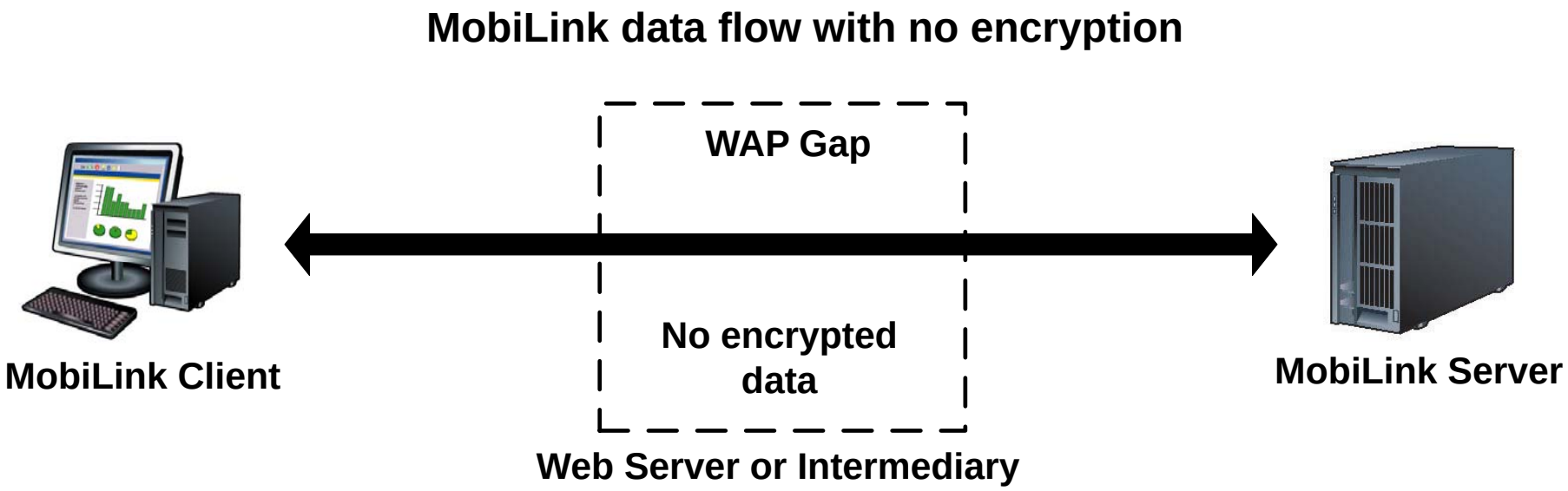
SECURE DATA TRANSFER

Data transfer security available with MobiLink

- Transport layer security
  - RSA, RSA_FIPS 140-2 certified
  - ECC
- Protocol layer security (end-to-end encryption)
  - RSA, RSA_FIPS 140-2 certified
  - ECC
- Virtual private network
  - Tunneled through the transport layer
  - Requires 3rd party software such as Cisco VPN client, Juniper VPN
  - Recommend transport layer and/or protocol layer security with VPN

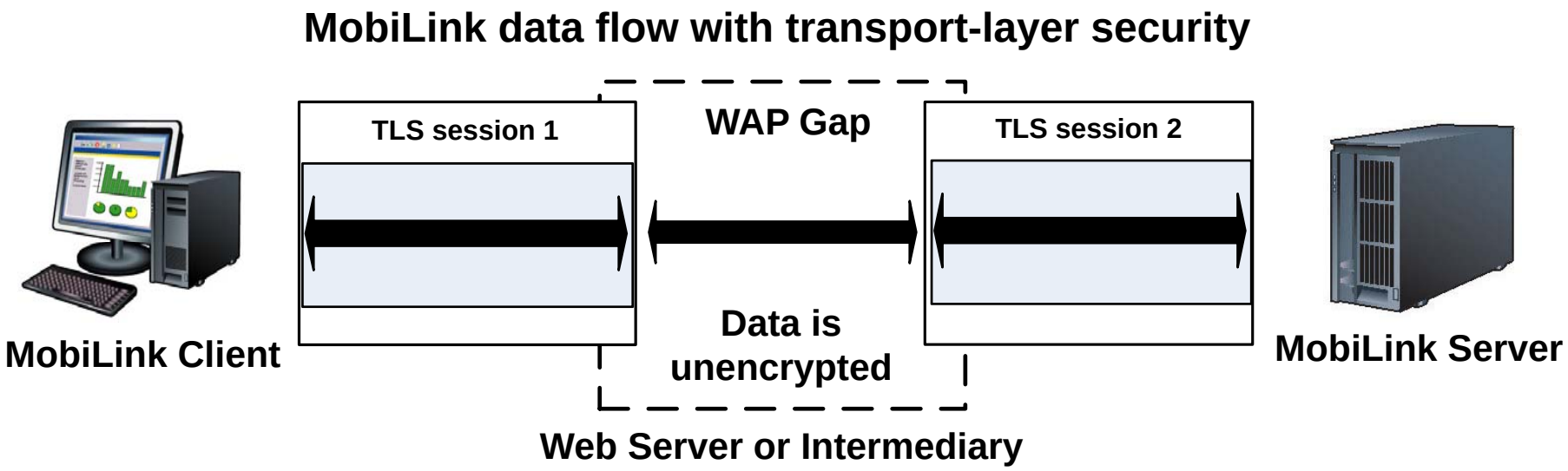
SECURE DATA TRANSFER

No encryption



SECURE DATA TRANSFER

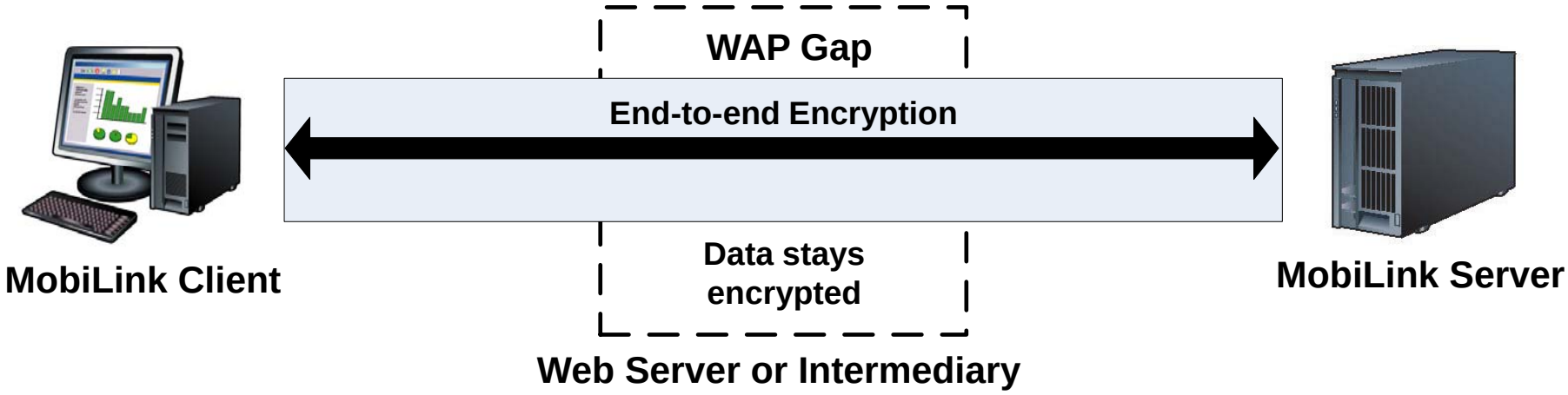
Transport Layer Encryption



SECURE DATA TRANSFER

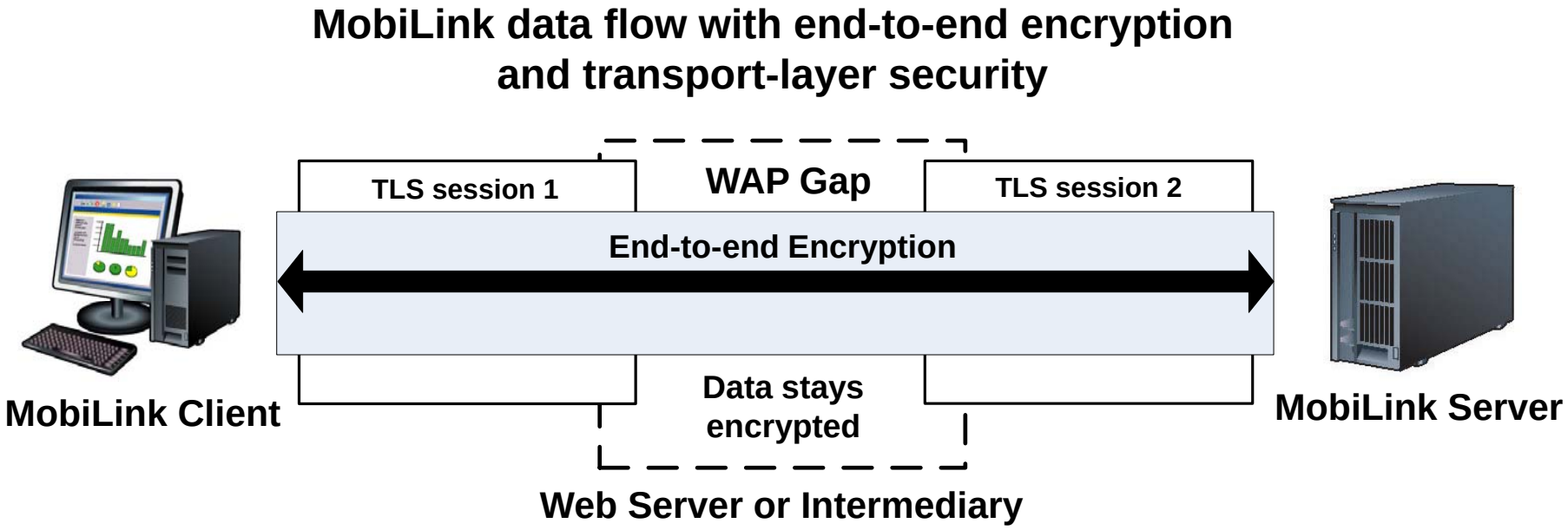
Protocol Layer Encryption

MobiLink data flow with end-to-end encryption



SECURE DATA TRANSFER

Transport Layer and Protocol Layer Encryption



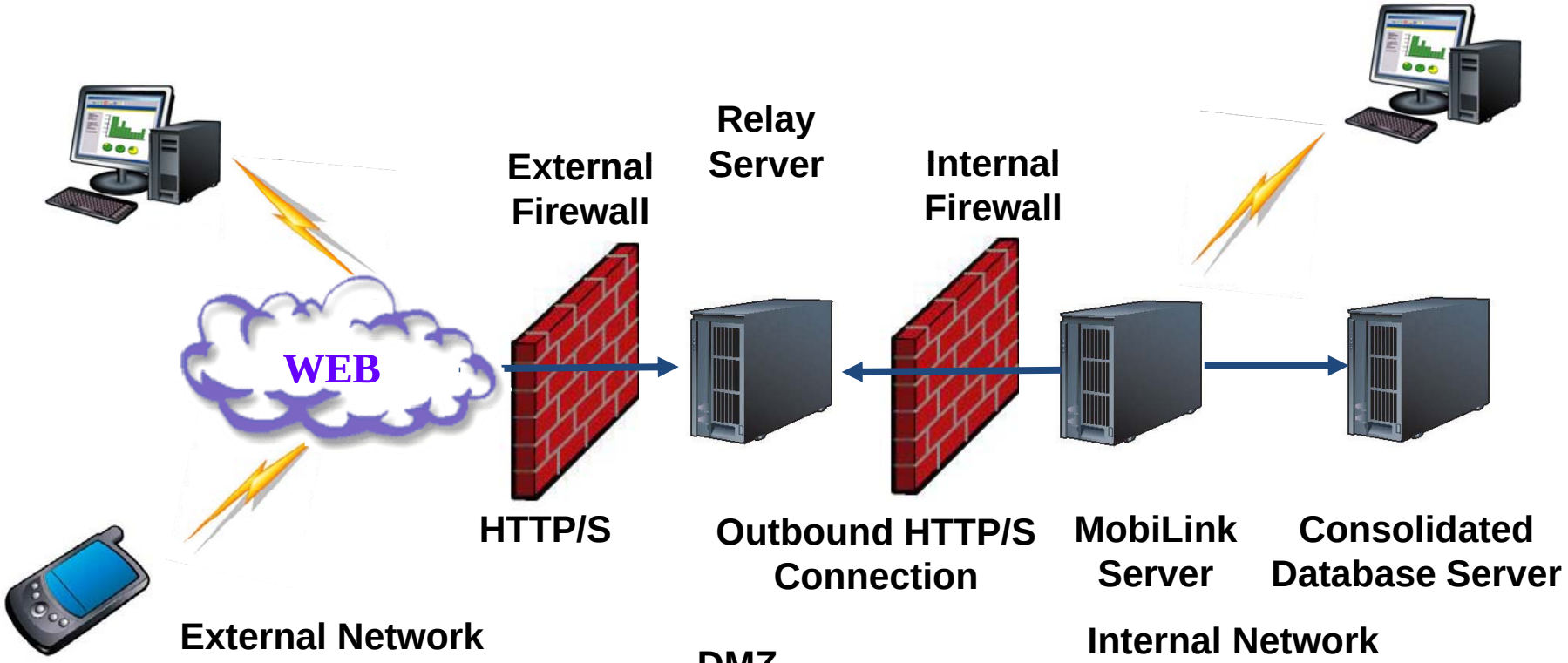
BUILDING SECURITY

How are we going to build secure mobile applications?

- Mobile devices and laptops
  - Security of devices and laptops
  - Security of data
  - IT policies and procedures

MOBILE APPLICATION VULNERABILITY

Where do security risks exist in a MobiLink synchronization environment?



SECURITY RISKS

Device and laptop vulnerabilities

- Theft and lost devices
  - Given enough time and resources all security can be broken
- Attacks against the device
  - Operating system and file system attacks
  - Unapproved and malicious software
- Access security workarounds
  - Via social engineering, password hacking or use of removable media to take data to an uncontrolled environment

SECURITY RISKS

Application and database vulnerabilities on device and laptop

- Database
  - Unauthorized user access
  - Hacking users and passwords
  - Unencrypted database file
- Application
  - Unauthorized user access
  - Hacking users and passwords
  - Unencrypted temporary file storage
  - Insecure code

SECURING PHYSICAL ENTITIES

Securing physical devices and laptops running the mobile application

- Software security can be ineffective if physical access to the device is available
  - Device loss, theft or inappropriate decommissioning
    - Store device in a protected environment
    - Remove all data from a device before discarding
      - Data Erasure
  - Require specific entry credentials
- Encrypt the storage card in the device
- Access security on device
  - Afaria provides comprehensive management and security capabilities for mobile data and devices

SECURING PHYSICAL ENTITIES

Securing physical devices and laptops running the mobile application

- Leverage IT policies and procedures
  - Educate end users on policies and expectations
  - Provide consequences for failing to abide by policies and procedures
- Manage deployed hardware
  - Maintain inventory of all hardware
    - Afaria Inventory Manager
  - Implement remote patching mechanisms to ensure consistency
    - Afaria Software and Patch Manager
  - Establish procedures for disabling/erasing sensitive remote data in case of loss/theft
    - Afaria Remote Control and Security Manager
  - Device reclamation procedure
    - Erasing all data when device is returned to inventory or changes ownership

SECURING SOFTWARE

Securing application and database vulnerabilities

- Application and database considerations
  - User password policies
    - Forced password changes, password guidelines, and validation
  - Custom login procedures
  - Restrict DBA authority
    - Create a non-DBA user for the application or each user
  - Disable an account after a set number of invalid login attempts
- Encrypt database stored on the device (same as data center)
- Enforce password policies (same as data center)

SECURING SOFTWARE

Securing application and database vulnerabilities

- Application coding
  - Program defensively with security in mind
  - Trusted code should not call untrustworthy code
  - Compartmentalize code to minimize damage possible from a single module
  - Use standard tested components
  - Keep routines simple
  - Hiding information in binaries can be discovered
    - Internal hacking can occur
  - Remove all information from application code when no longer required
    - Zero out variable information and temporary space
  - Consult security experts and use security auditing software
  - Use trusted methodology that has proven success

INEVITABLE CASE

Prepare for the inevitable

- Create a security plan to deal with breaches
  - Expire keys and code
  - Remove unnecessary data from the device when not necessary or before discarding
    - Data Erasure
  - Afaria Remote Control and Security Manager

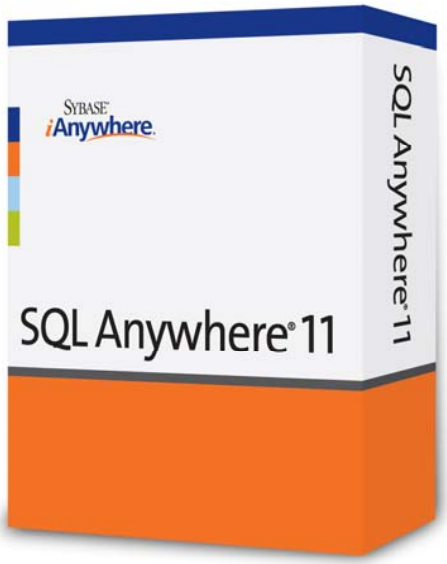
RECAP ON BUILDING SECURITY

How are we going to build secure mobile applications?

- Need to consider security in the following components:
  1. Enterprise data center security
  2. DMZ and internal network security
  3. Data transmission from device to middleware
  4. Mobile devices and laptops
- Need to consider the level of security requirements to meet your business needs

RESOURCES

- Where to go from here…
  - SQL Anywhere website
    - http://www.sybase.com/sqlanywhere
  - Download the developer edition
    - http://www.sybase.com/detail?id=1055872
  - Try out the samples! (**%SQLANYSAMP11%**)
  - Look at the documentation
    - http://dcx.sybase.com
  - Newsgroups
    - http://www.sybase.com/detail_list?id=10891
  - White Papers
    - http://www.sybase.com/detail?id=1062460
  - SQL Anywhere Tech Corner
    - http://www.sybase.com/developer/library/sql-anywhere-techcorner



SYBASE TECHWAVE SYMPOSIUM 2009

Sybase Professional Services

www.sybase.com/professional-services/consulting/products

- Our Professional Services Organization can help you…
  - Upgrade from previous versions
  - Install and configure SQL Anywhere 11 with high availability options
  - Build a rapid proof of concept using tried-and-tested application templates, toolkits, and frameworks
    - Includes BlackBerry development (www.sybase.com/blackberry)
  - Learn more about SQL Anywhere through customized training and mentoring
  - Plan your architecture, distributed systems design, or application design
  - Tune and enhance performance
  - Test synchronization scalability

> The technology and the assistance we've received from iAnywhere's Professional Services team have enabled us to do things that would otherwise have been much more difficult and expensive given our business requirements.
>
> *Khaled El Emam*
> CTO
> TrialStat

> Pearson benefited from the expert knowledge of iAnywhere Solutions Professional Services, helping their developers quickly gain knowledge in order to accelerate the development of SuccessMaker.
>
> *Kelli Anne Hodges*
> Curriculum Specialist
> Pearson Digital Learning

SECURITY CONSIDERATIONS FOR MOBILE APPLICATIONS

Thank you FOR ATTENDING