Possible Crypto projects

Dr Tay Kian Boon

Cryptosystem

- Security of cryptosystem depends on
  1. Crypto algorithm (symmetric & public)
  2. Hash functions
  3. Random number generators used in key generation
  4. Implementation
- Practical crypto – such as TLS (how to attack weak TLS implementations)
- So you can work on any of the above
- However not all areas are easy or interesting to do

Crypto Algorithms -Symmetric

- For symmetric crypto algorithms such as AES, no easy or interesting areas to work on.
- You can in principle develop an encryption software with AES and using good random number generators
- At most a B+ project
- Can be A minus & above if you develop interesting & novel weak AES software but show how to attack them

Crypto Algorithms -Public

- Interesting public key algorithms
  - RSA
  - Knapsack
  - ECC
  - Diffie-Hellman Key Exchange
- For RSA, you can work on weak parameters and show how to attack them (real size RSA mod gets more marks)
- For DLP problem you can work on weak parameters and show how to attack them (real size primes get more marks)
- For ECDLP you can also work on weak parameters and show how to attack them (real size primes get more marks)

Crypto Algorithms –Post Quantum

- RSA and ECC will succumb to sizable quantum computers
- PQ algos resist quantum computer
- There are a few of them in NIST PQ competition website
- For those who want to work on these, you must do at least one of them, implement them, and show attacks against baby parameters
- Possible to get A minus & above

RNGs

- You can also study on RNGs.
- Attack some weak ones-at least period of length 2^128
- Possible to get good grades if you do a few

TLS

- Attack some weak implementations of TLS
- Survey of some TLS attacks & Implement at least one attack

Hash Functions

- Study general attacks against reduced sized secure hash functions, such as birthday attacks, pollard method etc
- Possible to get good grades if there are interesting investigations

Others

- You can propose your own
- Perhaps Ransomware, Weak VPNs etc
- Berkeley crypto projects:

http://people.eecs.berkeley.edu/~daw/cs276/projects.html

- Read Nadia Heninger, papers such as Mind your Ps and Qs etc

Project Expectations

- Form groups of 2.
- Then email me cc buddy (cant change buddy half-way)
- Can work on 2 smaller projects or 1 mega project
- For 2 projects, each must know your buddy project well.
- Grading will depend on technical depth, execution & Q&A
- In general, expected work load: 2-4 full day work
- Deliverable: 8 minute presentation with demo, 2 min Q&A
- I might ask some of you to submit codes

Some Good (free) Crypto Books

- Handbook applied Crypto (F)

https://cacr.uwaterloo.ca/hac/

- Cryptography by Nigel smart (F)

https://homes.esat.kuleuven.be/~nsmart/Crypto_Book/

- Cryptography by Boneh & Shoup (free for now)

https://toc.cryptobook.us/

Trends in data protection & Encryption Technologies

https://link.springer.com/book/10.1007/978-3-031-33386-6

Codebook By Simon Singh (from historical to present)-not free

Other Interesting FREE books

- Infosec Handbook
- https://link.springer.com/book/10.1007/978-1-4302-6383-8
- Managing Risks and information Security
- https://link.springer.com/book/10.1007/978-1-4302-5114-9