CNT5410 - Computer and Network Security: Introduction

Professor Kevin Butler
Fall 2015
Assoc. Prof. Kevin R. B. Butler

Research Interests:

➢ Security in Computer Systems and Networks
➢ Enterprise and Portable Storage Security
➢ Embedded & Cyber-Physical Systems Security
➢ Cloud Computing Security
➢ Privacy-Preserving Computing
➢ Mobile Phone Security & Privacy
➢ Interdomain Routing Security
➢ Secure Data Provenance

Research Highlights:

1. NSF CAREER Award (2013)
2. 50 Peer-Reviewed publications, national/int’l media coverage
3. TPC Chair of ACSAC (2014) and Vice-Chair of IEEE SP (2016)

Tel: (352) 392-1200
butler@cise.ufl.edu
http://www.cise.ufl.edu/~butler/

Room E454
Research Interests:
➢ Security for Cellular and Mobile Networks
➢ Mobile Application Security and Malware
➢ Telephony Provenance and Authentication
➢ Systems Security
➢ Emergency Alerts and Disaster Recovery
➢ Mobile Web Security

Research Highlights:
1. NSF CAREER Award (2010)
2. Alfred P. Sloan Fellow (2014)
3. TPC Chair of WiSec (2014)
4. Co-founder - Pindrop Security

Assoc. Prof. Patrick G. Traynor

tel: (352) 392-1200
traynor@cise.ufl.edu
http://www.cise.ufl.edu/~traynor/

Room E458
Research Interests:

➢ System on Chip Security
➢ Security Policy
➢ Software Security
➢ Social Engineering
➢ Systems Security

Research Highlights:

1. NSF CAREER Award (2012)
2. NSF PECASE (2012)
3. Organizer of NAE Frontier of Engineers Symposium (FOE) and Cyber Security Panel at FOE (2015)
Research Highlights:
1. NSF CAREER Award (2009)
2. Gift from Google’s CEO for Format-Transforming Encryption work
3. Organizer of Real World Cryptography conference, 2011 General Chair of CRYPTO

Research Interests:
- Cryptography
- Hash functions
- Authenticated Encryption
- Anonymity and Traffic Obfuscation
- Format Transforming Encryption
- Protocol Composition
Research Interests:
➢ Trustworthy Provenance-Aware Systems
➢ Communications & Network Security
➢ Embedded Device Security
➢ Mobile Phone Security & Privacy
➢ SSL/HTTPS Trust Enhancements
➢ Cloud Computing Security

Research Highlights:

1. UF Graduate School Fellow
2. 14 Peer-Reviewed publications
3. PC Member, ACSAC (2015), Web Chair of IEEE SP (2016)
Some bedtime stories ...
This course

- We are going to explore why these events are not *isolated*, *infrequent*, or even *unexpected*.

- Why are we doing so poorly in computing systems at protecting our users and data from inadvertent or intentional harm?

*The answer: stay tuned!*
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, intrusion detection, DDOS detection and mitigation, architecture/operating systems security, security policy, biometrics, web security, cloud security, and other emerging topics (as time permits)
You need to understand ...

- IP Networks
- Modern Operating Systems
- Discrete Mathematics
- Basics of systems theory and implementation
  - E.g., File systems, distributed systems, networking, operating systems, ....
Who should NOT take this class?

• Students without the necessary background courses.

• Students who have poor judgement.

• Students who are not willing to put forth significant effort.

• Students who are not interested in learning.

• Students interested in doing harm to people, property and infrastructure.
Goals

• My goal: *to provide you with the tools to understand and evaluate research in computer security.*
  
  ‣ Basic technologies
  ‣ Engineering/research trade-offs
  ‣ How to read/write/present security research papers
  ‣ Introduce you to the new Security Faculty at UF

• *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
  • www.cise.ufl.edu/class/cnt5410fa15

• Course assignments, slides, and other artifacts will be made available on the course website.

• Course textbook
  • Anderson, Security Engineering, 2nd edition: available for free on the web (readings will be on course web page)
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 (We will try to make announcements in class).
Grading

- Grading in this class will be distributed as follows:
  25% Course Research Project
  20% Mid-term Exam
  25% Final Exam
  20% Assignments
  10% Class Participation

- I reserve the right to give “Unannounced Learning Experiences”.

- You get the grade that you earn, so be sure that you earn a grade you like.
Readings

- There are a large amount of readings in this course covering various topics. These assignments are intended to:
  - Support the lectures in the course (provide clarity)
  - Augment the lectures and provide a broader exposure to security topics.
- Students are **required** to do the reading!

- About 10-20% of questions on the tests will be off the reading on topics that were not covered in class. You better do the reading or you are going to be in deep trouble when it comes to grades.
Lateness

• All assignments is due at the beginning of class.

• Late assignments are assessed a 15% per-day late penalty, with a maximum of four days.

• Students with legitimate reasons should contact the professor before the deadline to apply for an extension.

• Unless the problem is apocalyptic, don’t give me excuses.
Course Project

• End Result: Research Poster
  • Motivation for an Experiment
  • Background
  • Related Work
  • Experimental Approach
  • Experimental Evaluation

• I will provide sample topic areas
  • General Areas

• Start with an Existing System/Approach
  • Break It

• Improve It
  • Aim for a Research-Quality Result

• Written and oral communication are of tantamount importance!
Ethics Statement

• 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 and or institution.

• 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 Butler.
A Note on Academic Integrity

• As scientists and engineers, we must trust each other to make progress.

• Numerous examples exist to show the consequences of this breakdown.
  • Jan Hendrik Schon...

• Academic dishonesty, whether from cheating, copying, fabricating results or through any other dishonest practice will not be tolerated.
  • I take this very personally - you should too.
• Academic publications are written using \LaTeX.
  • Time to learn the tools of the trade.

• Your first assignment is to install a \LaTeX compiler on your personal computer and then write a one-page summary about:
  • Who you are
  • Where you came from
  • What your research interests are

• A printed copy of the resulting PDF and the \LaTeX source is due next Tuesday.
  • \textit{Word documents will receive a ZERO.}
Next Time...

- Security Engineering, Chapter 1
- Remember, you need to read it **BEFORE** you come to class!

- Start thinking about ideas for your semester project.
What is security?

- Harrison, Ruzzo and Ullman (1978)
  - “Prevent access by unauthorized users”

- Garfinkel and Spafford (1991)
  - “A computer is secure if you can depend on it and its software to behave as expected.”

- Neither are satisfactory - they fail to capture that security speaks to the behavior of others.

  - As expected by whom? Under what conditions? When?
Risk

• At-risk valued resources that can be misused
  • Monetary
  • Data (loss or integrity)
  • Time
  • Confidence
  • Trust

• What does being misused mean?
  • Privacy (personal)
  • Confidentiality (communication)
  • Integrity (personal or communication)

• Availability (existential or fidelity)

• Q: What is at stake in your life?
• A threat is a specific means by which an attacker can put a system at risk
  • An ability of an attacker (e.g., eavesdrop on a communication channel)
  • Independent of what can be compromised

• A threat model is a collection of threats that deemed important for a particular environment
  • A collection of attacker(s) abilities
  • E.g., A powerful attacker can read and modify all communications and generate messages on a communication channel

• Q: What were risks/threats in the introductory examples?
  ▶ Estonia? Yale/Princeton? Stuxnet? Wikileaks?
Vulnerabilities (attack vectors)

- A vulnerability is a systematic artifact that exposes the user, data, or system to a threat
- E.g., buffer-overflow, WEP key leakage
- What is the source of a vulnerability?
  - Bad software (or hardware)
  - Bad design, requirements
  - Bad policy/configuration
  - System Misuse
  - Unintended purpose or environment
    - E.g., student IDs for liquor store
An adversary is anyone attempting to circumvent the security infrastructure.

- The curious and generally clueless (e.g., script-kiddies)
- Casual attackers seeing to understand systems
- People with an axe to grind
- Malicious groups with sophisticated users (e.g., chaos clubs)
- Competitors (industrial espionage)
- Governments (seeking to monitor or disrupt activities)
Are users adversaries?

- Have you ever tried to circumvent the security of a system you were authorized to access?
- Have you ever violated a security policy (knowingly or through carelessness)?
Attacks

• An attack occurs when someone attempts to exploit a vulnerability

• Kinds of attacks
  • Passive (e.g., eavesdropping)
  • Active (e.g., password guessing)
  • Denial of Service (DOS)
    • What is DDoS?

• A compromise occurs when an attack is successful
  • Typically associated with taking over/altering resources
Participants

- **Participants** are expected system entities
  - Computers, agents, people, enterprises, …
  - Depending on context referred to as: servers, clients, users, entities, hosts, routers, …
- Security is defined with respect to these entities
  - Implication: every party may have unique view
- **A trusted third party**
  - Trusted by all parties for some set of actions
  - Often used as introducer or arbiter
Trust

• Trust refers to the degree to which an entity is expected to behave.

• What is an entity not expected to do?

• A trust model describes, for a particular environment, who is trusted to do what.

• You make trust decisions every day...
  • What are they?
  • Whom do you trust?

• Can you measure trust?
A **security model** is the combination of a trust and threat models that address the set of perceived risks

- The “security requirements” used to develop some cogent and comprehensive design

- Every design must have security model
  - LAN network or global information system? Java applet or operating system?

- The single biggest mistake seen in use of security is the lack of a coherent security model
  - It is very hard to retrofit security (design time)

- This class is going to talk a lot about security models
  - What are the security concerns (risks)? Threats?
    - Who are our adversaries?
  - Who do we trust and to do what?
  - Systems must be explicit about these things to be secure.
A Security Model Example

• Assume we have a University website that hosts courses through the web (e.g., Canvas)
  • Syllabus, other course information
  • Assignments submissions
  • Online Grading

• In class: elements of the security model
  • Participants (Trusted)
  • Adversaries
  • Risks
  • Threats