

Security Basics	
Symmetric Key	One key is shared by two users both encryption & decryption (substitution cipher, aes, des)
Assymmetric Key	Public and Private Key
Substitution Cipher	Mono-alphabetic cipher $2^{n/2}$
Diffie-Helman Exchange	Exchanging secret keys over insecure medium. Known large prime and base shared and a secret integer
DES	56-bit symmetric key, 64bit plain text US standard
AES	Replaces DES 128 bit
Axor0, AxorA	A, 0
Main Sec. Probs In Mobile?	Config. management, excessive privileges, privacy violations, poor session management

Security Basics (cont)	
Most problematic part in mobil apps?	Android abstraction layer
Preventing replay attacks?	Use a nonce
Pros of Symmetric Keys	No worry of replay or man in the middle attacks
Agreement on shared key	diffie helman or KDC
Certificate Auth	Binds pub key to part. entity. E registers with CA. When Alice wants bobs pub key, get the certificate, apply CA pub key and get bobs pub key.
Symmetric and Public Key Problems	Sym: establish shared key? (deffie-helman, KDC), Public Key(Man in middle) use CA

power/energy	
factors that affect power	power affects temp, but energy doesn't
equations	power/area proportional to temp
associations	higher current implies high power which increases cpu frequency
thermal runaway	power -> temp -> resistance decrease -> current increase I (cycle)
energy	affects battery life, power * time = E
energy harvesting	solar, wind -> high capacity, low leakage (low discharge), low capacity, high leakage (quick discharge), appliance

Certificate Authority

Certification authorities

- Certification authority (CA): binds public key to particular entity, E.
- E registers its public key with CA.
- E provides "proof of identity" to CA.
- CA creates certificate binding E to its public key.
- certificate containing E's public key digitally signed by CA - CA says "this is E's public key"

Recent Trends in Security	
ID vs Auth	Auth = username + pass, ID = passwd & something like biometric
Data injection	sending false radio signal to pace maker and inducing heart attack
Threat Model/Attack model	What the system thinks about the model. Believes attacker is much more powerful than he actually is. Attack model attacker believes it knows a lot about the system
Key establish ment in physi. sec.	Done using human body
Ways to fool machine	brute force feature guess, generate signal (generative), evasion, poison



Recent Trends in Security (cont)

Evasion attack create points to gain access without getting caught, alter features

Poison attack attacker can see the training set, injects their own data at key points, skews the lines

Biometric signals Signals that don't change like fingerprints

Physiological signals hard because constantly changing

Hardening Technique instead of line, have piecewise curves, or instead of line use polygon (polytope)

Internet Control Protocol Messages agent advertisement, agent solicitation, registration request, registration reply

Recent Trends in Security (cont)

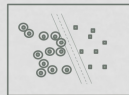
Foreign Agent Consumes less ip addresses than mobile host

security perform ance tradeoff Increase in security strength -> hardening Hardening implies more difficult classification boundaries May increase False positives or negatives How to find a balance between security strength and performance? Multi-objective optimization problem

Hardening Technique

HARDENING TECHNIQUE

- Measures to improve security of ML algorithms
- Fitness check



- Increase complexity of classifiers
- Convex polytope SVM



Internet of Things

Challenges of CPS hard to know how many sensors to use, what data to collect

Cyber Physical Systems embedding sensors into physical devices

Human to Human interaction person a thinks about a color red and that dot is displayed to another person in another country

3 characteristics of IOT devices anytime, anything, any place connection

USN application layer where apps are built to perform tasks using the sensors through middleware

middleware (Drivers) allows you to build apps on top of iot sensors

sensor networking layer (bottom) sensors are launched in environment and report to usn

Internet of Things (cont)

Difference between gps and tower based location management? gps needs clear line of sight and is more accurate. Tower based management is bad if you're not near tower, accessibility is less than gps.

what is iot Network of Physical Objects embedded systems with electronics, software, sensors enable objects to exchange data with manufacturer, operator, other devices through network infrastructure allow remote control direct integration computer + physical world Result: automation in all fields

Challenges in Security

Challenges resource constraints in medical sensors, poor software dev apps support, real-time requirements for health apps

RSA Example

```

RSA example
Bob chooses p=5, q=7. Then n=35, z=24
e=3 (n.e. relatively prime)
d=23 (n.d. relatively prime)
encrypt: letter m m^e mod n
decrypt: c c^d mod n letter
    
```

CUDA (cont)

__global__ As before, __global__ is a CUDA C keyword meaning — add() will execute on the device — add() will be called from the host

Network Sec

What is network security?

- Confidentiality:** only sender, intended receiver should "understand" message contents
 - sender encrypts message
 - receiver decrypts message
- Authentication:** sender, receiver want to confirm identity of each other
- Message integrity:** sender, receiver want to ensure message not altered (in transit, or afterwards) without detection
- Access and availability:** services must be accessible and available to users

RSA Continued

RSA: Why is that $m = (m^e \bmod n)^d \bmod n$

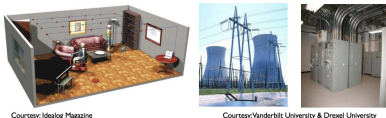
Useful number theory result: If p, q prime and $n = pq$, then: $x^y \bmod n = x^{y \bmod (p-1)(q-1)} \bmod n$

$$\begin{aligned}
 (m^e \bmod n)^d \bmod n &= m^{ed} \bmod n \\
 &= m^{ed \bmod (p-1)(q-1)} \bmod n \\
 &\quad \text{(using number theory result above)} \\
 &= m^1 \bmod n \\
 &\quad \text{(since we chose } ed \text{ to be divisible by } (p-1)(q-1) \text{ with remainder 1)} \\
 &= m
 \end{aligned}$$

memory management Host and device memory are distinct entities — Device pointers point to GPU memory May be passed to and from host code May not be dereferenced from host code — Host pointers point to CPU memory May be passed to and from device code May not be dereferenced from device code

challenges cps

CPS – Properties, Issues, Challenges



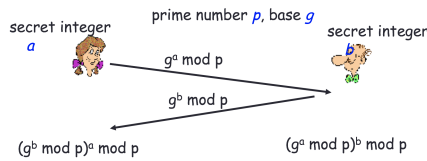
- Dynamic distributed large-scale systems to control physical process
- Cyber and physical components are integrated
- Operations in computing entities affect the physical world & vice versa.
- Potentially, human-in-the-loop
- Heterogeneous entities with order of magnitude difference in capabilities, e.g. sensors, medical devices, servers, handheld computing devices, and Humans

Key Issues

- Physical Interactions
- Critical Applications
- Automated Design & Validation

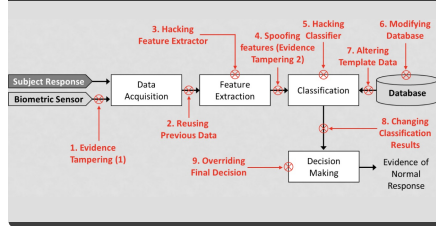
Diffie-Helman

Diffie-Hellman Key Exchange



Key: $(g^b \bmod p)^a \bmod p = (g^a \bmod p)^b \bmod p$

Threat Model



thread indexing

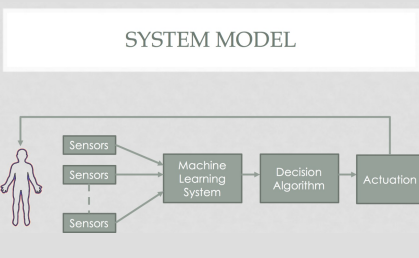
Indexing Arrays With Threads And Blocks

- No longer as simple as just using `threadIdx.x` or `blockIdx.x` as indices
 - To index array with 1 thread per entry (using 8 threads/block)
- ```

threadIdx.x threadIdx.x threadIdx.x threadIdx.x
0 1 2 3 4 5 6 7 0 1 2 3 4 5 6 7 0 1 2 3 4 5 6 7 0 1 2 3 4 5 6 7
blockIdx.x = 0 blockIdx.x = 1 blockIdx.x = 2 blockIdx.x = 3

```
- If we have  $M$  threads/block, a unique array index for each entry given by
- $$int \ index = \ threadIdx.x + \ blockIdx.x * \ M;$$
- $$int \ index = \ x + \ y * \ width;$$

### System Model



### CUDA

CUDA Terminology Host – The CPU and its memory (host memory) Device – The GPU and its memory (device memory)