

# Conclusion

# Course Summary

- ❑ Crypto
  - Basics, symmetric key, public key, hash functions and other topics, cryptanalysis
- ❑ Access Control
  - Authentication, authorization
- ❑ Protocols
  - Simple authentication
  - Real-World: SSL, IPSec, Kerberos, GSM
- ❑ Software
  - Flaws, malware, SRE, development, OS issues

# Crypto Basics

- ❑ Terminology
- ❑ Classic cipher
  - Simple substitution
  - Double transposition
  - Codebook
  - One-time pad
- ❑ Basic cryptanalysis

# Symmetric Key

- ❑ Stream ciphers
  - A5/1
  - RC4
- ❑ Block ciphers
  - DES
  - AES, TEA, etc.
  - Modes of operation
- ❑ Data integrity (MAC)

# Public Key

- ❑ Knapsack (insecure)
- ❑ RSA
- ❑ Diffie-Hellman
- ❑ Elliptic curve crypto (ECC)
- ❑ Digital signatures and non-repudiation
- ❑ PKI

# Hashing and Other

- ❑ Birthday problem
- ❑ Tiger Hash
- ❑ HMAC
- ❑ Clever uses: online bids, spam reduction
- ❑ Other topics
  - Secret sharing
  - Random numbers
  - Information hiding (stego, watermarking)

# Advanced Cryptanalysis

- ❑ Linear and differential cryptanalysis
- ❑ RSA side channel attack
- ❑ Knapsack attack (lattice reduction)
- ❑ Hellman's TMT0 attack on DES

# Authentication

- ❑ Passwords
  - Verification and storage (salt, etc.)
  - Cracking (math)
- ❑ Biometrics
  - Fingerprint, hand geometry, iris scan, etc.
  - Error rates
- ❑ Two-factor, single sign on, Web cookies

# Authorization

- ❑ ACLs and capabilities
- ❑ MLS — BLP, Biba, compartments, covert channel, inference control
- ❑ CAPTCHA
- ❑ Firewalls
- ❑ IDS

# Simple Protocols

- ❑ Authentication
  - Using symmetric key
  - Using public key
  - Establish session key
  - PFS
  - Timestamps
- ❑ Authentication and TCP
- ❑ Zero knowledge proof (Fiat-Shamir)

# Real-World Protocols

- ❑ SSL
- ❑ IPSec
  - IKE
  - ESP/AH
- ❑ Kerberos
- ❑ GSM
  - Security flaws

# Software Flaws and Malware

## ❑ Flaws

- Buffer overflow
- Incomplete mediation, race condition, etc.

## ❑ Malware

- Brain, Morris Worm, Code Red, Slammer
- Malware detection
- Future of malware

## ❑ Other software-based attacks

- Salami, linearization, etc.

# Insecurity in Software

- ❑ Software reverse engineering (SRE)
  - Software protection
- ❑ Digital rights management (DRM)
- ❑ Software development
  - Open vs closed source
  - Finding flaws (math)

# Operating Systems

- ❑ OS security functions
  - Separation
  - Memory protection, access control
- ❑ Trusted OS
  - MAC, DAC, trusted path, TCB, etc.
- ❑ NGSCB
  - Technical issues
  - Criticisms

# Crystal Ball

## □ Cryptography

- Well-established field
- Don't expect major changes
- But some systems will be broken
- ECC is a "growth" area
- Quantum crypto may prove worthwhile
- Beware of hype!

# Crystal Ball

## ❑ Authentication

- Passwords will continue to be a problem
- Biometrics should become more widely used
- Smartcard/tokens will be used more

## ❑ Authorization

- ACLs, etc., well-established areas
- CAPTCHA's interesting new topic
- IDS is a very hot topic

# Crystal Ball

- ❑ **Protocols** are challenging
- ❑ Very difficult to get protocols right
- ❑ Protocol development often haphazard
  - Kerckhoffs Principle for protocols?
  - How much would it help?
- ❑ Protocols will continue to be a significant source of security failure

# Crystal Ball

- ❑ **Software** is a huge security problem today
  - Buffer overflows should decrease
  - Race condition attacks might increase
- ❑ Virus writers are getting smarter
  - Polymorphic, metamorphic, what's next?
  - How to detect future malware?
- ❑ Malware will continue to plague us

# Crystal Ball

- Other **software** issues
  - Reverse engineering will not go away
  - Secure development will remain hard
  - Open source not a panacea
- OS issues
  - NGSCB will change things...
  - But for better or for worse?

# The Bottom Line

- ❑ Security knowledge is needed today...
- ❑ ...and it will be needed in the future
- ❑ Necessary to understand technical issues
  - The focus of this class
- ❑ But technical knowledge is not enough
  - Human nature, legal issues, business issues, etc.
  - Experience also important

# A True Story

- ❑ The names have been changed...
- ❑ "Bob" took my undergrad security class
- ❑ Bob then got an intern position
  - At a company that does security
- ❑ At a meeting, an important customer asked
  - "Why do we need signed certificates?"
  - After all, they cost money!
- ❑ The silence was deafening

# A True Story

- ❑ Bob's boss remembered that Bob had taken a security class
  - So he asked Bob, the lowly intern, to answer
  - Bob mentioned "man-in-the-middle" attack
- ❑ Customer wanted to hear more
  - Bob explained MiM attack in some detail
- ❑ The next day, "Bob the lowly intern" became "Bob the fulltime employee"