CIS551: Computer and Network Security

Jonathan M. Smith

jms@cis.upenn.edu

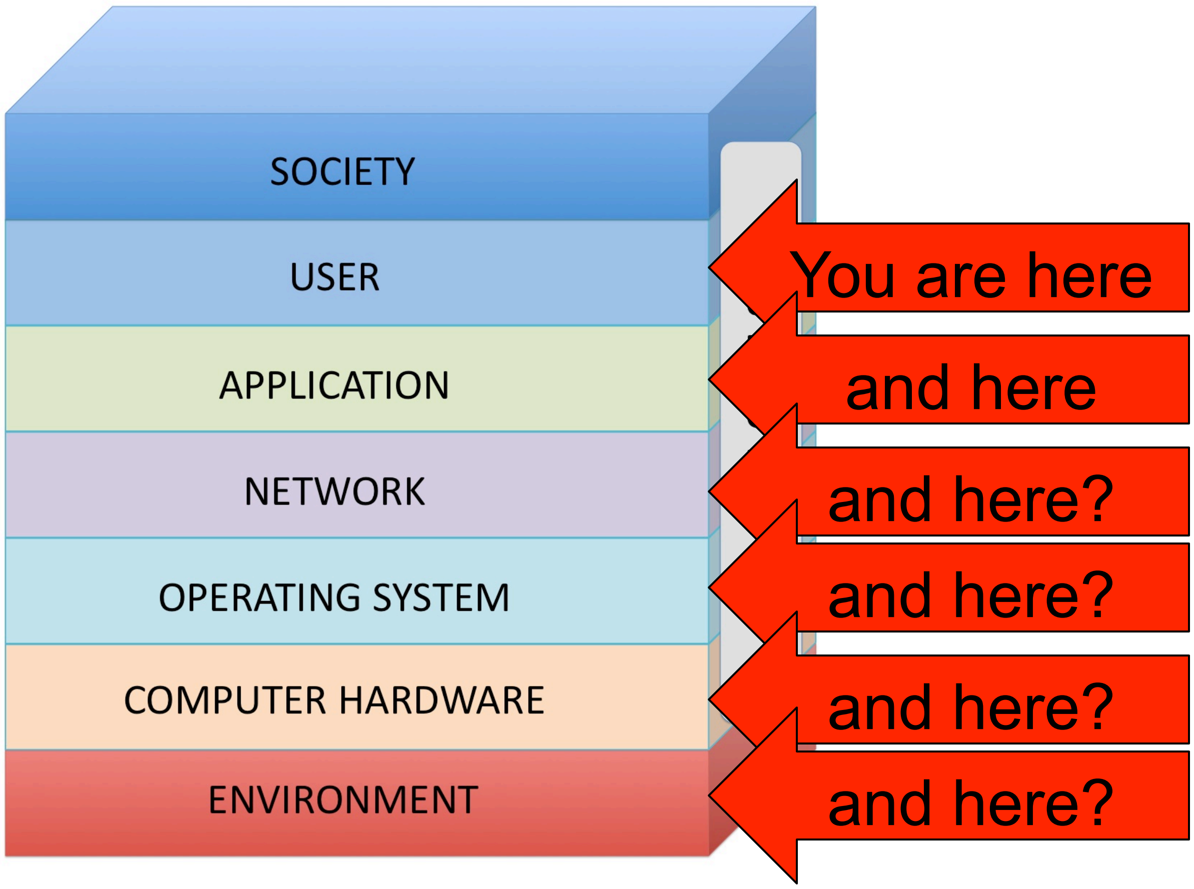
03/24/2014

Uses material from S. Zdancewic/C. Gunter

CIS551 Topics

- Computer Security
  - Software/Languages, Computer Arch.
  - Access Control, Operating Systems
  - Threats: Vulnerabilities, Viruses
- Computer Networks
  - Physical layers, Internet, WWW, Applications
  - Cryptography in several forms
  - Threats: Confidentiality, Integrity, Availability
- Systems Viewpoint
  - Users, social engineering, insider threats

Sincoskie NIS model



W.D. Sincoskie, *et al.* “Layer Dissonance and Closure in Networked Information Security” (white paper)

Uses material from S. Zdancewic/C. Gunter

Secure Channel

Alice

Bart

$K_B\{Hello!\}$ →

← $K_A\{Hi!\}$

K_A, K_B
k_A

K_A, K_B
k_B

Uses material from S. Zdancewic/C. Gunter

RSA at a High Level

- Public and private key are derived from secret prime numbers
  - Keys are typically ≥ 1024 bits
- Plaintext message (a sequence of bits)
  - Treated as a (large!) binary number
- Encryption is modular exponentiation
- To break the encryption, conjectured that one must be able to factor large numbers
  - Not known to be in P (polynomial time algorithms)
  - Is known to be in BQP (bounded-error, quantum polynomial time – Shor's algorithm)

Number Theory: Modular Arithmetic

- Examples:
  - 10 mod 12 = 10
  - 13 mod 12 = 1
  - (10 + 13) mod 12 = 23 mod 12 = 11 mod 12
  - 23 ≡ 11 (mod 12)
  - "23 is congruent to 11 (mod 12)"

- a ≡ b (mod n) iff a = b + kn (for some integer k)
- The *residue* of a number modulo n is a number in the range 0… n-1

Number Theory: Prime Numbers

- A *prime number* is an integer > 1 whose only factors are 1 and itself.

- Two integers are *relatively prime* if their only common factor is 1
  - gcd = greatest common divisor
  - gcd(a,b) = 1 if a,b relatively prime
  - gcd(15,12) = 3, so they're not relatively prime
  - gcd(15,8) = 1, so they are relatively prime

- Easy to compute GCD using Euclid's Algorithm

Finite Fields (Galois Fields)

- For a prime p, the set of integers mod p forms a *finite field*
- Addition + Additive unit 0
- Multiplication * Multiplicative unit 1
- Inverses: $n * n^{-1} = 1$ for $n \neq 0$
  - Suppose p = 5, then the finite field is {0,1,2,3,4}
  - $2^{-1} = 3$ because $2 * 3 \equiv 1 \bmod 5$
  - $4^{-1} = 4$ because $4 * 4 \equiv 1 \bmod 5$

- Usual laws of arithmetic hold for modular arithmetic:
  - Commutativity, associativity, distributivity of * over +

Euler’s *totient* function: $\phi(n)$

- $\phi(n)$ is the number of positive integers less than n that are relatively prime to n
  - $\phi(12) = 4$
  - Relative primes of 12 (less than 12): {1, 5, 7, 11}

- For p a prime, $\phi(p) = p-1$. Why?
- For p,q two distinct primes, $\phi(p*q) = (p-1)*(q-1)$
  - There are p*q-1 numbers less than p*q
  - Factors of p*q =
    - {1*p, 2*p, …, q*p} for a total of q of them
    - {1*q, 2*q, …, p*q} for another p of them
    - No other numbers
    - $\phi(p*q) = (p*q) - (p + q - 1) = pq - p - q + 1 = (p-1)*(q-1)$

q many multiples of p

All #s ≤ p*q

don’t double count p*q

p many multiples of q

Uses material from S. Zdancewic/C. Gunter

Fermat's Little Theorem

- Generalized by Euler.
- Theorem: If p is a prime then $a^p \equiv a \bmod p$.
- Corollary: If gcd(a,n) = 1 then $a^{\phi(n)} \equiv 1 \bmod n$.
- Easy to compute $a^{-1} \bmod n$
  - $a^{-1} \bmod n = a^{\phi(n)-1} \bmod n$
  - Why? $a * a^{\phi(n)-1} \bmod n$
    $= a^{\phi(n)-1+1} \bmod n$
    $= a^{\phi(n)} \bmod n$
    $\equiv 1 \bmod n$

Uses material from S. Zdancewic/C. Gunter

Example of Fermat's Little Theorem

- What is the inverse of 5, modulo 7?
- 7 is prime, so $\phi(7) = 6$
- $5^{-1} \bmod 7 = 5^{6-1} \bmod 7$

$= 5^5 \bmod 7$

$= (5^2 * 5^2 * 5) \bmod 7$

$= ((5^2 \bmod 7) * (5^2 \bmod 7) * (5 \bmod 7)) \bmod 7$

$= ((4 \bmod 7) * (4 \bmod 7) * (5 \bmod 7)) \bmod 7$

$= ((16 \bmod 7) * (5 \bmod 7)) \bmod 7$

$= ((2 \bmod 7) * (5 \bmod 7)) \bmod 7$

$= (10 \bmod 7) \bmod 7$

$= 3 \bmod 7$

$= 3$

Rabin-Miller Primality Test

- Is n prime?
- Write n as $n = (2^r)*s + 1$
- Pick random number a, with $1 \le a \le n - 1$
- If
  - $a^s \equiv 1 \bmod n$ and
  - for all j in {0 … r-1}, $a^{2^j s} \equiv -1 \bmod n$
- Then return composite
- Else return probably prime

How to Generate Prime Numbers

- Many strategies, but *Rabin-Miller* primality test is often used in practice.
  - $a^{p-1} \equiv 1 \bmod p$
- Efficiently checkable test that, with probability ¾, verifies that a number p is prime.
  - Iterate the Rabin-Miller primality test t times.
  - Probability that a composite number will slip through the test is $(1/4)^t$
  - These are worst-case assumptions.
- In practice (takes several seconds to find a 512 bit prime):
  1. Generate a random n-bit number, p
  2. Set the high and low bits to 1 (to ensure it is the right number of bits and odd)
  3. Check that p isn't divisible by any "small" primes 3,5,7,…,<2000
  4. Perform the Rabin-Miller test at least 5 times.

RSA Key Generation

- Choose large, distinct primes p and q.
  - Should be roughly equal length (in bits)
- Let $n = p*q$
- Choose a random encryption exponent e
  - with requirement: e and (p-1)*(q-1) are relatively prime.
- Derive the decryption exponent d
  - $d = e^{-1} \bmod ((p-1)*(q-1))$
  - d is e's inverse mod ((p-1)*(q-1))
- Public key: $K = (e,n)$ pair of e and n
- Private key: $k = (d,n)$
- Discard primes p and q (they're not needed anymore)

Uses material from S. Zdancewic/C. Gunter

RSA Encryption and Decryption

- Message: m
- Assume m < n
  - If not, break up message into smaller chunks
  - Good choice: largest power of 2 smaller than n

- Encryption: $E((e,n), m) = m^e \bmod n$
- Decryption: $D((d,n), c) = c^d \bmod n$

Example RSA

- Choose p = 47, q = 71
- n = p * q = 3337
- (p-1)*(q-1) = 3220
- Choose e relatively prime with 3220: e = 79
  - Public key is (79, 3337)
- Find d = 79^{-1} mod 3220 = 1019
  - Private key is (1019, 3337)
- To encrypt m = 688232687966683
  - Break into chunks < 3337
  - 688 232 687 966 683
- Encrypt: E((79, 3337), 688) = 688^{79} mod 3337 = 1570
- Decrypt: D((1019, 3337), 1570) = 1570^{1019} mod 3337 = 688

Uses material from S. Zdancewic/C. Gunter

Chinese Remainder Theorem

- (Or, enough of it for our purposes…)

- Suppose:
  - p and q are relatively prime
  - $a \equiv b \pmod{p}$
  - $a \equiv b \pmod{q}$
- Then: $a \equiv b \pmod{p*q}$

- Proof:
  - p divides (a-b) (because a mod p = b mod p)
  - q divides (a-b)
  - Since p, q are relatively prime, p*q divides (a-b)
  - But that is the same as: $a \equiv b \pmod{p*q}$

Proof that D inverts E

$c^d \bmod n$

$= (m^e)^d \bmod n$ (definition of c)

$= m^{ed} \bmod n$ (arithmetic)

$= m^{k*(p-1)*(q-1) + 1} \bmod n$ (d inverts e mod $\phi(n)$)

$= m*m^{k*(p-1)*(q-1)} \bmod n$ (arithmetic)

$= m \bmod n$ (C. R. theorem)

$= m$ ($m < n$)

$e*d \equiv 1 \bmod (p-1)*(q-1)$

Finished Proof

- Note: $m^{p-1} \equiv 1 \bmod p$ (if p doesn't divide m)
  - Why? Fermat's little theorem.
- Same argument yields: $m^{q-1} \equiv 1 \bmod q$
- Implies: $m^{k*\phi(n)+1} \equiv m \bmod p$
- And $m^{k*\phi(n)+1} \equiv m \bmod q$
- Chinese Remainder Theorem implies:
  $m^{k*\phi(n)+1} \equiv m \bmod n$
- Note: if p (or q) divides m, then $m^x \equiv 0 \bmod n$
  - Since $m < n$ we must have $m = 0$.