CRYPTOGRAPHY AND COMPUTER SECURITY : CURRENT TECHNOLOGY AND FUTURE TRENDS

Bruce Schneier

schneier@counterpane.com

http://www.counterpane.com

Counterpane Systems

101 East Minnehaha Parkway, Minneapolis, MN 55419

(612) 823-1098

Fax: (612) 823-1590

HOPE

9 August 1997

New York, NY

INTRODUCTION

Cryptography can do some really cool stuff.

- It can protect privacy.
  - It separates the security of a message from the security of the media.
- It can provide for anonymity.
- It can authorize someone.
- It can facilitate trust.
- It can allow for digital credentials (authentication).
- It can validate the integrity of information.
- It can ensure the fairness of financial transactions.
- It can provide an audit trail for later dispute resolution.
- Cryptography stops lying and cheating.

None of it is new.

- Everybody used to have privacy: electronic communications such as telegraph and telephone have reduced it significantly.
- Physical recognition—face, voice, handwriting—used to provide authentication.
- Cryptography allows us to take existing business and social constructs from the real world and move them to cyberspace.
- Cryptography makes levels of security and privacy that were only available to very few available to everybody.
- Cryptography is a technological equalizer.

All of it is increasingly important.

- More/faster computers and networks; more interconnectivity
  - “To a first approximation, every computer is attached to every other computer.”
- Remote access, autonomous agents, distributed processing
- Stored content of real value
- Communications of real value
- Commerce of real value
- Relationships forming and existing in cyberspace

Unfortunately, most of the security products out there are not secure.

- Almost no real products use cryptography.
- Those that do usually incorporate it in at the last minute
- And companies don't hire cryptographic engineers; they think they can do it themselves.
- The products are also inflexible, hard to use, and buggy.
  - People disable security systems in order to get work done.
- Existing solutions don't scale.
- Products don't usually solve the correct problem.
  - Sometimes they solve a slightly different problem.
  - Sometimes they are based on incorrect trust assumptions.
- Products sometimes cause more security problems than they solve.
- Operating systems are much more complex and buggy; this undermines the security of anything built on top of it.

People buy the stuff because they don't know any better.

- No "FDA" for computer security products
- Poor education among corporate buyers
- Active disinformation campaign by government
  - NSA has to deal with the "equities issue," whether to protect ours or to attack theirs.

This situation will get worse before it improves.

- The important stuff is handled electronically.
  - Manual processing is for the unimportant stuff.
  - More financial processing will move to cyberspace.
  - More medical information will move to cyberspace.
  - Judicial and law enforcement officials will depend more heavily on computer databases.
  - Companies will depend more heavily on networks and databases.
- Newer technology is less secure, not more.
  - Complex systems
  - Poorly-understood effects of new technologies
  - The rush to market

This situation will get worse (cont.)

- The best (cheapest, fastest, easiest) media is the most insecure.
  - Internet, cellular, video on demand, automated stock trading
  - Security adds complexity and decreases performance—somewhat.
- Telecommunications services continue to diversify.
  - More avenues of possible attack.
- More mobile solutions.
- Changes in cyberspace are coming faster and faster.
- Security goes against philosophy of the net.
- Security slows down progress.

THREATS IN THE DIGITAL WORLD

The unchanging nature of attacks

- Attacks against digital systems will be the same as attacks against their analog analogues.
- Criminals will attack commerce systems for financial gain.
- Privacy violations by marketers, criminals, police.

The changing nature of attacks

- Automation
  - Marginal profitability of each success acceptable
  - Marginal probability of success acceptable
  - Ease of casual privacy violations
- Action at a distance
  - Difficulty of tracing attacker
  - Difficulty of prosecution
  - Jurisdiction shopping
- Propagation of successful techniques
  - Hacker newsgroups, bulletin boards, mailing lists
  - Only the first needs skill; the rest can use software.

Adversaries

- Hackers: informal and institutional
- Insiders
- Lone criminals
- Commercial espionage
- Press
- Organized crime
- Terrorists
- National intelligence

Criminal attacks

- “How can I acquire the maximum financial return by attacking the system?”
- Forgery, misrepresentation, replay, repudiation
- Generally opportunistic
- Minimum necessary resources
- Focuses on low-tech flaws
- Focuses on the weakest systems
- Medium risk tolerance: willing to risk job or jail time.

Electronic commerce

- Fraud has been attempted against all commerce systems:
    - Weighted scales, shaved coinage, counterfeit currency, fake stock certificates,
    - Check, credit card, and ATM fraud.
- Electronic commerce will be no different.
    - Ease of automation
    - Difficulty of isolating jurisdiction
    - Speed of propagation
- Audit is essential.
    - Preventing crime is a lot harder than detecting crime.
    - Detecting crime is not enough, you have to prove it in court.
- Traditionally, fraud prevention has been reactive.
- We need to be proactive.

Identity Theft

- As more identity recognition goes electronic, identity theft becomes easier.
- As more systems require electronic identity recognition, identity theft becomes more profitable.
- We have lived for 30 years in the fiction that “mother’s maiden name” is good enough.
- We will never get back to that point again.
- Secure electronic commerce should not rely on electronic identity alone or security.

Privacy violations

- Targeted attack
  - Spying, stalking, industrial espionage
  - Cryptography can only protect up to the point where non-cryptographic attacks become cheaper.
  - End-to-end cryptography can protect absolutely against non-invasive attacks.
- Data harvesting
  - Generating a database of qualified "prospects."
  - Even moderate levels of cryptography, if ubiquitous, make the collection problem intractable.
  - Cryptography can protect absolutely.

Publicity attacks

- "How can I get the most publicity by attacking the system?"
- Attacker typically skilled, has access to significant resources and large amounts of time, but has few financial resources.
- Low risk tolerance: attacker willing to risk publicity, but probably not jail time.

Electronic vandalism

- Form of publicity attack
- Example: defacing web pages
- No profit motive
- Directed against “deserving” targets: political, corporate, etc.

Denial of service

- Example: flooding e-mail servers
- Almost impossible to protect against
- Cyberspace is designed for communication
- Only workable solution is to detect attacker and prosecute

Legal attacks

- "How can I discredit the system to prove my client's innocence?"
- Attacker does not need to discover flaws; he just has to discredit the system in the eyes of a judge and jury.
- Attacker can use the discovery process to demand details of target system.
- Attacker has all the resources of the publicity attack, plus significant financial support.
- Can be a well funded attack.

Information warfare

- Terrorism
- Covert operations
- Against individuals, companies, countries
- Against particular systems or parts of infrastructure
- Attack could originate from foreign soil
  - Jurisdiction problem.
- High risk tolerance: willing to risk life and limb
- Possibly very well funded

Attackers have it easier

- Attackers cheat.
- And the odds are in their favor.
  - An attacker needs to find one successful attack.
  - A defender needs to protectt against every possible attack.
- They can use techniques defenders never considered.
- They don't have to follow the defender's threat model.

WHAT CRYPTOGRAPHY CAN AND CAN'T DO

Basic Tools of Cryptography

- Symmetric encryption
  - Provides secrecy among parties who share a common key.
- Message authentication codes
  - Provides integrity checking and authentication
- Public-key encryption
  - RSA allows someone to receive secret messages from people he hasn't met yet.
  - Diffie-Hellman key exchange establishes a secret over an insecure channel.
- Digital signature schemes
  - Establishes integrity, authenticity, and non-repudiation.
- Secure hash functions
  - Used to reduce a message to a fixed size for signature.

Security problems solved by cryptography

- Privacy of stored data, messages, and conversations
- Secure electronic commerce
- Transaction non-repudiation
- User and data authentication
- E-mail security (encryption and authentication)
- Secure software updates
- Multi-party control
- Secure audit logs

Why cryptography can't really solve any of them

- The realities of the system often prevent cryptography from being applied where it is required.
- Implementation much harder than stringing these tools together.
- Mistakes are often added elsewhere in the process.
- There's lots of good cryptography out there; the problem is figuring out how to use it properly.
- Given any set of security criteria, it is possible to design a system that meets the criteria and is still insecure.
- "Buzzword compliant" is not enough.

Non-cryptographic parts of the solution

- Trust management
  - Trust is a complex social phenomenon, and cannot be solved with a single "certificate."
  - There is no global name space in the world.
  - There is no single level of assurance in the world.
  - Certificates are useless without some sort of liability.
- Access control
  - Authentication is not the same thing as authorization.
  - Authentication is automatic; authorization requires thought.

Non cryptographic parts of the solution (cont.)

- Human-computer transferance
  - Computer security works in the digital realm; transferring things from people to the digital world is very difficult.
  - There is no assurance that what you see is what you get.
  - There is no assurance that what you get actually works.
- Human-computer interactions
  - Security works better when it is visible to user.
  - On the other hand, user doesn't want to see security.
  - People find security intrusive.
  - People work around security measures.
  - People can't make intelligent security decisions.
- Passwords
  - People can't choose, remember, or keep good secrets.

Non cryptographic parts of the solution (cont.)

- Secure perimeters
  - Tokens: smart cards, access tokens, electronic wallets, dongles, hardware meters.
  - Tamperproof hardware is impossible.
  - Tamper resistant hardware is mostly impossible.
  - Tamper-evident hardware might work, sometimes.
  - Many systems rely on this anyway
  - Any system where the device and the secrets within the device are under the control of different people has a fundamental security flaw.

Non cryptographic parts of the solution (cont.)

- Key-escrow/key-recovery/GAK
  - It is easy to implement key backup, because it is in the interest of the user.
  - It is very difficult to implement GAK (Government Access to Key), because it is contrary to the interests of the user and must survive a hostile user.
- Relationships
  - Systems can leverage relationships between the parties.
  - An ongoing relationship reduces the incentive to attack the system, and increases the liklihood of detection.
  - Reputation can be important
  - Anonymous systems are much riskier.
- Protocols that rely on the "ethics of strangers"

The problem of testing security

- Flaws can be, and are, everywhere.
  - Areas of vulnerability include threat model, system design, implementation, user interface.
  - Two secure subsystems can interact to create new flaws.
- These flaws are common, and invisible
  - Security is orthogonal to functionality.
  - There is no such thing as a comprehensive security checklist.
  - Often the only feedback available to developers is the discovery (sometimes via the media) that they failed.
  - No amount of beta testing can ever uncover a security flaw.

The problem of testing security (cont)

- Experienced security testing can discover flaws.
  - Testing for any given weakness is easy.
  - Testing for all known weaknesses is very hard.
  - Testing for all possible weaknesses is impossible.
- Workable solutions
  - Hire experiences cryptosystem and security designers.
  - Test the system against a comprehensive attack list.
- Cryptography doesn’t have to be perfect, but the risks have to be manageable.
  - “A secure computer is one that has been insured.”

Needs for Privacy

- Most businesses (and governments) don’t need long-term security
- Mailing lists, business plans, negotiations, product research
- Commerce privacy needs are moderate.
- Financial information might need to be secure for a decade.
- Exceptions are embarrassments: personal, political, or business.

Needs for Authentication

- Authenticating sessions versus authenticating transactions
- Strength depends on application and transaction value
- Need for audit trail depends on application
- Audit trail must not only determine who committed fraud; it must be able to convince a jury that the person committed fraud, while at the same time not compromising the future security of the system.

EVALUATING CRYPTOGRAPHIC PRODUCTS

Security requirements

- Security requirements depend both on the value of what is being protected and the anticipated attacks.
- Most businesses don't need long-term security.
- Authentication needs depend heavily on the application.
- Electronic commerce needs depend on the value of the transaction: moderate privacy, moderate to strong authentication, good audit.
- Questions to ask
  - How valuable is the data or service being protected?
  - To whom it is valuable to?
  - Who does the system require me to trust?
  - What is the skill/time/resources necessary to attack the system?
  - What would the cost of compromise be, including loss of time and manpower, loss of reputation, costs to fix already-fielded systems?

Soundness of the cryptography

- Algorithms
  - Key length
  - Look for published algorithms that are generally considered to be secure: DES, IDEA, RC4, RC5, Blowfish, MD5, SHA, RSA, ElGamal, DSS.
  - If the algorithms are "Proprietary," they are probably lousy.
- Protocols
  - Look for published protocols that are generally considered to be secure: ESP, AH, SKIP, Photuris, SSH, S/WAN, SSL, PGP, S/MIME, SET, etc.
  - Avoid in-house proprietary designs that are unpublished.

Soundness of the cryptography (cont.)

- Specifications
  - Look for detailed specifications of the system. Any good security system can be published without adversely affecting security.
- Look for an attack analysis.
  - What is the cheapest attack?
  - What is the "low-skill" attack?
  - What attacks are outside the scope of the system?
  - What security assumptions is the system based on?
  - What happens if any of those assumptions are wrong?
  - What sorts of upgrade or disaster recovery plan does the system have?
- Look for security analyses by reputable cryptographers. Ask the manufacturer to provide copies of them. Be wary if there aren't any.

Compliance to standards

- Standards not only improve a product's security, but increase its potential interoperability.
- Commonality of public-key infrastructure allows certificate infrastructure to be used for a variety of applications.
  - X.509 is the current standard
  - But there is lot of room for improvement.
  - Watch SDSI/SPKI.
- E-mail encryption standard allows different mail programs to communicate securely with each other.
  - PGP vs S/MIME

Compliance to standards (cont.)

- IP security
  - The IETF is standardizing on a suite of protocols: ESP and AH.
- Transport layer security
  - The IETF is working on TLS, based on SSL 3.0.
- Tokens
  - This is currently a mess.
  - Cryptoki has problems.
  - Many proprietary products that don’t work with most applications.
- APIs
  - There are many; no one is clearly better.
  - It is probably impossible to make any one API suitable to everyone.

Legal restrictions

- Many countries have restrictions on cryptography: import, export, and use.
  - The U.S. government does not restrict the use of encryption, but has strong restrictions on its export.
  - There are three basic exportable types of encryption: home-grown, badly flawed cryptography, 40-bit cryptography, and escrowed cryptography.
  - The State Department is allowing the export of 56-bit DES if the exporter agrees to implement key escrow in short order.
  - More companies are implementing key escrow in order to gain export approval for their products. In many circumstances, these are suitable for corporate use.

Legal restrictions (cont.)

- U.S. regulations (cont.)
  - The U.S. has no restrictions on access-control or authentication systems; they only restrict products that use cryptography to provide privacy.
  - Additional allowances are made for financial institutions.
  - This is all in major flux right now.
- Patent issues
  - Public-key cryptography
  - Algorithm patents
  - Other patents

Ease of use

- Security vs. Functionality
  - Security often favors moving cryptography close to the application to maximize control.
  - Functionality often favors moving cryptography away from the application to maximize transparency.

Product availability

- The current products on the market are very immature
  - Inflexible, unforgiving, and hard to use
  - Buggy
  - Limited technical support
  - Poor integration with existing systems
- Hardware and software manufacturers seem to think it is possible to design a product and then build security in as an afterthought.
- Many buyers are forced to develop custom software.
- This can only get better.
  - The Internet enforces standards
  - Cryptography is migrating into end-user applications
- Beware government attempts to limit the availability of strong cryptography.

DEVELOPMENTS TO WATCH

Developments to watch

- Technologies
  - Tamper-resistant hardware
    - Chips
    - Tokens
    - Electronic wallets
  - Biometrics
    - Fingerprints
    - Keyboard latency
    - Etc.

Developments to watch (cont.)

- Trust management
  - Transfer of trust
  - Certificate issuance
  - Certificate storage and retrieval
  - Cross use of certificates
  - Certificate revocation
- Internet standards
  - TCP/IP, WWW, e-mail, telnet, rlogin, etc.
  - Will it allow the richness of human interaction: anonymity, aliases, trust, reputations?

Developments to watch (cont.)

- Human/computer interface
  - User friendly key-management
  - “Invisible” security
- Legal infrastructures to support cryptography
  - Digital signature acts
    - Existing attempts often misguided
  - Vehicles for electronic commerce
  - Criminal statutes to prosecute digital criminals
    - Laws are better when they are technologically invariant.
  - Solutions to the jurisdiction problem
- Government cryptography restrictions
  - Export/import/use control
  - Government access to key (GAK) requirements

Developments to watch (cont.)

- Advances in cryptography
  - New algorithms
    - NIST's Advanced Encryption Standard (AES)
    - Elliptic Curve Cryptography
    - Quantum cryptography
  - New attacks
    - More computers, faster computers, more efficient computation, fundamental advances in cryptanalysis
    - Quantum cryptanalysis
  - New infrastructures
    - Certificate management: issuance, retrieval, storage, revocation
    - Will they propagate the same mistakes?

Conclusions

- "The problem with bad cryptography is that it looks just like good cryptography."
- Successful attacks are often kept secret.
  - Unless attackers publicize
- We need to be proactive.
  - Understand the real threats to a system
  - Design systems with strong cryptography
  - Build cryptography into systems at the beginning
  - Build systems that scale
- Perfect solutions are not required, but systems that can be broken completely are unacceptable.

Conclusions (cont.)

- It is prudent to prepare the worst.
  - Systems fielded today could be in place 20 years from now.
  - Things will get worse before it gets better.
  - Things will get better.
- The social problems are much harder than the mathematics.

- "If you think cryptography can solve your problem, then you don't understand your problem and you don't understand cryptography."

FURTHER READING

- Cryptography
  - B. Schneier, *Applied Cryptography, Second Edition,* John Wiley & Sons, 1996.
  - A. Menezes, P. van Oorschot, S. Vanstone, *Handbook of Applied Cryptography,* CRC Press, 1997.
  - D. Stinson, *Cryptography: Theory and Practice,* CRC Press, 1995.

FURTHER READING (cont.)

- Network Security
  - S. Garfinkel and G. Spafford, *Practical UNIX and Internet Security,* O'Reilly and Associates, 1996.
  - C. Kaufman, R. Perlman, and M. Speciner, *Network Security,* Prentice-Hall, 1995.
  - W. Stallings, *Network and Internetwork Security,* Prentice-Hall, 1995.
  - W. Cheswick and S. Bellowin, *Firewalls and Internet Security,* Addison-Wesley, 1994.

FURTHER READING (cont.)

- E-Mail
  - B. Schneier, *E-Mail Security,* John Wiley & Sons, 1995.
  - S. Garfinkel, *PGP: Pretty Good Privacy,* O'Reilly and Associates, 1995.
- Electronic Commerce
  - P. Wayner, Digital Cash, *AP Professional,* 1995.
- Privacy
  - E. Alderman and C. Kennedy, *The Right to Privacy,* Aldred A. Knoph, 1995.
  - A. Cavourian and D. Tapscott, *Who Knows,* Random House of Canada, 1995.