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

Black Hat
9 July 1997
Las Vegas, NV

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 is 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.