Kerberos Password Security

A Real-World Analysis

Tom Wu <tjw@cs.stanford.edu>
Stanford University / Arcot Systems

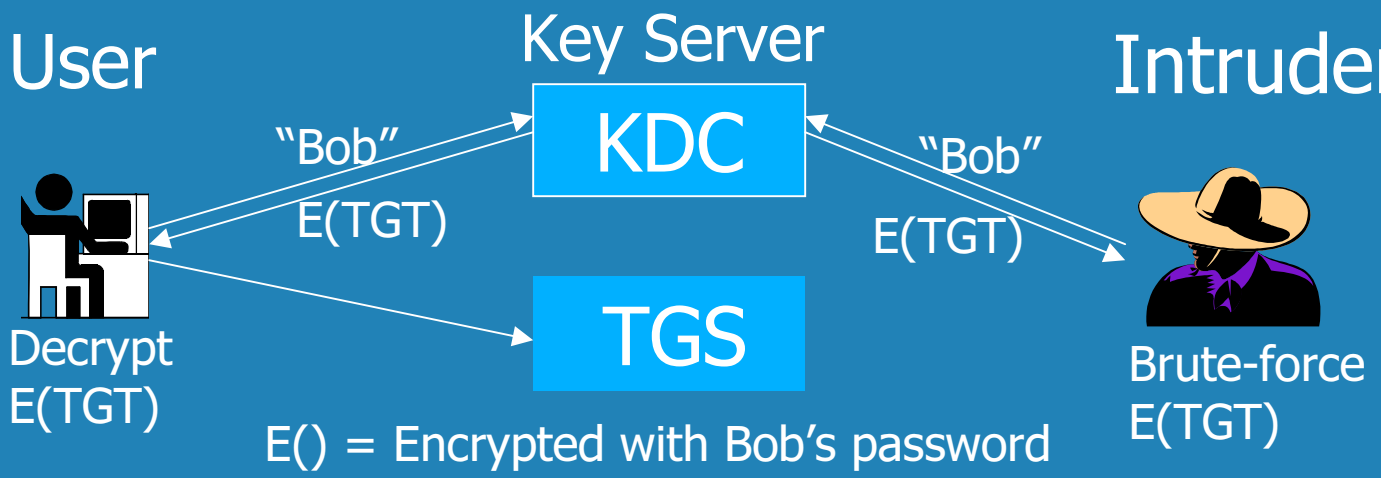
Topics Covered

- Background, known security problems with Kerberos V4 and V5
- Prevalent attitudes regarding password security
- Analysis of experimental password data
- Who is affected and what can be done?

Background

- Weaknesses in Kerberos V4 publicly known
  - 1991 - Bellovin & Merritt
- Password studies date back many years
  - 1979 - Morris & Thompson
  - 1989 - Feldmeier & Karn
  - 1992 - Spafford
- Many more papers on related topics

The Dictionary Attack



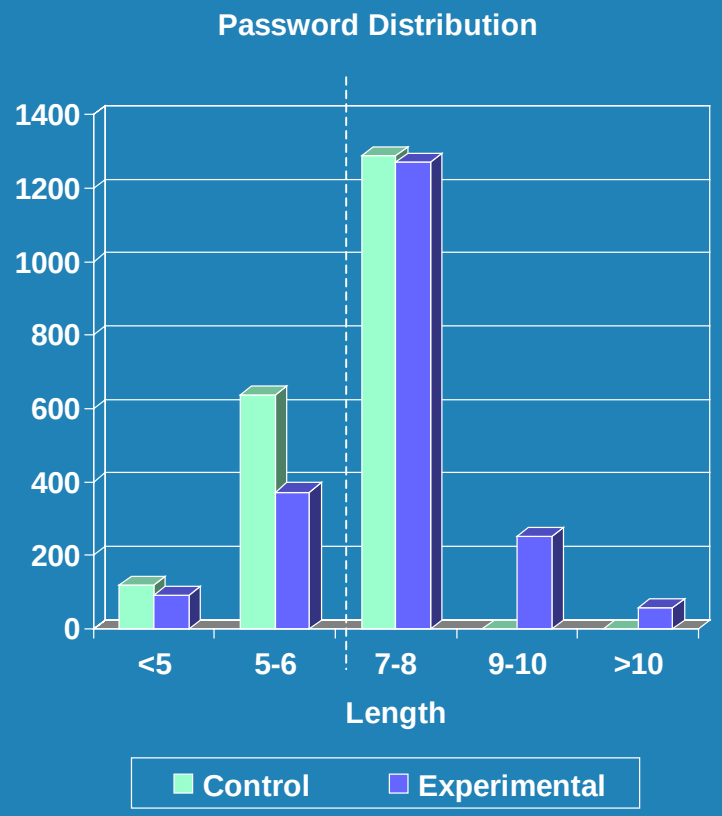
- Under Kerberos V4, attack is undetectable and can be carried out by anyone
- No sniffer or prior access needed

The Experiment

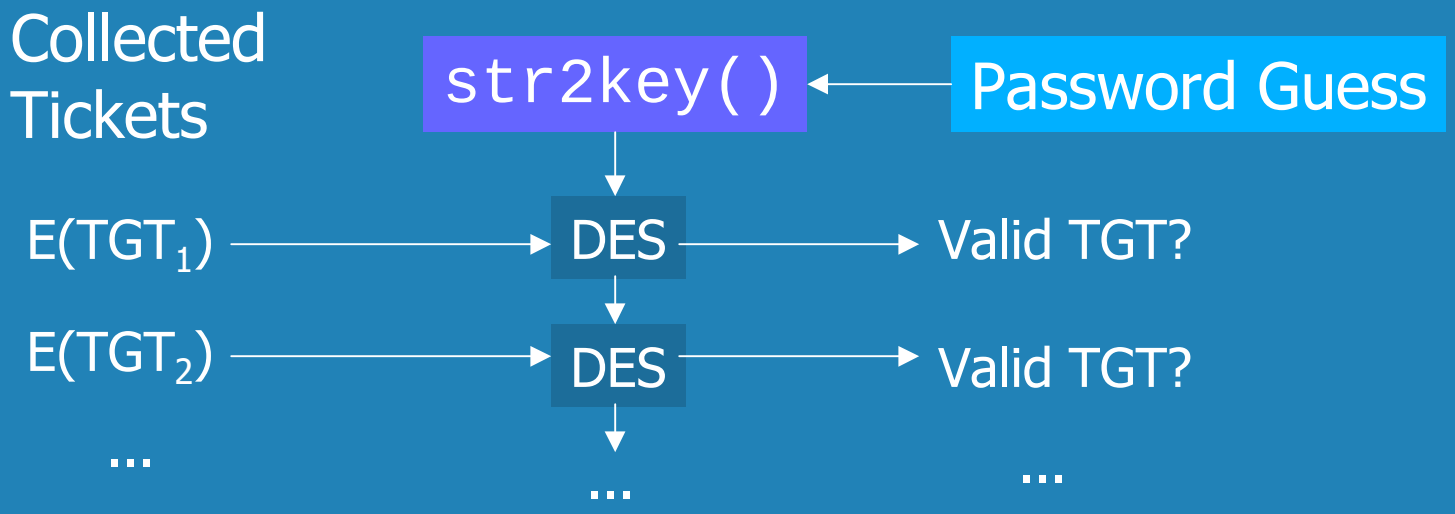
- Conducted on an actual Kerberos V4 domain during April, 1998 for two weeks
- "Strong" password-checking already in place
- Small cluster of SPARCstations (8 CPUs) performed brute-force computation

Experimental Results

- First success: 9 seconds
- Over 2000 passwords guessed in two weeks
- Green: 1992 study, no password checking
- Blue: 1998 study, with password checking
- Nearly 10% success rate



Implementation Details



- Tested each guess against entire database
- Slower `str2key()` only evaluated once per password guess

Optimizations

- Attack against Kerberos V4 KDC runs faster than attack against `/etc/shadow` files
  - Uses unmodified DES instead of `crypt()` (e.g. 3.3us instead of 110us)
  - Parity optimization further doubles speed
- Other optimizations possible
  - Dedicated hardware (e.g. Deep Crack)
  - Bitslice DES (Biham 1997)

Analysis of Results

- Password-checking had unintended effects
  - Users picked "just good enough" passwords
- Attack used larger and more up-to-date dictionary than checker
  - New word sets and rules can be tried quickly
  - Additional lists compiled via Internet, WWW
- Password choice limited by human memory
- *Problem gets worse with time...*

Long-Term Implications

- There really is no such thing as an "uncrackable" password
  - Computing power getting cheaper
  - Larger dictionaries easily built, searched
  - Keys can be brute-forced directly
- Kerberos V5 is only a partial solution
  - V5 adds "pre-authentication" - better security
  - A sniffer still defeats "naked" Kerberos V5

Better Solutions

- Kerberos V5 pre-authentication can accept stronger authentication (Jaspan 1993)
  - EKE - patent held by AT&T (license required)
  - SPEKE - patent held by D. Jablon (license required)
  - SRP - patent held by Stanford (Open Source, no royalties)

Authentication Economics

- Password enforcement is expensive!
  - Increased help-desk support costs
  - Lost productivity, user frustration
  - Sacrifices convenience for security
- Hardware tokens are expensive!
  - High initial cost of readers, tokens
  - Recurring costs for HW, SW support
- Strong authentication is cost-effective

Summary

- Kerberos V4: Subject to dictionary attack
- Password-checking: Moderate benefits, but at high cost
- Kerberos V5: Secure password technologies interface well with pre-authentication and provide a workable solution

`http://theory.stanford.edu/~tjw/kerberos.html`