Lecture 9

1 What are some problems with current PWs? - hard to remember, hard to secure, breaches suck

2 List some authentication issues - biometrics unreliable, password maintenance is annoying

3 PW AAAs? - Authentication (and identification) for ensuring you are who you say. Authorization - for controlling access to information and resources. Access control - restrict authorization and authentication

5 Why encrypt PWs? - so if breached, harder to recover

6 Why hash PWs? - fast check passwords, hard inversion

7 Describe how dictionary attack works - precompute table of hashes, do simple lookups

8 What is a ranbow table? What is the mathematical relationship between the chain length and the size of the table? - recall hw 4. Now take a breath and calm down.

Lecture 10

1 Symm. Vs Asymm? Why is Symm considered better? - symm is fastrer by 3-4 magnitudes. Asym needs private keys, key authorities, etc. (Sym - see MITM on midterm1 sheet)

4 Describe Tenex PW break, how many attempts are needed? -

2 MITM on DH? What does this teach us? - see midterm 1 cheatsheet

3 NTS Asymm and its anomality? - 1. A sends $A, N_{a\,Kb}$ 2. B sends $N_a, N_{b\,Ka}$, 3. A sends $N_{b\,Kb}$. Anomality - free decryption in step 3

4 What is a nonce for? - ensure freshness, avoid replay attacks

5 Describe NTS symmetric protocol and its anomality?

6 Describe Ottway-Rees and its anomality.
1. $A \rightarrow B : M, A, BN_a, M, A, B_{Ka}$
2. $B \rightarrow S : M, A, BN_a, M, A, B_{Ka}, N_b, M, A, B_{Kb}$
3. $S \rightarrow B : M, N_a, Kab_{Ka}, N_b, Kab_{Kb}$
4. $B \rightarrow A : M, N_a, Kab_{Ka}$
Anomality - block message 4, replay 2, capture 3, send diff Kab to A.

Lecture 11

1 3 qualities of chaums anon digicash? - anonymous, secure, transfer only

2 What are some issues with virtual currencies? - double spending, legitimacy, inflation, creation. What approach does Bitcoin take? - hashing, mining, proof rather than trust central auth

3 What does Bitcoin transfer look like? - Sign(prev transaction + new owner's pub key)

4 Bitcoin consists of chains of transactions

5 How does Proof of Work work? - hash to get some number of leading zeros in hash.

6 Show the overall Bitcoin process - get block, generate hash that satisfies nonce, sign transaction

7 How do you break ties? - longest chain wins

8 Show that reverting ins HARD - in order to fake a block, need to back calculate multiple nonces faster than new ones created.

9 How is new block creating controlled? - global pool of nodes, mining reward halved every 2 years or so.

10 How does miner gain incentive? - reward for hashing the blocks of transactions

Lecture 12

1 Web is said to be an example of "bolt-on security". What does this mean? - original web for researchers, not commerce and e-war.

2 What makes web security particularly hard? - very complicated systems, decades of bugs

3 Describe the URL components - `protocol://domain.tld/path/to/resource?argumen1=foo`

4 Give some examples of command injection attacks. `do.php?cmd=wipe_system.bash`

5 What are some issues with input sanitization? - hard to catch everything, we can always escape the escape.

6 Whats a possibly better way to defend against command injection? - white listing, separate parsing trees.

7 Briefly describe modern web server structure - distributed system, frontend, database, app, etc.

8 Show some SQL commands - SELECT * FROM table1 WHERE user = vania

9 Give an example of SQL Injection scenario - semizolon to terminate command, then malicious command after. Can also add quote and then a command, to escape the string.

10 How do you defend against SQL injection? - input sanitization, white listing, execvp rather than arbitrary system calls, set parsing trees.

Lecture 15

1 What are the 3 (maybe +1) communication security goals? - Confidentiality, Integrity, Availability

2 There are many possible attacks on network in all layers. C - can sniff, I - can inject, A - jamming/flooding

3 Describe eavesdropping on Link-layer - wireshark, wiretap, overhwelm wifi

4 Describe disruption on Link-Layer - flooding

5 Describe spoofing on Link-layer - make bogus message, send out

6 Difference between on-path and off-path? - on path, see victim traffic. Easy spoof. Off-path - blind, must inferm packet values, can brute force seq numbers.

7 Describe IP-layer threats. (What technique do you use to launch attack on integrity, availability and confidentiality?) - arbitrary src/dst, can flood, can manipulate routing

8 Describe DHCP. What layer is this protocol in? (What does DHCP offer message look like?) - discover server, get IP

9 Describe how you launch attack via DHCP - race condition, send IP first. rogue AP. Also set fake DNS/gateway

10 Describe TCP Data Injection - get prev seq numbers, increment and send the packet - port and src/dst known

11 Describe TCP Disruption attack - fake data - chinese firewall, disconnect signals (RST)

12 How does blind-spoofing work with TCP? - guess seq numbers and port/dst

13 Network level Dos attacks? Solution? - cloudflare, killing agressive clients, stateless servers, amplification, botnets, extorton, etc.

14 Tx. Level Dos attacks? Solution? - SYN flooding. solution - encode state in SYN cookie, only when returned do you save state

15 Application level Dos attack? Solution? - expensive calls (sql lookups, searches, etc).

Lecture 13

1 Show the basic structure of web traffic and details of what GET and POST request look like - Use 168 info. Basically packets and stuff.

2 What is XSS? - Cross site scripting - evil.com causes user to perform actions on examplebank.com

3 Stored XSS? - save malicious JS comment in database, calls POST on bank transfer

4 Reflected XSS? - click on link that send user to `examplebank.com/<script>evil()<script>`, SOP thinks it's legit.

5 What is SOP? - same origin policy, only scripts from site can access cookies and elements on page

6 What are some ways to prevent XSS? - SOP, smarter browsers, parse URL before clicking, compare to result, escaping untrusted html

7 What is, and how does CSRF work? How do you prevent it? - not stealing cookies, rather forging one single request. - img src=`bank.com?steal_money`, ie, evil GET request. Use tokens on actual page to fix.

8 What is, and how does drive-by downloads work? How do you prevent it? -

9 What is, and how does click-jacking work? - messing with mouse pointer to lie to people about what they are clicking on.

- Various defenses: Sanitize all inputs, white list allowed commands, have tokens on page to stop CSRF, have SQL parse trees be separate from query, sandbox in browser, blacklist bad sites.

Lecture 17

1 Why do some use circumvention programs like TOR? - avoid censorship, seek anonymity

2 What are some basic censorship techniques? - blacklist IP, use ISP to block DNS, RST packets

3 Why is privacy on public internet difficult to achieve? - all packets open to inspection, timing attacks, also NSA sucks

4 Describe basic Chaums mix with diagrams - untraceable email. senders and receivers known, but not mapping

5 Mix cascade? Why is this good? - hard to see who talking to who

6 How does randomized routing work? - just pick random node, let last one actually send to client

7 How does onion routing work? Explain with diagrams - see pic.

8 What are some disadvantages of using mixnet? Propose some possible solutions - mixnet may be under control of NSA, multiple ones allow better solutions

9 How does TOR circuit setup work? - each router only knows next destination.

10 TOR connection consists of AAA, BBB, and CCC node - 3 internal nodes. entry, mid, exit.

11 Describe with diagrams how creating hidden servers work - make intro points, eventually add to directory

12 Describe with diagrams how using+a hidden server work - ask service lookup provider, then reach server

13 Why doesnt China use TOR? - packets easily identified and killed. tor nodes murdered

14 Sybil attack on P2P? - create large number of relays, add to network, do timing correlations and other analysis

Lecture 16

1 Explain DNS in high-level - map name to IP

2 Describe DNS Look-up with diagram - iterative - walk down chain, keep asking for url resolver

3 What is in the Answer section? What is id? RR? TTL? - Answer has hostname, IP, type of record, and TTL, transaction ID matches reply with original request

4 What is in the Authority section? - tells us which NS responsible for answer

5 What is in the Additional section? - extra info for cache

6 What Tx. Protocol does DNS use?

7 Describe DNS cache poisoning with example attack - include google.com redirect to own IP in addtl section

8 Describe DNS blind-spoofing with example attack assuming the client doesnt use random id - send random "responses", client will think it asked for them.

9 What if the client uses random id? - need to guess

x Kaminsky DNS poisoning: race to poison DNS, by forcing DNS lookup for known fake URL

10 Describe the defense method against DNS blind spoofing - also add ports and ID field to match requirements

11 What is a firewall? - program that filters traffic

14 What are some advantages and disadvantages of using firewall? - risk model hard, takes up resources, need to keep it updated.

Lecture 14 - TCP review

- OSI model: Application, Presentation, Session, Transport, Network, Data link, Physical
- Link Layer: includes device driver and network interface card
- Network Layer: handles the movement of packets, i.e. routing
- Transport Layer: provides a reliable flow of data between two hosts
- Application Layer : handles the details of the particular application
- TCP Handshake
  C→S: SYN, SeqNum = x
  S→C: SYN/ACK, seqNum = y, ACK = x + 1
  C→S: ACK, ack = y + 1
- SYN flooding - anonymized source, open hella connections

1. Relax, GPA does not matter anymore.
2. Think of the cash you'll make after graduation.
3. Do the best you can, and have no regrets!

Author: Ivan Smirnov (http://ivansmirnov.name), collaborated with Tsion Behailu (http://tsion.me)