1. 기업명: (주)윈스

2. 기업소재지: 경기도 성남시 분당구 삼평동633 판교세븐벤처밸리 2동 7층

3. 기업 현황:

   가. 대표 이사: 김대연

   나. 설립 년도: 1998

   다. 직원 수: 386명

   라. 주 개발/판매품: 네크워크보안 침입방지시스템/SNIPER IPS

   마. 홈페이지: www.wins21.co.kr

4. 프로젝트 주제 명: SNORT와 HyperScan오픈소스를 활용한 PCRE 기반의

고성능 탐지 알고리즘 개발

5. 프로젝트 내용:

오픈소스 SNORT와 HyperScan에서는 PCRE 기반의 패킷내 시그니처 탐지기능을 제공한다. 하지만 성능제약이 존재하여 고성능 네트워크 환경에서 전수 패킷 검사를 위해서는 성능이 부족하다.

성능 개선을 위한 전처리/후처리 알고리즘을 개발한다.

   1st: SNORT 오픈소스내 HyperScan을 활용한 패킷 패턴매칭을 이해한다.

   2nd: 2000개 이상의 시그니처 패턴에대해 전처리를 통해 제공된 샘플 패킷에 대한 탐지 성능을 향상시킬 알고리즘을 고안한다.

   3rd: 다양한 트래픽 환경에서 탐지 성능 검증한다.

6. 필요 지식: SNORT 오픈소스, PCRE 문법, 네트워크 패킷

7. 교육/훈련 효과: 네트워크 보안의 이해, 오픈 소스를 활용한 알고리즘 개발

8. 개발 기간: 3개월

9. 개발 인원: 3인

10. 기업체 담당자: 조학수(연구소장) [marius71@wins21.co.kr](mailto:marius71@wins21.co.kr), 031-622-8605

1. 기업명: (주)윈스

2. 기업소재지: 경기도 성남시 분당구 삼평동633 판교세븐벤처밸리 2동 7층

3. 기업 현황:

   가. 대표 이사: 김대연

   나. 설립 년도: 1998

   다. 직원 수: 386명

   라. 주 개발/판매품: 네크워크보안 침입방지시스템/SNIPER IPS

   마. 홈페이지: www.wins21.co.kr

4. 프로젝트 주제 명: 패킷 스트림에 존재하는 공통 문자열 추출 알고리즘 개발

5. 프로젝트 내용:

고성능 네트워크 환경에서 불시에 DDoS 공격으로 인해 트래픽이 폭증하는 사례가 있다. 담당자는 신속하게 네트워크에 흐르는 트래픽에서 공통 패턴을 가지는 DDoS Dummy 트래픽을 파악하고 이를 제어 하여 장애를 예방하고자 한다.

   목표: 주어진 샘플 패킷에 대해 Longest Common String(LSC:최장길이 공통 문자열)을 찾아낸다.

   과정: n개의 패킷이 존재할 때 알려지지 않은 LCS를 찾는 것의 computational complexity를 계산하라.

   해결: 최적의 LCS를 추출하는 것이 불가하다면 정해진 연산횟수 내에 근사한 답을 찾아낼 수 있는 알고리즘을 고안하라.

6. 필요 지식: 알고리즘

7. 교육/훈련 효과: 네트워크 보안에 필요한 알고리즘 개발

8. 개발 기간: 3개월

9. 개발 인원: 3인

10. 기업체 담당자: 조학수(연구소장) [marius71@wins21.co.kr](mailto:marius71@wins21.co.kr), 031-622-8605

1. 기업명: (주)윈스

2. 기업소재지: 경기도 성남시 분당구 삼평동633 판교세븐벤처밸리 2동 7층

3. 기업 현황:

   가. 대표 이사: 김대연

   나. 설립 년도: 1998

   다. 직원 수: 386명

   라. 주 개발/판매품: 네크워크보안 침입방지시스템/SNIPER IPS

   마. 홈페이지: www.wins21.co.kr

4. 프로젝트 주제 명: 악성코드에 대한 행위기반 Clustering 기법 개발

5. 프로젝트 내용:

악성코드를 분석하는 방법은 코드 그 자체를 분석하는 정적분석기법과 실행하여 행위 또는 API를 분석하는 동적분석기법이 있다. 이중 CUCKOO 샌드박스는 가상환경에서 악성코드를 실행하여 호출되는 API를 결과파일로 제공해준다. 참고논문을 이해하고 API call-list 바탕으로 보다 효율적인 Clustering 기법을 제시하라.

참고논문 : Lee, Taejin, et al. "Automatic malware mutant detection and group classification based on the n-gram and clustering coefficient." *The Journal of Supercomputing*(2015): 1-15.

6. 필요 지식: 알고리즘

7. 교육/훈련 효과: 악성코드 동적분석 및 Machine Learing 이해

8. 개발 기간: 3개월

9. 개발 인원: 3인

10. 기업체 담당자: 조학수(연구소장) [marius71@wins21.co.kr](mailto:marius71@wins21.co.kr), 031-622-8605

1. 기업명: (주)윈스

2. 기업소재지: 경기도 성남시 분당구 삼평동633 판교세븐벤처밸리 2동 7층

3. 기업 현황:

   가. 대표 이사: 김대연

   나. 설립 년도: 1998

   다. 직원 수: 386명

   라. 주 개발/판매품: 네크워크보안 침입방지시스템/SNIPER IPS

   마. 홈페이지: www.wins21.co.kr

4. 프로젝트 주제 명: Document Tagging을 이용한 Malware Naming

5. 프로젝트 내용:

악성코드에 대한 Naming은 백신 제조사 마다 다른 방법으로 이름을 정의한다. 특정 악성코드가 발견되었을 때 잘 알려진 악성코드의 변종인지 아니면 신종인지에 따라서 그룹을 나누고 이름을 분류하는 것이 악성코드 분석전문가와 보안전문가에게 해 묵은 과제이다.참고논문을 이용하여 VirusTotal에서 각 백신마다 정의한 악성코드 Name에 대해 최적의 Name과 그룹을 정의하라.

악성코드는 변종이 방대하다 따라서 행위분석 후 유사한 악성코드에 같은 그룹의 이름을 부여하는 것이 이 과제의 핵심이다.

참고논문: Yeung, Ching‐man Au, et al. "SPEAR: SPAMMING‐RESISTANT EXPERTISE ANALYSIS AND RANKING IN COLLABORATIVE TAGGING SYSTEMS." *Computational Intelligence* 27.3 (2011): 458-488.

예)https://www.virustotal.com/ko/file/57073fc904f7c0462a41dcd8830b593a0e44fc50d66a5b2c4b7430842f731b89/analysis/

6. 필요 지식: 악성코드 동적 분석, Machine Learning

7. 교육/훈련 효과: 악성코드 동적분석 및 Machine Learing 이해

8. 개발 기간: 3개월

9. 개발 인원: 3인

10. 기업체 담당자: 조학수(연구소장) [marius71@wins21.co.kr](mailto:marius71@wins21.co.kr), 031-622-8605