IT 3003 – Lab 4 Group Assignment Team 1

Joel N Chin Sue
Chris Leonard
Daniel Schroeder
Levis Owino
Michael Lees
Ryan Shah

Secure Data Transfer Software

In today's digital age, the secure transfer of data over the internet is of paramount importance for individuals and businesses alike. The need for confidentiality, integrity, and availability of data during transmission has led to the development of various secure transfer protocols and software. This conceptual framework for a state-of-the-art Secure Data Transfer Software (SDTS), designed to facilitate the ultra-secure transmission of data between two points, effectively mitigating the risks of associated with hacking attempts, data breaches, and unauthorized access.

Core Features

End-to-End Encryption

SDTS employs robust end-to-end encryption (E2EE) mechanisms, ensuring that data is encrypted at the source and only decrypted by the intended recipient. Leveraging advanced cryptographic algorithms, such as AES-256 and RSA-4096, SDTS ensures the confidentiality of data against eavesdropping and interception attempts.

Secure Authentication

To establish a secure connection, SDTS implements a two-factor authentication (2FA) system, incorporating something the user knows (password or passphrase) and something the

user possesses (a secure token or a biometric identifier). This significantly reduces the risk of unauthorized access due to stolen or weak passwords.

Data Integrity Checks

Utilizing cryptographic hash functions, such as SHA-256, SDTS performs data integrity checks at both the sending and receiving ends. This ensures that the data has not been tampered with during transmission, safeguarding against man-in-the-middle (MITM) attacks and data corruption.

Anti-Replay Protection

SDTS incorporates anti-replay protection mechanisms, ensuring that intercepted data cannot be fraudulently retransmitted to the recipient. This is achieved through the use of sequentially numbered packets and timestamps, making each data packet unique and preventing replay attacks.

Anonymity and Privacy

Through the use of onion routing techniques and secure virtual private networks (VPNs), SDTS offers users anonymity and privacy during data transmission. This prevents third parties from tracing the data transfer back to the source or the recipient, further enhancing security.

Secure File Shredding

Post-transfer, SDTS provides secure file shredding capabilities, allowing for the safe deletion of sensitive data from the source device. This feature ensures that data remnants are irrecoverable, protecting against unauthorized access to discarded or old data.

Implementation

SDTS is designed to be platform-agnostic, offering secure data transfer capabilities across various operating systems, including Windows, macOS, Linux, and mobile platforms

(iOS and Android). The software is built on a modular architecture, allowing for easy updates and the integration of new security features as they emerge.

User Interface

The user interface (UI) of SDTS is designed with simplicity and usability in mind, ensuring that users of all technical levels can securely transfer data without requiring extensive technical knowledge. The UI provides clear instructions, real-time transfer status, and easy access to advanced settings for power users.

Compliance and Standards

SDTS adheres to international security standards and regulations, including GDPR for data privacy, HIPAA for health information, and PCI DSS for financial data. This compliance ensures that SDTS is suitable for use in various industries, including healthcare, finance, and legal sectors.

Target Audience

SDTS will target a wide range of customers with critical needs for secure data transmission. The primary target audience includes businesses/enterprises in highly regulated industries like finance, healthcare, and government as well as small-to-medium-sized organizations that lack the resources to implement high-level data security measures. SDTS will also cater to remote workers, distributed teams, and privacy-conscious individuals who require a trusted platform to safely share sensitive information.

PR Plan for the Secure Data Transfer Software

Our Public Relations plan, or PR Plan, for the Secure Data Transfer Software, is currently as follows:

- Prior to the SDTS's launch, we will give a showcase of the prototype models. We will run several simulations, showcasing how the prototypes already have a high level of capability and can only increase in quality from there, showcasing this not only to stakeholders, but also a multitude of our customers.
- After this showcase, we continue to show off more and more updated versions, and as more upgrades form, we also begin to showcase more deliverable information, such as a release date, a starting price, and potential plans for our data transfer software.
- Alongside the showcase of this software, we also give an idea of our developmental pipeline, where, while not completely making our processes known, we do clue in our stakeholders and potential customers as well.
- Once the product is properly finalized, we then send multiple copies to individuals for showcases of the full program, while also giving a demonstration of the final version of our SDTS
- After the release, we begin to continuously maek updates, while also implementing a customer service and direct hotline system to allow for our customers to have the best means by which our product can directly receive feedback so as to make improvements and software updates throughout the beginning lifespan, as having immediate services to then account for potential oversights not seen in the developmental process allows for an increase in positive Public Relations

Key Competitors

Established Enterprise Solutions

Companies like Citrix, Microsoft, and Google offer secure file-sharing/data transfer capabilities as part of their broader enterprise collaboration suites. While these solutions provide

a certain level of security, they often lack the specialized features and customization options available in SDTS.

Dedicated Secure File Transfer Tools

Platforms like Thru, Accellion, and Globalscape are dedicated secure file transfer solutions that focus on data encryption, access control, and compliance. While these tools offer robust security features, they may be less user-friendly/adaptable to the evolving needs of modern businesses.

Open-Source Alternatives

Solutions like AxCrypt, VeraCrypt, and GnuPG provide open-source secure data transfer capabilities. While these options can be cost-effective, they typically require a higher level of technical expertise and may not offer the same level of support/seamless user experience as SDTS.

General List of Necessary Tools and Software

Regarding the staffing and financial requirements for the company or product, a substantial portion of the budget, approximately 40%, is allocated for employee salaries. The team consists of Software Engineers with annual salaries ranging between $80,000 and $150,000, Network Security Analysts earning $70,000 to $120,000, UX/UI Designers with a salary bracket of $60,000 to $120,000, Sales Representatives who earn between $50,000 and $100,000, and Customer Support Specialists whose salaries range from $40,000 to $80,000.

For the operational infrastructure, which accounts for 30% of the budget, the necessary equipment includes high-performance servers priced between $5,000 and $10,000 each for the data center, networking equipment such as routers, switches, and firewalls costing between $20,000 and $50,000 for the full setup, and workstations for employees that could range from

$800 to $2,000 each. Additionally, cybersecurity tools and software will require an investment of $50,000 to $100,000 for various licenses and subscriptions. Communication tools, including VoIP phones and video conferencing systems, are estimated at $10,000 to $20,000, and office furniture and supplies will cost between $20,000 and $50,000.

The physical space needed for operations, which is 15% of the considerations, involves securing office space for the workforce and a data center for server and network equipment. The rent is highly variable, influenced by location, size, and market rates, but is generally expected to fall within $5,000 to $20,000 monthly for office spaces and $10,000 to $30,000 for data center facilities.

Lastly, general operating costs, also accounting for 15% of the budget, encompass internet and phone services estimated at $2,000 to $5,000 monthly, utilities including electricity and water which may cost $3,000 to $6,000 monthly, software licenses and subscriptions pegged at $10,000 to $20,000 annually, and miscellaneous office supplies and expenses ranging from $5,000 to $10,000 monthly. This comprehensive financial outline supports the structured development and sustained operation of the company or product, ensuring a well-equipped and efficiently run business infrastructure.

Summation of Budgetary Expenditures

Based on the requirements and expenses previously listed, we have a couple of options for the capital we will need to start. If we look at the upper limit of all possible expenses we discussed, then the amount of capital we would need would be $2,793,000, which is 1.5 times our initial highest estimated cost of $1,862,000. Although this figure exceeds our original high-end estimate, considering a more flexible budget can provide us with additional safety nets and opportunities for unexpected costs or enhancements in quality. However, we can also consider

our low end, being an estimate of $1,319,000. While this budget would save us a considerable sum of capital, it also has a high chance of degrading the quality of our product, leaving us with a bad reputation and potentially causing us to fail. By adjusting our sights to 1.5 times our initial high-end estimate, we proactively account for unforeseen expenditures, thereby safeguarding the project's future and potentially elevating our product's quality and market readiness. This adjustment ensures we're prepared for both expected and unexpected challenges, solidifying the project's foundation, and increasing our potential success.

Funding Strategy for Startup Costs

The way we will raise capital for our secure data transfer software product will be a few ways. First once we get our plan ready and proof of concept, we can seek funding from investors. These can be industry specific investors already in the field. The product should also explore and consider using crowdfunding which would involve getting money for funding from people who are involved or interested in using it. Once these steps are completed, we can get revenue from licensing fees or subscription costs.

Product Violability

Given the increasing demand for secure digital communication and the heightened awareness around data privacy and cybersecurity, the Secure Data Transfer Software (SDTS) appears to be highly viable in today's market. Its emphasis on cutting-edge security features like end-to-end encryption, secure authentication, data integrity checks, and compliance with international standards addresses the critical concerns of both individual users and organizations across various sectors. As businesses and individuals alike seek more secure methods to protect their sensitive information from cyber threats, SDTS's comprehensive approach to security, combined with its user-friendly design, positions it well for adoption and success. Furthermore, its modular architecture ensures adaptability and longevity in the rapidly evolving tech

landscape, making it not just a solution for today but a scalable platform for tomorrow's security challenges.