Encryption for Cloud Services Security: Problem or Panacea?

@Zulfikar_Ramzan / CTO / www.elastica.net
SaaS

No visibility / control

On-Premise
Many pieces to Buy, Assemble & Operate
NOT SURE WHY PEOPLE THINK SaaS SECURITY IS HARD!

WE’LL JUST ENCRYPT OUR DATA! PROBLEM SOLVED!
TENOR OF THIS TALK

- ACADEMIC PERSPECTIVE
- BROADLY ACCESSIBLE
- NOT AN ACADEMIC TALK
WHAT IS ENCRYPTION AND HOW MIGHT IT BE USED TO SECURE SAAS APPLICATIONS?

CHALLENGES, WORKAROUNDS, LIMITATIONS TO WORKAROUNDS

MARKETING MYTHBUSTERS

BROADER PERSPECTIVES ON SAAS SECURITY
WHAT IS ENCRYPTION?

- Keyed transformation that converts plaintext to ciphertext
- Transformation should look “random” to any computationally bounded adversary with extensive black-box access to encryption / decryption routines
- Security predicated on secrecy of the key (and not on secrecy of algorithm) – Kerchoff’s Principle
ENCRYPTION FOR SaaS

- Attempt to encrypt data en-route to SaaS Provider (e.g., via forward proxy, reverse proxy, etc.).
- Decrypt traffic en-route from SaaS provider back to user.
Key SaaS Encryption Hurdles

SaaS is not just storage! Need search, sort, analytics!

Preserve Format?

Manage Keys
Approaches

- Homomorphic Encryption
- Searchable Encryption
- Order-Preserving Encryption
- Format-Preserving Encryption
- Selective Tokenization
Fully Homomorphic Encryption [Gentry et al.]

- Allows arbitrary computation on encrypted data
- Permits search, sort, SQL queries, etc., on cloud encrypted data

- Still very impractical
- Have to relax security (being able to manipulate encrypted data can be a big deal)
- Newer (and less well studied) assumptions
Searchable Symmetric Encryption

- Permits keyword search on encrypted data
- Much faster than fully homomorphic encryption
- Works by having a separate encrypted index

- Only permits very basic keyword search
- Information leaks (deterministic encryption)
- Scale issues as index gets bigger
Order-Preserving Symmetric Encryption

- Encrypts data, while retaining sorted order
- Much faster than fully homomorphic encryption
- Still significant performance overhead
- Weaker security since information leaks
Format-Preserving Encryption

- Able to preserve format needed by SaaS application
- Fairly efficient (practical)

- Weak security especially if final format must be short
- General security of schemes not as well vetted
Tokenization

- Elegant way to handle format preservation
- Fairly efficient (practical)
- Provides compliance boundary

- Only selective protection (fewer use cases)
- Might inhibit analytics
- New burden of maintaining look-up table
- Have to worry about scale
Mythbusters (SaaS Encryption Edition!)

We use AES for encryption
...therefore we are secure!

AES isn’t a security panacea. It’s a tool. Perfectly good tools can be used in completely bad ways.
Mythbusters (SaaS Encryption Edition!)

- FIPS Certification is usually limited to one aspect of system security.
- Different types of certification have different implications (algorithm vs. library)
- May have perfectly valid algorithm, but used in an insecure way.

We use are FIPS 140-x certified ...therefore we are secure!
Mythbusters (SaaS Encryption Edition!)

We use proprietary, home-grown methods...

- Cryptographic algorithms and protocols should only be designed by people who really know what they are doing
- Even experts get it wrong sometimes, so you need extensive peer review
For each security capability needed in the context of on-premises applications, analogous functionality is needed for SaaS applications.
Is good encryption / tokenization a panacea for SaaS Security?

SaaS is more than storage (search, sort, analytics)

Promising research, but fundamental limitations

Important to avoid getting caught up in the hype

Encryption: just one piece of security stack
Further Info:

Search: {Elastica} + (SOC Talks | Blog)

@zulfikar_ramzan, @elasticainc

Thank you