CS4264: Principles of Computer Security

Gang Wang
Fall 2016
About This Class

• Tue./Thu. 3:30 PM - 4:45 PM in New Classroom Building 120

• Instructor
  – Gang Wang, Assistant Professor of Computer Science
  – Office hour: After class, by appointment (gangwang@vt.edu)
  – Office location: 2202 Kraft Drive, Knowledge Works II, RM 2223

• TAs
  
  **Fang Liu** ([fbeyond@vt.edu](mailto:fbeyond@vt.edu))
  Office hour: Tue. 5 - 7 PM
  106 McBryde Hall

  **Stefan Nagy** ([snagy2@vt.edu](mailto:snagy2@vt.edu))
  Office hour: Fri. 10 - 11 AM
  106 McBryde Hall

• If any student needs special accommodations because of a disability, please contact me in the **first week of classes**
Textbook

• Introduction to Computer Security.
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 | Assignments | Grading | Policies**

<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>Tuesday/Thursday 3:30 PM - 4:45 PM in New Classroom Building 120</td>
</tr>
<tr>
<td>Office Hour</td>
<td>By appointment. His CRC office is in KnowledgeWorks II, room 2223. (Reachable via CRC shuttle)</td>
</tr>
<tr>
<td>TAs</td>
<td>TBA (<a href="mailto:xxx@cs.vt.edu">xxx@cs.vt.edu</a>), office hours: Monday 3:30 PM - 5:30 PM, TBA</td>
</tr>
</tbody>
</table>

**Announcements**

8/15/16: The first class will be on Tuesday of August 22, 2016.

**Class Description**

The topics of this class include survey of computer security problems and fundamental computer security design principles and models for software systems; Cryptographic models and methods; Modern cyber security techniques for robust computer operating systems, software, web applications,

- Use [Scholar](http://people.cs.vt.edu/~gangwang/class/cs4264/) Canvas system to submit homework/assignments
  - [https://canvas.vt.edu/courses/32151](https://canvas.vt.edu/courses/32151)
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, ID management, 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 and exploits, 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
  – Every Thursday, 10 minutes
  – A group of 3 students
    o Form your group ASAP
    o Send me an email to claim the time slot (group members + time)
    o First presentation on September 1st
    o Please send me your topic one week before the presentation
  – Choose your own topic, related to real-world security
    e.g., Target data breach incident, Nevada Creech Air Force Base security breach, FireEye Intrusion Detection tool ...
Grading

<table>
<thead>
<tr>
<th>Category</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>

• 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 in any ways
Policies

• **Late policy**
  – No late submission is allowed
  – One-day “time bank” for assignments (written/programming)
    o No need ask permission to use, just submit late (but no later than 24 hours)
    o 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**
  – More in class site. When in doubt, ask me
Computer and Network Security

A BIT OF HISTORY
Evolving Landscape Of Attacks

[1980’s – early 1990’s]
curiosity fueled hacking: capability demonstration of hackers

[late 1990’s – present]
Financial driven attacks: spam, stealing credit cards, phishing, large-scale botnets

[late 2000 – present]
Targeted attacks: stealing proprietary information, information warfare

Challenges caused by:
Scale, complexity, anonymity

Internet was a friendly place. Security problem then was
-- Barbara Fraser
Mariposa botnet 12 million IPs; Stolen data belonging to 800K users; Malware changes every 48 hours; Attacker uses real name in DNS.

http://pandalabs.pandasecurity.com/mariposa-botnet/

<table>
<thead>
<tr>
<th>#</th>
<th>Cities</th>
<th>%</th>
<th>IPs</th>
</tr>
</thead>
<tbody>
<tr>
<td>1</td>
<td>Seoul</td>
<td>5,36%</td>
<td>761,444</td>
</tr>
<tr>
<td>2</td>
<td>Bombay</td>
<td>4,45%</td>
<td>631,927</td>
</tr>
<tr>
<td>3</td>
<td>New Delhi</td>
<td>4,27%</td>
<td>605,518</td>
</tr>
<tr>
<td>4</td>
<td>Mexico</td>
<td>3,89%</td>
<td>551,705</td>
</tr>
<tr>
<td>5</td>
<td>Bogotá</td>
<td>2,68%</td>
<td>380,487</td>
</tr>
</tbody>
</table>
Multiple points where you can stop data exfiltration

Employee
- Data encryption on PC
  - Avoid social engineering attack
  - Patching

Work-place PC
- Secure OS
  - e.g., memory protection
- Secure applications
  - e.g., Email authentication
  - e.g., Browser sandbox

An organization

Internal servers
- Data encryption on server
- Patching

firewall
- IDS (intrusion detection system)
- IPS (intrusion prevention system)

Internet

server
- Data loss prevention (DLP)
A bit of history: Crypto and network security

• Stream cipher (Caesar’s cipher, ~60 BC)
• World war I and II for radio, wireless communication (e.g., Battle of Midway 1942)
• Information security
  – Access control models, e.g., Bell-LaPadula model (1973), Biba model (1975), Clark-Wilson model (1987)
  – Information flow
  – Confidentiality, integrity, availability, authenticity
• Public-key cryptography
  – Diffie-Hellman key exchange (1976)
  – RSA public key (1978)
• Arpanet (1960s) and network security protocols
  – SSL/TLS, IPSec, DNSSec, email security, mobile/sensor network security
• Web (late 1980s) and web security
  – Phishing, cross-site scripting, drive-by download, mobile code exploits
Most abused infection vectors

Malware download through drive-by-download and piggy-backing download
http://blog.trendmicro.com/most-abused-infection-vector/
Computer Virus

• 1972 Sci-Fi novel “When HARLIE Was One” features a program called VIRUS that reproduces itself

• First academic use of term virus by PhD student Fred Cohen in 1984, who credits advisor Len Adleman with coining it

• In 1982, high-school student Rich Skrenta wrote first virus released in the wild: Elk Cloner, a boot sector virus infecting the boot-sector of a floppy disk
  – Virus copies itself from disk to disk
  – boot sector was a popular target as it is executed automatically

• Brain (another boot-sector virus), by Basit and Amjad Iqbal in 1986, credited with being the first virus to infect PCs (MS-DOS)
  – https://youtu.be/lnedOWfPKT0?t=129
Computer Worm

- First worm in the lab of John Shock and Jon Hepps at Xerox PARC in the early 80s
- CHRISTMA EXEC written in REXX, released in 1987, targeting IBM VM/CMS systems with e-mail service
- The first Internet worm was the Morris Worm, written by Cornell student Robert T. Morris Jr.
  - Spafford’s analysis: [http://spaf.cerias.p](http://spaf.cerias.p)
  - Exploited stack buffer overflow vulnerability
- Love letter worm in 2000
  - A Visual Basic program disguised as a love letter
  - love-letter-for-you.txt.vbs
- Watch how Code Red worm spreaded in 2001
  - [http://www.youtube.com/watch?v=v6GnX3ZhuAg](http://www.youtube.com/watch?v=v6GnX3ZhuAg)