BSP: PAKE und Täuschungs Kennwörter

Student: Steve Meireles Tutor: Marjan Skrobot

2024

Inhaltsverzeichnis

Wissenschaftliche Frage

Wie erkennt man, ob eine Kennwort-Datei im Besitz von Eindringlingen ist und kann man gleichzeitig Phishing-Angriffe verhindern?

Honeywords

- Falsche Passwörter zur Kennwort-Datei hinzufügen
- Honeychecker ist ein seperates und robustes System
- Honeychecker speichert die Postionen der richtegen Kennwörter
- Honeychecker alarmiert System Administrator beim Auslösen eines Honeywords

PAKE Protokolle

- Sicher eine Lang-Zeit-Schlüssel mit einem geteileten schwachen Passwort
- Diese Protokolle ermöglichen das mit Hilfe von zyklischen Gruppen

SweetPAKE: Alice und Bob

Lass Alice und Bob zwei Parteien sein

1. Alice generiert öffentlicher Schlüssel und privater
2. Alice schickt öffentlicher Schlüssel zu Bob
3. Bob genereriert eine List von Lang-Zeit Schlüsseln
4. Verschlüsselt jeden Schlüssel dieser Liste
5. Bob schickt die Liste zur Alice
6. Alice entschlüsselt jedes Element bis erfolgreich
7. Alice schickt dann die Position des korrekten Kennworts zur Bob
8. Bob schickt die Position zum Honeychecker
9. Honeychecker checkt ob die Kennwort-Datei in Besitz von Eindringle ist

Technische Arbeit

- Implementation von SweetPAKE
- Muss schnell genug sein

Vier Hauptfunktionen:

- generate(): Erster Schritt des SweetPAKE-Protokolls
- encryption(): Verschlüsselungsschritt
- decryption(): Entschlüsselungsschritt
- retrieve_key(): Schlüsselabrufschritt

Technische Arbeit: Abschnitt

```
def gen(self):
        #gen function
        group = self.params.group
        self.rundom_exponent = group.rundom_exponent(self.entropy_f)
        self.y1_elem = group.Base1.exp(self.rundom_exponent)
        self.y2_elem = group.Base2.exp(self.rundom_exponent)
        Y2_elem = self.y2_elem.elementmult(group.password_to_hash(self.pw))

        #self.outbound_message = (self.y1+self.Y2) <-- apk
        y1_bytes = self.y1_elem.to_bytes()
        Y2_bytes = Y2_elem.to_bytes()
        self.outbound_message =  y1_bytes + Y2_bytes

        username_size = len(self.username).to_bytes()

        outbound_id_und_message = self.side + username_size + self.username + self
    .outbound_message

        return outbound_id_und_message
```

Schlussfolgerung

Wie erkennt man, ob eine Kennwort-Datei im Besitz von Eindringlingen ist und kann man gleichzeitig Phishing-Angriffe verhindern?

- SweetPAKE ist eine gute Antwort
- Kombiminiert Stärken von PAKE und Honeywords
- Mit der Implementierung kann man dies austesten

Thank you for your attention!