

LU11b - Angriffsvarianten BruteForce

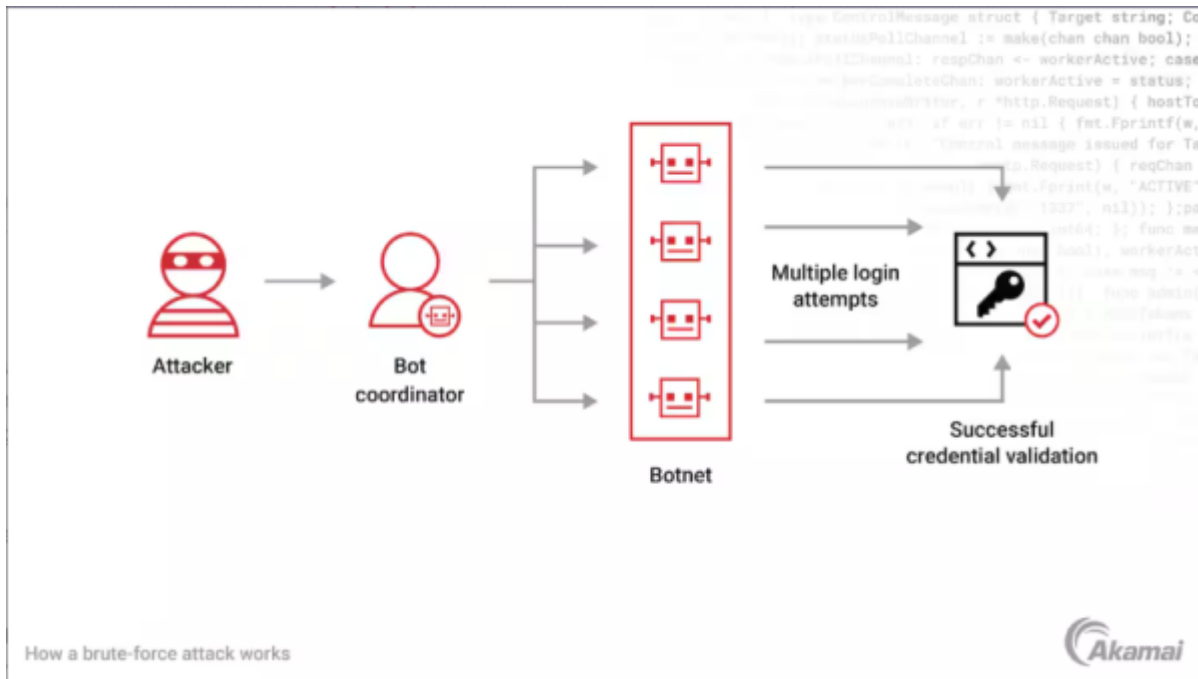
Alle Möglichkeiten testen

Für viele Probleme in der Informatik sind keine effizienten Algorithmen bekannt. Der natürlichste und einfachste Ansatz zu einer algorithmischen Lösung eines Problems besteht darin, einfach alle potenziellen Lösungen durchzuprobieren, bis die richtige gefunden ist. Diese Methode nennt man *Brute Force Suche* (engl. brute force search).



Parallelisiert

Hohe Rechnerleistungen können in Form von Computerclustering kombiniert werden, was wiederum das Auffinden von Passwörtern massiv verkürzt. Konkret können unterschiedliche Rechner unterschiedliche Teilbereiche der Kombinationenmenge unter sich aufteilen. Heute wird das mit sogenannten BotNets durchgeführt.



2.3.3 Erstellen und Verwenden von Wörterbücher Wird die Anzahl der auszuprobierenden Passwörter durch Reduktion der Möglichkeiten auf Einträge aus einem „Wörterbuch“ (bzw. Zusammensetzungen derer) eingeschränkt, spricht man auch von einem Wörterbuchangriff (engl. dictionary attack 2.3.4 Tools für Brute Force Attacken Einfache Brute Force Attacken wie beispielsweise das Knacken von passwortgeschützten Zipfiles oder Office Anwendungen können bereits mit kostenlosen Tools durchgeführt werden. Ein Beispiel für ein solches Tool ist Advanced Office Password Recovery



Volkan Demir

From:
<https://wiki.bzz.ch/> - **BZZ - Modulwiki**

Permanent link:
<https://wiki.bzz.ch/modul/m183/learningunits/lu11/02?rev=1758278322>

Last update: **2025/09/19 12:38**

