Advanced System Security

CSE544 - Spring 2007
Introduction Computer and Network Security
Professor McDaniel
What is in a list?

The tale of Jonnie Thomas ...
This course is a systems course covering general topics in computer and network security. We will investigate the tools and problems of contemporary security. Topics will include:

- network security, authentication, security protocol design and analysis, key management, program safety, intrusion detection, DDOS detection and mitigation, architecture/operating systems security, security policy, group systems, biometrics, web security, language-based security, and other emerging topics (as time permits)
You need a basic understanding of …

• IP Networks
• Modern Operating Systems
• Security, cryptography, ...
• Discrete Mathematics
• Basics of systems theory and implementation
  ‣ E.g., File systems, distributed systems, networking, operating systems, ....
Why are we here? -- Goals

• My goal: *to provide you with the tools to execute and evaluate research in computer security.*
  ‣ Basic technologies
  ‣ Engineering/research trade-offs
  ‣ How to read/create/teach security research.

• *This is going to be a hard course.* The key to success is sustained effort. Failure to keep up with readings and project will likely result in poor grades, and ultimately little understanding of the course material.

• *Pay-off:* security competence is a rare, valuable skill
Course Materials

• Website - I am maintaining the course website at
  http://www.cse.psu.edu/~mcdaniel/cse544
  ‣ Course assignments, slides, and other artifacts will be made available on the course website.

• Course reading materials
  – A *lot* of papers.
Course Calendar

- The course calendar as all the relevant readings, assignments and test dates
- The calendar page contains electronic links to online papers assigned for course readings.
- Please check the website frequently for announcements and changes to the schedule. **Students are responsible for any change on the schedule** (I will try to make announcements in class).
Grades

- Grading policy
  - 30% Presentations
  - 20% Class Participation
  - 50% Course Project

- Lateness policy - Assignments and project milestones are assessed a 10% per-day late penalty, up to a maximum of 4 days. Unless the problem is apocalyptic, don't give me excuses. Students with legitimate reasons who contact the professor before the deadline may apply for an extension.
Skills Building

• One of the objectives of this course is to develop skills in public presentation, including what and how to tell a technology story.

  ‣ Papers: How and **why** to write a paper, the different parts, how they get evaluated ....

  ‣ Presentation: This is the whole course, and your performance will determine your grade to a great extent.

• **We will start learning to do this today.**
Presentations

• Everyone in the class is going to give one or two lectures covering a paper assignment.
  ‣ Ranging from 30 minutes to 1.25 hours, depending on the topic and the student’s public speaking experience
  ‣ You are to develop the entire lecture from scratch, which means all figures, diagrams, and words should be generated by you
    • Divergence from this rule will be deemed plagiarism
  ‣ I and the other students will “grade” each other on the presentation completeness, organization, content, and delivery

• NOTE: the in class presentation SHOULD NOT be the first time you give the talk!
Projects

• This is the standard security course project, which will cover the structure of next week. This should be some novel work in security research. Groups are allowed, but the expectations of the maturity and results increase linearly with the number of students.
  ‣ Ongoing work in OK.
  ‣ Work with other professors must be cleared with both Prof. McDaniel and the advising Prof. (discouraged)
  ‣ Often leads to MS thesis or other PhD leading work.
This course considers topics involving personal and public privacy and security. As part of this investigation we will cover technologies whose abuse may infringe on the rights of others. As an instructor, I rely on the ethical use of these technologies. Unethical use may include circumvention of existing security or privacy measurements for any purpose, or the dissemination, promotion, or exploitation of vulnerabilities of these services. Exceptions to these guidelines may occur in the process of reporting vulnerabilities through public and authoritative channels. Any activity outside the letter or spirit of these guidelines will be reported to the proper authorities and may result in dismissal from the class.

When in doubt, please contact the instructor for advice. Do not undertake any action which could be perceived as technology misuse anywhere and/or under any circumstances unless you have received explicit permission from Professor McDaniel.
How to create a lecture?

• Here, we are talking about the presentation of a conference or journal paper.
  ‣ What are the objectives of a talk?
  ‣ What are the objectives of a lecture?
A talk ...

• Your objectives in a talk are to ...
  ‣ Introduce the topic area
  ‣ Identify the theme of the work
  ‣ Establish your bona fides (credentials)
  ‣ Convince the listener the work is correct
  ‣ Convince the listener to read the paper

• Q: What does a talk not do?
A lecture ...

• Your objectives in a *lecture* are to ...
  ‣ Introduce the topic area
  ‣ Identify the theme* of the work
  ‣ Establish your bona fides (credentials)
  ‣ Convince the listener the work is correct
  ‣ Convince the listener to read the paper that is was worth reading
  ‣ Introduce/educate on topic, technology, methodology, and style
  ‣ Show how the work fits into the larger body of research

• Q: What does a lecture not do?
Grains of SANs

• **Rethinking storage**: what if storage was a fixed physical substance like grains of sand
  ‣ Mobile,
  ‣ Flexible (reorganization),
  ‣ Cheap,
  ‣ Resilient, ....

• What *applications* and *behaviors* would this enable?
  ‣ The “split” filesystem operation -- suppose Alice and Bob each have access to a filesystem that contains their data concerning project “Goosefood”, then Alice gets on an Airplane?
  ‣ Vehicle maps in a car of information devices
Designing **Granular Storage**

• Designing such a system requires us to rethink the way storage systems are constructed.
  ‣ **Organization** - how do we allocate data to the memory spots to ensure that the data can be accessed quickly and correctly?
  ‣ **Security** - how do we ensure the confidentiality, integrity, and authenticity of the data is preserved?
  ‣ **Reliability** - how do we ensure replicate/encode data to ensure it is survivable after separation events, and embraces new data as it joins events occur?

• This body of work will embrace the lessons of past storage systems research, but extends it in unusual ways.
  ‣ RFID protocols, highly separable storage, frequent “failures”
Mapping

• Q: *What* were the elements of the lecture?
• Q: *How* were the elements of the lecture handled?
  ‣ area
  ‣ theme
  ‣ topic
  ‣ methodology
  ‣ style
  ‣ placement in literature

• You should be answering these questions in considerably more depth than show in the previous example.