AntiPhish Project Presentation

Brian Witten

December 2006

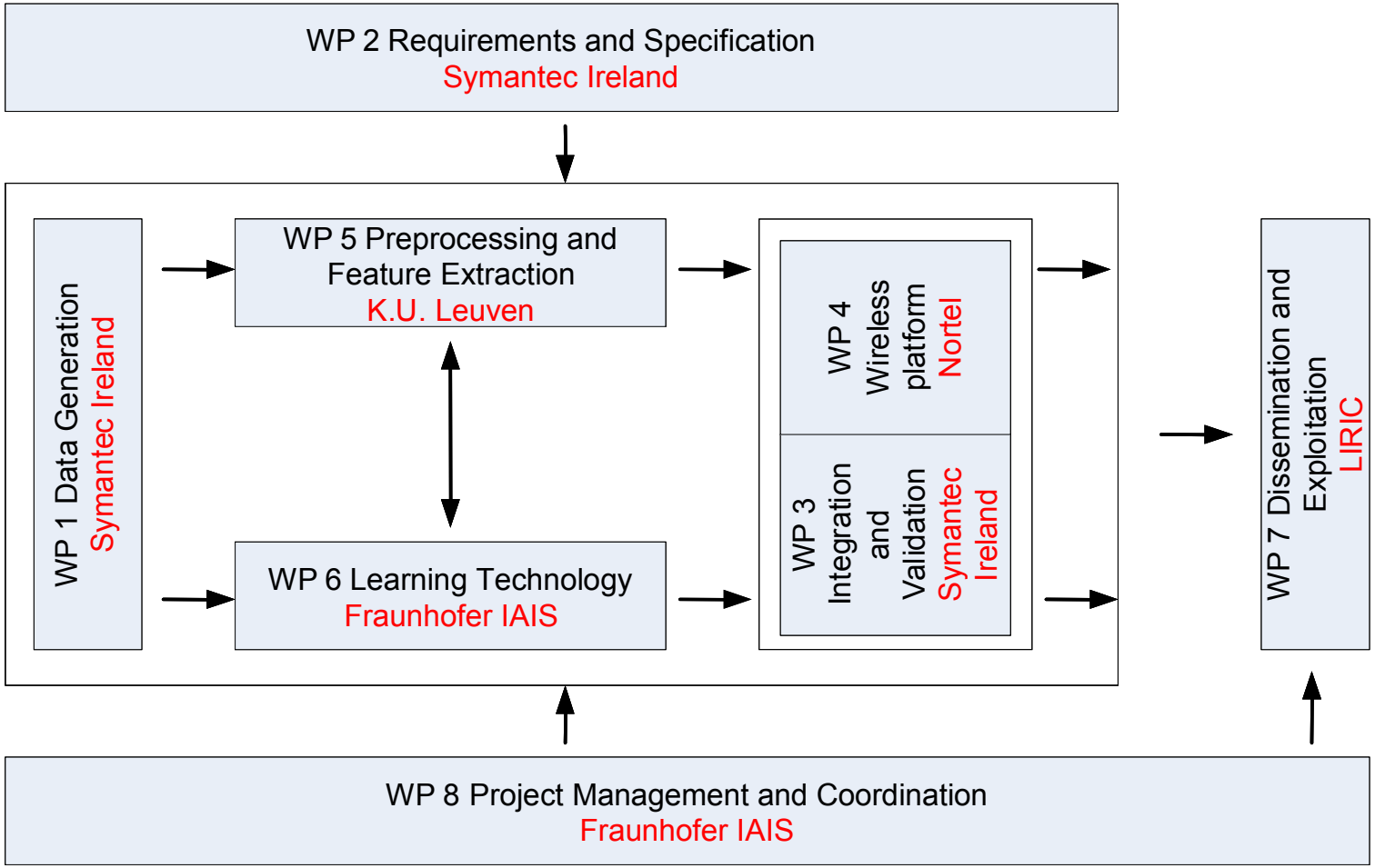
Agenda

1. Work Package 2 – Requirements and Specification
2. Work Package 1– Data Generation and Dissemination
3. Work Package 5 – Message Pre-processing & Feature Extraction
4. Work Package 6 – Advanced Learning Technology
5. Work Package 3 – Integration and Validation
6. Work Package 4– Wireless Platform
7. Work Package 7– Dissemination and Exploitation
8. Work Package 8– Project Management and Coordination

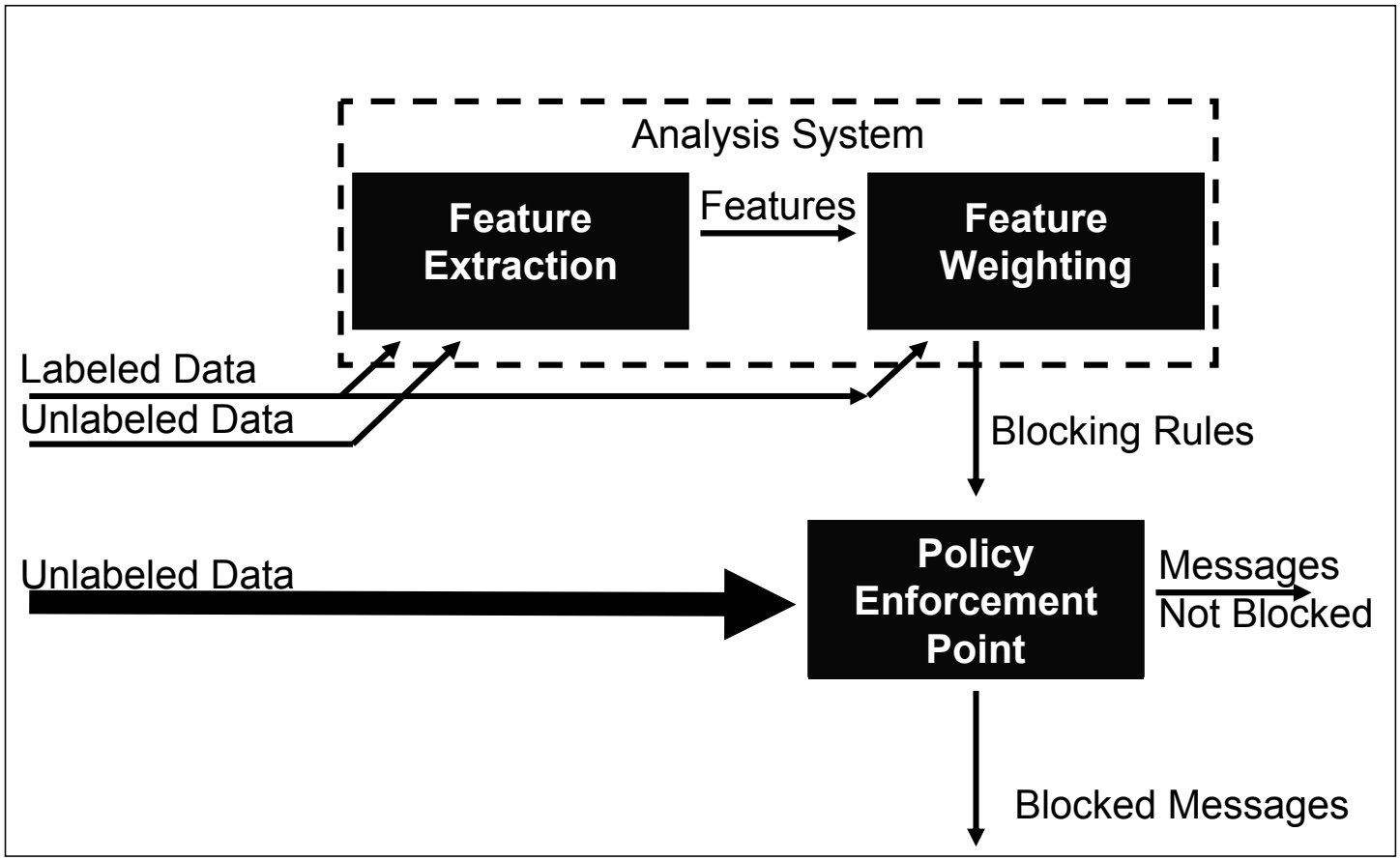
Work Package 2 – Requirements and Specification

- Architecture (Work Package Depiction)
- Architecture (Run-Time Depiction)
- Performance Requirements
- Continued Change in Spam and Phishing Threats: Image Spam
- Projected Revision to Run-Time Architecture

Work Package 2 – Architecture Specification (Work Package Depiction)

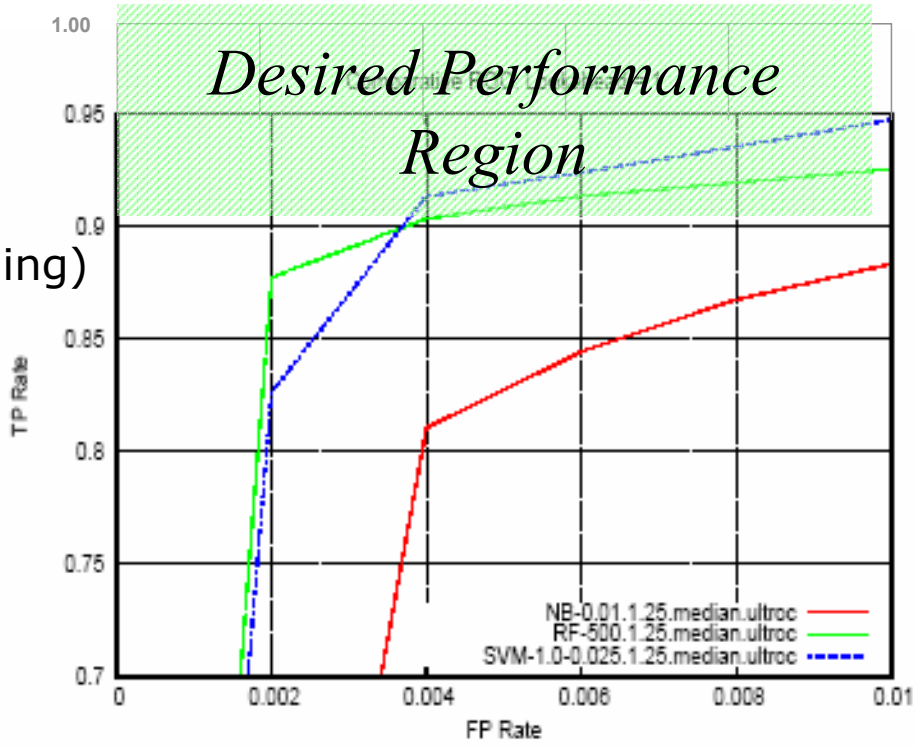


Work Package 2 – Architecture Specification (Run Time Depiction)



Work Package 2 – Performance Requirements

- Develop dynamic feature selection of sufficient quality to beat past performance of machine learning (ML) techniques, even where ML techniques were optimized with static feature selection.
- Performance Points:
  - A: Prototype (Phishing)
  - B: Production Requirement (Phishing)
  - C: Production Goal (Phishing)
  - D: Brightmail (Spam, Current)
- Additional requirements include number of messages per minute, volume per minute in megabytes, and with reasonable hardware and staff availability constraints.

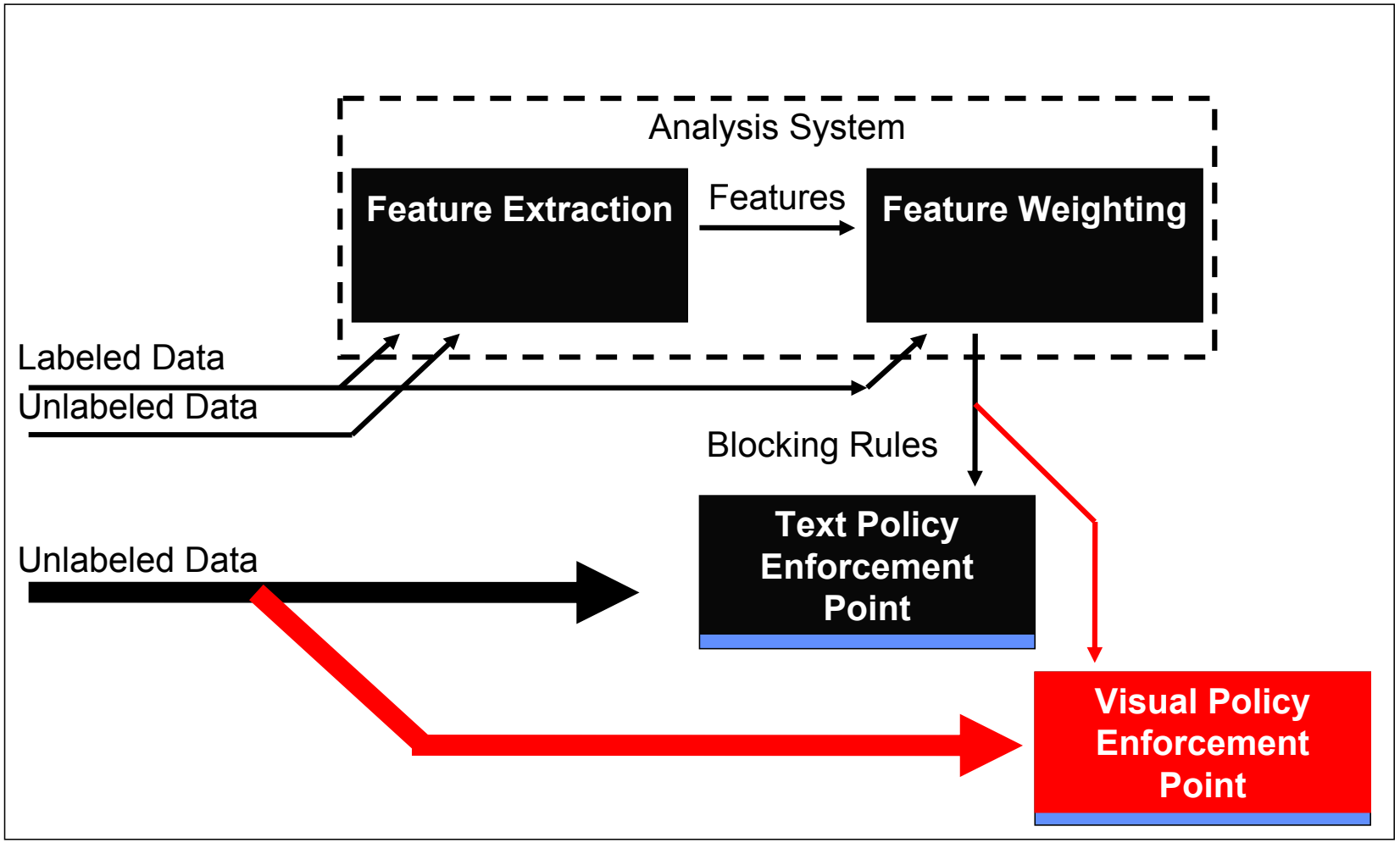


Continued Change in Spam and Phishing Threats: Image Spam

- Older image salting techniques were visually discernable.
- Some of the newer image salting techniques are more dangerous in Phishing because they are not visually discernable.
- However, because realism and effectiveness of Phishing attacks are highly correlated, this makes Optical Character Recognition (OCR) techniques more applicable to Phishing than other Spam.
- OCR requires more CPU
- So this may require broadening our architecture.

Example of Older Image Salting Techniques

Work Package 2 – Proposed Revision to Run Time Architecture



Work Package 1– Data Generation

- Privacy Agreements completed with both Fraunhofer and K.U.Leuven
  - Final draft is presented on the right.
- First dataset:
  - 32 GB of Spam
  - 500 MB of Ham in English
  - Nearly 100 MB of Ham not in English
- Second dataset:
  - Collecting 5GB with old hardware
  - New hardware should work faster

We currently process billions of messages per day. The datasets represent the very small fraction of messages that can be shared while respecting privacy concerns.

symantec.

NON-DISCLOSURE AGREEMENT FOR SENSITIVE INFORMATION

This agreement (the "Agreement") is made between Symantec LIRIC Limited, Symantec Limited ("Symantec") and ("Second Party") and is entered into on , 2006 (the "Effective Date").

WHEREAS, Symantec and the Second Party (collectively the "Parties") are parties to a Specific Targeted Research Project Consortium Agreement, dated (the "Consortium Agreement") and Symantec is disclosing or making available for access certain Sensitive Information (as defined below);

WHEREAS, the Parties are wishing to specify the confidentiality provisions of the Consortium Agreement for such Sensitive Information;

NOW THEREFORE, in consideration of the mutual promises and covenants contained in this Agreement, the Parties agree as follows:

1. Sensitive Information.
(a) Symantec and Second Party agree that specific information to be provided by Symantec under the Consortium Agreement will be treated as sensitive information (as defined below) and the additional terms and conditions of this Agreement shall apply. The terms and condition set out in this agreement are in addition to the provisions of the Consortium Agreement. In the event of any conflict between the terms of this Agreement and the Consortium Agreement, the terms of this Agreement shall prevail.
(b) "Sensitive Information" shall include any databases made available by Symantec to Second Party and any information that Symantec designates to be sensitive. Should Symantec wish to designate a package of information as Sensitive Information, it is sufficient for Symantec to mark the package as Sensitive Information and Symantec does not need to mark each individual document or part of the package as sensitive.
(c) The Sensitive Information is being provided by Symantec to the Second Party exclusively for use in the context of the research of the Second Party being performed as part of and necessary for the research effort under the Consortium Agreement.
(d) Each Party will nominate a contact person that is dealing exclusively and centrally with the exchange of Sensitive Information to ensure compliance with the requirements set forth herein (the "Gatekeeper"). The Second Party's Gatekeeper shall not be exchanged without the prior written consent of Symantec. In the event the Second Party's Gatekeeper departs from the Second Party or would like to be relieved of his duties and the parties cannot agree on a replacement, all Sensitive Information shall be destroyed or returned to Symantec prior to the Gatekeeper's departure.

2. Restrictions.
(a) The Second Party shall use Sensitive Information only for the purpose of research under the Consortia Agreement and shall not use or exploit such information for their own benefit or the benefit of a third party without the prior written consent of Symantec. For the avoidance of doubt, no data based upon the Sensitive Information or the research of the Sensitive Information shall be used for any other purpose, including but not limited to (i) any published statistics of what companies are being targeted and/or phished; (ii) any phishing samples for any research papers; and/or (iii) being published in any way.
(b) The Second Party shall not publish, disclose or allow disclosure of any Sensitive Information in whole or in part to third parties, including other parties to the Consortium Agreement except that the Second Party may only disclose such information to its employees that (i) are working on the research under the Consortium Agreement, (ii) have a need-to-know for the purpose of performing research under the Consortia Agreement and (iii) that are bound by substantially similar requirements as provided herein.
(c) The parties agree that Sensitive Information shall be held confidential for an unlimited period of time.
(d) The Second Party may disclose Sensitive Information in accordance with judicial or other governmental order or process provided that the Second Party shall: (i) give Symantec notice prior to such disclosure reasonably sufficient to give Symantec the opportunity to contest the disclosure; and (ii) ensure that the disclosure is limited in content and distribution to the extent reasonably possible.

(e) The Second Party shall take security precautions to maintain the confidentiality of the Sensitive Information at least as great as the precautions which it takes to protect its own Sensitive Information, but no less than commercially reasonable efforts.

3. Rights. The Second Party shall return or certify the destruction of all originals, copies, reproductions and summaries of Sensitive Information (i) upon completion of the research under the Consortium Agreement, (ii) upon termination of this Agreement, (iii) upon expiry or termination of the Consortium Agreement, and/or (iv) at the Disclosing Party's request.

4. Miscellaneous.
(a) The Second Party agrees to conform to all national and EU law and policies for handling of private data in all applicable jurisdictions in relation to the Sensitive Information.
(b) All Sensitive Information is and shall remain the property of Symantec. Symantec does not grant any license or title rights to the Second Party in this Agreement.
(c) This Agreement may be modified or waived only by a separate written agreement signed by an authorized officer of both Parties expressly so modifying or waiving any provision of this Agreement.
(d) If any provision of this Agreement shall be held, for any reason, to be illegal, invalid or non enforceable, the remaining provisions shall nonetheless be legal, valid and enforceable.

IN WITNESS WHEREOF, the Parties have executed this Agreement:

SECOND PARTY

Company Name:
Address:
By:
Name:
Title:
Date:

SYMANTEC LIMITED

Ballycoolin Business Park
Blanchardstown, Dublin 15, Ireland
By:
Name:
Title:
Date:

SYMANTEC LIRIC LIMITED

Hines Meadow, St.Cloud Way,
Maidenhead, SL6 8XB,
Berkshire, United kingdom
By:
Name:
Title:
Date:

Symantec Legal Form EMEA
ema-AntiPhish-10May06

Work Package 5: Message Preprocessing / Feature Extraction

- Message Preprocessing
  - Message instantiation.
  - Message text extraction
  - Message structure extraction
- Feature Extraction
  - T5.1 – salting features
  - T5.2 – syntactic features
  - T5.4 – structure & layout features
- Gathering statistics

Work Package 5: Message Preprocessing / Feature Extraction

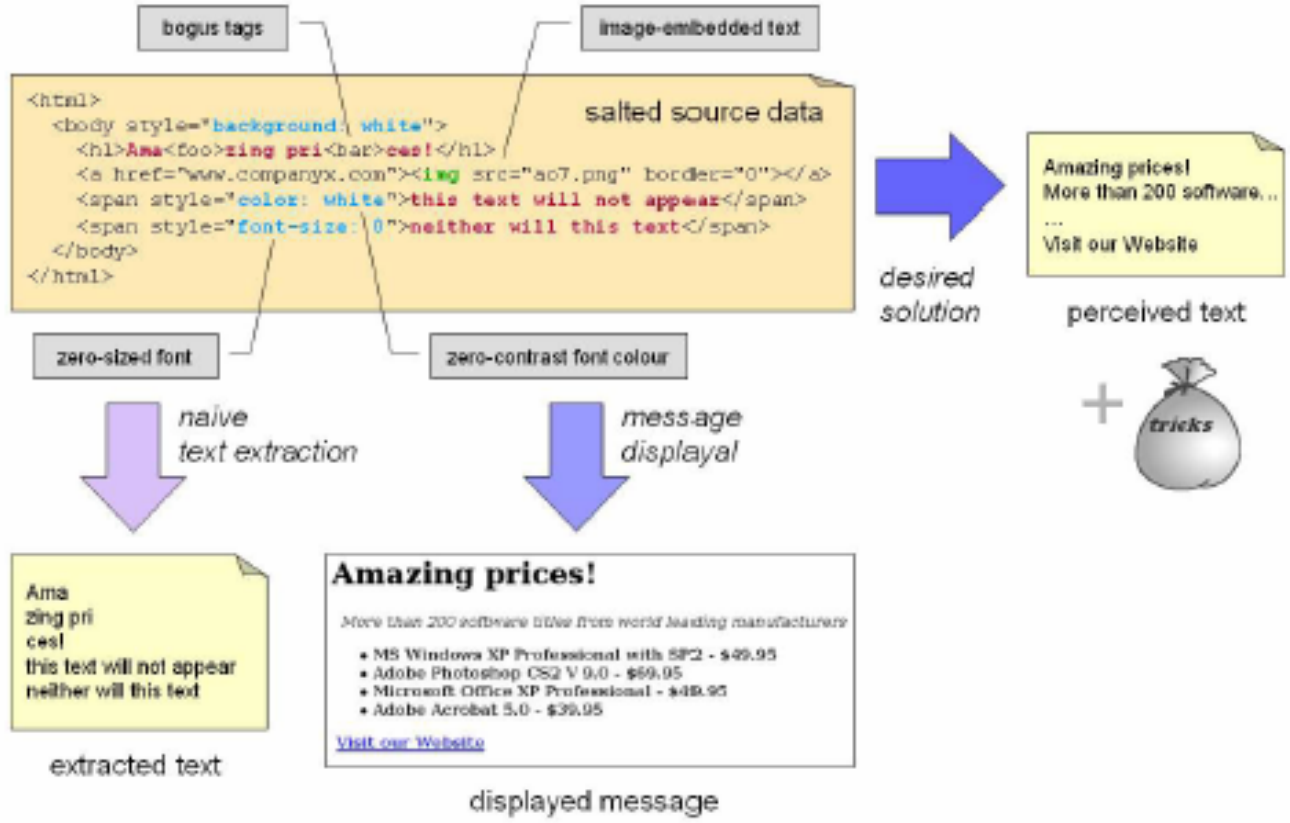


Illustration 1: The problem of text salting (left), and the desired solution (right)

Work Package 6 – Advanced Learning Technology

Implement a number of algorithms:
tradeoff: speed vs. performance vs. memory

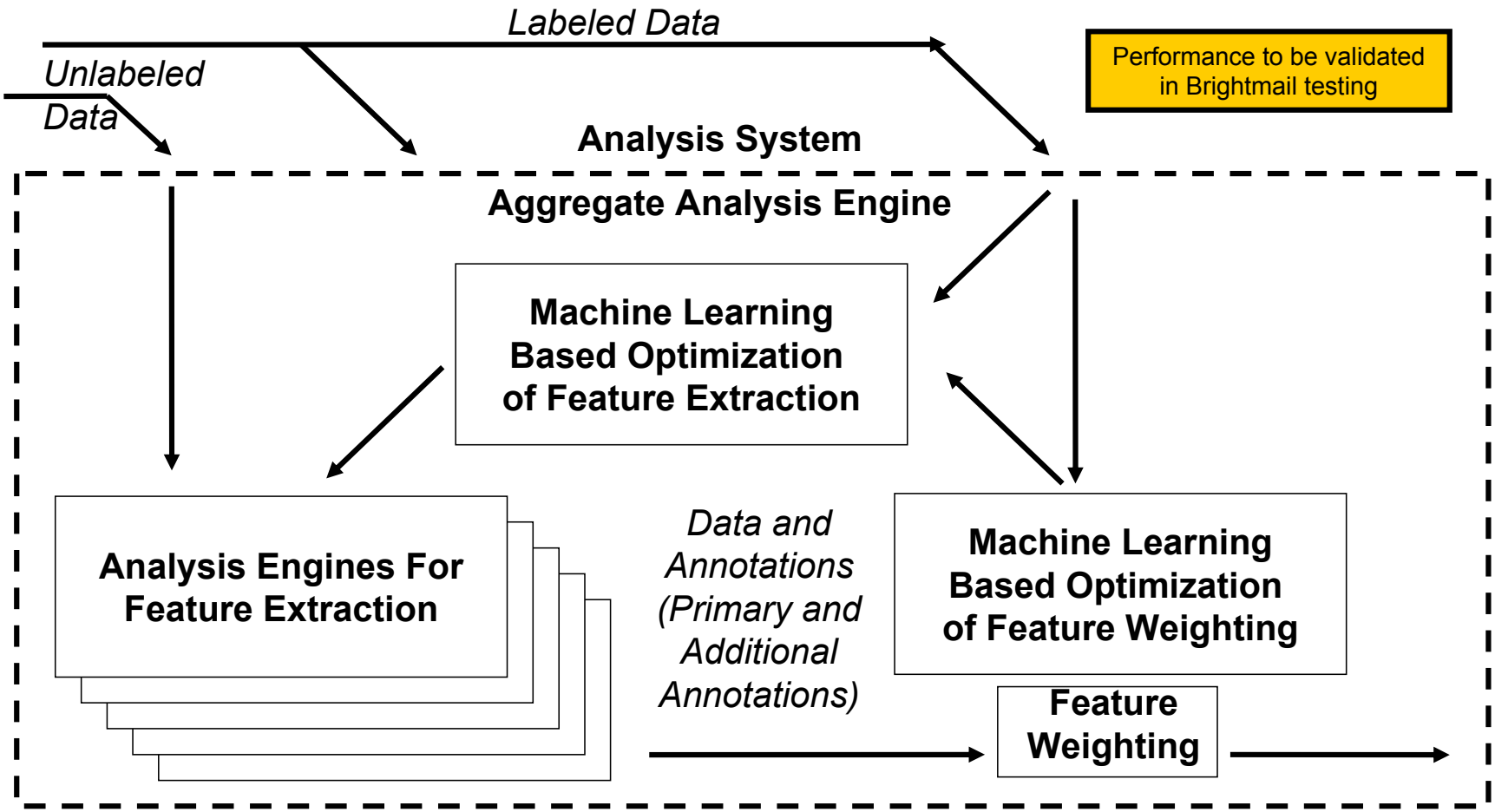
- On-line learning with kernels (Kivinen et al 2001)
  Very efficient for very high dimensional learning.
- Implement Perceptron
  passive: do nothing if no error
  increase margin (conv. Theorem)

$$\hat{y}_i = sign(\langle w_i, x_i \rangle)$$

$$w_{i+1} = \begin{cases} w_i & \text{if } \hat{y}_i = y_i \\ w_i + y_i x_i & else \end{cases}$$

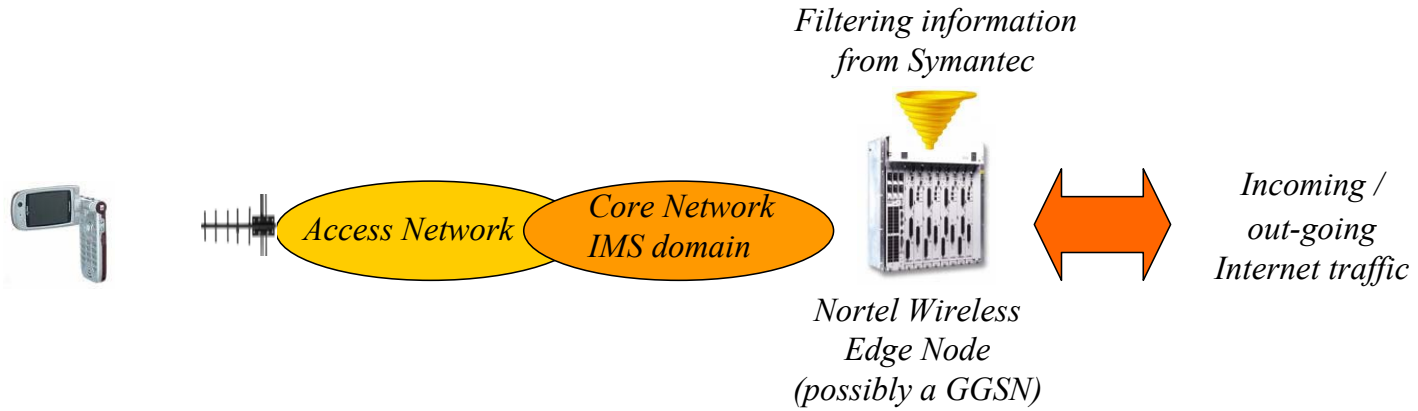
- Implement MIRA [Crammer 04,06]
  passive: do nothing if no error
  aggressive: learn current example perfectly
- Investigate LASVM [Bordes et al. 05]
  select / drop support vectors; online learning approaching SVM-solution
- Investigate L2-SVM [Keerthi, DeCoste 05]
  square loss, 400-fold speed increase vs. usual SVM

Work Package 3 – Proposed Integration Architecture



Work Package 4– Wireless Platform

- Apply AntiPhish techniques to Wireless environment, with a specific focus on legacy 3GPP network architectures
- Demonstrate applicability to the ever growing wireless traffic, including mail, SMS, MMS, …
- Current architecture is:
  - access type agnostic (e.g. 2G/GSM, 3G/UTRAN, 4G/LTE and possibly WLAN access)
  - compatible with 3PGG upcoming "Enhanced Packet Core" evolutions being studied



Work Package 7 – Dissemination and Exploitation

- Licensing agreements have been established between Symantec and Nortel, Tiscali, Fraunhofer, and K.U.Leuven for the commercial exploitation of the research
- On December 4, 2006, Symantec issued a press release on behalf of the consortia members with their approvals
  - Several periodicals covered the press release
  - Translations are now hosted on Symantec websites in many languages throughout Europe
  - The full text of this press release is given on the next slide.

News Release

CONTACT:
Melissa Martin
Symantec Corporation
+1 (408) 517 8475
melissa_martin@symantec.com

Mike Bradshaw
Connect Public Relations
+1 (801) 373 7888
mikeb@connectpr.com

European Commission Awards Funding to Symantec, Fraunhofer-Gesellschaft, Nortel, K.U.Leuven, and Tiscali for Joint Antiphishing Research

CUPERTINO, Calif. – Nov., 29, 2006 – Symantec Corp. (Nasdaq: SYMC) today announced that the European Commission has awarded funding to Symantec, Fraunhofer-Gesellschaft, Nortel, Katholieke Universiteit (K.U.) Leuven, and Tiscali for critical research in phishing prevention. Being singled out for funding by the European Commission's highly competitive selection process underscores the exceptional research capabilities provided by these organizations.

The goal of the three-year AntiPhish project is to develop antiphishing technologies that help to protect and secure the global email communication infrastructure. With this goal, AntiPhish targets the Information Society Technologies Sixth Framework Programme (FP6) objective aimed at forming scientific, technical, and industrial excellence towards a global dependability and security framework to ensure security, privacy, and trust in complex communication networks and information infrastructures.

"Our AntiPhish consortium is privileged to be part of this important international effort," said Brian Witten, director of government research in Symantec Research Labs. "The research we undertake will leverage the collaborative capabilities of leading research organizations and be driven by the practical, hands-on experience of industry participants who have expertise with fighting spam on a global scale. This new technology will then move from a test laboratory to implementation at Tiscali, one of the largest and most interconnected Internet service providers in the world."

"We are very happy to be part of this joint effort," said Domenico Dato, R&D manager at Tiscali, "The Antiphish research will be among the activities of Tiscali Labs, our research and development hub that was set up for implementing and testing innovative products and services. Being an active part of this project will allow us to provide our customers with state-of-the-art spam and phishing prevention technologies, thus considerably improving their Internet experience."

(More)

Each of the five partners will offer a unique and critical contribution to the AntiPhish project. The effort is managed by project coordinator Institute for Intelligent Analysis and Information Systems (IAIS) of Fraunhofer-Gesellschaft, the largest organization for applied research in Europe. Fraunhofer IAIS is located in St. Augustin, Germany, and focuses on research on innovative systems for data analysis and information extraction.

Symantec Research Labs is Symantec's global research division and has developed and helped commercialize numerous technologies across Symantec's business areas. Commercialized technologies from the group include the company's recently announced Symantec Database Security, Symantec's first antispam technology, generic exploit blocking technology that proactively blocks fast-spreading threats, and technology to help protect our nation's critical power-grid infrastructure.

K.U.Leuven is the oldest university of the Low Countries and the largest Flemish university. The Leuven, Belgium-based university carries out fundamental and applied research in all academic disciplines. The AntiPhish project is researched by the Legal Informatics and Information Retrieval group of this university.

Nortel is a recognized leader in delivering communications capabilities that enhance the human experience, ignite and power global commerce, and secure and protect the world's most critical information. Nortel does business in more than 150 countries. For more information, visit Nortel on the Web at www.nortel.com.

Tiscali is one of the main independent European telecommunications companies. With one of the largest and most interconnected IP networks in the world, Tiscali is able to supply its customers, residential and business, with a full range of services. Tiscali is headquartered in Cagliari, Italy. More information at www.tiscali.com.

More information on the AntiPhish consortium can be found at http://www.antiphishresearch.org/home.html.

About Symantec

Symantec is the world leader in providing solutions to help individuals and enterprises assure the security, availability, and integrity of their information. Headquartered in Cupertino, Calif., Symantec has operations in 40 countries. More information is available at www.symantec.com.

###

NOTE TO EDITORS: If you would like additional information on Symantec Corporation and its products, please visit the Symantec News Room at http://www.symantec.com/news. All prices noted are in U.S. dollars and are valid only in the United States.

Work Package 8 – Project Management and Coordination

- Schedule of Meetings Held to Date
  - Darmstadt, DE (30.01.-01.02.2006)
  - Bonn, DE (01.06.2006)
  - Cagliari, IT (11.09.2006)
  - Leuven, BE (10.01.2007)
- Coordination is also done through e-mail mailing lists, a private web server providing Basic Support for Collaborative Work (BSCW), and monthly teleconferences.
- Changes in Participation
  - On departure of Thomas Hofmann from Fraunhofer IPSI, responsibility with Fraunhofer shifted to Fraunhofer IAIS

Summary

- Concluding the first year of a three year effort
- Fraunhofer and K.U.Leuven are making rapid progress in lab
- Spam and Phishing threats are adapting quickly, and the AntiPhish consortia is adapting quickly to these threats
- Emphasis for the coming year will be on completing the lab prototype and integrating it with current systems for field tests