CS4264: Principles of Computer Security
Who am I?

- **Gang Wang**
  - Assistant Professor of Computer Science at VT (2016-Present)
  - PhD from University of California, Santa Barbara (2016)
  - *Research topics:* Security, Data Mining, Internet Measurements

- Office hour: after class, by appointment (gangwang@vt.edu)

- Office: 2202 Kraft Drive, KWII, RM 2223
Class Website

- Course site: [http://people.cs.vt.edu/~gangwang/class/cs4264/](http://people.cs.vt.edu/~gangwang/class/cs4264/)

---

### CS4264: Principles of Computer Security

**Schedule | Grading | Policies | Canvas Site**

<table>
<thead>
<tr>
<th>Instructor</th>
<th>Gang Wang (<a href="mailto:gangwang@vt.edu">gangwang@vt.edu</a>)</th>
</tr>
</thead>
<tbody>
<tr>
<td>Time/Location</td>
<td>MW 2:30 PM - 3:45 PM Torgersen Hall 3100</td>
</tr>
<tr>
<td>Office Hour</td>
<td>After class or By appointment. My CRC office is in KnowledgeWorks II, room 2223 (Reachable via CRC shuttle)</td>
</tr>
<tr>
<td>TAs</td>
<td>Location: 106 McBryde Hall TBA</td>
</tr>
<tr>
<td>Final Exam</td>
<td>May 13, 2019; 2:05PM - 4:05PM</td>
</tr>
</tbody>
</table>

- Use Canvas to submit your assignments and project reports
TAs

Peng Peng
(pengp17@vt.edu)
office hour: TBA

Limin Yang
(liminyang@vt.edu)
office hour: TBA

Andrew Bond
(dbond07@vt.edu)
office hour: TBA

*If any student needs special accommodations because of a disability, please contact me in the first week of classes*
Let’s get to know you

- Introducing yourself to 2 people near you (5 minutes)
Textbook

- Introduction to Computer Security.
Goals for this Course

- Critical thinking
  - How to think like an attacker
  - How to reason about threats and risks
  - How to balance security costs and benefits

- Technical skills
  - How to protect yourself
  - How to manage and defend systems
  - How to design and program secure systems

- Learn to be a security-conscious citizen

- Learn to become a “hacker” (an ethical one)
Topic Overview

1. **Security basics and definitions**: Confidentiality, integrity, availability, attack models

2. **Cryptography**: Basic crypto primitives, Secret and public key crypto, Digital signatures, Message authentication

3. **Network security**: Network protocols and attacks, SSL, IPSec, Intrusions and intrusion detection, Firewalls, Worms, botnets

4. **Web security**: Browser security, JavaScript, ActiveX, Public key infrastructure, Email authentication, spam detection and prevention, Cloud computing security

5. **Operating system security**: Authentication, password security, Access control, memory/data/file protection, Security protocols, Kerberos

6. **Software security**: Memory errors, buffer overflow, shellcode, Information flow, covert channel, isolation, Polymorphic virus and detection

7. **Privacy**: Anonymity, anonymous routing, TOR, Data loss prevention, Data anonymization
**Expected Work**

- Attend all lectures, read required chapters
- Take in-class quizzes
- Finish assignments **independently**
- **Attack/Defense of the week presentation**
  - 10 minutes before each class
  - Choose your own topic, related to real-world security
  - A group of 3 students --- form your group ASAP
  - Claim the time slot (the link is also available on the class website):
    - [https://docs.google.com/document/d/1un1Y1-u6GFCpO0U9nVAsHPrnVj_kJAwiki_ZwXDRheYw/edit?usp=sharing](https://docs.google.com/document/d/1un1Y1-u6GFCpO0U9nVAsHPrnVj_kJAwiki_ZwXDRheYw/edit?usp=sharing)

**E.g., Equifax data breach, recent DDOS attacks**
Grading

- Sum up the points obtained from each category (x out of 100)
- Use the following scale to determine the letter grade:
- I do not curve the grades

<table>
<thead>
<tr>
<th>Component</th>
<th>Percentage</th>
</tr>
</thead>
<tbody>
<tr>
<td>Class participation, in-class quizzes</td>
<td>10%</td>
</tr>
<tr>
<td>Weekly presentation</td>
<td>10%</td>
</tr>
<tr>
<td>Written assignments (~3)</td>
<td>18%</td>
</tr>
<tr>
<td>Programming assignments (~3)</td>
<td>20%</td>
</tr>
<tr>
<td>Midterm exam (close-book, close-note)</td>
<td>18%</td>
</tr>
<tr>
<td>Final exam (close-book, close-note)</td>
<td>24%</td>
</tr>
</tbody>
</table>
Policies

- **Late policy**
  - No late submission is allowed *(with extremely rare exceptions)*
  - One-day “time bank” for assignments (written/programming)
    - No need ask permission to use, just submit late (but no later than 24 hours)
    - Can only be used *once*

- **Regarding policy**: similar to “NFL Coaches Challenge” rule
  - You have one (1) challenge for the re-grading of *assignments*
  - Challenge successful → keep the challenge
  - Challenge failed → permanently lose it

- **Virginia Tech honor code**
  - Finish homework/exams *independently*. No “github” code!
  - More in class site. When in doubt, ask me
No “Force Add” in the Class

- “force add” deadline has been passed. 😞
- Please Do Not stop by the CS office to make an appeal in person
- You can send them an email
Questions?
Security Fail
Threat Models, Security Goals and Assumptions

- **Security goal** (aka the definition of security):
  - What does it mean to be secure?

- **Threat model**: defines possible attacks (defenses) for a given asset/system

- **Security assumption(s)**:
  - Who/what is trusted
  - What does the attacker know
  - What resource/capacity does the attacker have?

Security is relative …

- **Economy**: if the attacking cost is much higher than the profits
- **Time**: if it takes “too long” to finish the attack (e.g. 100 years)
Meet the Adversary

“Computer security studies how systems behave in the presence of an adversary.”

The adversary
a.k.a. the attacker
a.k.a. the bad guy

* An intelligence that actively tries to cause the system to misbehave.
“Know your enemy.”

- Motives?
- Capabilities?
- Degrees of access?
The Security Mindset

- Thinking like an attacker
  - Understand techniques for circumventing security.
  - Look for ways security can break, not reasons why it won’t.

- Thinking like a defender
  - Know what you’re defending, and against whom.
  - Weigh benefits vs. costs:
    - No system is ever completely secure.
  - “Rational paranoia!”
High-Level Approaches

Attacks

Defenses
Why Study Attacks?

Identify vulnerabilities so they can be fixed.
Create incentives for vendors to be careful.
Learn about new classes of threats.
  - Determine what we need to defend against.
  - Help designers build stronger systems.
  - Help users more accurately evaluate risk.
“Insecurity”?  

**Level-2 Problem: “Weakness”**  
Factors that predispose systems to vulnerability

**Level-1 Problem: “Vulnerability”**  
Specific errors that could be exploited in an assault.

**Level-0 Problem: “Assault”**  
Actual malicious attempt to cause harm.

“Attack”  
Assault recipe, vulnerabilities are ingredients
Thinking Like an Attacker

- Look for weakest links – easiest to attack.

- Identify assumptions that security depends on. Are they false? Can I make them false?

- Think outside the box: Not constrained by system designer’s worldview.

Practice thinking like an attacker:
For every system you interact with, think about what it means for it to be secure, and image how it could be exploited by an attacker.
Exercises

- How can you abuse the signup sheet for the in-class presentation?

- Please don’t actually do it 😊
Thinking as a Defender

- Security policy
  - What are we trying to protect?
  - What properties are we trying to enforce?

- Threat model
  - Who are the attackers? Capabilities? Motivations? Knowledge?
  - What kind of attack are we trying to prevent?

- Risk assessment
  - What are the weaknesses of the system?
  - What will successful attacks cost us?
  - How likely?

- Countermeasures
  - Costs vs. benefits?
  - Technical vs. nontechnical?

Challenge is to think rationally and rigorously about risk.

Rational paranoia.
CIA/AAA Properties

- **Confidentiality**
  - In Communication: How to protect confidentiality of email, surfing history?
  - In System: How to control the access (aka authorization)

- **Integrity** means no tampering, but is a broad concept
  - File integrity – has a file been tampered with?
  - Communication integrity - error detection and correction
  - System integrity – has a computer been compromised? (enterprise security)

- **Availability**
  - Network availability: How to distinguish flash crowd from DDOS attack?
  - System availability: Fault-tolerant, graceful degradation, QoS control
CIA/AAA Properties (Con’t)

- **Authenticity**
  - How to prove who you are to a system (what you have, what you know)
  - How to prove the origin of an email

- **Anonymity**
  - How to remain anonymous (untraceable)?
  - Sometimes referred as privacy

- **Assurance**
  - How trust is provided and managed?