***3413ICT NETWORK SECURITY - Assignment 1***

***Designing Technical Security Plan for***

***Medium-Scaled Wide Area Network***

Anthony Guevara  
S2877416

Ashmore, QLD, Australia

anthony.guevar@griffithuni.edu.au

*Abstract*—This electronic document is a “live” template and already defines the components of your paper [title, text, heads, etc.] in its style sheet. *\*CRITICAL: Do Not Use Symbols, Special Characters, or Math in Paper Title or Abstract*. (*Abstract*)

Keywords—component; formatting; style; styling; insert (key words)

# Introduction (*Heading 1*)

The purpose of this paper is to provide technical details on meeting a customer’s security requirements. A medium scale motel has a number of LAN segments located at different branches across Australia. These branches are located in Gold Coast, Sydney, Melbourne, and Perth with the headquarters located in Brisbane. Currently the LAN segments are not interconnected and operate independently of one another. The client has requested that they would like to connect all of the different branches allowing secure communication to headquarters in Brisbane.

# Requirements

## Workflow

The client has requested that the implementation

First, confirm that you have the correct template for your paper size. This template has been tailored for output on the A4 paper size. If you are using US letter-sized paper, please close this file and download the file “MSW\_USltr\_format”.

## Security

The template is used to format your paper and style the text. All margins, column widths, line spaces, and text fonts are prescribed; please do not alter them. You may note peculiarities. For example, the head margin in this template measures proportionately more than is customary. This measurement and others are deliberate, using specifications that anticipate your paper as one part of the entire proceedings, and not as an independent document. Please do not revise any of the current designations.

# Prepare Your Paper Before Styling

Before you begin to format your paper, first write and save the content as a separate text file. Keep your text and graphic files separate until after the text has been formatted and styled. Do not use hard tabs, and limit use of hard returns to only one return at the end of a paragraph. Do not add any kind of pagination anywhere in the paper. Do not number text heads-the template will do that for you.

Finally, complete content and organizational editing before formatting. Please take note of the following items when proofreading spelling and grammar:

## Abbreviations and Acronyms

Define abbreviations and acronyms the first time they are used in the text, even after they have been defined in the abstract. Abbreviations such as IEEE, SI, MKS, CGS, sc, dc, and rms do not have to be defined. Do not use abbreviations in the title or heads unless they are unavoidable.

## Units

* Use either SI (MKS) or CGS as primary units. (SI units are encouraged.) English units may be used as secondary units (in parentheses). An exception would be the use of English units as identifiers in trade, such as “3.5-inch disk drive.”
* Avoid combining SI and CGS units, such as current in amperes and magnetic field in oersteds. This often leads to confusion because equations do not balance dimensionally. If you must use mixed units, clearly state the units for each quantity that you use in an equation.
* Do not mix complete spellings and abbreviations of units: “Wb/m2” or “webers per square meter,” not “webers/m2.” Spell units when they appear in text: “...a few henries,” not “...a few H.”

Identify applicable sponsor/s here. If no sponsors, delete this text box (*sponsors).*

* Use a zero before decimal points: “0.25,” not “.25.” Use “cm3,” not “cc.” (*bullet list*)

## Equations

The equations are an exception to the prescribed specifications of this template. You will need to determine whether or not your equation should be typed using either the Times New Roman or the Symbol font (please no other font). To create multileveled equations, it may be necessary to treat the equation as a graphic and insert it into the text after your paper is styled.

Number equations consecutively. Equation numbers, within parentheses, are to position flush right, as in (1), using a right tab stop. To make your equations more compact, you may use the solidus ( / ), the exp function, or appropriate exponents. Italicize Roman symbols for quantities and variables, but not Greek symbols. Use a long dash rather than a hyphen for a minus sign. Punctuate equations with commas or periods when they are part of a sentence, as in

*a**b*    

Note that the equation is centered using a center tab stop. Be sure that the symbols in your equation have been defined before or immediately following the equation. Use “(1),” not “Eq. (1)” or “equation (1),” except at the beginning of a sentence: “Equation (1) is ...”

## Some Common Mistakes

* The word “data” is plural, not singular.
* The subscript for the permeability of vacuum **0, and other common scientific constants, is zero with subscript formatting, not a lowercase letter “o.”
* In American English, commas, semi-/colons, periods, question and exclamation marks are located within quotation marks only when a complete thought or name is cited, such as a title or full quotation. When quotation marks are used, instead of a bold or italic typeface, to highlight a word or phrase, punctuation should appear outside of the quotation marks. A parenthetical phrase or statement at the end of a sentence is punctuated outside of the closing parenthesis (like this). (A parenthetical sentence is punctuated within the parentheses.)
* A graph within a graph is an “inset,” not an “insert.” The word alternatively is preferred to the word “alternately” (unless you really mean something that alternates).
* Do not use the word “essentially” to mean “approximately” or “effectively.”
* In your paper title, if the words “that uses” can accurately replace the word using, capitalize the “u”; if not, keep using lower-cased.
* Be aware of the different meanings of the homophones “affect” and “effect,” “complement” and “compliment,” “discreet” and “discrete,” “principal” and “principle.”
* Do not confuse “imply” and “infer.”
* The prefix “non” is not a word; it should be joined to the word it modifies, usually without a hyphen.
* There is no period after the “et” in the Latin abbreviation “et al.”
* The abbreviation “i.e.” means “that is,” and the abbreviation “e.g.” means “for example.”

An excellent style manual for science writers is [7].

# Using the Template

After the text edit has been completed, the paper is ready for the template. Duplicate the template file by using the Save As command, and use the naming convention prescribed by your conference for the name of your paper. In this newly created file, highlight all of the contents and import your prepared text file. You are now ready to style your paper; use the scroll down window on the left of the MS Word Formatting toolbar.

## Authors and Affiliations

The template is designed so that author affiliations are not repeated each time for multiple authors of the same affiliation. Please keep your affiliations as succinct as possible (for example, do not differentiate among departments of the same organization). This template was designed for two affiliations.

### For author/s of only one affiliation (Heading 3): To change the default, adjust the template as follows.

#### Selection (Heading 4): Highlight all author and affiliation lines.

#### Change number of columns: Select the Columns icon from the MS Word Standard toolbar and then select “1 Column” from the selection palette.

#### Deletion: Delete the author and affiliation lines for the second affiliation.

### For author/s of more than two affiliations: To change the default, adjust the template as follows.

#### Selection: Highlight all author and affiliation lines.

#### Change number of columns: Select the “Columns” icon from the MS Word Standard toolbar and then select “1 Column” from the selection palette.

#### Highlight author and affiliation lines of affiliation 1 and copy this selection.

#### Formatting: Insert one hard return immediately after the last character of the last affiliation line. Then paste down the copy of affiliation 1. Repeat as necessary for each additional affiliation.

#### Reassign number of columns: Place your cursor to the right of the last character of the last affiliation line of an even numbered affiliation (e.g., if there are five affiliations, place your cursor at end of fourth affiliation). Drag the cursor up to highlight all of the above author and affiliation lines. Go to Column icon and select “2 Columns”. If you have an odd number of affiliations, the final affiliation will be centered on the page; all previous will be in two columns.

## Identify the Headings

Headings, or heads, are organizational devices that guide the reader through your paper. There are two types: component heads and text heads.

Component heads identify the different components of your paper and are not topically subordinate to each other. Examples include ACKNOWLEDGMENTS and REFERENCES, and for these, the correct style to use is “Heading 5.” Use “figure caption” for your Figure captions, and “table head” for your table title. Run-in heads, such as “Abstract,” will require you to apply a style (in this case, italic) in addition to the style provided by the drop down menu to differentiate the head from the text.

Text heads organize the topics on a relational, hierarchical basis. For example, the paper title is the primary text head because all subsequent material relates and elaborates on this one topic. If there are two or more sub-topics, the next level head (uppercase Roman numerals) should be used and, conversely, if there are not at least two sub-topics, then no subheads should be introduced. Styles named “Heading 1,” “Heading 2,” “Heading 3,” and “Heading 4” are prescribed.

## Figures and Tables

### Positioning Figures and Tables: Place figures and tables at the top and bottom of columns. Avoid placing them in the middle of columns. Large figures and tables may span across both columns. Figure captions should be below the figures; table heads should appear above the tables. Insert figures and tables after they are cited in the text. Use the abbreviation “Fig. 1,” even at the beginning of a sentence.

1. Table Styles

| Table Head | Table Column Head | | |
| --- | --- | --- | --- |
| Table column subhead | Subhead | Subhead |
| copy | More table copya |  |  |

1. Sample of a Table footnote. *(Table footnote)*
2. Example of a figure caption. *(figure caption)*

Figure Labels: Use 8 point Times New Roman for Figure labels. Use words rather than symbols or abbreviations when writing Figure axis labels to avoid confusing the reader. As an example, write the quantity “Magnetization,” or “Magnetization, M,” not just “M.” If including units in the label, present them within parentheses. Do not label axes only with units. In the example, write “Magnetization (A/m)” or “Magnetization (A ( m(1),” not just “A/m.” Do not label axes with a ratio of quantities and units. For example, write “Temperature (K),” not “Temperature/K.”

##### Acknowledgment *(Heading 5)*

The preferred spelling of the word “acknowledgment” in America is without an “e” after the “g.” Avoid the stilted expression “one of us (R. B. G.) thanks ...”. Instead, try “R. B. G. thanks...”. Put sponsor acknowledgments in the unnumbered footnote on the first page.

##### References

The template will number citations consecutively within brackets [1]. The sentence punctuation follows the bracket [2]. Refer simply to the reference number, as in [3]—do not use “Ref. [3]” or “reference [3]” except at the beginning of a sentence: “Reference [3] was the first ...”

Number footnotes separately in superscripts. Place the actual footnote at the bottom of the column in which it was cited. Do not put footnotes in the reference list. Use letters for table footnotes.

Unless there are six authors or more give all authors’ names; do not use “et al.”. Papers that have not been published, even if they have been submitted for publication, should be cited as “unpublished” [4]. Papers that have been accepted for publication should be cited as “in press” [5]. Capitalize only the first word in a paper title, except for proper nouns and element symbols.

For papers published in translation journals, please give the English citation first, followed by the original foreign-language citation [6].

1. G. Eason, B. Noble, and I.N. Sneddon, “On certain integrals of Lipschitz-Hankel type involving products of Bessel functions,” Phil. Trans. Roy. Soc. London, vol. A247, pp. 529-551, April 1955. (*references*)

We suggest that you use a text box to insert a graphic (which is ideally a 300 dpi resolution TIFF or EPS file with all fonts embedded) because this method is somewhat more stable than directly inserting a picture.

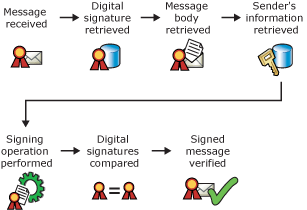
To have non-visible rules on your frame, use the MSWord “Format” pull-down menu, select Text Box > Colors and Lines to choose No Fill and No Line.

1. J. Clerk Maxwell, A Treatise on Electricity and Magnetism, 3rd ed., vol. 2. Oxford: Clarendon, 1892, pp.68-73.
2. I.S. Jacobs and C.P. Bean, “Fine particles, thin films and exchange anisotropy,” in Magnetism, vol. III, G.T. Rado and H. Suhl, Eds. New York: Academic, 1963, pp. 271-350.
3. K. Elissa, “Title of paper if known,” unpublished.
4. R. Nicole, “Title of paper with only first word capitalized,” J. Name Stand. Abbrev., in press.
5. Y. Yorozu, M. Hirano, K. Oka, and Y. Tagawa, “Electron spectroscopy studies on magneto-optical media and plastic substrate interface,” IEEE Transl. J. Magn. Japan, vol. 2, pp. 740-741, August 1987 [Digests 9th Annual Conf. Magnetics Japan, p. 301, 1982].
6. M. Young, The Technical Writer’s Handbook. Mill Valley, CA: University Science, 1989.

Abstract:  
  
Introduction:. :  
  
Proposed Network Model:  
[Diagram goes here]  
  
Technical specifications:  
Hardware requirements: Routers that support IPSec are required for implementation. A server must also be set up to manage Kerberos.  
  
Software requirements: Kerberos must be installed to manage access to the network as well as managing privileges once authorized inside the network.

The client has stated the following are required on a daily to weekly basis:

|  |
| --- |
| 1) The client segments’ users, at each branch, have paid-only access to the printers. |
| 2) The CEO has full access to all machines except client’s portable devices. |
| 3) The staff segment’s users of each branch office is required to send daily confidential progress report to the CEO via management segment of headquarter LAN. |
| 4) The local management of each branch has to send confidential income-expenditure report to the CEO on daily basis. |
| 5) The peer communication between branch managers is carried out on weekly basis, in the form of confidential business-strategic-plan report, to share weekly business activities and strategies. |
| 6) The headquarter and branch offices have monthly confidential video conference meeting to discuss monthly targets and devise operational plan for next month. |

Table 1  
  
Throughout this paper reference to table 1 will be made stating when workflow requirements are met.  
   
Both customers and staff have access to printing services. Before a print job can take place Kerberos will first authenticate the user to check that they have the appropriate privileges. Staff members are allowed to print indefinitely with no maximum printing cap, however if the service is abused restriction may be applied on either an individual basis or to all staff members at the clients regression.   
  
The administrator of Kerberos can set up the appropriate privileges for different users. The staff will have services available to them such as e-mail and Internet access and are able to request additional services if required and approved by management. Part of the required workflow stated that the CEO requires full access to all machines except the clients’ portable devices. Again, this can be achieved by configuring the correct service permissions to the CEO’s account.  
  
Kerberos will be used to authenticate users on workstations. The reason for selecting Kerberos is that once the required infrastructure is in place, it operates transparently to the end user and will not disturb workflow. A Kerberos realm will be setup at each campus and can be configured and managed remotely or directly on site.  
  
Initially, the client’s customers will not have privileges to access the printer without making a printing service purchase. After purchasing the printing service, the account will be credited and the Kerberos server will allow the user to print based on the amount of credit remaining the account. When a print job is requested, Kerberos will first validate the users account and check if there is enough credit remaining. If there is enough credit the user will be able to print. If not, they must purchase more credit.  
  
For this setup to work, Kerberos must be set up to work with CUPS (Common Unix Printing System) at each branch to act as print server. Once CUPS is established the status of the printers may be monitored remotely by administration.  
  
TLS will be used for secure communication between different branches. TLS has 2 modes of operation. AH and EPS. EPS will allow communication between the different campuses to be secure.  
  
The client has requested that the e-mail system is able to provide the following services in regards to e-mail: Authentication, Confidentiality, Compression, and E-mail compatibility. S/MIME (Secure Multipurpose Internet Mailing Extension) meets all of these requirements.  
  
In terms of general functionality S/MIME behaves similar to PGP. Both allow users to encrypt and sign messages and data can be signed using a digital signature. The difference is that S/MIME uses public key certificates and its key management is a hybrid between X.509 certificate hierarchy and PGP’s web of trust.  
  
*Authentication* is performed by a signing operation. This process involves adding the sender’s digital signature in addition to the message content. The following diagram visually depicst the signing process:  
[http://i.technet.microsoft.com/dynimg/IC129460.gif]  
  
On the recipient’s side, a verification procedure takes place to verify the authenticity of the digital signature. The recipient uses the sender’s message to generate another digital signature. The generated digital signature is then compared to the sender’s digital signature. If they match the signature is valid, if they don’t the signature is invalid.  
  
  
[http://i.technet.microsoft.com/dynimg/IC121094.gif]  
  
Encryption provides confidentiality during transit and storage. Only the intended recipients are able to view the contents of the message. The sender encrypts the outgoing message and the recipients decrypt the message   
  
<http://technet.microsoft.com/en-us/library/aa995740(v=exchg.65).aspx>  
  
Similar to PGP, SMIME uses radix 64 conversion to ensure e-mail compatibility.  
  
  
  
  
One of the issues with using S/MIME is that all workstations must be preconfigured with a list of trusted keys in addition to certificate revocation lists. The responsibility is local to ensure the certificates are maintained correctly, which could be seen as a potential con to using this technology. The certificates are signed by a certification authority.  
  
Authentication: A sender of a message is whom they claim they claim they are by providing digital signatures.  
Confidentiality: Other people whom the message is not intended for are unable to view the content of the message.   
Compression: The content of the message is zipped to create a smaller file size during transportation of the message.

E-mail compatability: An encrypted message can be converted to an ASCII string using RADIX 64 conversion.  
  
[1] W. Stallings, Principles and Network Security, 2nd Edition, Upper Saddle River, NJ: Prentice Hall, 1999, pp. 357-374

Another requirement asked by the customer is to have secure video conferencing. This can be achieved by implementing IP Security. IP Security can be used to secure branch connectivity over the Internet which will enable the company to communicate securely over the public WAN (Wide Area Network). Also, the business can now rely on the Internet instead of focusing on developing private infrastructure saving management overhead.   
  
  
In addition to branch office connectivity through the Internet the company will also benefit by being able to have secure access outside of the branches. If the users system is set up with IP security protocols they can achieve this by making a call to the ISP (Internet Service Provider) to gain access to the company network. This can reduce the cost of travelling expenses enabling employees to work remotely.  
  
The most beneficial part of implementing IP security is that all data is encrypted at the IP level. This means is that security ignorant applications will become inherently secure and security aware applications become more fortified. Since this technology operates on the transport layer it is transparent to the application layer and end users. This allows for a smooth integration without disturbing the workflow of other applications and users.

* The client will be able to perform video conferencing over IP Security with the appropriate architecture selection. Since the client has requested both Confidentiality as well as Authentication, the ESP (Encapsulating Security Payload) architecture has been selected to meet both of these requirements.