Relax. Your Data is Compliant.

Employing Encryption to Combat Data Theft

Derek Tumulak
Director of Product Management
Agenda

- Motivation and Risks
- Legislation and Compliance
- Defining Your Encryption Strategy
- Challenges in Using Encryption
- Critical Components of Data Encryption
- Ingrian Data Encryption Solutions
- RSA Conference – Real World Case Studies
- Questions?
Motivation and Risks
Why a comprehensive data privacy solution?

- Even with a fortified network perimeter, data storage systems can be breached via insecure storage management interfaces
- 75% of external-based attacks are tunneling through applications and go undetected by a range of traditional security mechanisms
- Most estimates cite that now over 50% of security breaches are perpetrated by internal staff

Data Provided by Gartner
Average of $14 Million per incident, ranging as high as $50 Million

Costs comprise of:
- costs of internal investigations
- outside legal defense fees
- notification and call center costs
- investor relations efforts
- discounted services offered
- lost employee productivity
- financial hit from lost customers.

Each lost record cost companies an average of $140

Average loss of 2.5% of all customers, ranging to as high as 11 percent
Motivation and Risks
2005 Survey of Data Breaches

Data Provided by Forrester Research
Majority of the cases involved a compromise of a PC based POS system.

None of these systems were PCI DSS compliant.

Source: Nick Percoco, Vice President, Spider Labs, AmbironTrustWave, speaking at the VeriFone Security & Emerging Technologies Conference, June 1, 2006.
Motivation and Risks
Application Threats

- Misconfigured servers can be compromised and can be used to extract sensitive information data from databases and other devices on the network
- Servers compromised by malicious administrators
- Authentication credentials can be stolen and used to extract information
- Malicious software can be installed onto web, application, and database servers
• Authentication credentials are not properly managed (i.e., *all applications use the same database username and password*)

• Authorization policies within a database are not properly defined (i.e., *database users often have access to sensitive information they do not require*)

• Servers compromised by malicious DBAs
Motivation and Risks
Physical Threats

- Physical theft of:
  - Tapes
  - Laptops
  - Servers
  - Desktops
  - Hard Drives

- Storage management interfaces can be compromised
• Legislation
  • SB 1386
  • AB 1950
  • Sarbanes-Oxley
  • Europe’s Data Privacy Act
  • Canada’s Personal Information Protection and Electronic Document Act (PIPEDA)
  • HIPAA
  • GLBA
  • Etc.

• Compliance Requirements
  • PCI Data Security Standard (CISP, SDP)
Requirement 3: *Protect Stored Data.*

- Keep cardholder information storage to a minimum
- Do not store sensitive authentication data subsequent to authorization.
- Mask account numbers when displayed.
- **Render sensitive cardholder data unreadable anywhere it is stored.**
- **Protect encryption keys against both disclosure and misuse.**
- Fully document and implement all key management processes and procedures.
• Introduces stiff disclosure requirements for businesses and government agencies that experience security breaches that might contain the personal information of California residents.

• According to California, personal information includes "an individual's **first name** or **first initial** and **last name** in combination with one or more of the following:

  - **social security number**
  - **drivers license number**
  - **account number**
  - **bank card information**
  - **passwords**
  - **PINs**
  - **access codes**.
Defining Your Encryption Strategy

First steps…

• Know your threat model

• **WHAT**—Identify what data you want to protect—this will dictate where and how you deploy encryption

• **WHERE**—Identify data locations

• **HOW**—Once you identify data type and data locations, you can evaluate encryption options to accommodate various platforms
Challenges in Using Encryption

- **Finding all of the sensitive data**
  - databases, files, intermediate servers, local storage on PCs and laptops, logs, backup tapes, portable media, etc.

- **Key management complexity**
  - Generation, distribution, storage, rollover, etc.
  - Dual-control and split knowledge

- **Geographically distributed environment**
  - Branch locations, retail stores, restaurant chains
  - Hub-and-spoke, peer-to-peer

- **Determining at what level to encrypt**
  - disk, file, database, application

- **Build v. Buy**
  - Commercial solution, native support, open source

- **Integration work**
  - deployment, custom coding

- **Impact on production systems**
  - Initial conversion and yearly key rollover
  - Performance considerations

- **Heterogeneous environments**
  What about the mainframe?
Critical Components of Data Encryption

Security  Manageability  Flexibility  Performance
• Enterprise key and policy management

• Advanced authentication and authorization

• Active alerting capabilities (SNMP traps, threshold monitoring)

• Standards-based approach to security and key management
• Centralized auditing and reporting
• Automated backup and recovery
• Highly intuitive management interface
• Multi-environment implementation with a wide range of support for different application environments

• Protection of information at POS locations in addition to data centers

• Integration with 3rd party application and security vendors
Critical Components of Data Encryption

- High performance encryption offload
- Scalable and reliable
- Solutions for transactional and batch environments
Ingrian Data Encryption Solutions
Ingrian i10 EdgeSecure
**Ingrian Presents…**

- **What:** Encryption Panel at RSA, “Encryption Demystified”
- **Who:** Panelists are industry experts who have successfully rolled out encryption at Revlon, Dell and Intuit
  Plus, ATW to share perspective on the evolving compliance landscape and the PCI 1.1 update
- **When:** Wed, Feb 7th at RSA Conference, San Francisco
- **Where:** The W Hotel (walking distance from the Moscone)
- **Why:** Educate organizations on how to select, deploy and operationalize encryption solutions to drive true business value for the enterprise

Pre-Announcement Registration, email your contact info to: Betty Liang, Director of Marketing, Ingrian (bliang@ingrian.com) 
(650) 261-2488 Direct
Space is Limited—Register Today
Questions?