SECURITY ATTRIBUTES FOR CLOUD STORAGE PROVIDERS

by Francis Chao
fchao2@yahoo.com

TuCSon COMPUTER SOCIETY

apcug An International Association of Technology & Computer User Groups

Web location for this presentation:

http://aztcs.apcug.org

Click on “Meeting Notes”

SUMMARY

- Some of the cloud storage providers have security attributes in order to increase their desirability for various customer groups.

SECURITY CERTIFICATIONS

- Zero Knowlege
- HIPAA
- SOC 2
- GDPR

ZERO KNOWLEDGE

- A cloud storage service proves zero-knowledge by implementing client-side encryption, where data is encrypted on the user's device before transmission, ensuring the provider never holds the decryption keys.

ZERO KNOWLEDGE (continued)

- Here is how a service proves they have zero knowledge: Client-Side Encryption (End-to-End): Data is encrypted on the user's device before leaving it.

ZERO KNOWLEDGE (continued)

- Here is how a service proves they have zero knowledge: Client-Side Encryption (End-to-End): Data is encrypted on the user's device before leaving it. The server only receives encrypted "gibberish" and cannot

ZERO KNOWLEDGE (continued)

- The server only receives encrypted "gibberish" and cannot decrypt it because it does not possess the user's private key.

ZERO KNOWLEDGE (continued)

- They prove this through open-source code auditing, independent third-party audits, and employing zero-knowledge proof protocols that verify passwords without storing them.

ZERO KNOWLEDGE (continued)

- Here is how a service proves they have zero knowledge: Client-Side Encryption (End-to-End): Data is encrypted on the user's device before leaving it.

ZERO KNOWLEDGE (continued)

- The server only receives encrypted "gibberish" and cannot decrypt it because it does not possess the user's private key.

ZERO KNOWLEDGE (continued)

- Open Source Code: The client-side code is publicly available for inspection. This allows security researchers to verify that the encryption actually happens locally and that no keys are transmitted to the server.

ZERO KNOWLEDGE (continued)

- Third-Party Audits: Credible providers employ independent security firms to audit their software and infrastructure to verify that no plaintext data or keys are accessible.

ZERO KNOWLEDGE (continued)

- Zero-Knowledge Proofs for Authentication: Instead of sending the actual password to the server, the client's device generates a cryptographic proof.

ZERO KNOWLEDGE (continued)

- The server uses this to verify the user knows the password without ever learning what the password is.No "Password Reset" Capability: A true zero-knowledge service cannot reset a forgotten password to grant

ZERO KNOWLEDGE (continued)

- No "Password Reset" Capability: A true zero-knowledge service cannot reset a forgotten password to grant access to existing files.

ZERO KNOWLEDGE (continued)

- If a user loses their passphrase/key, the data is permanently lost, proving the service did not have a backdoor.

ZERO KNOWLEDGE (continued)

- Network Analysis: Users can verify the service using tools like Wireshark or Fiddler to monitor network traffic to ensure no sensitive data is sent.

ZERO KNOWLEDGE (continued)

- Key Indicators:Files are encrypted before they leave the device.The provider cannot decrypt data, even with a warrant.

ZERO KNOWLEDGE (continued)

- The encryption key is generated from the user's password and never stored on the server.Examples of services that heavily promote zero-knowledge architectures include Proton and Sync.com.ProtonWhat is

ZERO KNOWLEDGE (continued)

- Examples of services that heavily promote zero-knowledge architectures include Proton and Sync.com.

HIPAA

- The Health Insurance Portability and Accountability Act (HIPAA) of 1996 is a US federal law designed to protect sensitive patient health information from being disclosed without consent. It improves portability of health

HIPAA (continued)

- It improves portability of health insurance, reduces fraud, and sets national standards for protecting electronic health data through its Privacy and Security rules.Key Aspects of HIPAAWhat HIPAA stands

HIPAA (continued)

- Main Benefits: Provides individuals with rights to access their health records, request corrections, and ensures insurance coverage continues when changing jobs.Core Components (Rules):Privacy Rule: Sets

HIPAA (continued)

- Main Benefits: Provides individuals with rights to access their health records, request corrections, and ensures insurance coverage continues when changing jobs.Core Components (Rules):Privacy Rule: Sets

HIPAA (continued)

- Purpose: To protect health information (diagnoses, medications) from unauthorized sharing while enabling necessary data flow, ensuring patients have control over their records.Main Benefits:

HIPAA (continued)

- Main Benefits: Provides individuals with rights to access their health records, request corrections, and ensures insurance coverage continues when changing jobs.Core Components (Rules):Privacy Rule: Sets

HIPAA (continued)

- Core Components (Rules):Privacy Rule: Sets standards for protecting personal health information.Security Rule: Establishes safeguards (administrative, physical, technical) for electronic

HIPAA (continued)

- Security Rule: Establishes safeguards (administrative, physical, technical) for electronic protected health information (ePHI).

HIPAA (continued)

- Breach Notification Rule: Requires notifying individuals and HHS in case of data breaches.

HIPAA (continued)

- Who it Applies To: Covered entities (healthcare providers, health plans, clearinghouses) and their business associates who have access to patient data.

HIPAA (continued)

- Common examples of covered providers include doctors, clinics, psychologists, dentists, nursing homes, and pharmacies.

HIPAA (continued)

- HIPAA proof, or proof of HIPAA compliance, is documented evidence showing a covered entity or business associate is following Privacy, Security, and Breach Notification rules.

HIPAA (continued)

- Essential proof includes signed Business Associate Agreements (BAAs), risk assessments, updated policies and procedures, and training records.Core Elements of HIPAA ProofTraining Records:

HIPAA (continued)

- Core Elements of HIPAA Proof:
  Training Records: Documentation showing employee training completion, including dates and content covered.Risk Assessments: Regular,

HIPAA (continued)

- Risk Assessments: Regular, written risk analyses detailing how electronic Protected Health Information (ePHI) is secured.Policies & Procedures: Written documentation of security

HIPAA (continued)

- Policies & Procedures: Written documentation of security measures, including physical, administrative, and technical safeguards.BAAs: Signed agreements with third-party vendors (business associates) handling

HIPAA (continued)

- BAAs: Signed agreements with third-party vendors (business associates) handling PHI.Incident Response Records: Documentation of any breach response activities.Training

HIPAA (continued)

- Incident Response Records: Documentation of any breach response activities.Training Documentation RequirementsTo stand up to an audit, training records must show:Who was

HIPAA (continued)

- Training Documentation Requirements To stand up to an audit, training records must show:Who was trained.When they were trained.What content was covered.How they were trained.

HIPAA (continued)

- While there is no "official" HIPAA certification from the government, organizations demonstrate proof through: Retention: Maintaining documentation for at least six years.

HIPAA (continued)

- Audits: Conducting regular internal audits and self-assessments.
  Reporting: Utilizing reports from compliance software that tracks all HIPAA activities.

HIPAA (continued)

- Audits: Conducting regular internal audits and self-assessments.
  Reporting: Utilizing reports from compliance software that tracks all HIPAA activities.For individuals asking about a "HIPAA

SOC 2

- https://www.a-lign.com/articles/what-is-soc-2-complete-guide

GDPR

- https://en.wikipedia.org/wiki/General_Data_Protection_Regulation