How to write top conference papers in security?

Yongdae Kim

Security Top conferences

- Security
  - ISOC Network and Distributed System Security (NDSS)
  - IEEE Symposium on Security & Privacy (S&P, Oakland)
  - Usenix Security
  - ACM computer and communication Security (CCS)
- crypto
  - IACR International cryptology conference (crypto)
  - IACR European cryptology conference (Eurocrypt)

Other Related Top conferences

- computer architecture: ASPLOS, ISCA, MICRO
- AI, Machine Learning: AAAI, ICML, KDD, NIPS, WWW
- computer networks: SIGCOMM, NSDI
- Mobile computing: Mobicom, MobiSys
- Measurement: IMC
- Operating systems: OSDI, SOSP
- Programming languages: PLDI, POPL
- Human-computer interaction: CHI

Acceptance Rate

	NDSS	S&P	Usenix Sec	ACM CCS
2016	15.4%(60/389)	13.3%(55/413)	15.6%(72/463)	16.5%(137/831)
2015	16.9%(51/302)	13.5%(55/407)	15.7%(67/426)	19.8%(128/646)
2014	18.6%(55/295)	13%(44/334)	19%(67/350)	19.5%(114/585)
2013	18.8%(47/250)	12%(38/315)	15.9%(44/277)	19.8%(105/530)
2012	18%(46/258)	13%(40/307)	19.4%(43/222)	18.9%(80/423)
2011	20%(28/139)	11%(34/306)	17%(35/204)	14%(60/429)

분야 선정: Red Ocean

- 엄청나게 많은 Red Ocean
  - 예: Android, Software Security, System Security
  - 몇 가지 long term open problem을 제외하고는 엄청나게 빨리 움직이는 분야
  - 논문 쓰려면 참고 문헌만 100개
  - 컨퍼런스에서 만나는 사람들
  - 프로그램 커미티 혹은 그들만의 리그
  - 가장 중요한 것: up to date information, …

분야 선정: Blue Ocean

- "volte security cellular", "3d printer security", "medical device security", "drone security", …
- 전세계의 사람들이 가지고 있지 않으나 내가 갖고 있는 것은?
  - 데이터, 네트워크, 장비, 인프라, 새로운 분야, …
- 경쟁이 낮은 분야, 기존에 관심을 덜 받은 분야
- 즉, 기존에 한 번도 발표된 적이 없는 분야, 기술의 논문이 더 쉽다.
  - 두번째 논문, 세번째 논문? …
- 그렇지만 새로운 분야의 개척은 힘들다 기존에 그런 논문도 없다…

분야: Red Ocean 안의 Blue Ocean

- Red ocean 안에 Blue Ocean도 존재한다
- 기존 red ocean의 어려움 때문에 찾기는 매우 힘드나...
- 한번 찾을 경우 학계의 각광, 그리고 후속 논문들...
- 계속 red ocean이 지속된다면 많은 citation의 guarantee
- 예) 다른 분야의 연구를 보안으로 들고 오기
  - 센서 해킹, Low level Arch 등 다른 전공을 보안으로 (그냥 블루오션)
  - PL+보안, compiler+보안, Machine learning+보안...
  - 가장 어려운 점은 기존 보안인들을 설득하기...

분야: Blue Ocean 연구 잘 하기

- 대부분의 보안을 하는 사람들은 그 분야를 잘 모른다.
- 센서, complex Network Analysis, Low Level HW, …
- 따라서 논문의 Background Section이 매우 중요
- 전체적으로 사람들이 기존에 몰랐던 term을 이해하고 논문 전체를 포기하지 않고 읽게 만들어야 함.
- 이해하기 쉽고 눈에 보이는 Evaluation
  - 잘 날라가는 드론이 떨어진다.
  - 메모리 비트가 바뀌었는데 루트 권한을 받는다.
  - 비트 코인으로 돈을 번다.

공격 논문 vs. 수비 논문

- 공격 논문
  - 보안 학회가 아닌 TOP 학회에 나온 논문,
  - 실제 서비스되고, 많은 사람이 쓰기 있고, 공격 방식이 새롭고, ...
  - Intro, Background, Attack overview, Attack Design, Experiment, ...
  - 새로운 공격 논문은 새로운 문제를 찾는 것이고 따라서 문제가 어려울 경우 citation 가능성 높음
- 수비 논문
  - 보안학회에 나온 공격 논문에 대한 수비
  - 빨라야 하고, 새로운 공격이 생기지 말아야 하고, 불편하지 말아야 하고, 기존에 없었어야 하고, 수비 때문에 늦어지면 안 되고...
  - 기존 논문에 대한 확실한 이해
  - 따라서 Red Ocean 분야의 defense 논문은 엄청 쓰기 힘듦.

문제 먼저 혹은 답 먼저?

- 당연히 문제로 부터 Motivate되어 새로운 해결책을 찾는 것이 훨씬 더 논문을 쓰기 쉽다.
- 그렇지만 1) 어떨 때는 문제로 부터 답을 찾았는데, 그 답이 원래 문제를 풀지 않거나 혹은 2) 답을 구해 놓고 문제를 찾는 경우가 존재
  - 1번의 경우 제3자의 눈으로 정확하게 판단하는 것이 중요. 터널뷰에 빠지지 말자. 정말 맞다고 생각이 되면 제3자의 눈에서 열심히 설득
  - 1번의 경우, 문제가 틀리거나, 혹은 2번의 경우, 창의적인 생각을 가지고 새로운 문제를 찾기. 문제의 도메인이 바뀔 수도 있다.
  - 이 경우 Evaluation이 추가로 필요한 경우도 있음

Idea 찾기

- 앞에서 이야기한 모든 것 +
  - 뉴스를 follow 하기
  - 다른 분야의 논문들 최소한 제목은 훑어보기
  - Blackhat, Defcon 등 해킹 컨퍼런스 발표 follow up
- 대상이 선정되고 나면 시스템에 대한 정확한 이해
- 모든 attack vector에 대한 고민
  - 드론 공격 벡터: GPS, 센서, Telematics, 소프트웨어, 펌웨어 업데이트, OS, Fail Safe
- 어떻게 새로움을 만들까에 대한 고민
  - Related work, 연구 방법, 결과 improve, …

논문 구성

- 자신이 쓰고 싶은 논문의 내용과 가장 비슷한 논문을 선정해서 organization 잡기
- 그냥 무작정 쓰기 보다는 크게 구조를 먼저 잡고
- 각 장별로 패러그래프를 잡고
- 패러그래프의 내용까지 하나씩 하나씩 확정
- Intro - Background - Overview and Target System - Attack model - Vulnerabilities and Exploits - Evaluation - Discussion - Related work* - conclusion

Title, Abstract

- 제목은 sexy하게. 너무 짧은 제목은 ㅠㅠ 부제목 OK
  - The Postman Always Rings Twice: Attacking and Defending postMessage in HTML5 Websites.
  - When cellular Networks Met IPv6: Security Problems of Middleboxes in IPv6 cellular Networks
  - Frying PAN: Dissecting customized Protocol for Personal Area Network
- Reviewer의 선정과 깊은 관계: 제목과 Abstract만 읽고 Reviewer 선정
- Abstract
  - Title을 읽고 나면 Abstract가 읽고 싶게, Abstract를 읽고 나면 Intro를 읽고 싶게, Intro를 읽고 나면 논문 전체를 읽고 싶게
  - 따라서 Abstract는 High level로
- 모든 단어는 미리 정의를 하고 사용!

Intro

- 배경, 정의, 역사, 문제, 풀이, 평가, lessons learned, 구조
- 마치 한 편의 논문을 Intro만 읽고 나면 다 읽은 듯한
- 여전히 모든 (남이 모를 수 있는) 단어는 먼저 정의를 하고 사용
- Abstract가 1 min elevator pitch라면 Intro는 5 min elevator pitch
- 아무래도 본문을 다 쓴 다음에 쓰는게 더 좋음
  - ▷ 혹은 본인의 tone을 잡기 위하여 먼저 쓰나 논문 다 쓰고 나서 revise

Background

- 나의 contribution이 아닌 것들.
- 그러나 논문을 이해하는데 꼭 필요한 것들
- 기존 이론, 타겟 분야, 타겟 시스템, ...
- 너무 많이 쓰면 논문이 지저분해짐 꼭 필요한 내용만...

Attack Model

- 어떤 공격자를 가정하는지
- 강한 공격자에 대한 가정은 논문을 강하게 만듦
- 약한 공격자에 대한 가정은 논문을 약하게 만드나...
- 진짜 그런 가정만으로 충분한지 평가가 필요
- 때론 Attack model section에 시스템에 대한 가정도 함
  - 다양한 시스템은 다양한 operation 모드가 존재
  - 어떤 시스템을 대상으로 하는지 가정

Overview

- 앞에서 가정한 Attack model과 시스템 가정을 기반으로
- 전체 공격, 시스템에 대한 overview
- 복잡한 경우에만 필요

Vulnerabilities and Exploits

- Background를 바탕으로 취약점 분석 방법 소개
- 그리고 각각의 취약점 소개
  - 어떻게 찾았는지
- 다음에 이런 취약점이 어떤 심각한 공격으로 어떻게 연결되는지 소개
  - causes and results
  - 심각하면 심각할 수록 좋음 ㅋ ㅋ

Evaluation

- 공격 논문에서 가장 중요한 것 중 하나가 evaluation
- Theoretical evaluation, Experimental results, Empirical results, Numerical results, …
- 독자들이 궁금해 할 만한 모든 내용을 담아야
- 평가가 빈약했을 경우 결과에 대한 의심을 줄 수 있음
- comprehensive and precise

Discussion

- 모든 논문에 한계는 있음
- Reviewer들이 쓰기 전에 내가 먼저 자폭 모드 ㅋ ㅋ
- 제3자의 입장에서 본인 논문을 평가하고 한계에 대하여 솔직히
  - ▷ 물론 그 한계가 심각하지 않다고 설득이 필요함
- 뿐만아니라 extension 등 논문이 갖는 (앞의 내용에서 언급 못한) 다양한 한계점에 대하여 설득
- 뭐든지 찜찜한 점은 남겨두지 말기
  - ▷ 내가 찜찜한 건 리뷰어도 찜찜함.

Related work and Bibliography

- 내가 이 분야에 대하여 열심히 공부를 했는데 우리는 새롭다에 대한 주장
- 전체 분야에 대하여 논문, 해킹 컨퍼런스 발표, 뉴스 등 커버할 수 있는 내용을 다 커버
  - ▷ 물론 중요한 내용은 많이, 중요하지 않은 내용은 간단히
- Structuring이 필요
- Pc member 논문 챙겨주기 ;-)

concluding Remarks and Future work

- 논문 내용 정리
- Lessons learned
- 그리고 앞으로 나아갈 방향

Responsible Disclosure and Open Source

- 공격 논문에 대해서는 Responsible Disclosure를 해야한다.
  - 국내: KISA, 해외: 미국 CERT를 사용하는 것이 편리
  - 소송, follow-up 등 복잡한 과정이 간단하게 처리됨
- 합법적 취약점 분석
  - 불법일 경우 내용이 좋아도 떨어질 수 있음
- Open Source Release
  - 설계, 구현 논문의 경우, open source release를 하면 유리

논문 제출 후

- 절대 만족하면 안 됨
- 항상 부족한 부분이 존재
- 붙더라도 Shepherd가 붙을 수 있고, 따라서 미리미리 수정 및 내용 보강
- 기본적으로 논문을 쓸 때는 훨씬 더 많이 쓰고 줄여나가는 방향으로
- 만약 붙고 특별한 리뷰가 없으면 저널로 ㅎ ㅎ

Questions?

- Yongdae Kim
  - email: yongdaek@kaist.ac.kr
  - Home: http://syssec.kaist.ac.kr/~yongdaek
  - Facebook: https://www.facebook.com/y0ngdaek
  - Twitter: https://twitter.com/yongdaek
  - Google "Yongdae Kim"