Encryption and Common Sense

They aren't mutually exclusive

Michael Solomon
Solomon Consulting Inc.

PUG CHALLENGE EXCHANGE AMERICAS

Introduction

- Michael G. Solomon
- Solomon Consulting Inc.
  - OpenEdge, Roundtable, Security architecture
    - Since 1988 (Progress Version 4)
  - CyberSecurity Simulation attack team leader
    - Penetration testing, attack detection and response
- Emory University
  - Security and Privacy research
  - Private location proximity detection .

What we'll cover

- This talk is primarily about encryption for data at rest
  - In the database

- Encryption drivers - motivation
- What encryption really provides
- Types of encryption
- The problem with keys
- What to do next .

What are the drivers to implement encryption?

- Everybody's doing it
- A desire for "security"
  - Keep data from the bad guys?
- Compliance requirements
  - Regulatory
  - Standards
- Customer requirements
  - Example: Use encryption to protect laptops .

Important questions

- Why encrypt data?
  - How will encryption (technical solution) meet your goals (business problem)?
- Who are you expecting to attack your data?
- Why would anyone want your data?
  - Do they want it all?
  - Why do they want it?
  - What are they going to do with it?
  - If you love these questions, join me for
    - Session 288: "Why Hackers Love Your Database"
    - Tuesday, 1:00pm .

More important questions – what about risk?

- What risks does a lack of encryption pose?
- What types of attacks concern you?
- How likely are threats expected to be realized?
- What could you lose?
- What does encryption cost?
  - Money and time
- We will repeat these questions again .

Security trends

- SANS 2014 Security Trends Report
  - http://www.sans.org/reading-room
- Increased demand for persistent data encryption
  - Primarily due to increased regulation and reliance on outsourced data storage
- Cost barriers remain
  - Acquisition
  - Implementation
  - Performance
  - Maintenance .

http://www.sans.org/reading-room/whitepapers/analyst/2014-trends-reshape-organizational-security-34625

Know your enemies!

- **"If you know the enemy and know yourself, you will not fear the outcome of a hundred battles."**

  Sun Tzu, *The Art of War*

- Will a 6 foot fence protect trees from Giraffes?
- Controls have specific targets
- Who are your expected attackers?
  - Insiders? (regular/privileged users)
  - Business partners / Business competitors
  - Anonymous users
  - Hacktivists
  - Cybercriminals
  - State agents .

PUG CHALLENGE AMERICAS EXCHANGE

8

http://www.sans.org/reading-room/whitepapers/analyst/making-database-security-security-priority-34835

Encryption pros and cons

- Pros
  - Separation from device security (no breaches if stolen)
  - Control is on the data itself
  - Encryption provides confidentiality
    - But not always privacy
- Cons
  - Key management
  - Implementation expense
  - Unrealistic requirements and expectations
  - Compatibility barriers

http://www.spamlaws.com/pros_cons_data_encryption.html

A few definitions

- Data security
  - Confidentiality
  - Integrity
  - Availability
- Security breach
  - Disclosure, alteration or destruction, non-availability (DoS)
- Cryptography
  - Process of scrambling data, making it unreadable to unauthorized users
  - Should render access control useless
    - as long as keys are absolutely secure .

http://www.securityfocus.com/excerpts/20
http://www.dbtalks.com/uploadfile/brijesh_mcn/use-of-cryptography-in-database-security/

Cryptography

- Only changes the security problem
  - Doesn't remove it!
  - **Cryptography consolidates many secrets into very few secrets**
- Can ensure confidentiality and/or integrity
  - With some additional work
- The "**key is the key**" to gigabytes of data
  - Key granularity drives most technical decisions
  - If the cybercriminal gets the key, confidentiality is lost
  - If the data owner loses the key, availability is lost
    - Properly leveraged key disclosure can also cause loss of availability .

Encryption attack types

- Common attack types
  - Ciphertext-only
    - You're only really safe from this one (caveats abound)
  - Known ciphertext
    - Restricted domain values (state, salesrep codes, etc.)
  - Known plaintext
    - Is the data also stored unencrypted? (PDF, reports, other tables, etc.)
  - Chosen plaintext
    - Entering data into a database application
  - Brute force
    - Generally a restricted domain of plaintext .

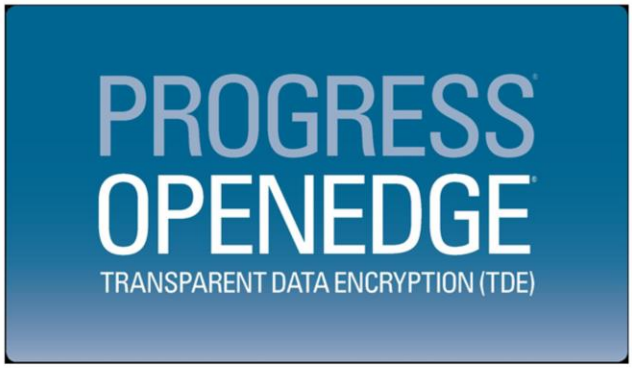
More attack types

- Physical theft
  - Whole server / Disk drive / Removable media
  - Laptop / Mobile device
  - Backup media
- Logical theft (encryption doesn't help here)
  - SQL/ABL injection (Yes, ABL injection)
    - Exchange 2005: INNOV-09, "How to Keep Hackers Out of Your Web Application"
  - Other data exfiltration methods
- Offline brute force
  - Far easier after a successful theft

http://en.wikipedia.org/wiki/SQL_injection
http://www.unixwiz.net/techtips/sql-injection.html
http://ferruh.mavituna.com/sql-injection-cheatsheet-oku/
http://download.psdn.com/media/exch_audio/2005/INNOV/INNOV-09_Solomon.ppt

While on the subject of physical security …

- Transparent Data Encryption (TDE)
  - Beware – easy is bidirectional
  - System must successfully distinguish between good and bad users
  - Often viewed as a deterrent to physical theft
    - Be careful about believing this!!!!
    - TDE does have utility in this domain
      - Backup media theft
  - We'll revisit this topic .



Encrypting Database Data

- Growing number of databases
- Outsourcing
  - Location independence
  - Authentication/access control difficulties
- Databases gladly provide data to “authorized” users
  - Technically, DMBS provides data, not database .

PUG CHALLENGE EXCHANGE AMERICAS

15

http://www.zdnet.com/article/database-encryption-demystified-four-common-misconceptions/

Types of Encryption

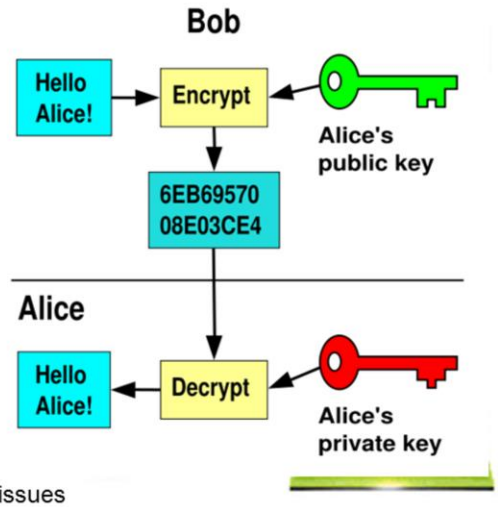
- Obfuscation (home grown schemes)
  - NEVER secure!
  - Cryptography is a very specialized domain
  - Attackers have very advanced cryptanalysis tools
- Hashing
  - Fixed length signature (not forensically sound)
  - One-way function
  - Potential utility in transient data
  - MD5, SHA-1, SHA-2, SHA-3, etc.
  - **OpenEdge supports MD5, SHA-1, SHA-256, SHA-512**
    - **MESSAGE-DIGEST .**

PUG CHALLENGE AMERICAS EXCHANGE

http://www.wisegeek.org/what-are-the-different-types-of-encryption-methods.htm

Types of Encryption

- Symmetric encryption (private key)
  - Single key for encryption and decryption)
  - Fast, but key exchange issues abound
  - Block cipher modes
    - Cipher Chaining Block (CBC) – Probabilistic
    - Electronic Code Block (ECB – Deterministic
  - DES, AES, Blowfish
  - **OpenEdge supports DES, DES3, AES, RC4**
- Asymmetric encryption (public key)
  - Key pairs, one to encrypt, the other to decrypt
  - Much slower than symmetric, but fewer key exchange issues
  - Can provide confidentiality or integrity
  - RSA, Diffie-Hellman. Paillier .



http://www.wisegeek.org/what-are-the-different-types-of-encryption-methods.htm

Encryption scope

- All encryption is not created equal!
  - Scope decisions affect performance and utility
- Column level
  - Fine granularity – positive control
  - Highest performance impact
  - Column selection can imply perceived value of data (to attackers)
  - Sorting difficulties for encrypted indexed values
- Database level
  - Transparent Data Encryption (TDE)
  - "Easy"
  - Specific attack vector protection
- File/volume level .

	Customer_id
1	74112
2	74113
3	74114
4	74115

http://www.sans.org/reading-room/whitepapers/analyst/transparent-data-encryption-technologies-practices-database-encryption-34915

Encryption keys

- **"With great power comes great responsibility"**

  Uncle Ben, *Spiderman*

- Key management is by far the toughest encryption challenge
- In-place key management degrades separation of duties
- Key scope decisions can have great impact
  - Few keys = easier management, but less granularity
  - Many keys = more granularity, but more difficult to manage
  - Future directions include functional encryption
    - Identity based encryption (IBE)
    - Hidden Vector encryption (HVE)
    - Attribute base encryption (ABE)
    - Secure location-based data .

A few encryption reminders

- Encryption is not authentication
- Encryption provides confidentiality
  - Authentication provides integrity
- Encryption (alone) does NOT provide integrity
  - Modified messages will still decrypt, but will be garbage
  - Bit rewriting attacks can alter encrypted messages
    - Encrypted cookies
  - Authentication does NOT provide confidentiality
- Always keep things straight (Cryptographic Doom Principle)
  - Encrypt, then authenticate
  - Authenticate, the decrypt .

https://paragonie.com/blog/2015/05/using-encryption-and-authentication-correctly
http://www.thoughtcrime.org/blog/the-cryptographic-doom-principle/

Questions you should ask

- What are the chances of an attacker gaining access to the data?
  - Probability of realization
- Does the data contain anything sensitive?
  - Confidential (or private)
- What could an attacker stand to gain from accessing the data?
- What could you, or your company, stand to lose if an attacker gained access to the data?
  - It's not just the data, it's potentially your reputation too.
- How much will it cost to implement? .

More question you should ask

- What are your legal obligations with regard to your data?
- If data are encrypted using a single global key, how will you keep the key safe?
- If the key is really safe, how will you use it to encrypt and decrypt data?
- If data are encrypted using multiple keys, how will you recover data if a customer loses their key/password? .

Even more questions you should ask

- If you are able to recover customer data, how does that affect its safety?
- What access will computer repair technicians, sysadmins, etc., have to your database server, and how will that affect data security? (It's not just about external hackers)
- What are the performance effects of encryption and decryption?
- What other mechanisms, like firewalls, physical security and employee vetting can be put in place? .

One-click cryptography install - ABL

- Well, not exactly
- Plan carefully – it is easy to make a mess of encryption
  - Program errors or key loss can render data unusable
  - Test, Test, and then test some more
    - More than you do now .

Caution: Progress Software Corporation recommends that you use the cryptographic features of ABL **only** if you have a well-grounded understanding of cryptography and its usage. Use of cryptography without the necessary preparation can result in permanent data loss. In general, cryptography can have significant negative impact on application performance and decrease effective data compression for data stored in a database.

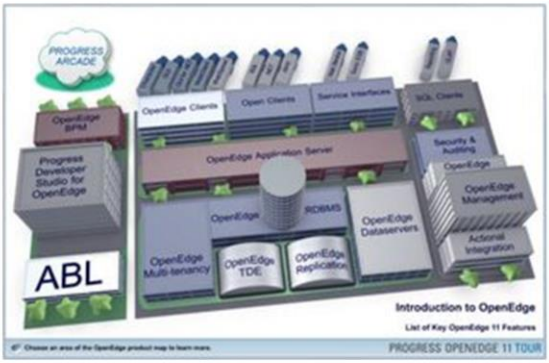
Key store (vault)

- You must plan for secure encryption key management
  - Essential for column-level encryption
- Key management issues (NIST guidelines)
  - Create / store / retrieve
  - Set scope
  - Age / Retire / Rekey / replace (compromised)
  - Audit
- See Exchange 2007 Presentation
  - DB-9 “Data Encryption Made Easy”
- Alternatives
  - Flat file
  - 3rd party solutions .

http://download.psdn.com/media/exch_audio/2007/DB/DB-9_Solomon.pdf
http://csrc.nist.gov/groups/ST/toolkit/key_management.html

OpenEdge encryption options

- ABL encryption
  - Hardest to implement
  - You manage the keys
  - More granularity, but loss of searching/indexing
- Transparent Data Encryption (TDE)
  - Easy (only 1 key – kind of)
  - Searches still work (In memory plaintext blocks)
  - Some granularity
- File/volume encryption
  - Operating system
  - 3rd party .



http://en.wikipedia.org/wiki/Comparison_of_disk_encryption_software
http://www.pcworld.com/article/2304851/so-long-truecrypt-5-encryption-alternatives-that-can-lock-down-your-data.html

Never roll your own encryption solution!

- Cryptography is a very complex science
- Your solution may be novel
  - IT WILL ALWAYS BE WEAKER!
- Secure encryption schemes require
  - Exhaustive design
  - Rigorous analysis
- **Always use proven algorithms and techniques!!**
  - OpenEdge DOES use proven algorithms .

http://www.fierceitsecurity.com/story/home-brewed-encryption-scheme-opens-millions-smart-meters-hacking-warn-rese/2015-05-12

Where to start?

- Don't just jump on the encryption bandwagon
- Do it right
  - Create an encryption policy (what and why)
    - SANS Reading Room
    - Include recovery procedures
  - Train your technical staff on encryption!!
  - Design controls needed to satisfy your policy
    - Manage your keys
  - Set expectations for customers
  - Audit and assess your solution .

http://www.sans.org/reading-room/whitepapers/analyst/making-database-security-security-priority-34835

https://www.owasp.org/index.php/Cryptographic_Storage_Cheat_Sheet

Takeaways

- Operate within your security policy
  - Prevent scope creep
- Employ risk management
- Implement encryption to solve specific problems
  - Non-trivial cost
- Plan key management
- Test key management procedures
  - Including encryption –related interruptions


time for questions


THANK
YOU!