Advanced Network Security

Taekyoung Kwon
tkkwon@snu.ac.kr

Overview

- objectives
  - Students learn basics of cryptography
  - Students understand Internet security with a focus on authentication
  - Students get familiar with blockchain technologies
- Course materials
  - Textbook
    - Any textbook on cryptography
  - Slides
  - References
    - Papers, standards

outline (1/3)

- blockchain
- bitcoin
- zerocoin
- ethereum
- Hyperledger fabric
- Smart contract programming

outline (2/3)

- PKC, certificate, PKI
- TLS, DANE, Let's encrypt
- OAuth, OpenID Connect

- Hash function
- Digital signature
- Zero knowledge proof

outline (3/3)

- As a team
  - Paper presentation
  - Team meeting
  - Project presentation

Team Formation

- Two or three guys will be one team
- each team presents a paper published in last 5 yrs
  - IEEE S&P, ACM CCS, USENIX Security, ISOC NDSS
  - ACSAC, ACNS, ESORICS, CSF, RAID, PETS
- each team performs a project
  - Smart contract
  - Academic proposal
    - Topics are not limited to authentication
- Presented paper can have no relation to your project

Term project

Academic proposal

- propose an idea better than the one(s) in the reference paper(s)
- Numerical analysis
  - Mathematical model
  - Simulation
  - Prototype
- Analyze pros and cons

Smart contract

- Any interesting service
  - Highlight the difference from the reference program
- example
  - Crowdfunding
  - Voting
  - Oracle
  - ...
- Ethereum
  - Solidity
- Hyperledger fabric
  - Go, node.js

administrivia

- Classroom: 301-101
- Time: Tue. and Thu., 11:00am – 12:15pm
- TA: Junghwan Lim
  - jhlim@mmlab.snu.ac.kr
- Slides and announcements
  - http://etl.snu.ac.kr

evaluation

- 25%: mid-term exam
- 25%: final exam
- 15%: paper presentation
- 20%: term project
- 15%: attendance
  - Two latenesses will be counted as one absence
  - Students absent 4 times or more may get grade F
  - I will try my best to start every class 11:00am, sharp

My office hour

- During one hour before the classes on Tue. and Thu.
  - My office: 301-503
- tkkwon@snu.ac.kr; tkkwon98@gmail.com
- Phone: 880-9105

- It is safe to send me email for appointment in advance

No cheating

- *Zero Tolerance Cheating Policy*
- Cheating in this class is defined as knowingly or unknowingly participating in the submission of unoriginal work for any test.
  - Answer to roll-call on behalf of another guy is also cheating
- If I find out that a student has cheated
  - Assign a fail grade to the student
  - Dismiss the student for the remainder of the class

Manners in the class

- Eating/drinking is OK
  - as long as noise is tolerable
  - As long as not smelly
- Going to restroom is OK
- Turn off your phones, audio devices,…
- Using laptops, tablet PCs is OK
  - Only for class
  - mute mode

april

25 March	26	27	28	29	30/31 March
1 April	2 Hyperledger fabric	3	4 Hyperledger fabric	5 Team grouping	6/7
8	9 IOTA	10	11 Mid-term	12 paper candidate upload	13/14
15	16 Certificate/PKI	17	18 TLS	19 Paper presentation schedule	20/21
22	23 DANE, OAuth	24	25 Smart contract programming	26	27/28
29	30 Team meeting	1 May	2	3	4/5

may

29 April	30 April	1 May	2 Team meeting	3	4/5
6	7 paper presentation	8	9 paper presentation	10	11/12
13	14 paper presentation	15	16 paper presentation	17	18/19
20	21 PKC	22	23 Zero knowledge proof	24	25/26
27	28 Zerocoin, zerocash	29	30 Final exam	31	1/2 June
3	4	5	6	7	8/9

june

27 May	28	29	30	31	1/2 June
3	4 Team meeting	5	6 Team meeting	7	8/9
10	11 Project presentation	12	13 Project presentation	14	15/16
17	18	19	20	21	22/23
24	25	26	27	28	29/30
1 July	2	3	4	5	6/7