“Cracking” and Computer Security

Ethics and Computing
Chapter 4

Motivation

- Computer security is crucial for trust
- “Cracking” activity is harmful, costly and unethical
- Legal system is slow to adapt
- Security measures are mostly effective
- Many systems don’t use them
  - Lack of expertise
  - Inconvenience
Codes of Ethics

- AITP
  - Do not exploit the weakness of a computer system for personal gain or personal satisfaction
- ACM
  - Respect privacy of others
  - Access computers only when authorized

- IEEE
  - Avoid injuring others, their property, reputation, or employment by false or malicious action
- Software Engineering
  - Use the property of a client or employer only in ways properly authorized, and with the client’s or employer’s knowledge and consent
Hacking vs. Cracking

- Traditional Hacker
  ◆ Self-motivated
  ◆ Technically accomplished
  ◆ Creative
  ◆ Productive
  ◆ Positive

Hacking vs. Cracking

- Unethical Hacker or “Cracker”
  ◆ Self-motivated
  ◆ Technically accomplished
  ◆ Creative
  ◆ Not productive
  ◆ Not positive
What is Cracking?

- Illegitimate use of a computer system
- Legitimate use
  - You use a valid account assigned for your use by a legitimate administrator of the system
  - Your use is consistent with the established policies for the system
  - Software you create not intended to circumvent established policies

Cracker Activities

- Trojan horse programs
- Virus programs
- Worm programs
- Logic bomb programs
- Sniffing
- Spoofing
- Flooding
Trojan Horse Programs
- Masquerades as a legitimate program
- Hides unwanted functions
- Trojan horse “login” program
- Can also be self-replicating

Virus Programs
- Self replicating
- Means of delivery
  - Downloaded software
  - Floppy disk
  - Email
  - Web
- Avoid detection
  - Expand existing code
  - Replace existing code
  - Polymorphic
- E.g., Melissa
Worm Programs

- Similar to viruses
- Short-lived
- Spread via the network
- Swamp resources
- E.g., Internet Worm

Logic Bomb Programs

- Waits for some condition
- Disrupts normal system operation
Sniffing and Spoofing

- **Sniffing**
  - Monitor network activity for login/password sequences

- **IP spoofing**
  - Masquerading as a machine with privileged access to target machine

Flooding

- **Ping flooding**
- **Denial-of-service attacks**
- **Flooding target machine with bogus traffic to block legitimate traffic**
- **SYN (synchronization) flooding**
  - Flood target computer with SYN requests whose ACKnowledgement is never returned
Who Are Crackers?

- Profiles
  - Novice
  - Student
  - Tourist
  - Crasher
  - Thief

Novice Crackers

- Young, emotionally immature
- Surface-level interest in security
- Willing to try proven methods, but unlikely to originate new techniques
- Little thought to consequences
Student Crackers

- Serious technical interest in security
- Desire to experiment with cracker techniques
- Perceived benign intent of learning or educating

Tourist Crackers

- Talents of Student
- Less benign, “peeping tom” motivation
- Break in and look around
  - Emails
  - Databases
  - System tools
  - Other machines
Crasher

- High level of technical expertise
- Motivated by desire to crash system
- Vandal
  - Desire to create more problems than just crashing system
  - Especially defacing public web pages

Thief

- Explicit criminal activity
  - Stealing credit card numbers or other valuable data
  - Altering records
Other Cracker Profiles

- Spy
- Terrorist
- Angered ex-employee
- Spurned suitor

Case Study

- U.S. vs. Craig Neidorf [1990]
- Electronic newsletter *Phrack*
  - Unauthorized access to computer and telecommunications systems
  - Roadmap to 911 phone system
- Denning article and responses
Case Study

- 911 information claimed proprietary
- Neidorf (16) charged with fraud and theft
  - Hacking phone system or “phreaking”
- Defense showed 911 information available to the public
- Charges dropped

Case Study: Denning

- Unauthorized access
  - 6 months in prison
- Unauthorized access with harmful intent
  - 5 years
- Unauthorized modification
  - 5 years
Responses

- Parker, SRI
  - Swift punishment
  - Encourage good behavior
- Levy, author of “Hackers: Heroes…”
  - Crackers, as a whole, beneficial
- Spafford, Purdue
  - Amount of damage considered in sentencing, not conviction

Responses

- Rotenberg, CPSR
  - Charges should not have been filed
  - Actions were not directly harmful
- Bloombecker, NCCCD
  - Crackers reflect our social values
    - Technological competence and impatience with the property rights of others
    - We continue to reward wizardry and ignore ethical behavior
Responses

- Stallman, GNU Project
  - Unauthorized access harms no one and should not be a crime
  - Laws against unauthorized access reflect the urge to control, stifling free society
  - Penalties will drive crackers to paranoia and eventually crime

Policies and Laws

- UTA Computer and Information Technology Usage Policy
  - [http://www.uta.edu/uta/wwwteam/citup.html](http://www.uta.edu/uta/wwwteam/citup.html)
- UTA Network Usage Guidelines
  - [http://www.uta.edu/acs/usage.htm](http://www.uta.edu/acs/usage.htm)
- Texas Computer Crimes Statute
  - [http://www.utexas.edu/policies/computercrimes.html](http://www.utexas.edu/policies/computercrimes.html)
Security Measures

- Risk analysis
  - Identify system weaknesses
- Audit logs
  - Altered by crackers if kept on disk
- Firewalls
  - Packet filtering

Security Tools

- COPS
- SATAN
- Tripwire
- Computer Emergency Response Team (CERT)
  - http://www.cert.org
Prevention

- Better security measures
- More widespread use of measures
- Better laws, stiffer penalties
- “Cracking is not cool” slogans
- Education
- Ethics

Points to Remember

- Crackers different from hackers
- Cracker activities are unethical, unprofessional, and usually illegal
- Legal system is adapting to better handle cracker crimes
- WWW and e-commerce increase the potential for harm
- Organizations lax in use of security measures