Analyse du systÃÍme de sÃľcuritÃľ du drone : *AR.Drone 2.0 Quad-Copter*

[Codages et SÃľcuritÃľ des RÃľseaux]

CLAURE CABRERA Oscar Mike
Filiere ISSC
ENSIMAG
Grenoble, France
oscar-mike.claure-cabrera@ensimag.grenoble-inp.fr

DOYEN-LE BOULAIRE Marine
Filiere ISSC
ENSIMAG
Grenoble, France
marine.doyen-le-boulaire@ensimag.grenoble-inp.fr

ABSTRACT

Les drones ont commencÃľ pour etre utilisÃľs au profit des forces armÃľes ou de sÃľcuritÃľ dâĂŹun ÃL'tat, mais de plus en plus ont aussi des applications civiles comme la recherche, le cinema, et l'environnement.

CâĂŹest Ãă cause de ces nouveaux opprtunitÃľs de marche qu'on a commencÃľ Ãă commercialiser les drones pour cibler diffÃľrents activitÃľs...

Drones de plus en plus utilisÃľes, source de attaques...

Dans cet article on fait lâĂŹÃľtude du systÃÍme de communication de lâĂŹAR.Drone 2.0 Quad-Copter auquel suive lâĂŹÃľtude de faiblesses dans le systÃÍme et la dÃľmonstration de possibles scÃľnarios dâĂŹattaque.

(Il faut continuer a faire le blah blah)

Categories and Subject Descriptors

H.4 [**Information Systems Applications**]: Miscellaneous; D.2.8 [**Software Engineering**]: Metrics—*complexity measures, performance measures*

General Terms

Theory

Keywords

Security, Drone

1. INTRODUCTION

LâĂŹAR.Drone est un drone Quad-Copter commandÃľ Ãă distance grÃćce Ãă lâĂŹapplication AR.FreeFlight disponible pour les apparails mobiles de plateforme iOS et Android. La connexion c'est faite sur un rÃľseau Wi-Fi non-sÃľcurisÃľ montÃľ par le drone aprÃÍs son lâĂŹallumage, auquel tout appareil peut se connecter et envoyer des instructions et recevoir la tÃľlÃľmetrie et le flux vidÃľo.

MÃłme si lâĂŹAR.Drone 2.0 nâĂŹest pas un drone professionnel, ses caractÃľristiques physiques et facilitÃľ de control, grÃćce Ãă lâĂŹapplication AR.FreeFlight font de lui un outil puissante. LâĂŹAR.DRONE offre aussi la possibilitÃľ, en utilisant son propre SDK, de dÃľvelopper des applications diverses ciblant la recherche, la sÃľcuritÃľ, les jeux, la cinÃľmatographie, etc.

2. DÃL'VELOPPEMENT *(MAIN BODY)*

Typically, the body of a paper is organized into a hierarchical structure, with numbered or unnumbered headings for sections, subsections, sub-subsections, and even smaller sections. The command `\section` that precedes this paragraph is part of such a hierarchy.[1] LaTeX handles the numbering and placement of these headings for you, when you use the appropriate heading commands around the titles of the headings. If you want a sub-subsection or smaller part to be unnumbered in your output, simply append an asterisk to the command name. Examples of both numbered and unnumbered headings will appear throughout the balance of this sample document.

Because the entire article is contained in the **document** environment, you can indicate the start of a new paragraph with a blank line in your input file; that is why this sentence forms a separate paragraph.

2.1 SystÃÍme de Communication

Une fois allumÃľ, l'AR.Drone 2.0 mis en place un point d'access non-securisÃľ appelÃľ ardrone2-XX ou XX est une sÃľquence de nÃžmeros apparentement alÃľatoires. 090933. DÃľjÃă connectÃľ, on est capable de faire un scan de ports ciblant l'adresse IP du drone (192.168.1.1), en utilisant l'application NMAP. Le rÃľsultats de ce scan nous-montre que on a ports ouvertsÂă:

[1] This is the second footnote. It starts a series of three footnotes that add nothing informational, but just give an idea of how footnotes work and look. It is a wordy one, just so you see how a longish one plays out.

Table 1: Resultat de l'analyse de ports du AR.Drone

Port	Nom du service	Commentaires
21	FTP	/Data/Video/
23	Telnet	Access ROOT
5555	freeciv	streaming du video

C'est trÃĺs important de remarquer que les services FTP et TELNET ne sont pas securisÃl's (protegÃl's par mot de passe) c'est suffi de se connecter Ãă le rÃl'seaux proposÃl' par le drone et initialiser ces services vers les ports, par defaut, de FTP (21) et TELNET (23).

2.2 SystÃĺme Interne

penser Ãă quelque lignes ici :(

2.3 Scenarios d'attaque

Ici on dÃl'taile deux possible scenarios d'attaque ciblant le AR.Drone

2.3.1 RÃl'initialisation du drone

Le processus programe.elf contrÃt'le est le chargÃl' de commander le drone. Si on termine ce processus tout le systÃĺme de control se reinitialise et crash le drone.

On peut donner un scenario d'attaque trÃĺs basique dans lequel on termine succesivement le processus controleur du drone. A continuation on detail les pas a suivre pour effectuer ce type d'attaque

- Faire un script qui cherche le PID du processus Âń program.elf Âż et le termine cycliquement. - Se connecter Ãă le reseau non-securisÃl' proposÃl' par l'AR.Drone - Transferer ce script au drone (via FTP), lui donner des permises d'execution et lancer le script (via TELNET)

2.3.2 DÃl'connection du client propietaire

2.4 Citations

Citations to articles [1, 3, 2, 4], conference proceedings [3] or books [6, 5] listed in the Bibliography section of your article will occur throughout the text of your article. You should use BibTeX to automatically produce this bibliography; you simply need to insert one of several citation commands with a key of the item cited in the proper location in the `.tex` file [5]. The key is a short reference you invent to uniquely identify each work; in this sample document, the key is the first author's surname and a word from the title. This identifying key is included with each item in the `.bib` file for your article.

The details of the construction of the `.bib` file are beyond the scope of this sample document, but more information can be found in the *Author's Guide*, and exhaustive details in the *LaTeX User's Guide*[5].

This article shows only the plainest form of the citation command, using `\cite`. This is what is stipulated in the SIGS style specifications. No other citation format is endorsed.

Table 2: Frequency of Special Characters

Non-English or Math	Frequency	Comments
Ø	1 in 1,000	For Swedish names
π	1 in 5	Common in math
\$	4 in 5	Used in business
Ψ_1^2	1 in 40,000	Unexplained usage

Figure 1: A sample black and white graphic (.eps format).

2.5 Tables

Because tables cannot be split across pages, the best placement for them is typically the top of the page nearest their initial cite. To ensure this proper "floating" placement of tables, use the environment **table** to enclose the table's contents and the table caption. The contents of the table itself must go in the **tabular** environment, to be aligned properly in rows and columns, with the desired horizontal and vertical rules. Again, detailed instructions on **tabular** material is found in the *LaTeX User's Guide*.

Immediately following this sentence is the point at which Table 1 is included in the input file; compare the placement of the table here with the table in the printed dvi output of this document.

To set a wider table, which takes up the whole width of the page's live area, use the environment **table*** to enclose the table's contents and the table caption. As with a single-column table, this wide table will "float" to a location deemed more desirable. Immediately following this sentence is the point at which Table 2 is included in the input file; again, it is instructive to compare the placement of the table here with the table in the printed dvi output of this document.

2.6 Figures

Like tables, figures cannot be split across pages; the best placement for them is typically the top or the bottom of the page nearest their initial cite. To ensure this proper "floating" placement of figures, use the environment **figure** to enclose the figure and its caption.

This sample document contains examples of **.eps** and **.ps** files to be displayable with LaTeX. More details on each of these is found in the *Author's Guide*.

As was the case with tables, you may want a figure that spans two columns. To do this, and still to ensure proper "floating" placement of tables, use the environment **figure*** to enclose the figure and its caption.

Note that either **.ps** or **.eps** formats are used; use the `\epsfig` or `\psfig` commands as appropriate for the different file types.

Table 3: Some Typical Commands

Command	A Number	Comments
`\alignauthor`	100	Author alignment
`\numberofauthors`	200	Author enumeration
`\table`	300	For tables
`\table*`	400	For wider tables

Figure 2: A sample black and white graphic (.eps format) that has been resized with the `epsfig` command.

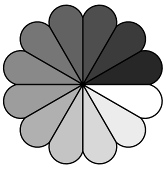

Figure 3: A sample black and white graphic (.ps format) that has been resized with the `psfig` command.

2.7 Theorem-like Constructs

Other common constructs that may occur in your article are the forms for logical constructs like theorems, axioms, corollaries and proofs. There are two forms, one produced by the command `\newtheorem` and the other by the command `\newdef`; perhaps the clearest and easiest way to distinguish them is to compare the two in the output of this sample document:

This uses the **theorem** environment, created by the `\newtheorem` command:

THEOREM 1. *Let f be continuous on $[a,b]$. If G is an antiderivative for f on $[a,b]$, then*

$$\int_a^b f(t)dt = G(b) - G(a).$$

The other uses the **definition** environment, created by the `\newdef` command:

Definition 1. If z is irrational, then by e^z we mean the unique number which has logarithm z:

$$\log e^z = z$$

Two lists of constructs that use one of these forms is given in the *Author's Guidelines.*

and don't forget to end the environment with figure*, not figure!

There is one other similar construct environment, which is already set up for you; i.e. you must *not* use a `\newdef` command to create it: the **proof** environment. Here is a example of its use:

PROOF. Suppose on the contrary there exists a real number L such that

$$\lim_{x\to\infty} \frac{f(x)}{g(x)} = L.$$

Then

$$l = \lim_{x\to c} f(x) = \lim_{x\to c} \left[gx \cdot \frac{f(x)}{g(x)} \right] = \lim_{x\to c} g(x) \cdot \lim_{x\to c} \frac{f(x)}{g(x)} = 0 \cdot L = 0,$$

which contradicts our assumption that $l \neq 0$. □

Complete rules about using these environments and using the two different creation commands are in the *Author's Guide*; please consult it for more detailed instructions. If you need to use another construct, not listed therein, which you want to have the same formatting as the Theorem or the Definition[6] shown above, use the `\newtheorem` or the `\newdef` command, respectively, to create it.

A *Caveat* for the TEX Expert

Because you have just been given permission to use the `\newdef` command to create a new form, you might think you can use TEX's `\def` to create a new command: *Please refrain from doing this!* Remember that your LATEX source code is primarily intended to create camera-ready copy, but may be converted to other forms – e.g. HTML. If you inadvertently omit some or all of the `\def`s recompilation will be, to say the least, problematic.

3. CONCLUSIONS

This paragraph will end the body of this sample document. Remember that you might still have Acknowledgments or Appendices; brief samples of these follow. There is still the Bibliography to deal with; and we will make a disclaimer about that here: with the exception of the reference to the LATEX book, the citations in this paper are to articles which have nothing to do with the present subject and are used as examples only.

4. ACKNOWLEDGMENTS

This section is optional; it is a location for you to acknowledge grants, funding, editing assistance and what have you. In the present case, for example, the authors would like to thank Gerald Murray of ACM for his help in codifying this *Author's Guide* and the **.cls** and **.tex** files that it describes.

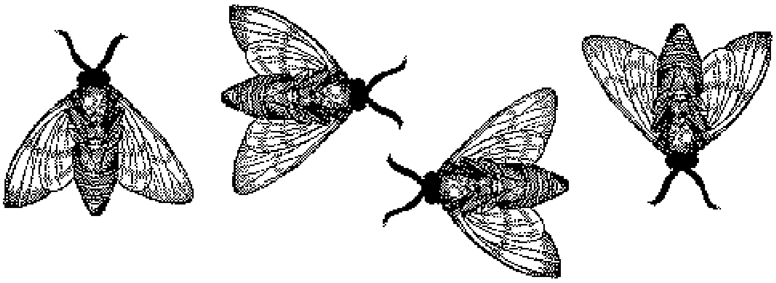

Figure 4: A sample black and white graphic (.eps format) that needs to span two columns of text.

5. REFERENCES

[1] M. Bowman, S. K. Debray, and L. L. Peterson. Reasoning about naming systems. *ACM Trans. Program. Lang. Syst.*, 15(5):795–825, November 1993.

[2] J. Braams. Babel, a multilingual style-option system for use with latex's standard document styles. *TUGboat*, 12(2):291–301, June 1991.

[3] M. Clark. Post congress tristesse. In *TeX90 Conference Proceedings*, pages 84–89. TeX Users Group, March 1991.

[4] M. Herlihy. A methodology for implementing highly concurrent data objects. *ACM Trans. Program. Lang. Syst.*, 15(5):745–770, November 1993.

[5] L. Lamport. *LaTeX User's Guide and Document Reference Manual.* Addison-Wesley Publishing Company, Reading, Massachusetts, 1986.

[6] S. Salas and E. Hille. *Calculus: One and Several Variable.* John Wiley and Sons, New York, 1978.

APPENDIX

A. HEADINGS IN APPENDICES

The rules about hierarchical headings discussed above for the body of the article are different in the appendices. In the **appendix** environment, the command **section** is used to indicate the start of each Appendix, with alphabetic order designation (i.e. the first is A, the second B, etc.) and a title (if you include one). So, if you need hierarchical structure *within* an Appendix, start with **subsection** as the highest level. Here is an outline of the body of this document in Appendix-appropriate form:

A.1 Introduction

A.2 The Body of the Paper

A.2.1 Type Changes and Special Characters

A.2.2 Math Equations

Inline (In-text) Equations

Display Equations

A.2.3 Citations

A.2.4 Tables

A.2.5 Figures

A.2.6 Theorem-like Constructs

A Caveat for the TEX Expert

A.3 Conclusions

A.4 Acknowledgments

A.5 Additional Authors

This section is inserted by LATEX; you do not insert it. You just add the names and information in the `\additionalauthors` command at the start of the document.

A.6 References

Generated by bibtex from your .bib file. Run latex, then bibtex, then latex twice (to resolve references) to create the .bbl file. Insert that .bbl file into the .tex source file and comment out the command `\thebibliography`.

B. MORE HELP FOR THE HARDY

The acm_proc_article-sp document class file itself is chockfull of succinct and helpful comments. If you consider yourself a moderately experienced to expert user of LATEX, you may find reading it useful but please remember not to change it.