Wrocław University of Technology

Internet Engineering

Tomasz Surmacz

Secure Systems and Networks

Version: *30.09.2012 23:49*

30▷09▷2012 23.49
full text (142 pages)
final

Wrocław 2011

Contents

List of Figures

Chapter 2

Basic security in computer systems

XXX (General intro – source of problems, social engineering, basic security principles) more

2.1 The main problem are people

Although it is possible to automate many access rules and procedures and deploy very sophisticated security policies, research shows that the weakest link in the computer system security are the people who use it. This is not even because people want to break the security intentionally, but due to several factors. These include:

- Lack of understanding for the rules.

  People tend to create simple, easy to remember passwords or store them in easily accessible places, such as a yellow sticky note under the table. Or are easily tricked to give away information that should be kept

Characters used	no. of passwords	breaking time required
4-digit password (PIN code)	10000	1.2 seconds
typical language vocabulary	100000	12 s
4-letter password	456976	1 minute
8-digits password	$1 \cdot 10^8$	3 hours 25 mins
6-letter password	$3 \cdot 10^8$	11 hours
8-letter password, lowercase	$2 \cdot 10^{10}$	302 days
8-character password, lowercase and digits	$2.8 \cdot 10^{12}$	11 years
8-letter password, mixed case	$5 \cdot 10^{13}$	212 years
8 characters, all ASCII 32-127	$7 \cdot 10^{15}$	28594 years
8 characters, all keyboard 1-127	$6.7 \cdot 10^{16}$	268246 years
All possibilities for MD5 hash function	$3.4 \cdot 10^{38}$	$1.3 \cdot 10^{27}$ years
Estimated age of the Universe		10^{10} years

Table 3.1: Strength of different passwords

may either work on a partial dictionary, or can be given a subset of all passwords. So the time needed to crack some passwords decreases in linear proportion to the number of computers that participate in the task. E.g. if we could afford to dedicate 1 000 000 computers for such a job, the time required decreases by 6 orders of magnitude, i.e. just over 3 months for a 8-digit password that may contain any characters of codes 1-127.

There are a lot of ready-to-use passwords crackers available from the Internet. Some of the most commonly used include John the Ripper, THC Hydra and the original crack program. There are also system- or application-specific crackers that can be dedicated to cracking passwords needed for accessing *PDF* or *ZIP* files, cracking WEP/WPA keys (Aircrack or Airsnort), or "recovering" passwords used to protect MS-Windows systems (e.g. Cain and Abel or SolarWinds). A useful list of available crackers may be found in [Lyo06].

misuse. So do not leave your phone on your desk when making a coffee break and do not leave your terminal unlocked, especially if you have an online banking session still opened somewhere.

3.2.4 Tokens

Tokens are small pieces of hardware that can be used as authentication devices, much like the keys may be used to open locks. For token authentication to succeed, the user has to prove that he has the token with him which may be checked in many ways. Tokens connected to RS232, parallel or USB port of a computer system may be used as a kind of a hardware license key, but nowadays it is much easier to depend on some short cryptographic data to be shown by a token itself and entered by a user.

Figure 3.4: RSA OTP tokens

Tokens may either work as standalone devices independent of the outside world (i.e. only producing some output needed for authentication) or work bidirectionally – requiring some input (a challenge) and producing the adequate response. Challenge-response tokens either require this data to be entered numerically through the built-in keypad, or contain some input device, such as photodiode, to allow some simple transmission by a "blinking" a special applet on the computer screen and holding the token in the right position to receive that data. Once the data is entered into the token, it calculates the response and displays in on a LCD screen, so that it may be typed by a user wishing to authenticate himself. The response calculation algorithm has to be secret, otherwise the token function could be duplicated.

section! login services – spoofing, no server verification

methods of authentication, first of all it checks the credentials of the connecting host/client for any signs of spoofing, and only then allows alternative authentication methods, such as user login keys (similar to certificates).

login services – spoofing, no server verification

4.6.2 FTP

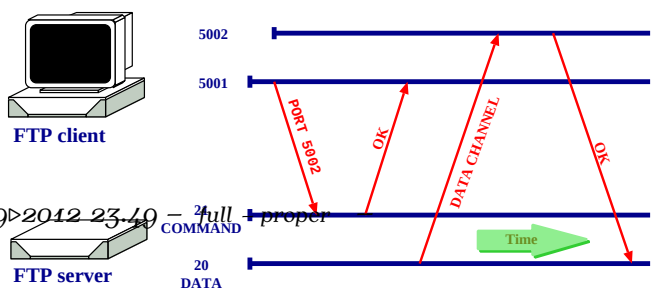
FTP protocol is one of the most complex and sophisticated protocols developed so far. Its main goals are to provide a fast an reliable data transfer with maximum possible transfer rates, but also allowing to abort the lengthy transfers at any time or to resume transfers that have failed for any reason. All servers allow also conversion between text formats between Unix/DOS/Mac machines, and modern servers allow features like file compression "on the fly" or transfer of the whole directories with a single GET command.

The way that FTP protocol works is actually quite complicated and may not work in modern firewalled networks by default. Port 21 is used for control connection and port 20 for data transfer. FTP server can operate either in *active mode*, which is the default for most of the clients, or the *passive mode*, which is preferred by the web-based clients such as FIREFOX. These two modes of operation are shown in fig. 4.8.

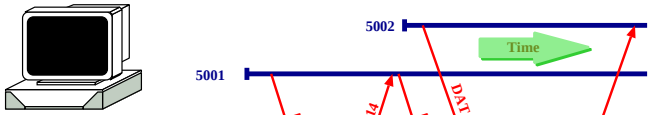
In active mode (fig. 4.8(a)) the client connects first to port 21 of the server and issues commands, but commands requiring data transfer, such as `DIR`, `GET` or `RETR` cause the client to issue a `PORT` command, informing a server about the port number that client has opened. It is the server then who opens the connection to the client from its own port 20 and the data is transferred using this new connection, while the old one may still be used to issue other commands (e.g. to abort the transfer). When transfer is complete, this connection is closed automatically.

wrapfig verify

Data transfer in passive mode (fig. 4.8(b))



(a) FTP in active mode



dancing X-mas tree program', 'Here are nude pictures of you in a ZIPped .exe file, use this password to uncompress the archive: ...').

section! e-mail reliability

E-mail reliability

e-mail reliability

section! viruses and mal-ware in email

Viruses and other malware

viruses and malware in email

Mail servers are safe XXX Mostly treat emails as black-boxes MIME extensions allow many types of data to be sent: images, HTML files, sounds Clients are buggy Inappropriate execution of attachments helps spreading viruses

rewrite

Open Relays

E-mail systems pre-date the Internet and deep in their design the basic mode of operation is still accept-store-forward. Much the same, as the traditional Post system works – letters are accepted over the counter or from postboxes, then they are sorted and forwarded to next Post Office in the chain, which either delivers the letter locally, or forwards it to the next Post Office, closer to the final destination.

All e-mail servers work in a similar way, forwarding messages on behalf of other systems, in a shared effort to deliver them to final users. However, what was good when the general system-to-system connectivity was not very common, leads now to a mail-relay vulnerability often abused by spammers. A spammer that has poor Internet connectivity (either in terms of a poor bandwidth or if his IP address is filtered by anti-spam filters) may connect to a vulnerable e-mail system and inject his spam messages there. The vulnerable MTA server will accept such a message and try to deliver it to all the recipients, even if they are not located on the server's system. Each such a

by `identd` which show unusual number of outgoing connections.

section! botnets and zombies

5.4 Botnets

botnets and zombies

5.5 Phishing attacks

The term *phishing* comes from joining together two words – *password* and *fishing* and describes the fraudulent actions of setting up fake servers collecting sensitive information from unsuspecting users – such as passwords (hence the name), usernames, credit card numbers, authorization tokens for bank operations, etc. Phishing attacks are usually targeted at popular social web sites, auction sites, online banks, but also the IT departments of various big institutions.

The typical attack starts with sending a bait – a massive e-mailing to a targeted or random group of users. The mail itself may look like that shown in fig. 5.1 – it will warn the user that his/her access to the mentioned service is now limited due to some unusual activity detected and that the user should log in immediately to resolve the problem and regain the full access to the account. The confirmation link is then provided which may look like a legitimate link to the mentioned service, but in fact leads to the fake site which has been previously set up in order to intercept user login attempts. This fake site will mimic the real one, otherwise the users could instantly tell that something is wrong.

In the sample e-mail shown in fig. 5.1 the link is shown twice – once in the mail body where it looks like the Amazon reference (but in fact is a *link name*), and second time – in the "References" section, where all links are expanded to show their actual targets. This is how textual e-mail clients (such as MUTT or PINE) show such e-mails. Webmail-type browsing in FIREFOX or

```
From: "Amazon.com" <account-update@amazon.com>
Subject: Revision to Your Amazon.com Account

  Amazon Information
  We are contacting you to inform you that our Account Review
  Team identified some unusual activity in your account. In
  accordance with Amazon's User Agreement and to ensure that
  your account has not been compromised, access to your account
  was limited. Your account access will remain limited until this
  issue has been resolved.  This process is mandatory, and if not
  completed within the nearest time your account or credit card
  may be subject for temporary suspension. To securely confirm
  your Amazon information please click on the link bellow:
  [1]https://www.amazon.com/cgi-bin/webscr?cmd=login-run

  We encourage you to log in and perform the steps necessary to
  restore your account access as soon as possible. Allowing your
  account access to remain limited for an extended period of time
  may result in further limitations on the use of your account
  and possible account closure.

References

  1. http://96.10.247.13/evo/www.amazon.com/index.html
```

Figure 5.1: Phishing e-mail targeting Amazon.com users

Internet Explorer will show just the name, and the actual link target will be shown in the browser status line only when the mouse cursor is over the link name. And even not for certain, as some bugs in Internet Explorer may truncate the link being shown, or some special characters in the link may cause only the trailing part of the link being visible, and that part may look like the normal link.

Modern browsers contain mechanisms to warn users against some of the phishing attacks – the ones that have been already reported. The list of sites hosting the fake pages is maintained and updated regularly, so that a

Mode	Description
ECB Electronic Code Book	Each plaintext block is encoded independently of other blocks
CBC Cipher Block Chaining	Instead of just the plaintext, the algorithm is fed with the XOR of the plaintext and the previous ciphertext.
CFB Cipher Feedback	Input is processed n bits at a time (les then or equal to the block size). Previous ciphertext is used as input to produce the pseudorandom data which is then xored with current plaintext.
OFB Output Feedback	Similar to CFB, except the input is not the final ciphertext, but the output of the DES encryptor (i.e. before XOR-ing it with the plaintext)
CTR Counter	Every plaintext block in XORed with an encrypted counter, which is incremented with each block
CTS Ciphertext Stealing	Used in addition to ECB or CBC for padding the last plaintext block with the high order bits of the second to last cipherblock (stealing it from the output). The new full last block is then encrypted and exchanged with the stolen cipherblock, truncated by removing the stolen bits, so that the overall message length does not change.

Table 7.1: Block cipher modes of operation

blocks that has been sent so far, so encrypting the same plaintext several times results in different cipherblocks. It is simply done by XOR-ing each plaintext block fed to the encryptor with the cipherblock obtained in the previous round. This however means that if a single encrypted block is lost or altered during transmission, it will be not possible to decrypt the rest of the transmission. A little modification of this mode called *Output Feedback Mode* (OFB, see fig. 7.2) helps overcoming this problem by moving where this chaining information is attached – if a single block is malformed, it will

Bibliography

[Ale01] Aleph One. Smashing the stack for fun and profit. *Phrack*, 49, April 2001. http://www.phrack.org/archives/49/.

[Bau05] Michael D. Bauer. *Building secure servers with Linux*. O'Reilly & Associates, Inc., second edition, 2005.

[BH10] M. Brown and R. Housley. Transport Layer Security (TLS) Authorization Extensions. RFC 5878 (Experimental), May 2010.

[BSB05] Daniel J. Barrett, Richard E. Silverman, and Robert G. Byrnes. *SSH: The Secure Shell: The Definitive Guide*. O'Reilly & Associates, Inc., second edition, 2005.

[Che92] W.R. Cheswick. An evening with Berferd, in which a cracker is lured, endured, and studied. In *Proceedings of the Winter USENIX Conference (San Francisco)*, January 1992.

[Cor10] The MITRE Corporation. Top 25 most dangerous software errors. http://cwe.mitre.org/top25/index.html, December 2010.

[CZ95] D. Brent Chapman and Elizabeth D. Zwicky. *Building Internet Firewalls*. O'Reilly & Associates, Inc., September 1995.

[DA99] T. Dierks and C. Allen. The TLS Protocol Version 1.0. RFC 2246 (Proposed Standard), January 1999.

Index

Todo list