"DUE PAROLE" SU
VIRUS E PROBLEMI DI SICUREZZA

I problemi che si presentano sono di:

- **segretezza** → divulgazone di informazioni a non autorizzati
- **integrità** → le risorse sono modificate da non autorizzati
- **disponibilità** → le risorse non sono disponibili agli autorizzati

A causare tali problemi possono essere *intrusi* (persone o programmi).

Gli intrusi-persone possono agire come:

- *mascherati*: sfruttano l'identità di un utente legittimo
- *approfittatori*: sono utenti legittimi, che compiono azioni non lecite per loro
- *clandestini*: prendono il controllo da superuser e ne approfittano per sopprimere i controlli

Il metodo tipico con cui agisce un intruso mascherato è procurarsi la password di qualche utente. Anche se tali password sono cifrate, con MOLTO tempo a disposizione la cifratura può essere rotta.

Più facile indovinare una password se si può provare sistematicamente un insieme di parole "probabili": in uno studio su 13797 login ne sono state indovinate il 24% provando 62000 parole "comuni". Ad esempio:

il nome dell'utente 2.4%
il nome del coniuge o dei figli 2.2%
il cognome della madre o della moglie 1.1%
nomi di città, di sportivi, di personaggi famosi, film, cartoni ecc.
tra 0.6% e 0.1%

VIRUS E …

Gli intrusi-programmi sono generalmente detti virus, in realtà la classificazione completa è la seguente:

- **Batteri:** programmi che si replicano e consumano risorse del sistema
- **Bombe logiche:** un insieme di condizioni è controllato periodicamente, quando esse si verificano, viene eseguito un attacco
- **Botola**: entry point segreta che permette di evitare l'autenticazione in accesso
- **Cavallo di Troia:** funzione segreta nascosta ed eseguita entro un programma
- **Verme (worm):** programma che si propaga mandando copie di se stesso lungo una rete, eventualmente compiendo azioni non volute
- **Virus:** codice incluso in un programma, che include in altri programmi una copia di se stesso, eventualmente compiendo azioni non volute

Una distinzione si fa dal punto di vista della

- *Capacità di replicarsi*: virus, batteri e vermi la possiedono, gli altri no
- *Autonomia*: batteri e vermi sono programmi a se stanti, gli altri richiedono un programma ospite

I virus generalmente attraversano quattro "fasi":

1. fase dormiente, in cui è inattivo in attesa di un evento
2. fase di propagazione, in cui mette una copia di se stesso in altri eseguibili, o in aree di sistema
3. fase di innesco, in cui viene attivato da un evento esterno o interno
4. fase di esecuzione vera e propria, in cui ci si accorge della presenza del virus perché sono eseguite operazioni non previste

Si possono classificare i virus nelle seguenti tipologie:

1. **parassiti**: sono ospitati in files eseguibili, che diventano "più lunghi"
2. **residenti in memoria**: sono in un programma residente e infettano ogni altro programma via via che viene caricato in memoria
3. **virus di boot**: sono presenti nel boot sector e si diffondono facendo boot da tale periferico
4. **virus segreti**: impiegano "trucchi" per non venire scoperti, es. compressione
5. **virus polimorfi**: cambiano ad ogni infezione, non è possibile cercare una loro "firma", contengono un motore di mutazione

… E ANTIVIRUS

Gli antivirus devono

1. Rilevare l'infezione e localizzare il virus
2. Identificare la specie di virus e altri files dove si è propagata
3. Rimuovere le tracce del virus dai programmi infettati

Se non è possibile identificare o rimuovere il virus, l'antivirus cancella semplicemente il programma infetto.

I programmi antivirus si evolvono in continuazione (come del resto i virus!). Questo porta ad identificare quattro generazioni di antivirus.

Prima generazione: analizzatori di files. Controllano che la lunghezza degli eseguibili non cambi e cercano particolari sequenze di bit nel codice, tipiche di un virus già conosciuto. In generale non riescono ad eliminare i virus "nuovi".

Seconda generazione: analizzatori euristici. Possono identificare la presenza di un virus aggiungendo un checksum o un codice hash agli eseguibili, e controllando che il conto "torni", quindi possono identificare e rimuovere anche virus "nuovi". Possono anche cercare i motori di mutazione e i codici di cifratura dei virus segreti. Queste due generazioni agiscono su files eseguibili mentre essi non sono in esecuzione, ma sul disco.

Terza generazione: programmi residenti in memoria che cercano di rilevare le azioni illecite dei virus, cioè la presenza in un processo in esecuzione, piuttosto che la presenza “passiva” in un file.

Quarta generazione: pacchetti che comprendono le tecniche precedenti, piu’ capacità di controllo dell’accesso, che limitano le possibilità di penetrazione anche degli intrusi.