


FACULTY OF SCIENCE
DEPARTMENT OF
COMPUTING SCIENCE




UNIVERSITY OF
ALBERTA


LaTeX

The worst document creation tool in the world.
Except for all of the others.

© 2007

Department of Computing Science |  UNIVERSITY OF ALBERTA

LaTeX: What is it?

- A markup language for typesetting
 - ... a *what*?
- Extension of TeX
- Common in math, CS, engineering
- Not WYSIWYG
- Creepy lion: 

© 2007

LaTeX: What is it?

- Same principle as HTML and CSS
- You specify *what* content is separate from *how* it is displayed
 - `\title{An Introduction to LaTeX}`
- Your LaTeX document is “compiled” or “made” or “typeset”

LaTeX: Why?

- Separate writing from typesetting
- Auto image & table placement, auto numbering
- Easy bibliography, acronyms, table of contents...
- Math formulas
- Quick & easy format changes
- Formatting is usually done for you
- Collaboration (version control)

Detecting Privacy Infractions in e-Commerce Applications: A Framework and Methodology

Michael Smit
Faculty of Computer Science
Dalhousie University
Halifax, Nova Scotia
Email: smit,mcallist,slonim@cs.dal.ca

Michael McAllister
Faculty of Computer Science
Dalhousie University
Halifax, Nova Scotia
Email: mcallist@cs.dal.ca

Jacob Slonim
Faculty of Computer Science
Dalhousie University
Halifax, Nova Scotia
Email: slonim@cs.dal.ca

Abstract—This research describes a framework and methodology for managing the privacy policy of an enterprise, including creation (based on factors like privacy legislation and consumer preferences), validation and verification, deployment and enforcement, and compliance testing for business processes and software. To validate the framework, one module (compliance testing) is implemented for an existing prominent electronic commerce software application. Our unique approach monitors the personal information sent and received by the software application and converts it to a standardized representation. At defined points in the electronic commerce workflow, the transmissions are compared to a set of privacy rules to ascertain compliance. Non-compliant transmissions of personal information are labelled 'privacy infractions' and are addressed by stopping the workflow or by generating a report and alerting the administrator.

1. INTRODUCTION

Privacy was once defined as the "right to be let alone" [1]. As new technology developed, this definition was extended to include the notion that individuals should have control over when and to whom they divulge personal information and what the recipient may do with the personal information upon receipt. Improved database management systems, distributed and federated databases, data mining algorithms, and software applications enable the collection, aggregation, sharing and use of a growing amount of information, but can also offer the specification of individual privacy preferences and better privacy protection and compliance verification.

The collection, use, and dissemination of information is a crucial element of the knowledge economy for the e-

enterprise must determine its privacy policy. Once an enterprise has created its internal policy on privacy, the policy is verified and approved before being deployed throughout the enterprise. Once the policy is deployed, the enterprise must ensure that its employees, business processes, and software comply with the policy. As the influences on the enterprise change, or as the enterprise changes (e.g., a merger or acquisition), so will its policy on privacy; the revised policy must again be implemented by the employees, business processes, and software applications. When revising its policy, the enterprise must either ensure that existing customers agree to the new policy or develop a mechanism to operate under both the original and the new policies. Given the quantity of information collected and the capabilities of electronic commerce software applications, verifying the compliance of software applications is a complex process.

This paper informally describes an enterprise privacy policy management framework. This framework enables the process of determining enterprise privacy policy based on the influence of factors from both outside and inside the enterprise, validating and verifying this privacy policy, deploying and enforcing this privacy policy, and testing employees, business processes, and software applications for compliance with this written privacy policy.

To demonstrate the feasibility of the privacy compliance testing module, a proof-of-concept implementation is presented. This implementation does not require modifying the original software application. This methodology builds a

© 2007

DETECTING PRIVACY INFRACTIONS IN E-COMMERCE APPLICATIONS: A FRAMEWORK AND METHODOLOGY

Michael Smit*, Michael McAllister, Jacob Slonim
Faculty of Computer Science, Dalhousie University, Halifax, NS, Canada
smit,mcallist,slonim@cs.dal.ca

Keywords: e-commerce, privacy, software testing, enterprise privacy policy management, privacy infraction detection

Abstract: This research describes a framework and methodology for managing the privacy policy of an enterprise, including creation (based on factors like privacy legislation and consumer preferences), validation and verification, deployment and enforcement, and compliance testing for business processes and software. To validate the framework, one module (compliance testing) is implemented for an existing prominent electronic commerce software application. Our unique approach monitors the personal information sent and received by the software application and converts it to a standardized representation. At defined points in the electronic commerce workflow, the transmissions are compared to a set of privacy rules to ascertain compliance. Non-compliant transmissions of personal information are labelled 'privacy infractions' and are addressed by stopping the workflow or by generating a report and alerting the administrator.

1 Introduction

Privacy was once defined as the "right to be let alone" (Brandeis and Warren, 1890). As new technology developed, this definition was extended to include the notion that individuals should have control over when and to whom they divulge personal information and what the recipient may do with the personal information upon receipt. Improved database management systems, distributed and federated databases, data mining algorithms, and software applications enable the collection, aggregation, sharing and use of a growing amount of information, but can also offer the specification of individual privacy preferences and better privacy protection and compliance verification.

The collection, use, and dissemination of infor-

experts predict continued increases until at least 2010 (Statistics Canada, 2006). The sustained growth of e-commerce will require that businesses manage personal information in a manner that meets a variety of preferences, requirements, and incentives held by the businesses' stakeholders.

In addition to consumer requirements and legislative requirements, an enterprise will have privacy requirements based on the cost-benefit analysis of privacy protections, industry standards, its contracts with other enterprises, and the privacy policies of its competitors. From these requirements, an enterprise must determine its privacy policy. Once an enterprise has created its internal policy on privacy, the policy is verified and approved before being deployed throughout the enterprise. Once the policy is deployed, the

© 2007

Detecting Privacy Infractions in e-Commerce Applications: A Framework and Methodology

Michael Smit, Michael McAllister, Jacob Slonim
Faculty of Computer Science
Dalhousie University
Halifax, Nova Scotia
smit, mcallist, slonim@cs.dal.ca

Abstract

This research describes a framework and methodology for managing the privacy policy of an enterprise, including creation (based on factors like privacy legislation and consumer preferences), validation and verification, deployment and enforcement, and compliance testing for business processes and software.

To validate the framework, one module (compliance testing) is implemented for an existing prominent electronic commerce software application. Our unique approach monitors the personal information sent and received by the software application and converts it to a standardized representation. At defined points in the electronic commerce workflow, the transmissions are compared to a set of privacy rules to ascertain compliance. Non-compliant transmissions of personal information are labelled 'privacy infractions' and are addressed by stopping the workflow or by generating a report and alerting the administrator.

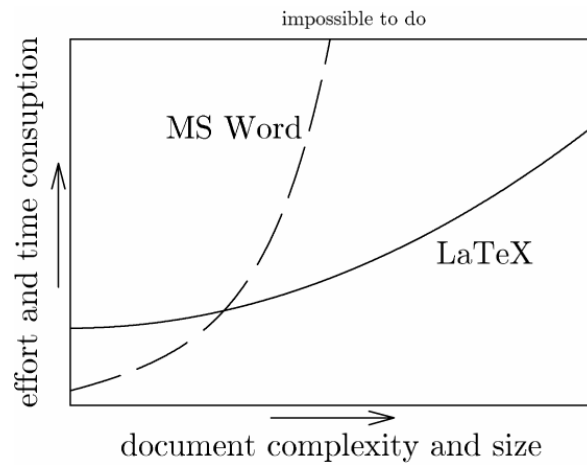
1 Introduction

Privacy was once defined as the "right to be let alone" [4]. As new technology developed, this definition was extended to include the notion that individuals should have control over when and to whom they divulge personal information and what the recipient may do with the personal information upon receipt. Improved database management systems, distributed and federated databases, data mining algorithms, and software applications enable the collection, aggregation, sharing and use of a growing amount of information, but can also offer the specification of individual privacy preferences and better privacy protection and compliance verification.

The collection, use, and dissemination of information is a crucial element of the know-

LaTeX: Why?

- Separate writing from typesetting
- Auto image & table placement, auto numbering
- Easy bibliography, acronyms, table of contents...
- Math formulas
- Quick & easy format changes
- Formatting is usually done for you
- Collaboration (version control)



- <http://www.ifs.hr/~mpinter/miktex.html>

LaTeX: How?

- **Create a LaTeX file (usually from an existing one)**
- **Create a bibtex file**
- **“Compile” the files**
 - latex <filename>
 - bibtex <filename>
- **View the output (default: DVI)**
- **Convert DVI output to another format**

Creating file

- **Get yourself a good text editor**
 - Syntax highlighting
 - Some can compile latex within the editor
- **Usually based on existing template**
 - From conference
 - From your previous works
 - From freely available starter documents
- **Get a quick reference and a reference**

Creating bibtex

- **Do not recommend typing it manually (though you can!)**
- **Academic sources often provide bibtex**
 - citeseer, wikipedia, acm, IEEE, etc)
- **Editing tools**
 - Bibedit, jabref...

```
@Book{latex,  
  author = {L. Lamport},  
  title = {\LaTeX\ A Document  
Preparation System --- User's Guide  
and Reference Manual},  
  publisher = {Addison-Wesley},  
  year = {1994},  
  address = {Reading, MA}  
}
```

LaTeX Software

- **On some (many?) default Linux distributions**
 - Otherwise use your package manager
- **On all U of A CS *nix machines**
- **Windows version: Miktek**

View DVI

- **Windows: Yap (with Miktex)**
- **Unix: xdvi**

Convert DVI

- **DVI contains no embedded fonts or images**
- **Convert to PDF, ps, png...**
 - dvipdfm, dvips, dvipng
 - “pdflatex” converts LaTeX to PDF

Some tricky bits

- **Images**
 - Can't just include a JPG – needs to be PS
- **Some LaTeX tools assume A4 paper size**
- **Figure placement is done the LaTeX way**
- **Adding citations requires you to run “latex, bibtex, latex, latex”**
- **Tables are... “inconvenient”.**
- **In general, Google is your friend**

Real Stuff!

- A LaTeX file has two parts:
 - Preamble
 - Content

A few demos

Resources

- <http://www.ctan.org/tex-archive/info/lshort/english/lshort.pdf?action=/starter/>
- <http://www.miktex.org/>