

LU09b - Angriffsvarianten BruteForce

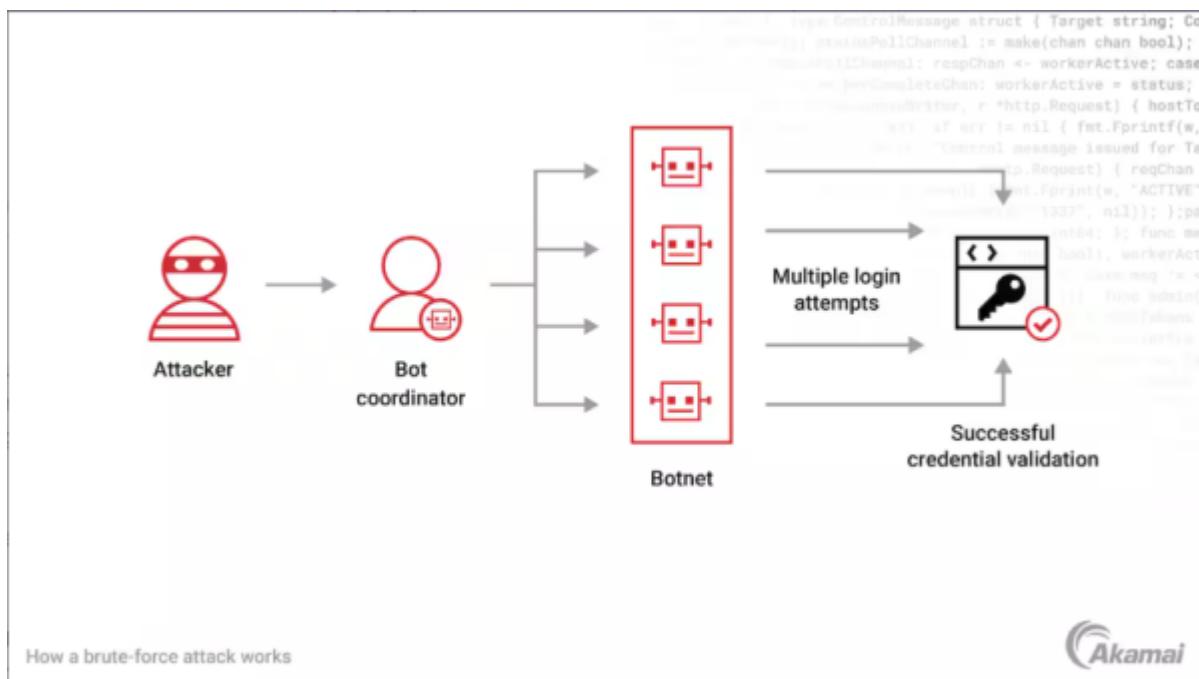
Alle Möglichkeiten testen

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).



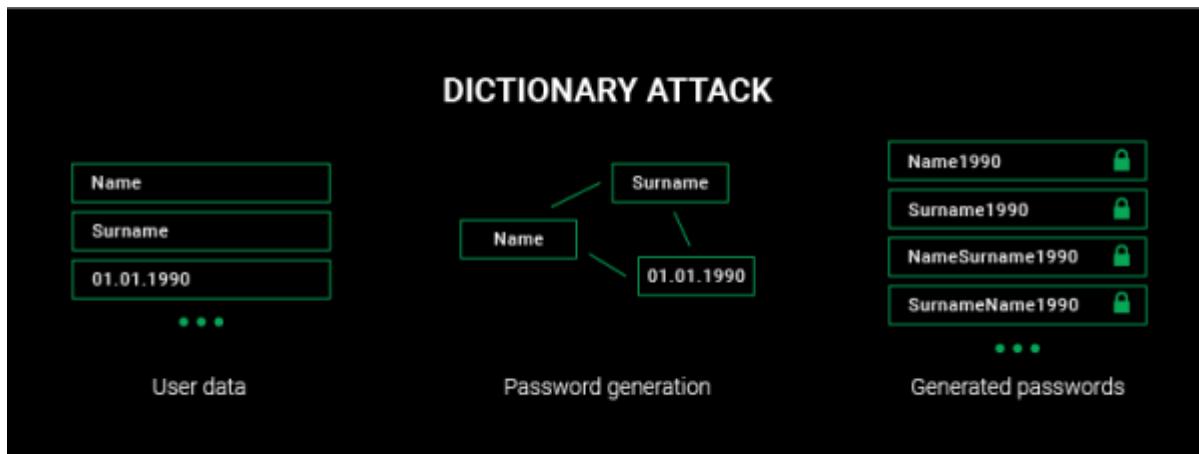
Parallelisiert

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.



Dictionary / Wörterbuch

Anstatt zufällige Symbolkombinationen zu erraten, können Hacker auch vorhandene Wörter aus einem Wörterbuch durchprobieren. Oft verwenden Menschen Wörter in ihren Passwörtern, um sich diese besser merken zu können – das erleichtert Hackern die Arbeit. Brute-Force-Software kann sogar die Wörterbuchpasswörter mutieren, um die Erfolgschancen zu erhöhen.



Rainbow Tables

Rainbow tables sind vorberechnete Tabellen, die Hashwerte mit möglichen Klartextpassworden verknüpfen, um die inverse Suche zu beschleunigen. Statt jedes Passwort neu zu bruteforcen, schaut ein Angreifer den Hash nach in der Tabelle nach und findet so schnell das zugehörige Passwort, wenn vorhanden. Die Methode erfordert grosse Rechen- und Speicherressourcen für die Erstellung, reduziert aber die Kosten beim Angriff. Kurz gesagt: clever vorverarbeitetes Lookup.

RAINBOW TABLE	
Plaintext	MD5 Checksum
123456	bfbKJ*(Y)BDnjn3219cbjwhc9HCNSdjn3210fhnAJH*W*CnjwnkoIAfJC9N346
123456789	cbjwhc9HCNSdjn3210fhnAJH*W*CnjwnkoIAfJC9N346NJRsd99x8andjn932
password	ndcsanHN(U8*(Djnd3b293rgbfjHD*hnfsksjcc*HCnenfc3h82f9hcnaJnc982h3
12345678	jkbxnct98gbf9xm(M*A(MHD9@mx3nf9p9xprKND*DNa@BDnjq9ifnjeasc9q23v
qwerty	NURsd99x8andmlkjn30q(&*XVBa8cbNB4kcba98Oijknqc2h9*(BXJnnqfnjsic9
1234567	cn2390bcqijknzdzcnu9b-cmwnnoiencv0*(&TGDXBxb87w*&XGBjs9chscb(
111111	KNCS)EF*njemdzvndsnvi304bgsjNXB(SHCNUZnscknBAJNCisnfca9*(&(Y8jk



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



Permanent link:
<https://wiki.bzz.ch/modul/m183/learningunits/lu09/02>

Last update: **2025/12/08 09:08**