
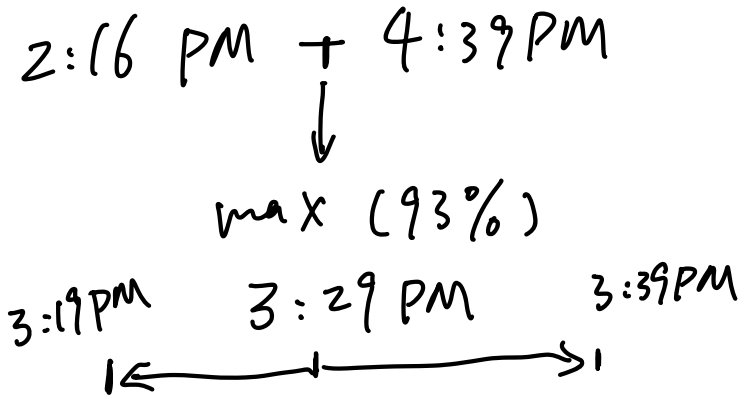


1. Eclipse
  2. Intro to security
  3. Authentication 
- 



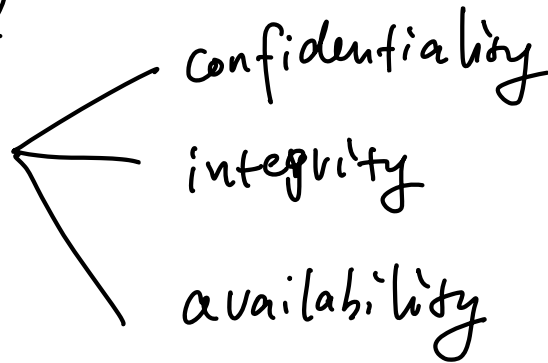
Admin.

- Lab3 regrading
- Lab5

### • Security

- Security assumptions?
- how strong the adv. are?
- entity to protect?

### • OS/Systems Security



# 45th IEEE Symposium on Security and Privacy

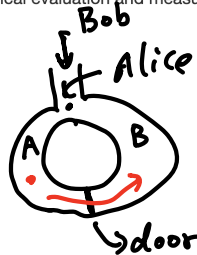
Sponsored by the IEEE Computer Society Technical Committee on Security and Privacy  
in cooperation with the International Association for Cryptologic Research

## Call For Papers

Since 1980 in Oakland, the IEEE Symposium on Security and Privacy has been the premier forum for computer security research, presenting the latest developments and bringing together researchers and practitioners. We solicit previously unpublished papers offering novel research contributions in any aspect of security or privacy. Papers may present advances in the theory, design, implementation, analysis, verification, or empirical evaluation and measurement of secure systems. Theoretical papers must make a convincing case for the relevance of their results to practice.

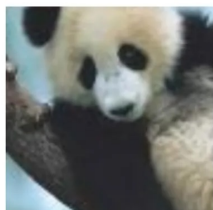
Topics of interest include:

*zero-knowledge.*



*2018.  
• meltdown  
• spectre*

- Applied cryptography
  - Attacks with novel insights, techniques, or results
  - Authentication, access control, and authorization
  - Blockchains and distributed ledger security
  - Cloud computing security
  - Cyber physical systems security
  - Distributed systems security
  - Economics of security and privacy
  - Embedded systems security
  - Formal methods and verification
- Hardware security
  - Hate, Harassment, and Online Abuse
  - Human-centered security and privacy
  - Intrusion detection and prevention
- Machine learning and computer security
  - Malware and unwanted software
  - Network security and measurement
- ✓ Operating systems security
  - Privacy-enhancing technologies, anonymity, and censorship
  - Program and binary analysis
  - Protocol security
  - Security and privacy metrics
  - Security and privacy policies
  - Security architectures
  - Security for at-risk populations
  - Software supply chain security
- Systems security
  - User studies for security and privacy
  - Web security and privacy
  - Wireless and mobile security/privacy



“panda”

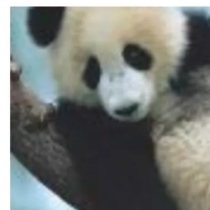
57.7% confidence

+ .007 ×



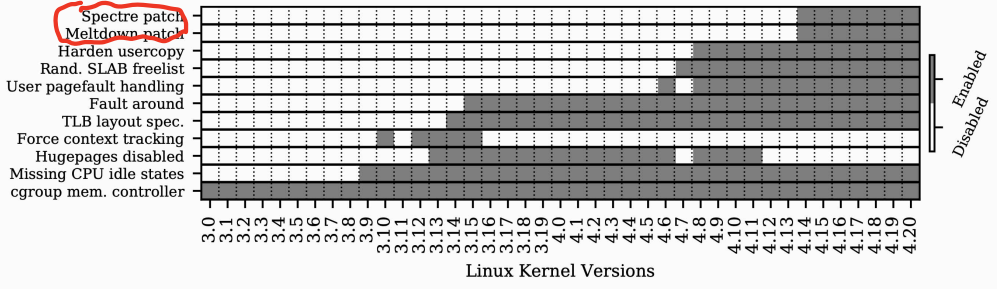
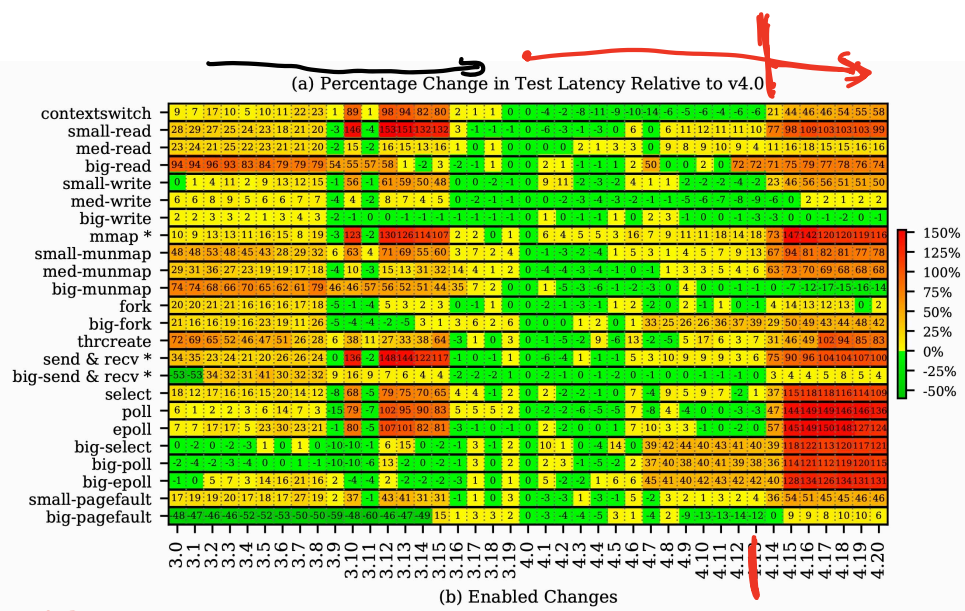
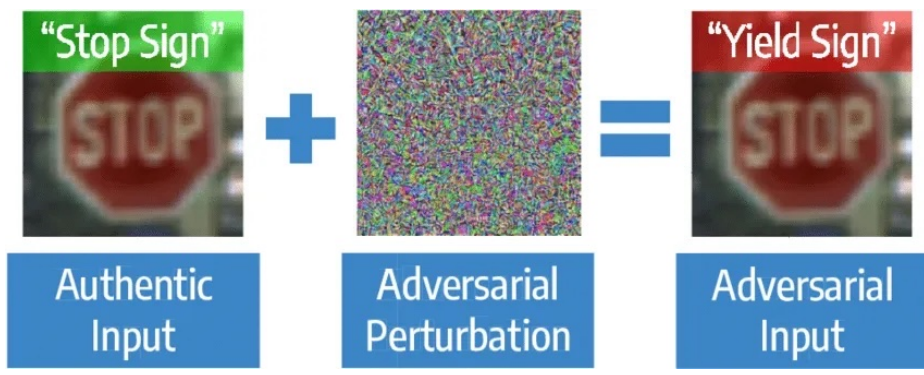
noise

=

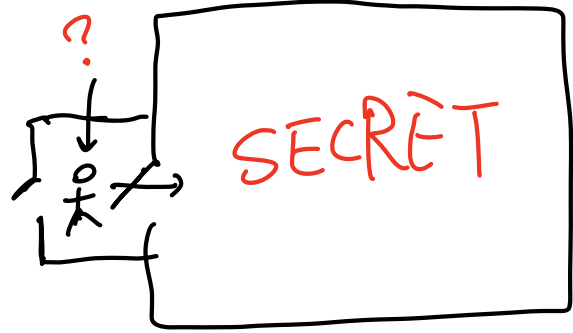


“gibbon”

99.3% confidence

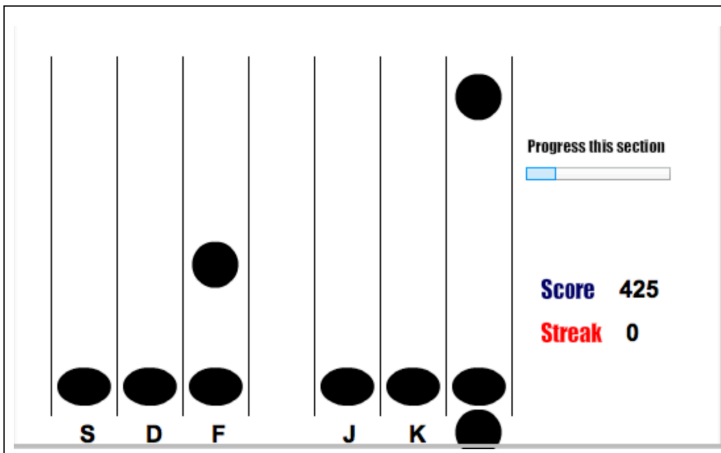


Authentication

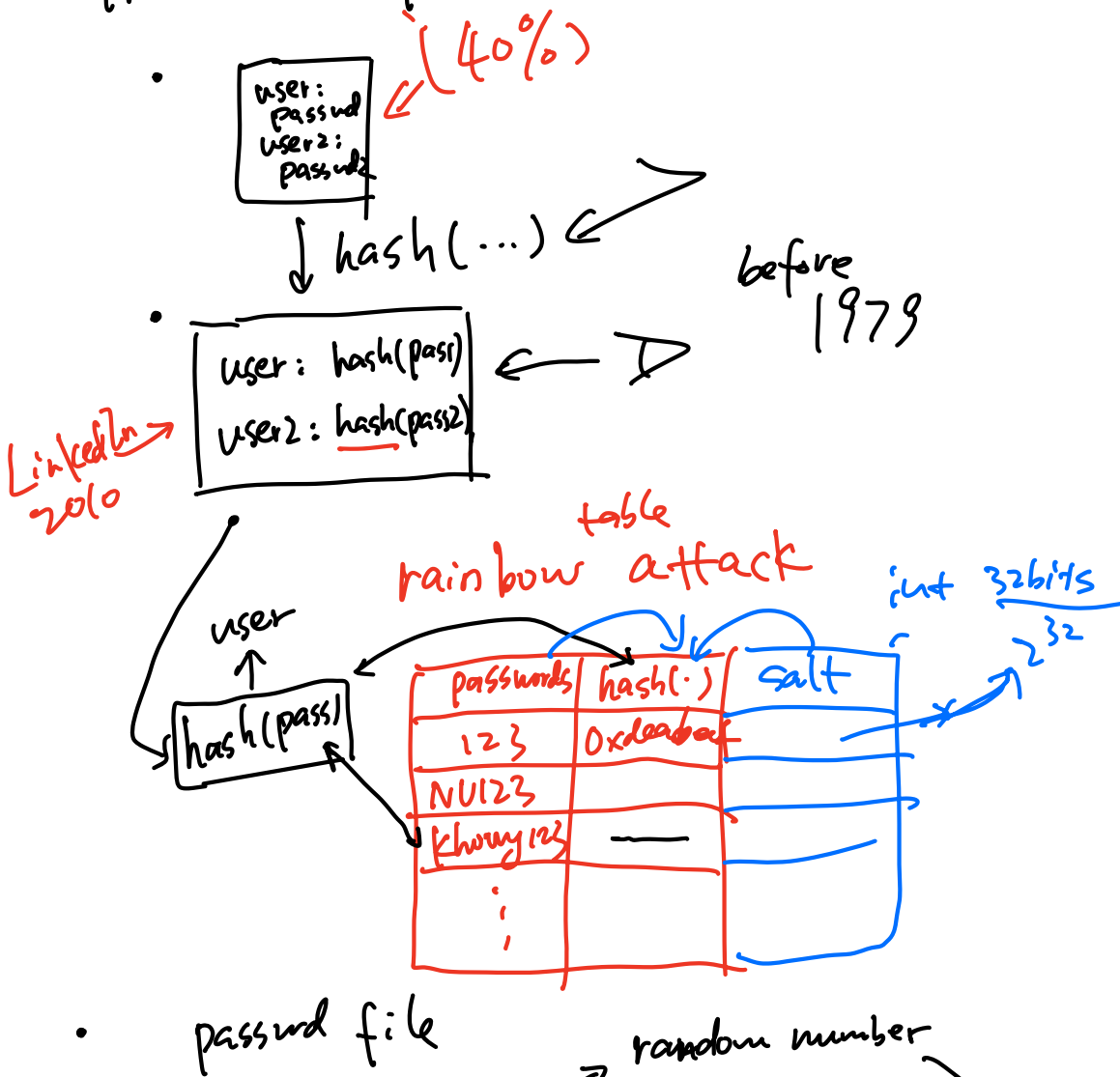


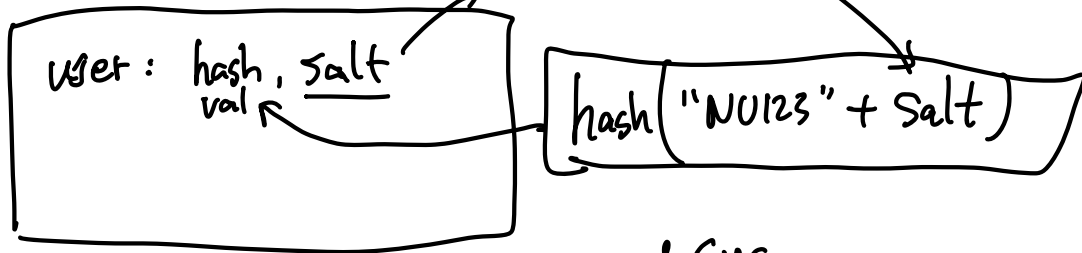
- fingerprint
- password + planted device in head

- algo (time) → pass code
- 3rd party app
- zero-knowledge



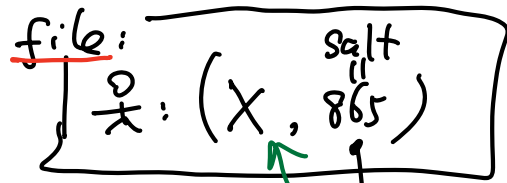
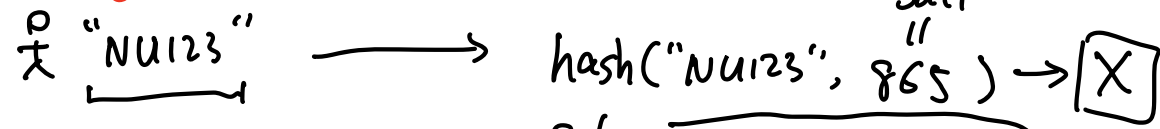
• Approach 1: password





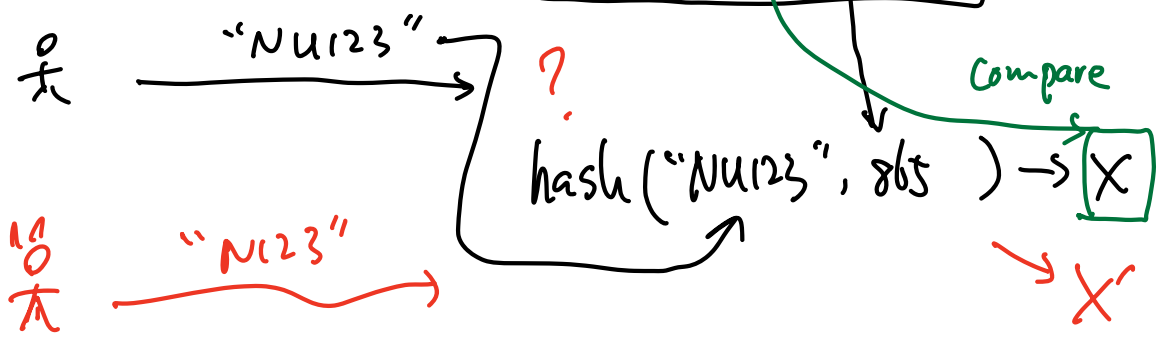
Register: (1979)

password sys



Q:

login



- Approach 2: based on what you have
- Approach 3: base on what you are

Q: option 1: 50%, lose \$500  
 option 2: 0.1%, lose all your money

option 1



option 2

