CNS'05 Lecture 15

Crypto in Society

Review

Assignment 10 forensics

Cyclone

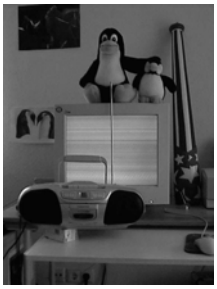
- Safe dialect of C
- Joint project of AT&T and Cornell
- Retains basic syntax (front end to gcc)
- adds features such as pattern matching, algebraic datatypes, exceptions, region-based memory management, and optional garbage collection
- not vulnerable to a wide class of bugs that plague C programs: buffer overflows, format string attacks, double free bugs, dangling pointer accesses, etc
- Bounds checking at runtime, "Fat pointers"
- Slightly slower than native C, faster than Java

miscellany

- Electronic attacks
- Quantum and molecular computers

Electronic sniffing

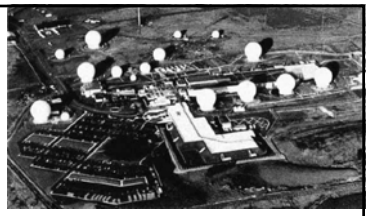
- wire taps or wireless nets
- TEMPEST
  - Van Eck radiation
  - sense key strokes
  - simple electronics to remotely capture your display
  - Signals leaked on power cords …
- countermeasures -- shielding



Tempest for eliza

program to send out AM signal from your monitor to your radio – play mp3's

Project ECHELON



World-wide electronic spying network or myth?

Twenty listening stations around the world - five in the US, three in Australia, two in the UK, then others in New Zealand, Germany, Puerto Rico, Japan, Hong Kong, Cyprus, Guam.

Sniffer vans, aircraft, satellites, insects (a fly on the wall)

Tap trans-ocean cables, satellite traffic, internet traffic, cell phones, ...

Is anyone listening?

Electronic attacks

Differential Fault Analysis (DFA)

- Bellcore and Biham
- Microwave your smart card or stir-fry your PC cause single bit errors in the crypto ouput

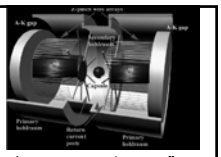
– suppose your smart card calculates $N = P \times Q$
– the card outputs N (P and Q are secret)
– radiate your card as it calculates N, so it now outputs N' with a single bit changed in either P or Q
– Say the error is at bit number k, where you don't know what k is and you don't know whether it's in P or Q. In other words you've done one of the following:

1) replaced P with $P + 2^k$ (changed a zero bit to a one)
2) replaced P with $P - 2^k$ (changed a one bit to a zero)
3, 4) same as above but changed Q instead of P.

– Now you run the calculation and get the product N', which is one of the following cases:
1) $(P + 2^k) Q = PQ + 2^k Q$
2) $(P - 2^k) Q = PQ - 2^k Q$
3) $(Q + 2^k) P = PQ + 2^k P$
4) $(Q - 2^k) P = PQ - 2^k P$

– By subtracting N from N', you now know delta = $2^k Q$, or $-2^k Q$, or $2^k P$, or $-2^k P$
– you don't know which.
– But if P and Q are both 1024 bits long, you need only loop through the 1024 possible values of k, for each of the four cases above, and see which one of them gives you a factor of N.

EMP



electromagnetic pulse

"Please turn off all laptop computers, CD and cassette players."

- fry the electronics
- nuclear explosion (messy)
- EMP bomb/ HERF gun (cheap – magnetron + wave-guide)
  - –thump-mobile zapper
  - –disable PCs, alarms, etc. (a "pinch" in Ocean's Eleven)
  - –subtly alter logic/RAM -- remotely re-program ?

Weirder attacks

breaking DES with molecular computing
- one liter of water with 10^{17} strands DNA
- break DES in 916 steps, 32 extractions/step
- one extraction/hour implies 4 months to break DES

factoring with quantum computers
- wave-particle duality
- multi-state "machine"
- computations transform the wave function and alter all states in one step
- takes polynomial time

Wanted: DNA and quantum programmers

working: quantum encryption (polarized photons)

Crypto's role in society

- US crypto history
- Information society
  - –Need for crypto: military, government, enterprise, personal
  - –Good guys vs bad guys
- US policy
  - –Laws
  - –Standards and validation
  - –Research funding

US crypto history

- Cypto province of NSA til the 1970's
- 1970's academic research, D-H, RSA
  - –Crypto research submitted for NSA review (since 1980, voluntary)
- Commercial crypto
  - –Financial institutions, NBS/DES (1975)
  - – Escrowed encryption (1994)
  - –NIST AES (2000)
- Laws
  - –Trading with the Enemy Act (1917), export control act (1949)
  - –Export Administration Act (1969) dual-use technologies, US munitions list and International Traffic in Arms Regulations (ITAR)
  - –Computer security ACT (1987)
  - – NIST standards/evaluations

The need for secrecy

- Government/political
- Military
- Medical (HIPAA)
- Financial transactions
- Manufacturing
  - –trade secrets
  - –planning/marketing data
- Music/images (copyright)
- personal

US govt agencies roles:

NSA – military/spy/diplomat strong crypto

DIA – military operational security

FBI – US computer crime

DHS – counter-terrorism

NIST – commercial crypto, validation

DoC – export controls

NSF/NSA/NIST – crypto research

Standards:

IEEE

ISO

FIPS

IETF

Privacy

- Do you have a right to privacy?
  - –4th amendment
  - –Wiretap laws
- Do you have a right to use encryption?
  - –Terrorists?
  - –Criminals?
- Enterprise privacy – login banners

Any or all uses of this system and all files on this system may be intercepted, monitored, recorded, copied, audited, inspected,

- University privacy
- Health/financial privacy laws
  - –Gramm-Leach Bliley act (GLBA) – financial data
  - –Sarbaes-Oxley (SOX) – exposing/tainting financial data
  - –Health information portability accountability act (HIPAA)
  - –Children's online privacy protection act (COPPA)

Anonymity

- Right to anonymity?
- Multiple personae
- Anonymous emailers
- Anonymous proxy browsers (anonymizer.com)
- Anonymous purchases (digital cash)
  - Untraceable purchases
- E-vote

Crypto law

- Homeland security act
- US patriot act (domestic terrorism)
  - Free speech, right to assembly
- Federal codes relating to
  - computer fraud & abuse act (CFAA) – computer access
    - computer intrusions
    - fraud
  - intellectual property -- trademarks/copyright
  - porn
  - cyber stalking
  - search and seizure (wiretap/sniffing, ISP records)

Sentencing guidelines

- Potential/actual loss $$
- Level of sophistication of attack
- For commercial or personal benefit
- Malicious intent
- Messin' with national defense, national security, justice
- Messin' with critical infrastructure
- Threat to people, public health

Crypto market

- Demand limited by
  - Unaware of need
  - Uncertainties over gov't policies
  - High cost, reduced performance
  - Insecure environment
  - Ease of use
  - Lack of validation/certification of products
  - Lack of interoperability and standards
  - Lack of PKI
- Supply limited by
  - Crypto skills in product designers
  - Difficult to integrate into products
  - hardware vs software
  - Export controls

Export control

- Prevent terrorists/criminals from using strong crypto
- US ITAR, Dept. of Commerce
  - Crypto software considered a munitions
  - Crippled crypto (40-bit)
  - Apply for license
  - Key escrow (Clipper)
  - Can't ship Linux with DES/ssh etc.
  - Hurt US crypto business
- Wassenaar agreement ('98)
  - 32 countries agree to export 56-bit or less crypto

Three little pigs

The first little pig built his security out of straw – 56 bit crypto

The big bad wolf had no problem – he was a brute

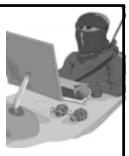
The second little pig built his security out of escrowed sticks

The big bad wolf bought his escrow key from a corrupt official

The third little pig built his security out of strong (non-escrow) bricks, and lived happily ever after .... Or did he?

- his crypto was strong but his key management was weak
- or his computer security was weak and his keys were stolen
- or he was arrested for using illegal crypto
- or he lost his keys, and all the king's horses and all the king's men couldn't restore his data again ⊗

Information Warfare



- Physical destruction of info-handling facilities
- Denial of service
- Insertion of bogus information, destroy or modify data
- Retrieval of tactical/strategic info from opponent's info systems
- Insertion of malware to alter behavior or take over info systems
  - Trojan horse
  - "mole"
- Attack infrastructure info systems … extortion
  - power grid
  - flight control
  - command and control (SCADA)
  - financial systems

Is IW a real threat?

You be done!

Attacks & Defenses
- Risk assessment✓
- Viruses✓
- Unix security✓
- authentication✓
- Network security ✓
  Firewalls,vpn,IPsec,IDS
- Forensics✓
- Secure coding ✓

Cryptography
- Random numbers✓
- Hash functions✓
  MD5, SHA,RIPEMD
- Classical + stego✓
- Number theory✓
- Symmetric key✓
  DES, Rijndael, RC5
- Public key✓
  RSA, DSA, D-H,ECC

Applied crypto
- SSH ✓
- PGP ✓
- S/Mime ✓
- SSL ✓
- Kerberos ✓
- IPsec ✓
- Crypto APIs ✓

REVIEW

- Objective: understand vulnerabilities, practice safe computing
- Goals: integrity, privacy, availability
- PAIN: privacy, authenticity, integrity, non-repudiation
- Topics: risks/countermeasures, digital crypto, applied crypto

	Lectures
1.	Risk, viruses
2.	UNIX vulnerabilities
3.	Authentication & hashing
4.	Random #s classical crypto
5.	Block ciphers DES, RC5
6.	AES, stream ciphers RC4, LFSR
7.	**MIDTERM** ☹
8.	Public key crypto RSA, D-H
9.	ECC, PKCS, ssh/pgp
10.	PKI, SSL
11.	Network vulnerabilities
12.	Network defenses, IDS, firewalls
13.	IPsec, VPN, Kerberos, secure OS
14.	Secure coding, crypto APIs
15.	review

vulnerabilities

scare you

- info warfare
- social engineering, phishing
- PC viruses
- Windows/UNIX bugs (buffer overflows), setuid root
- network attacks … bad packet! Naughty packet!
  - sniffers
  - denial of service
  - spoofing/hijacking
  - server buffer overflows

Threats
- interruption
- interception
- modification
- fabrication

actual incidents

Attackers and motives

- amateur
- insider (greed, disgruntled)
- kids
- hackers
- criminals
- spies
- sociopath (terrorist/vandal)

Motives
- money
- retribution
- Sport/attribution
- pathological
- political/military

Attacks are easy
- Point, click, attack
- Virus kits
- Root kits
- Lots of vulnerable machines (cable/dsl) … hard to track

Security is hard

- We have good design principles
- We have good mathematics/crypto
- We have good policy and procedures

Why isn't this working?

Security is an art and a process
No stronger than the weakest link
Threats and countermeasures continue to change

Why security is hard

- software is complex and has bugs
- updating software is hard
- protecting memory is hard (swap area)
- erasing info on disk is hard
- generating random numbers is hard
- physical security is hard
- privacy vs accountability
- people make mistakes
- adaptive adversary

security is a process, not a product

Computers at Risk

"The developers of secure software cannot adopt the various probabilistic measure of quality that developers of other software can. For many applications, it is quite reasonable to tolerate a flaw that is rarely exposed and to assume that its having occurred once does not increase the likelihood that it will occur again. It is also reasonable to assume that logically independent failures will be statistically independent and not happen in concert. In contrast, a security vulnerability, once discovered, will be rapidly disseminated among a community of attackers and can be expected to be exploited on a regular basis until it is fixed."

countermeasures

prevention, detection, response

- risk assessment
- good programming techniques
- good authentication
- strong access control (OS, firewalls)
- detect and respond (IDS/IPS, logs, patches, backups)
- forensics, laws, and social response
- encryption
- backup/recovery

" The attacker need find only one of possibly many vulnerabilities to succeed. The security specialist must develop countermeasures for all." -- Computers at Risk

Microsoft's 10 immutable Laws of Security

Law #1: If a bad guy can persuade you to run his program on your computer, it's not your computer anymore
Law #2: If a bad guy can alter the operating system on your computer, it's not your computer anymore
Law #3: If a bad guy has unrestricted physical access to your computer, [or data] it's not your computer anymore
Law #4: If you allow a bad guy to upload programs to your website, it's not your website any more
Law #5: Weak [or weakly protected] passwords trump strong security
Law #6: A computer is only as secure as the administrator is trustworthy [and is aware of threats and countermeasures]
Law #7: Encrypted data is only as secure as the decryption key
Law #8: An out of date virus scanner is only marginally better than no virus scanner at all
Law #9: Absolute anonymity isn't practical, in real life or on the Web
Law #10: Technology is not a panacea

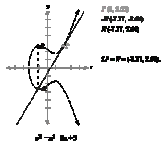
Need for encryption

privacy
- cryptographic separation
- file encryption
- email encryption
- digital signatures
- MAC -- encrypt unkeyed hash

message encryption
- authentication exchange
- info privacy (personal, commerce)
- virtual private networks
- IP security extensions
- defeat IP spoofing/splicing/seq. guessing

Mathematics of cryptography

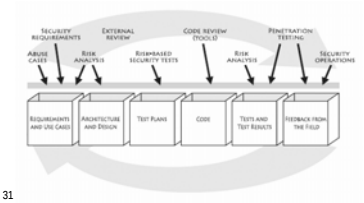
- Mod arithmetic, gcd, CRT (shift cipher, Hill, RSA, D-H, ECC)
- Polynomial arithmetic over GF(2^n) (LFSR, ECC, AES, CRC)
- Testing primes, irreducible polynomials, generators
- Random number generation (keys, IV, blinding, k for DSS)
- BIG integer arithmetic
- Nonlinear Boolean functions (Bent)
- Factoring and discrete logs
- Elliptic curves
- Computational complexity



Security through mathematics

Software engineering for security

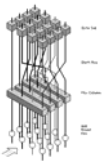
- Secure design with risk analysis
- Secure implementation
- Security testing
- Secure deployment
- Root cause analysis for bugs
- Policy and training



Design principles

- **Principle of least privilege**
  - Give only those privileges needed to complete a task
- **Principle of fail-safe defaults**
  - Access should be denied unless it is specifically permitted
- **Principle of economy of mechanism**
  - Security mechanisms should be as simple as possible
- **Principle of complete mediation**
  - All accesses to objects must be mediated
- **Principle of open design**
  - Security should not depend on secrecy of design or implementation
- **Principle of separation of privilege**
  - Don't grant permission based on a single condition (su: password+wheel grp)
- **Principle of least common mechanism**
  - Mechanisms used to access resources should not be shared
- **Principle of psychological acceptability**
  - Security mechanisms should not make resource access more difficult

Crypto tools



- hash -- MD5, SHA, RIPEM, Panama
- secret key -- DES, RC5, IDEA, Blowfish, Rijndael
- public key -- D-H, RSA, SHA, ElGamal, ECC
- support (libs OpenSSL, classes/methods)
  - big number library
  - random number generation
  - prime testing

- issues -- key management, PKI, escrow, export

Best practices

- Secure by default
- Make your code crypto-agile
- Use two key pairs -- signing key, encrypting key
- Keep IV secret (derive from key material)
- Truncate HMAC's
- Check return values
- Defense in depth

Have you learned to practice safe computing?

- There's not just one thing to being safe
- Understand the threats and vulnerabilities
- Insure authenticity
  - Message authentication
  - User authentication (strong passwords)
  - Entity authentication (PKI)
- Insure privacy (encryption)
- Write code with the adversary in mind
- Configure defensively
  - Anti-virus, anit-spyware, firewall, IDS
- Question your trust assumptions
- Be ever vigilant

Applied security

- PGP
- ssh
- ssl
- S/MIME, cfs
- IPsec/VPN
- Kerberos
- class assignments
  1. Email hello and virus du jour
  2. Risk assessment & password cracking
  3. PGP and code review
  4. Hashing/HMAC to ncp
  5. Classical ciphers
  6. encryption and compression
  7. AES to ncp
  8. Diffie-Hellman to ncp
  9. ncp with ssl
  10. forensics

questions

- Can you hide a password in an executable?
- Can two parties establish a secret?
- Do you have a right to anonymity on the Internet?
- Should (can) a government control encryption?
- Can a computer generate a random number?
- Can you assure the time of a digital signature?
- Can you encrypt with a hash function? hash with an encryption function?
- Should software vendor be liable for bugs?
- Should bugs/vulnerabilities be published?

readings

seminal papers
- Lamport, Diffie-Hellman, RSA

- Textbook
- Social engineering and phishing
- How to Own the Internet (faster worms)
- Why Johnny can't encrypt
- Need for Secure OS
- Smart cards for authentication and authorization
- Reflections on trusting trust
- Steganalysis and secret languages
- Snake oil
- ssh and sel design papers
- Time-stamping digital documents
- Deletion of info on magnetic media
- Software defect reduction

- Stack overflows
- Stalking the wily hacker
- Software generation of random numbers
- DES and its strength against attacks, DES X
- Minimal key lengths for symmetric ciphers
- The need for two key pairs
- Security problems in the TCP/IP suite
- Network insecurity through IP packet filtering
- Why crypto is harder than it looks

Crypto research

- Auto-immune / anti-virus systems
- Better/faster firewalls/IDS/IPS
- Wireless security (cell, 802.11, sensors, bluetooth)
- Public key management, cross-realm authentication
- Identification/authentication
- Authorization (role-based, carry info in cert's)
- Backtracking spoofed packets, DDoS
- Mathematics of encryption/hashing
- Info warfare defense/offense
- Secure apps/OS, software assurance, secure coding
- Forensics

Crypto future

Jobs?
- research/teaching
- consultant
- chief security officer
- law enforcement (forensics)
- tech (firewalls, IDS)
- secure hardware/software design
- military – cyber soldier

- security built in (hardware, OS, apps)
- public key infrastructure
- cyber insurance (accountability)
- IPsec/VPNs
- crypto cards/tokens
- biometrics
- wireless security
- e voting, e cash – technically yes, socially/politically no?
- export restrictions?
- quantum/molecular crypto
- blended threats (spam, phishing, trojans, ID theft)
- infowar, cyber terrorism

Take-home final

- http://www.cs.utk.edu/~dunigan/cns06/final.exam.asc