

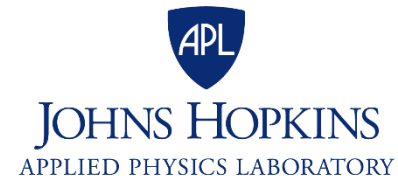
WELCOME TO NETWORK SECURITY

EN.600.424

Fall 2018

Lecture Notes

SETH JAMES NIELSON



EDUCATION PHILOSOPHY

TECHNICAL	NON TECHNICAL
THEORY	PRACTICE
EDUCATED	SKILLED
TEACHER	STUDENT



THE 5 ORDERS OF IGNORANCE

- 0th Order: Known Knowns
- 1st Order: Known Unknowns
- 2nd Order: Unknown Unknowns
- 3rd Order: Unknown methods for discovering unknown unknowns
- 4th Order: Unknown methods for exploring the orders of ignorance
- (Adapted from Phillip Armour, “The Five Orders of Ignorance”)

ANOTHER VIEW OF SKILL AND EDUCATION

- 0th Order: Known Knowns

SKILL

- 1st Order: Known Unknowns

- 2nd Order: Unknown Unknowns

- 3rd Order: Unknown methods for discovering unknown unknowns

- 4th Order: Unknown methods for exploring the orders of ignorance

EDUCATION

- (Adapted from Phillip Armour, “The Five Orders of Ignorance”)

THEORY VS. PRACTICE

XSS, GDS, ???	Specific XSS Bug
Composition Bug	XSS, CSRF
WHY DOES STUFF BREAK?	WHAT BREAKS TODAY?
THEORY	PRACTICE



BALANCING TEACHER AND STUDENT

- The best education happens when both *despise* mediocrity
 - Teacher must be completely committed to student success
 - Student must be completely committed to *becoming* excellent
- Shared vision!
- There are no short cuts for either teacher or student!
 - Success requires sufficient time
 - Success requires sufficient sacrifice (“you get what you pay for”)
 - Success requires sufficient humility

STUDENT + TEACHER



MEDIOCRITY

**Sufficient Time
Sufficient Sacrifice
Sufficient Humility**



SHARED VISION

BALANCE IS HARD

- I have ***REVISED*** the curriculum this semester
- Significantly more technical content
 - Special focus on network protocols
 - This requires that I scale back broader concepts
- GOAL: Integrate “big picture” thinking into every lecture

CLASS POLICIES: *CHEATING*

- Don't do it.
- Really, don't do it.
- If you have questions about whether something is cheating, ask me
 - Do not plagiarize; if you use somebody else's material, cite it
 - Do not get help from anyone except me on solo assignments
 - When working in groups, I recommend paper trails to protect yourself
- Consequences of cheating:
 - Failure on the assignment plus a 10% reduction to your course grade
 - Damaged reputation (The security community is small)

CLASS REPOSITORIES

- <https://github.com/CrimsonVista/NetworkSecurityFall2018>
 - Class Materials
 - Class Discussion
 - Links to other Repo's for frameworks, game etc
- You will need your own private git repo
 - Teacher and CA's will need access
 - GitHub should have academic (free) pricing
 - Or, you can use BitBucket
 - Later, will form a “company” with it's own repo

PROGRAMMING REQUIREMENTS

- This class is programming intensive
- You must be able to create client/server code in Python3
- There will be a programming test next class period
 - In-class, timed
 - You will complete one-or-more networking-based programs
 - Each program will be worth a certain number of points
 - If you do not score at least 50, you will need to drop or create a remediation program

PLAYGROUND OVERVIEW

- Playground is an “overlay” network
- It allows us to create a world that is easy to hack
- You build your own security protocols within the overlay
- Compatibility with other students requires standards

PLAYGROUND ENGINEERING TASKFORCE

- Similar to the Internet Engineering TaskForce (IETF)
- Forms a committee that must develop common class specifications
- Every student is a non-voting participant; virtual meetings
- 5 students will be selected to be voting members of the PETF
- Students will submit proposed PLAYGROUND Request for Comments' (PRFC's) as part of labwork
- Voting members will choose one to be the class specification

GROUP-SPECIFIC SPECIFICATIONS

- Sometimes, specifications will not be binding on the entire class
 - Optional features
 - Features designed/developed by a group or groups
- The “owner(s)” of the design must still publish the specification as a PRFC

A WORD ABOUT ETHICS

- Please don't ever use this class as justification to behave unethically
- You have to know how the bad guy thinks, but you don't have to be the bad guy!
 - "It is from their foes, not their friends, that cities learn the lessons of building high walls" (Aristophanes)
- One purpose is to learn (safely) behave like a bad guy
 - If you want to engage in behavior that you're not sure is safe, ASK ME
 - Make sure your attacks really are confined to the playground nodes
- If you "attack" another student's real computer, code, systems, passwords, etc
 - You will face academic discipline
 - Depending on what you do, maybe civil/criminal penalties

QUESTIONS!

- If there's time left in class, ask me questions
- Otherwise, come see me at office hours!