Mobile Cheat Sheet

by rschacht via cheatography.com/23536/cs/11637/

Security Basics

Symmetric Key	One key is shared by two users both encryption & decryption (substiution cipher, aes, des)
Assymetric	Public and Private Key
Substitution Ciper	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 privleges, privacy violations, poor session management

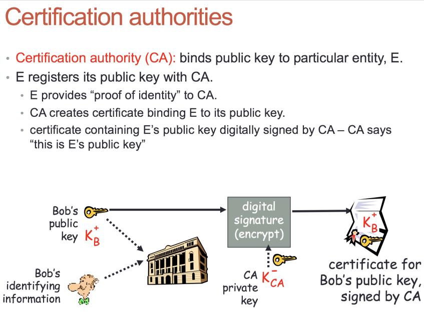
Security Basics (cont)

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	asffects battery life, power * time = E
energy harvesting	solar, wind -> high capacity, low leakage (low discharge), low capacity, high leakage (quick discharge), appliance

Certificate Authority



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 establishment in physi. sec.	Done using human body
Ways to fool machine	brute force feature guess, generate signal (generative), evasion, poison

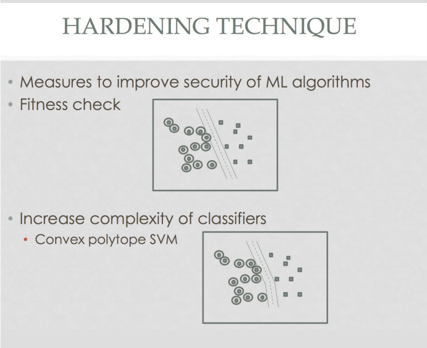
Recent Trends in Security (cont)

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 performance 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



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 charactertistics of IOT devices	anytime, anything, any place connetion
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

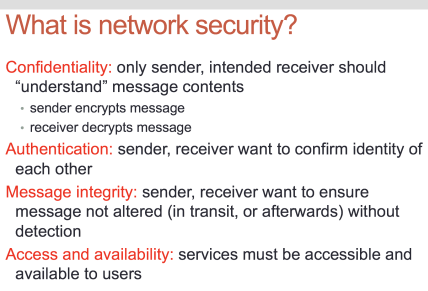
Internet of Things (cont)

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

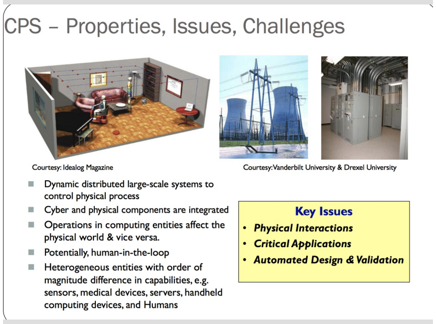
Challenges in Security

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

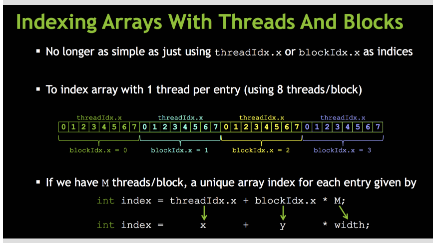
Network Sec



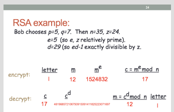
challenges cps



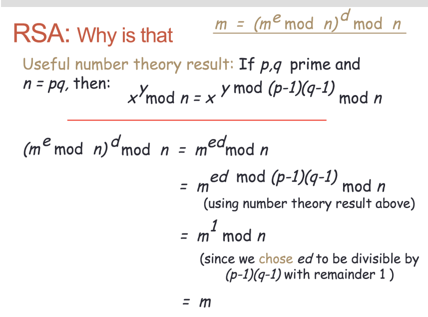
thread indexing



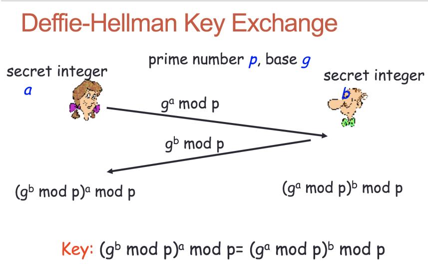
RSA Example



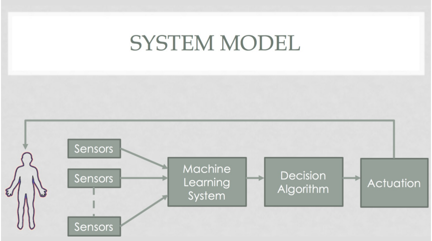
RSA Continued



Diffie-Helman



System Model



CUDA

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

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
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

Threat Model