

# Network Security with Cryptography

Dr. Richard E. Smith  
Principal Systems Engineer  
Secure Computing Corporation  
2675 Long Lake Road  
Roseville, MN 55033 USA  
<http://www.securecomputing.com/>

612-628-2780  
[smith@securecomputing.com](mailto:smith@securecomputing.com)

“Internet Cryptography” web site: <http://www.visi.com/crypto/>

Copyright 1998 Richard E. Smith. All rights reserved.

## Networking is Beneficial

- Finish more tasks in less time
- Communicate efficiently with your customers and clients
- Publish the latest information about your work at a very low cost

The benefits of networking must be greater than the costs and the risks.

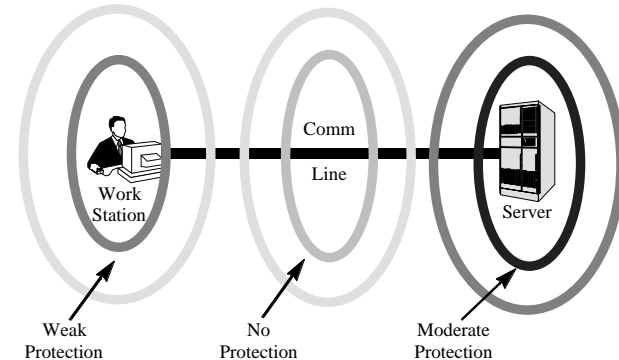
Otherwise, why bother with it?

## Outline

- Introduction
- Automatic cryptography
  - Link encryption
  - Secret key management
  - Virtual private networks with IPSEC
  - Public key management
- User controlled cryptography
  - World Wide Web security
  - Electronic mail security

## Networking Adds Risks

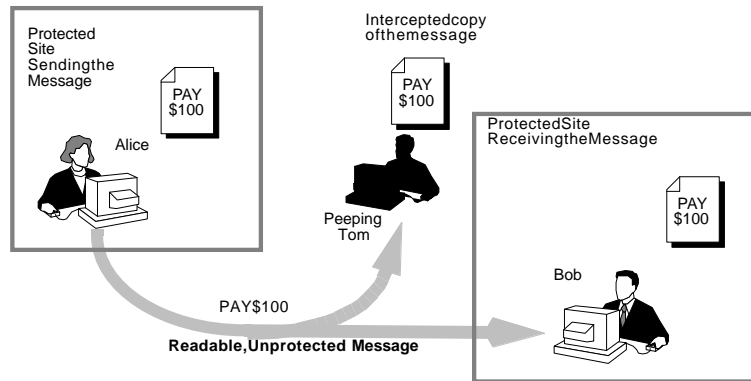
- Attackers exploit gaps in software, hardware, and procedures.



- Networking produces more gaps to attack.

## Risk: "Sniffing"

- Often just annoying, unless the message is a password!

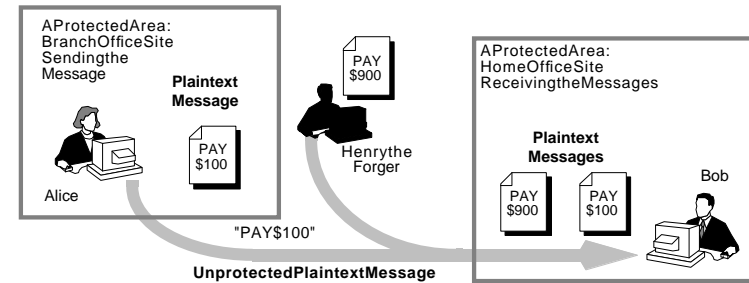


August 13, 1998

ic1.fm - 5

## Risk: Forged Transactions

- Companies must send valuable messages to get work done.



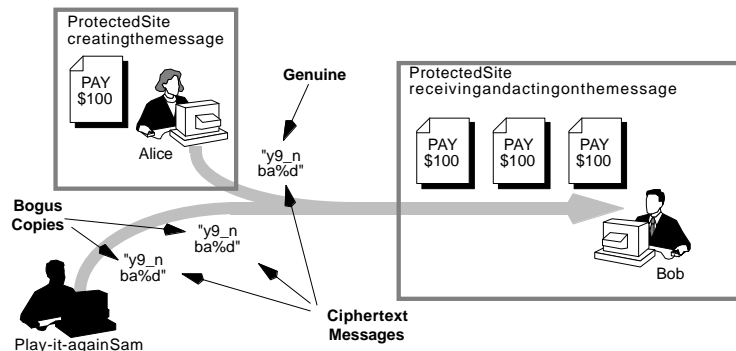
- How can Bob tell the difference between a legitimate, valuable message and a forged one?

August 13, 1998

ic1.fm - 6

## Risk: Replay

- Attacker could replay a cryptographically protected message and the message may look completely legitimate.



- TCP/IP can detect "accidental" replay, but not "malicious" replay.
- Must have a reliable way of detecting duplicate messages

August 13, 1998

ic1.fm - 7

## Achieve Connectivity And Protection

- First, look at your connection needs
  - Fully automatic versus user controlled protection
  - Fully secured versus "mixed" accesses
  - Preplanned versus unexpected connections
- Second, choose products that support the needed connections, and that cover the risks:
  - Brute force eavesdropping
  - Message replay
  - Message modification

August 13, 1998

ic1.fm - 8

## Different Types of Connectivity

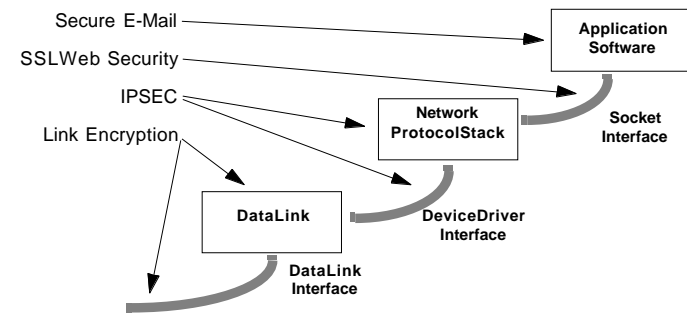
- Fully automatic versus user controlled protection
  - Is protection always turned "on" even when the overhead is unnecessary?
  - Can we disable protection when it prevents communication with some other user or site?
  - Can data be sent without protection by accident?
- Fully secured versus "mixed" accesses
  - Do we only share messages with associated hosts?
  - Can we communicate with commercial hosts and services?
- Preplanned versus unexpected connections
  - Will all communications be arranged ahead of time?
  - Must we talk safely with new and unplanned hosts?

August 13, 1998

ic1.fm - 9

## Different Types of Products

- Each is installed in a different place in your computer



- Each supports different connection needs

August 13, 1998

ic1.fm - 10

## Choose Products for Connection Needs

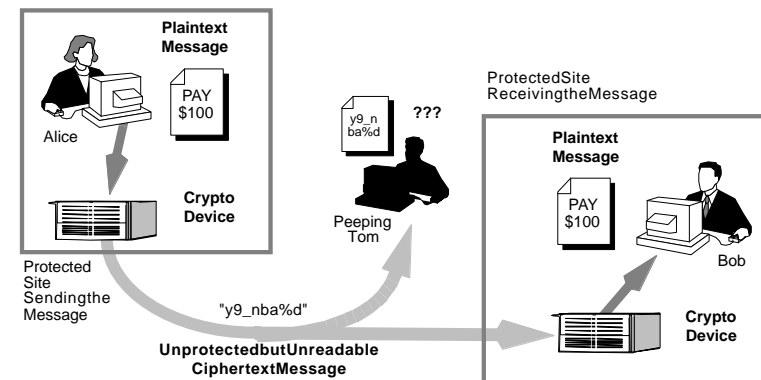
- Product Options Today
  - Firewall Encryption for Virtual Private Networks (VPNs)
    - IP Security Protocol (IPSEC)
  - Web Encryption for Electronic Commerce
    - Secure Sockets Layer (SSL)
  - E-Mail Encryption
    - Pretty Good Privacy (PGP), Secure MIME (S/MIME), Privacy Enhanced Mail (PEM), Message Security Protocol (MSP)
- Connection Needs that Affect the Choice
  - Centralized versus Distributed Connections
  - Individual versus Shared ("Proxy") Crypto
  - Secured versus Mixed Accesses

August 13, 1998

ic1.fm - 11

## The Basic Application

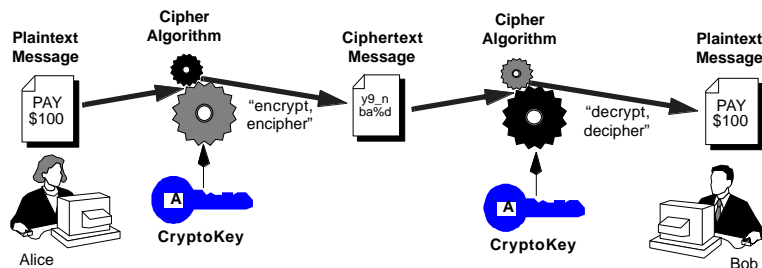
- Cryptography separates "insiders" from "outsiders"



August 13, 1998

ic1.fm - 12

## Cryptographic Terms



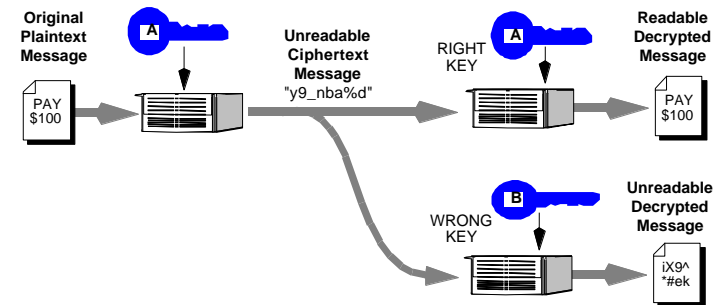
- A **cipher algorithm** is a well defined procedure that converts the message between plaintext and ciphertext and back.
- A **crypto key** is a binary data item whose contents are randomly chosen and kept secret from outsiders.

August 13, 1998

ic1.fm - 13

## Secret Keys Enforce the Separation

- Keys are binary data items containing random, secret bits.



- Attackers can not read messages even if they have the same crypto equipment. They must also have the correct secret key.

August 13, 1998

ic1.fm - 14

## How Safe Is Encryption?

It is relatively reliable, unless the attackers can:

- **Guess secret keys**
  - Brute Force Attacks
  - Shortcut Attacks
- **Cause trouble without guessing any keys**
  - Message Modification
  - Message Replay

Plus, there are the common problems of installation errors, infiltration, system damage, and stolen secrets.

August 13, 1998

ic1.fm - 15

## Brute Force Attacks

- 1. How long does it take to test all possible crypto keys?

Crypto Algorithm	Key Size	Time to Search for the Right Key
Exportable RC4	40 bits	dozens of computers for hours
DES	56 bits	thousands of computers for months
Full RC4 or IDEA	128 bits	trillions of years - nobody's done it yet

- “Cracking” must be repeated for each new key
- 2. Is there a “shortcut” that eliminates some keys?
  - **Computationally secure** - too many keys and no shortcuts
    - A sliding measure - “nobody’s done it so far”
- 3. Does more than one valid decryption make sense?
  - **Unconditionally secure** - numerous sensible decryptions exist, so you can’t tell if you guessed the key correctly

August 13, 1998

ic1.fm - 16

## Shortcut Attacks: The Netscape Experience

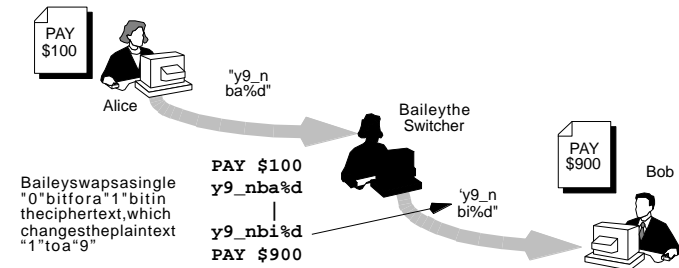
- Early versions of *Netscape Navigator* (Versions 1 and 2)
- Generated Keys by sampling internal computer variables
  - Examples: time of day, amount of free disk space, amount of free memory, etc.
  - Attacker sharing the same computer could also sample these variables -- yielding an **entering wedge**
  - Researchers demonstrated that this dramatically reduces the range of plausible crypto keys -- cracking becomes easy
- More truly "random" sources of randomness
  - Variations in disk speed when accessing same locations
  - Variations in motion while moving the mouse (PGP)
  - External sources of random signals (noisy diodes, Lava lamps, cosmic emission, tables of random digits,...)

August 13, 1998

ic1.fm - 17

## Forgery Without the Key

- Encryption does not protect against modifications
- Attackers can rewrite messages if they know what they say



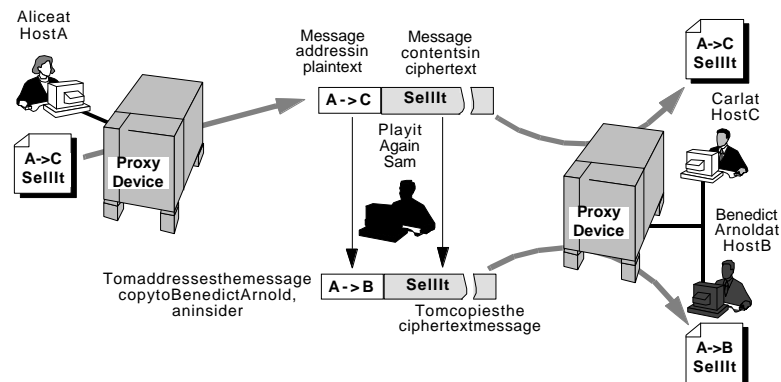
- Many ciphers are vulnerable to this attack
  - RC4 commercial cipher used in Web commerce
  - Theoretically uncrackable "one time pad" cipher used by spies

August 13, 1998

ic1.fm - 18

## Decryption Without the Key

- An attack by an "insider"



August 13, 1998

ic1.fm - 19

## Avoiding the Pitfalls

- Use well known techniques based on "open" standards.
  - Well known devices, technologies, and algorithms have well known strengths and weaknesses.
  - If a problem is discovered, both the problem and the solution will eventually become public knowledge.
  - It is much harder to learn about problems in proprietary technologies.
- Pay attention to the system's integrity: use competent, professional operators and maintenance personnel.
- Recognize that all technologies fail in one way or another.
  - Build systems that limit the damage from any single failure.
  - Build systems whose components keep useful records.

August 13, 1998

ic1.fm - 20

## Automatic Cryptography

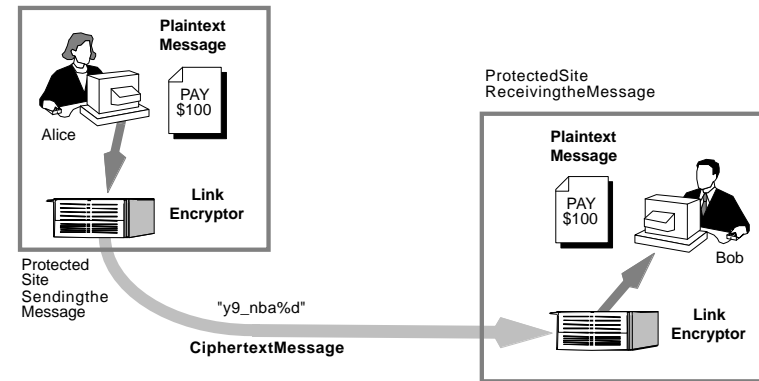
- General Features
  - Completely hidden from existing software
  - Users can't disable it by accident
- Link Encryptions
  - Mature, widely available product
  - Requires dedicated, point to point connections
  - Reliable but inflexible and costly
- Encrypting Routers and Firewalls
  - New product
  - Connects across public networks like the Internet
  - More flexible, lower cost, but harder to configure correctly

August 13, 1998

ic1.fm - 21

## Link Encryption

- Encrypts all data at the "data link" layer

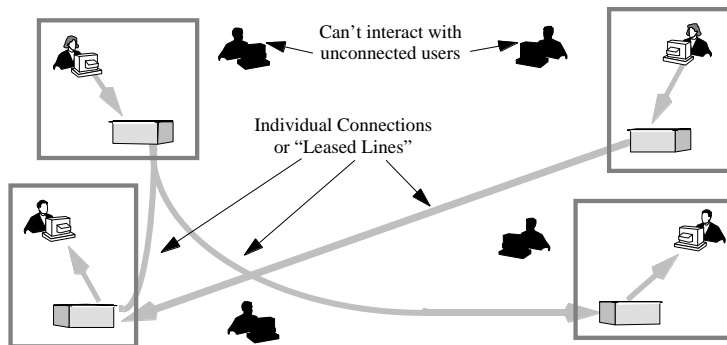


- No "mixed" access, no unexpected connections.

August 13, 1998

ic1.fm - 22

## Link Encryption Between Sites

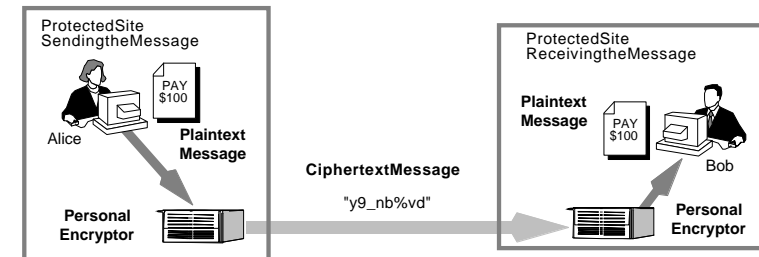


- Must have a dedicated point-to-point link for each stream of encrypted data.

August 13, 1998

ic1.fm - 23

## Per-User Link Encryption



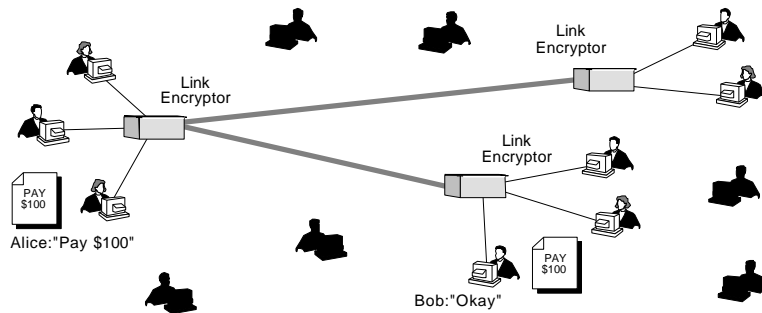
- Can give strong confidence in the identities of the sender and recipient, since nobody else is using the same crypto keys
- More expensive: requires more crypto hardware and/or software, and more key management (one set per user)

August 13, 1998

ic1.fm - 24

## "Proxy" Link Encryption

- Share the crypto hardware and keys among multiple users



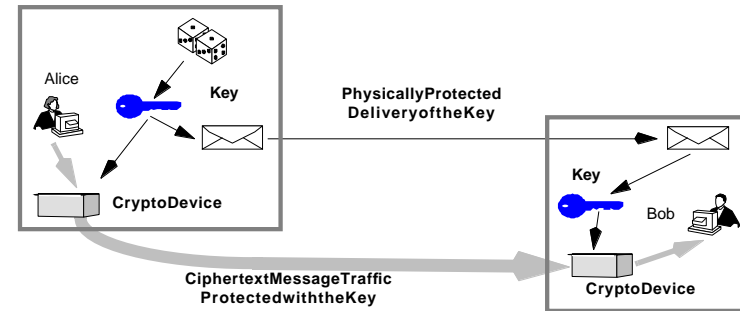
- Mixed benefit
  - Less hardware and administration yields lower cost
  - Can't use the crypto to identify individual user messages

August 13, 1998

ic1.fm - 25

## Secret Key Management

- We physically protect the smaller, secret key instead of physically protecting all of the data that traverses the network.



- Keys must be changed periodically: the longer we use a key, the more likely that an attacker has figured out what it is.

August 13, 1998

ic1.fm - 26

## Key Management Challenge

- The challenge has two parts:
  - Keys must be as hard as possible to steal or predict.
  - Keys must be easy to change periodically, "per session."
- Key Management Techniques
  - Manual Keying:** distributes each key "by hand."
  - Pre-shared Keys for Automatic Rekeying** (i.e. ANSI X9.17)
    - Distribute "key encryption keys" (KEKs) ahead of time.
    - Use the KEKs to exchange "session keys" during use.
  - KDCs - Key Distribution Centers** (i.e. Kerberos)
    - Give everyone a key for communicating with the KDC.
    - The KDC distributes "session keys" for communicating between pairs of hosts.
- We will examine "Public Key" techniques later.

August 13, 1998

ic1.fm - 27

## Secret Keys and the "Cryptonet"

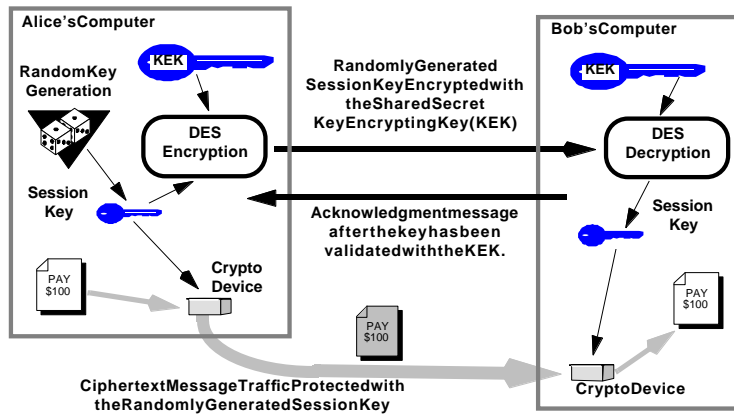
- Everyone who shares a particular secret key can communicate securely with the others sharing that key.
- A **cryptonet** is a group that shares a particular secret key.
- Traditional cryptonets could be very large.
  - Benefit:** it was simple to distribute a key so that everyone in a particular enterprise could communicate safely.
  - Problem:** it was impossible to change the key if the enterprise was very large (the **revocation** problem).
- Today, cryptonets are as small as possible.
  - Ideally,** a cryptonet has exactly two members.
  - Benefit:** it is simple to revoke a key.
  - Problem:** the number of key pairs needed by a very large enterprise is too large to manage: a combinatorial explosion.

August 13, 1998

ic1.fm - 28

## Pre-Shared Keys with ANSI X9.17

- Rekeying is safer, but we still have the cryptonet problem.



August 13, 1998

ic1.fm - 29

## Key Distribution Center (KDC)

- The KDC centralizes the generation of session keys. Every user is assigned a secret key (their KDC key) that they use when sending messages to the KDC. When the KDC generates a session key to allow two users to communicate, two copies of the key are returned, one encrypted with each of the users' KDC keys.
- Benefits of KDCs
  - One key per user: no combinatorial explosion of keys.
  - Mature technology.
- Problems with KDCs
  - Security depends on the KDC always remaining secure.
  - KDC must always be on-line to generate new keys.
  - Spoofing and replay attacks on KDC users (older protocols).

August 13, 1998

ic1.fm - 30