CS 294-28: Network Security

Prof. Vern Paxson

http://inst.eecs.berkeley.edu/~cs294-28/

http://www.icir.org/vern/cs294-28/

vern@cs

January 25, 2008

What Is This Class?

- Brand new graduate course on network security
  - Brand new = it will be bumpy at times
  - Graduate = focus on reading papers, participatory discussion, major project
  - Network security = how do we keep our computer networks functioning as intended & free of abuse
  - Network = heavy emphasis on global Internet
    - And not much emphasis on host-side issues

Target Audience

- Course intended to:
  - Provide grounding necessary for pursuing PhD research in network security
  - Provide breadth for those undertaking research in other areas of security
  - Eventually evolve into regular grad offering complementing CS 261
- Not intended to:
  - Summarize Internet security issues / technology / practices

Prerequisites

- EE 122 (undergrad networking) or equivalent
- Basic network security notions
  - Firewalls, public-key crypto, spoofing, buffer overflow attacks
- A willingness to thoughtfully read a lot of technical papers

Who Am I?

- New professor in CS
  - New = “it will be bumpy at times” :-)
  - Also affiliated with *International Computer Science Institute* and the *Lawrence Berkeley National Lab*
- Contact:
  - vern@cs, http://www.icir.org/vern/
  - Office hours M 3-4PM in 615 Soda
    - And by appointment, sometimes at ICSI
      - http://www.icsi.berkeley.edu/where.html
  - Phone: 643-4209, 666-2882
    - Email works *much* better!
  - Hearing impaired: please be ready to repeat questions & comments!

Who Am I?, con’t

- Research focuses on network security & network measurement
- Been around the block
  - 10+ years on both topics
  - PC chair/co-chair of SIGCOMM, USESEC, IEEE S&P (“Oakland”), HotNets
- CCIED = NSF Cybertrust *Center for Internet Epidemiology & Defenses*
  - Large-scale compromise, i.e., worms & now botnets
  - 5 year effort joint w/ UCSD (through 2009)
- “Bro” *network intrusion detection system* (NIDS) running 24x7 at LBNL (since 1996!)

My Perspectives/Biases

- I am an empiricist
  - It can be amazing how different a very large system behaves in practice vs. how you would expect it to …
    - … if you only measure in a confined laboratory environment
- A vital, easily overlooked facet of security is *policy*
- Much of network security is necessarily reactive, unprincipled, incomplete

Perspectives/Biases, con't

- The goal is risk management, not bulletproof protection.
  - Much of the effort concerns "raising the bar" and *trading off resources*
  - This applies to research as well as practice
- Key notion of threat model: what you are defending against
  - This can differ from what you'd expect
  - E.g., the Department of Energy …

Who Are You?

- Take background survey at *http://tinyurl.com/3b3xgz*
  - Part of homework #1
- Q: how many of you have taken CS 261?
- Q: how about CS 261 last semester?
- Q: how about Prof. Song's CS 294 last semester?
- Q: how many are comfortable with using *bSpace* for announcements/resources?
- Q: how many have opted in for *bSpace* email notifications?
  - (Whatever that means)

What's Expected of You?

- Read 2-3 papers/week
  - There is an art here regarding figuring out which facets to spend time on and which not
- Write mini-reviews of each paper
  - Mini-review = a few sentences for each of
    - What are the paper's main contributions?
    - What parts of the paper do you find unclear?
    - What parts of the paper are questionable?
      - E.g., methodology, omissions, relevance
    - Given the contributions, what issues remain? What related ideas does it bring to mind?
  - Email me your reviews > 24 hours prior to corresponding lecture
    - Late = 50% penalty (no credit if after lecture summary)

What’s Expected of You?, con’t

- Participate in lecture discussion of the paper & the topic
- “Scribe” 1-2 lectures/semester
  - Scribe = write up summary of lecture suitable for posting on course web site
  - Due 1 week after lecture
    - Send me PDF or HTML
  - Inspect syllabus and tell me which lecture(s) you’d like to scribe (FCFS)
  - (I’ll decide soon whether it’s 1 or 2 lectures based on class size)

What’s Expected of You?, con’t

- Undertake a significant project
  - Individually or in a team of two (encouraged)
    - Discuss w/ me if you want a larger team
- Can involve:
  - Measurement study characterizing/exploring a network security issue
  - Substantive analysis/assessment of security issues for a given network system
  - Development of a new mechanism or technique
  - Deep, thoughtful literature survey of an area
  - Develop & assess a new threat

Project, con’t

- Proposals due within a couple of weeks
- *Related Work* writeup due before Spring Break
- Short status report due a few weeks later
- Final project due at end of semester
  - Written as a conference-style paper
- Aim high!
  - End result should be workshop-caliber
  - The best should be within shouting distance of publication-caliber
- Find a topic that grabs you
  - Feel free to run preliminary ideas by me

Grading

Homework + Participation	20% + 15%
Scribing	15%
Project	50%

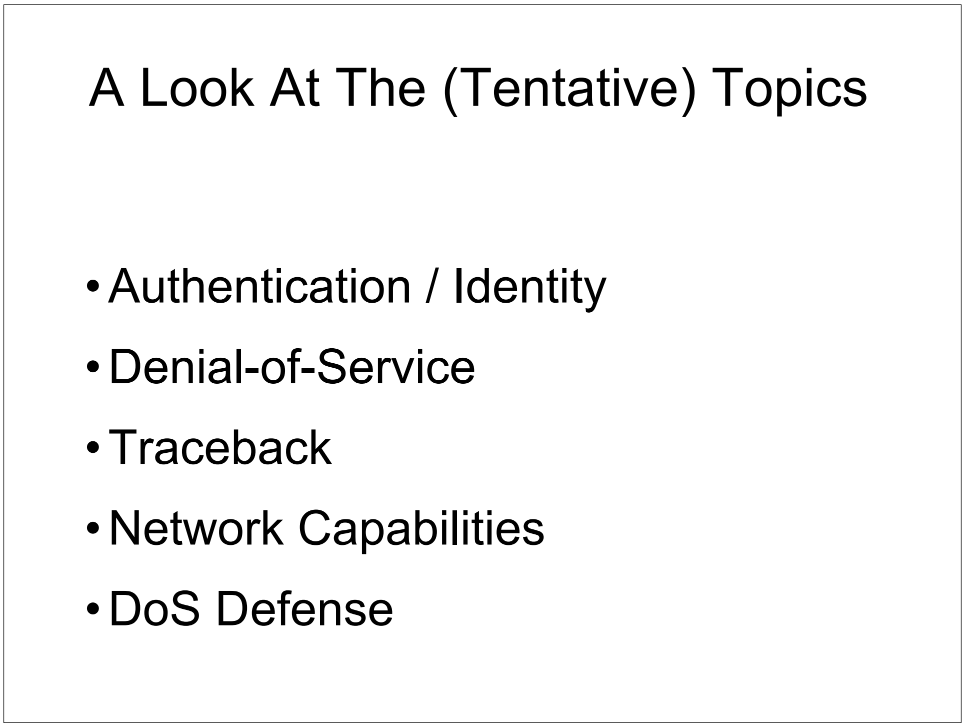
Lecture Format

- Each lecture starts from a core paper (sometimes 2)
- For the most part, seminal paper that opened new area or developed key new insight
  - Not “bleeding edge” or comprehensive
- Lecture will cover main contributions …
- … but then go from there into related considerations (sometimes taken from the optional reading) in an interactive fashion
- What to cover & where to go driven in part by thoughts/considerations from HW writeups

Ethics

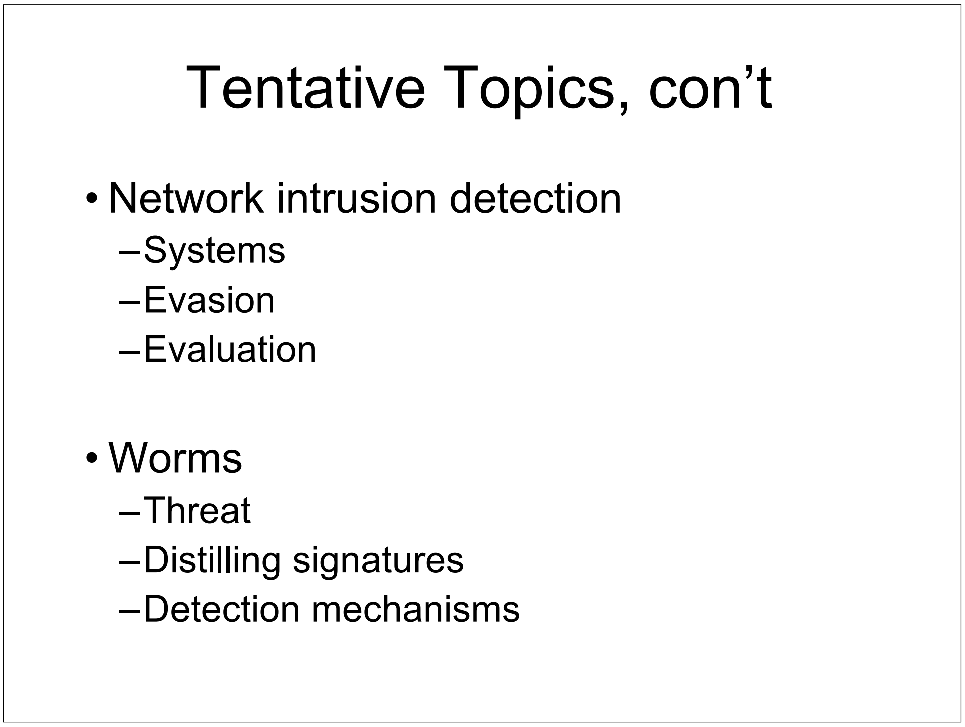
- We will be discussing attacks - some quite nasty! - and powerful eavesdropping technology
- None of this is in *any way* an invitation to undertake these in any fashion other than with informed consent of all involved parties
- If in some context there’s any question in your mind, come talk with me first

- Oh and: for homeworks, please do your own work



A Look At The (Tentative) Topics

- Authentication / Identity
- Denial-of-Service
- Traceback
- Network Capabilities
- DoS Defense



Tentative Topics, con’t

- Network intrusion detection
  - Systems
  - Evasion
  - Evaluation

- Worms
  - Threat
  - Distilling signatures
  - Detection mechanisms

Tentative Topics, con’t

- Forensics
- Scanning
- Side Channels
- Traffic Analysis (2)
- Web Attacks
- Botnets
- Attack infrastructure

Tentative Topics, con’t

- Anonymity
- Infrastructure Protection
- Secure Routing
- Wireless
- Peer-to-Peer
- Cellular / VOIP
- Trace anonymization
- The Underground Economy

Give Feedback

- Regarding syllabus
  - Topics/subtopics you'd like explored
  - Particular papers
- Post-lecture
  - We can revisit at beginning of next lecture
- Course mechanics
- Anonymous is fine if you want
  - Either using a remailer
  - Or just a note under my door (615 Soda)

Next Lecture

- Authentication & Identity
- Homework #1 due Sunday 1PM
  - Writeup for Needham/Schroeder paper
  - Background survey
  - Optional: read/write up *Do's & Don'ts* paper