המכללה האקדמית להנדסה ע"ש סמי שמעון

הגשת הצעה תוך שימוש בפאזלים נעולי זמן

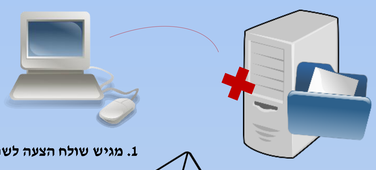
פרויקט מספר 26 | אבישג סבן | בהנחיית: אלונה קוצ'י

בעיה

1. מגיש שולח הצעה לשרת
2. ההצעה לא הגיעה לשרת בשל חוסר קישוריות השרת למחשב.
3. מגיש שולח את ההצעה
4. השרת בודק את ההצעה ומזהה שזמן ההגשה עבר ולכן דוחה את הבקשה0
5. השרת שולח ללקוח שהבקשה נדחתה כי הוגשה לאחר המועד הסופי להגשה

REJECTED

פתרון



1. מגיש שולח הצעה לשרת
2. ההצעה לא הגיעה לשרת בשל חוסר קישוריות
3. דפדפן מפיק עדות לכך שההגשה הייתה מוכנה בזמן.
4. דפדפן שולח את ההצעה ביחד עם העדות
5. אם יש התאמה בין העדות להצעה, ההצעה תתקבל גם אם היא הגיעה לאחר המועד הסופי להגשה
6. השרת שולח ללקוח שהבקשה התקבלה

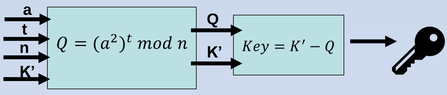
ACCEPTED

שיטה

בשלב הראשון מחשב הלקוח צריך לפענח את ערך המפתח שאיתו הוא הולך לבצע את הצפנת ההצעה. זמן הפענוח מוגדר מראש ולא ניתן לקצרו, כך כשמתקבל המפתח, זוהי למעשה הוכחה לכך שהדפדפן השקיע את הזמן הנדרש, ושההצעה הייתה מוכנה לפני .

בשלב השני ההצעה מוצפנת בעזרת המפתח שהופק בשלב הראשון. ההצעה, יחד עם הצפנתה מוגשות לשרת. השרת בודק שפענוח ההצפנה זהה לערך של ההצעה. אם הבדיקה עברה בהצלחה, ההצעה מתקבלת גם אם מועד ההגשה הסופי עבר.

רקע מתמטי – פאזלים נעולי זמן



ישנו יחס ישיר בין ערך t לבין כמות הזמן שתידרש לבצע את החישוב. יש לכוון את t בהתאם לערך זמן T, לאחר מועד סיום ההגשה, שעד אליו נוכל להגיש הצעה באיחור.

תוצאות

המימוש בוצע באמצעות תוכנה web. צד שרת נכתב ב-C# וצד לקוח נכתב ב-javascript. התוכנה מצליחה לשמור על שרידות בכך שתוצאות ביניים נשמרות בתוך cookie. כך שגם אם הדפדפן קרס, ניתן להמשיך את החישוב מהמקום שהוא נעצר. כמו כן, נשמרת הזמינות של הדפדפן למשתמש בעזרת שימוש ב- web worker המאפשרים לתהליך פענוח המפתח לרוץ ברקע, ובכך מונעים מהדפדפן להיות unresponsive.

פיתוח עתידי ומגבלות

התוכנה לא תומכת בבדיקת תקשורת, באופן מחזורי, כך שאם מוחזרת התקשורת ולא עבר זמן ההגשה, ההצעה נשלחת ישירות ותהליך הפקת ההוכחה מופסק. כמו כן התוכנה לא תומכת במקרה שבו בסיום ההוכחה אין תקשורת בין השרת למגיש, ניתן להוסיף אלמנט של פאזלים הדרגתיים, כך שללקוח יהיו מספר מפתחות עבור זמנים הגדלים בהדרגתיות, נניח מפתח עבור 10 דקות, מפתח עבור שעה ומפתח עבור שעתיים.

הנדסת תוכנה