Studenten CSC: voeg een verslag toe met een reflectie over de veiligheid van dergelijk stemproces. Zijn er kwetsbaarheden, en zo ja: hoe zou je dit beter kunnen beveiligen?

De mogelijke kwetsbaarheden:

Ik dacht gelijk aan de manipulatie van de stemgegevens. De stemgegevens (keuze van de kiezer) worden in het geheugen opgeslagen en verwerkt. Hackers zouden theoretisch toegang kunnen krijgen tot deze gegevens en ze kunnen manipuleren voordat ze worden opgeslagen of verwerkt.

Om dit te voorkomen in mijn stemsysteem kan ik end to end encryptie implementeren dat ervoor zorgt om de stemgegevens tijdens het hele proces versleuteld blijft. Dit gaat eigenlijk de gegevens alleen in een versleutelde vorm worden doorgegeven en verwerken.

Ik heb wat verder gezocht en zag genoeg voorbeelden die de end to end encryptie uitleggen om dit te kunnen implementeren in mijn code. Zoals op YouTube heb je Computerphile, The net ninja, traversy media, en academind dat veel video's hebben over verschillende concepten. Tegenwoordig hebben we AI zoals chatgpt en er zijn nog veel meer dat code genereert voor voorbeelden en ook uitleg om die concepten te begrijpen.

De chipkaarten en de autorisatie om te stemmen is gemaakt op eenvoudige voorwaarden. Dit kan kwetsbaar zijn voor ons. Want als kwaadwillende persoon ons systeem wilt aanvallen met geavanceerde technieken/aanvallen dan zou ons chipkaart autorisatie dit niet halen door hoe eenvoudig de voorwaarden waren om dit te maken.

Oplossing voor dit zou beter authenticatiemethoden gebruiken. Zoals digitale handtekeningen en certificaten om de geldigheid van de chipkaarten en de autorisatie te verifiëren. Bij AP is dit ook, we gebruiken de authenticatie applicatie om in te loggen. We kunnen pas inloggen op digitap als we de juiste 2 cijfers geven die we krijgen in de authenticatie applicatie bij poging tot aanmelden. Dus we kunnen dit een extra beveiliging laag toevoegen waardoor we dan beter beveiligd zijn.

Bij de USBStick kunnen we een wachtwoord instellen om de gegevens te beschermen als die in verkeerde handen valt.

Chipkaarten kunnen we ook een wachtwoord geven en ook instellen dat als die kwijtgeraakt worden of gestolen worden dat die Chipkaarten onmiddellijk ongeldig maken.

Bijvoorbeeld:

Een functie maken met verifieer_code(self, ingevoerde_pincode)

Dan uitleg geven wat de functie doet en eronder terug returnen self.pincode == ingevoerde_pincode). De self.pincode komt dan van een andere functie die de "pincode" als een parameter ingaf.

Stemcomputer kunnen we ook beter beveiligen, omdat dit ook kan lijden tot manipulatie van het stemproces door kwaadaardige. We zouden ook hier een wachtwoord of authenticatie proces kunnen implementeren voordat het gebruikt kan worden.

Ik denk dat mijn elektronische stemsysteem zeker veiliger zou zijn, als ik dit zou aanpassen in mijn code.