

LU09b - Angriffsvarianten BruteForce

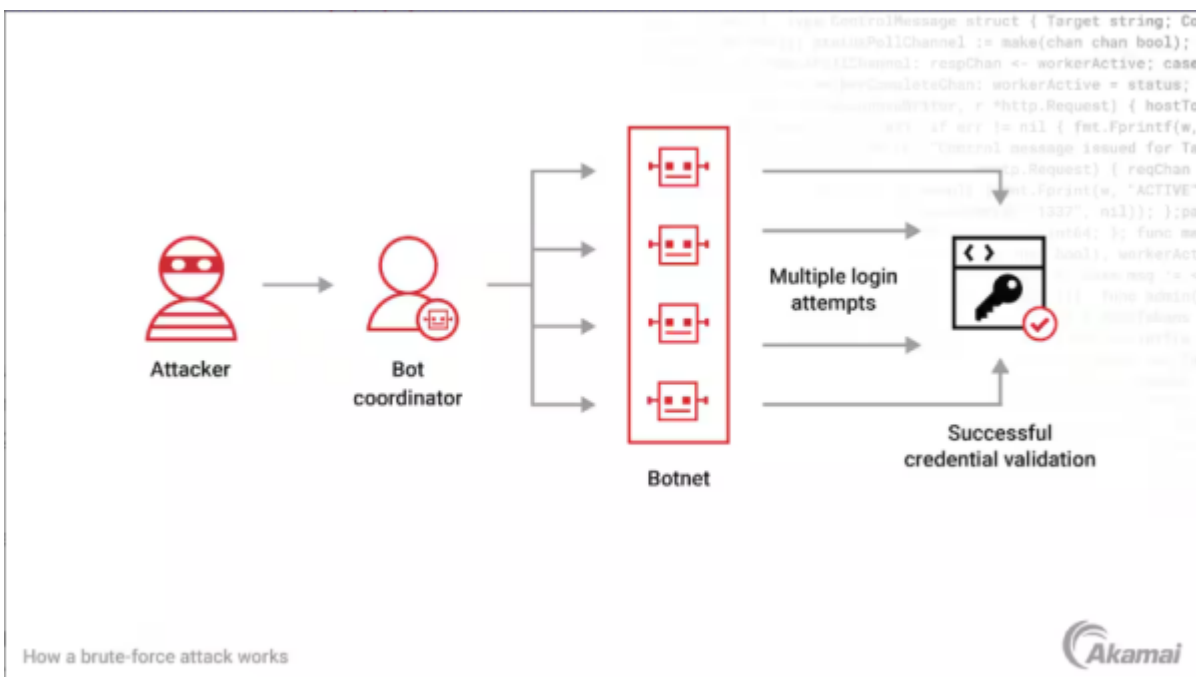
Alle Möglichkeiten testen

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).



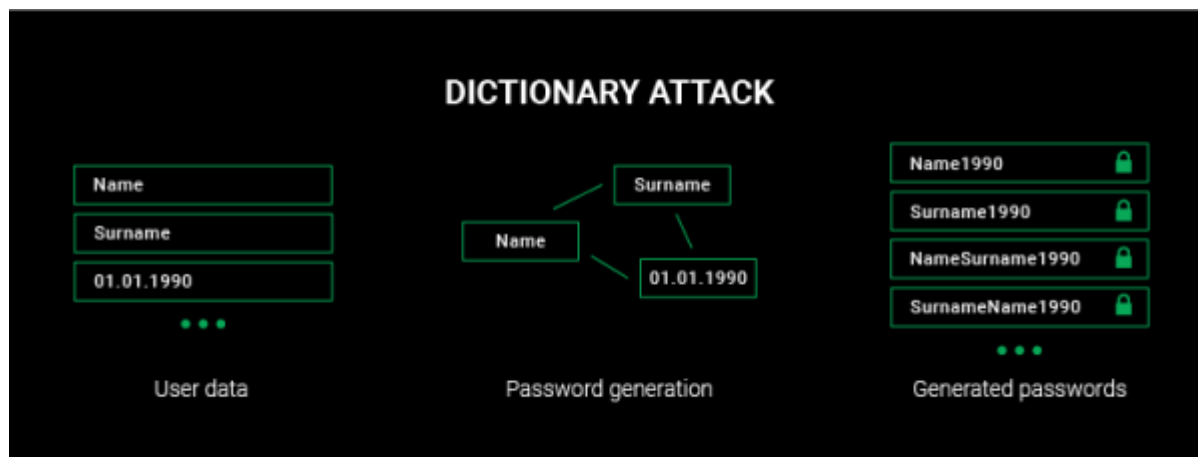
Parallelisiert

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 Klartextpasswörtern verknuepfen, 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 zugehoerige Passwort, wenn vorhanden. Die Methode erfordert grosse Rechen- und Speicherressourcen fuer die Erstellung, reduziert aber die Kosten beim Angriff. Kurz gesagt: clever vorverarbeitetes Lookup.

The table shows a mapping between plaintext passwords and their MD5 checksums. The columns are 'Plaintext' and 'MD5 Checksum'.

Plaintext	MD5 Checksum
123456	bfbKJ*(Y)BDnjn3219cbjwhc9HCNSdjn3210fhnAJH*W*CnjwnkoIAFJC9N346
123456789	cbjwhc9HCNSdjn3210fhnAJH*W*CnjwnkoIAFJC9N346NJRsd99x8andjnx932
password	ndcsanHN(UB*(Djnd3b293rgbfjHD*hnfkajcc*HCnerfc3h82f9hcnAJnc982h3
12345678	jkbnct9@gbf9xm(M*A(MHD98mx3nfp9xprfKJND*)DN@8Dnjq9ifnjeasc9q23v
qwerty	NJRsd99x8andmlkn30q(&*XVBa8cbNBAkcb098Oijknqc2h9*(BXJnnqfjnsic9
1234567	cn2390bcqijknsdzkcnu9b-cmwnoienvcv0*(&TGVXBxb87w*&XGBjs9chscb\
111111	KNC5)EF*njemdzvndsni304bgsjNXB(SHCNJZnscknBAJNCisnfcna9*(&YBjk



Volkan Demir

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**

