Principles of Computer Science I

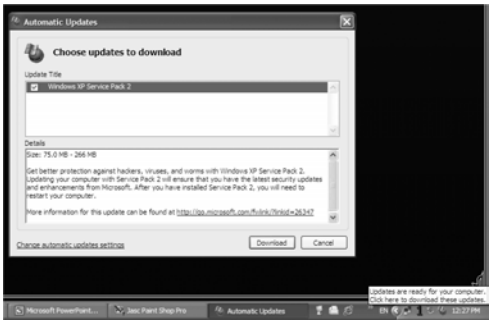
Prof. Nadeem Abdul Hamid

CSC 120A - Fall 2004

Lecture Unit 10

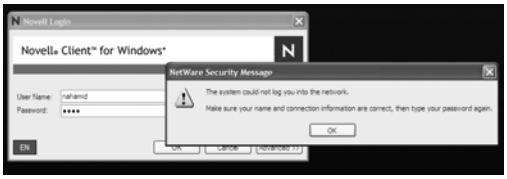
Computer Security & Privacy

Update and Security Patches



Scenario

There are a few minutes until class begins. You stop by the computer lab to check your email…



Gentlemen don't read other people's mail

- Henry Stimson, 20th century US diplomat

- **Risks to security and confidentiality**
  - **Internet or any computer environment set up for communication**
- **Protecting your account(s)**
  - **How paranoid should you be?**
- **Authentication**
  - **Process of having the operating system (or other service) verifying that someone trying to log on is a registered user**
  - **Usually a <username> <password> combination**
  - **Is that safe enough?**

A Brief(case) Example

- **Combination lock on briefcases**
  - **3 digits, range 0 to 9**
    = 10 * 10 * 10 = 1,000 possibilities
- **Cracker**
  - **person trying to get the password**
  - **2 seconds/try = 1,000 secs on average = 17 mins**
  - **Could just use a knife to cut through cover**

Security Factors

- **Number of digits (positions)**
  - **4 digits = 10,000 possibilities = 3 hours**
- **Number of possibilities per position**
  - **26 letters, 3 positions = 26*26*26 = 17,576 possibilities = 5 hours**
- **Time per trial**
  - **2 seconds vs. 20 seconds**
  - **System delays one minute after 3 failed attempts in a row**
- **Alternatives**
  - **Physical/brute force option…**

Cracking Computer Passwords

- A computer can try a different combination every millionth of a second
  - 6 positions = less than a second to try all possibilities
  - Usually systems force something like a delay of 1 minute after 3 failed login attempts
  - But sometimes cracker can try passwords on own system
- Need to increase # of password positions and possible values per position

Password Systems

- Letters + numbers + punctuation = 96 different characters (let's say 100)
- Six position password = 10^{12} possible combinations
- At 1 million (10^6) tries per second, still take a computer 1 million seconds = 17,000 mins = 275 hours = 10+ days
  - Add seventh position = 1,000 days = 3 years
  - Eight-character password = 300 years
    - But a computer 100 times faster brings it back down to 3 years
    - Or 100 computers working simultaneously trying 1 million combinations/sec brings it down even more

Dictionary Attacks

- Before trying all random possibilities, try only words from a "dictionary"
  - English and foreign-language words
  - Names of people, places, companies, organizations
  - Or personal data related to the person whose password it is: birthday, family members' name, friends' names…
  - Few minutes to run through combinations from several dictionaries
- Good password should survive such attack
  - Not be a word/name in any language
  - Kind of hard to do… at least throw in some random punctuation

Encryption

- A complementary method of preserving confidentiality
- Transfer/store information in a form incomprehensible to an outsider
- Encryption plays important role in authentication and password protection

"Cryptograms"

IFOJ LKFJN DCE LNPNC XNDJL DVF FOJ IDMRNJL UJFOVRM IFJMR FC MRSL KFCMSCNCM, D CNQ CDMSFC, KFCKNSPNE SC BSUNJMX, DCE ENESKDMNE MF MRN GJFGFLSMSFC MRDM DBB ANC DJN KJNDMNE NHODB. -- D BSCKFBC

- Letter frequencies:
  - A = 1 B = 6 C = 16 D = 14 E = 7 ....
- Edgar Allen Poe challenged newspaper readers to send him encrypted messages using *several different* substitution alphabets, and he deciphered every one he received

Caesar Cipher

- Shift every letters forward by three
  - "ZAP" → "CDS"
- On the computer, characters are really numbers
  - Just replace each char c with (c+3)%26
- Decryption…?
- Generalization: use a variable k instead of 3
  - $f(c) = (c + k) \% 26$
  - k is known only to the sender and receiver
- Problem: still relatively easy to break, by examining frequency of letters

One-Time Pads

- Have a sheet of numbers (known only to sender and receiver)
  - *e.g.* 3 4 19 23 4 16 9 2 12 10 ...
- Shift each letter of the message by the number corresponding to it
  - L: (12 + 3) % 26 = 15 = O
  - I: (9 + 4) % 26 = 13 = M
  - S: (19 + 19) % 26 = 12 = L
  - T: (20 + 23) % 26 = 17 = Q
  - E: (5 + 4) % 26 = 9 = I
  - N: (14 + 16) % 26 = 4 = D

One-Time Pads (cont.)

- This method is absolutely secure
- Problem(s):
  - Both sender and receiver must coordinate their sheet of numbers (can only use the sheet once)
  - If sheet of numbers is ever intercepted, coded messages can be read by the "bad guy"

Modern Day Encryption

- Techniques that are virtually unbreakable ("strong encryption")
- Darn keys!
  - Common to all the approaches we mentioned earlier
  - Synchronizing or distributing necessary shared information (key word/phrase/cipher sheet) is a basic problem
  - Possible to securely distribute keys without risk of interception?

A Padlock Scenario

- (Meet Alice and Bob)
  - Alice puts message in a metal box and locks with her padlock (she has the only key); mails to Bob
  - Bob can't open it, but attaches his own padlock to the box and mails it back to Alice, doubly-locked
  - Alice unlocks her padlock and mails back to Bob
  - Bob unlocks his and can extract the message
- With triple postage and delays, message can be exchanged through untrusted intermediaries (post office/courier service)
- Electronic equivalent: not so simple… (Diffie-Hellman-Merkle)
  - Generate a secret, mutually known key over insecure channels using two-way interaction

Public Key Encryption

- Alice has 100 identical padlocks (she has the only key); sends them (still open) to all her friends
  - Anyone wants to send Alice a secret message: puts it in a box and closes the padlock; now only Alice can open it and get the message
- Instead of padlocks, Alice distributes a public key (password) which allows anyone to encrypt a message that only she can decrypt using a secret key (password)
  - Asymmetric encryption system
  - Proposed by Diffie, 1975
  - Mathematical implementation: 1977

Rivest, Shamir, Adleman (RSA) Encryption

- Depends on using the product of two large prime numbers (100 or more digits)
- Factoring numbers that are product of two large primes is very hard, even using all the expected computer power for the next century
  - Only algorithm known so far to factor a number N is to simply try dividing by all possible primes up to N
- Product of the primes is the public key, actual primes are used for the decryption
- Uses exponentiation and modulus (%) to encrypt and decrypt short messages

Digital Signatures

- Used to validate identity
- Use the RSA algorithm in reverse (encrypt with private key, use public key to decrypt)
- Juliet sends message to Romeo, breaks it into two parts
  - Main Body = "Dear Romeo, … love, … love, … love …" (sparing the details)
  - Signature = "Sealed with kisses this 23rd day of April, 1595, at 10:30 PM, your loving Juliet."
  - Encrypts only the signature using her private key, and then encrypts entire message using Romeo's public key
  - Only Romeo can decrypt the entire message to find the body. Then he uses Juliet's public key to decrypt the signature… only she could have encrypted it with the corresponding private key

PGP, Encryption for the Masses

- *http://web.mit.edu/network/pgp.html*
- RSA strong encryption free for noncommerical use
- Phil Zimmerman
  - Made RSA practical for nonprogrammer, nontechnologist
  - Reduced computer power needed to use the algorithm
  - "P"retty "G"ood "P"rivacy

Attacks to Computer Systems

- Computer break-ins
  - Unauthorized user somehow gains access to an account on the system
  - Then tries to obtain "superuser"/"root"/adminstrator privileges
  - With superuser privileges, few limits to damage that can be caused
- Common defense
  - Firewall: restrict network access to computers from outside the system
    - Severe restrictions on legitimate users, false sense of security, can have weaknesses

Denial-of-Service (DOS)

- Simple, non-subtle attack
- Overload a server by sending millions of requests/emails/etc.
- Attacks made from other systems that have been compromised/broken into
  - Hard to trace actual perpetrator
- Used to mask/divert attention from other kinds of attacks, or to disable other software defense mechanisms

Man-in-the-Middle

- Alice sending messages to Bob; Charlie listening in (like a wire-tap)
- Charlie can do more than listen in…
  - Alice asks Bob (her banker) to transfer $100 from her business acct to her personal one, supplies all her appropriate passwords and authentication
  - Charlie intercepts message, changes $100 to $10,000 and replaces Alice's personal acct number with another one set up for this purpose, then sends message on to Bob; uses all the passwords/authentication already provided by Alice
  - Bob sends back confirmation reply to Alice saying $10,000 has been transferred; Charlie intercepts and changes $10,000 back to $100
  - Alice doesn't realize until her next bank statement; Charlie's already withdraw his cash and is in Hawaii

Political/Social Issues

- Law enforcement officials: Make laws disallowing strong encryption/forcing it to be weak
  - (paraphrasing NRA) "If strong encryption were illegal, then only criminals would use it."
  - Since some thieves wear gloves to avoid leaving fingerprints, gloves should be illegal
- Govt labels strong encryption as a "munition" – illegal to export munitions without a license; so that foreign govts cannot communicate without NSA being able to monitor them
  - Realistically? With Internet, and impossibility of controlling every floppy disk, tape, CD-ROM going out of country?

Viruses, Trojan Horses

- Be very wary of those emails ☺
- Don't click!
- Be careful what software you install
- Pirated copies of software (*e.g.* too-good-to-be-true free download of Norton AntiVirus) may be loaded with virus payload
- If not careful: your computer could be used for launching DOS attacks, spreading virus-infested emails, storing illegal files…

A Final Problem

- Losing your password
- Go to C&T to retrieve it
  - Means someone's keeping track of it
    - How much is someone being paid and how much would someone else being will to pay for those passwords?
  - Well, usually can't retrieve passwords; only reset to a new one
    - Forgetting it = Embarrassing nuisance
- Losing key to encrypted files
  - Oops!
  - Well, maybe you can break the encryption to get your data back
    - But then that wasn't a good encryption scheme… someone else could have broken it
  - Write down the key… weakens security but is a compromise to avoid losing data entirely?