

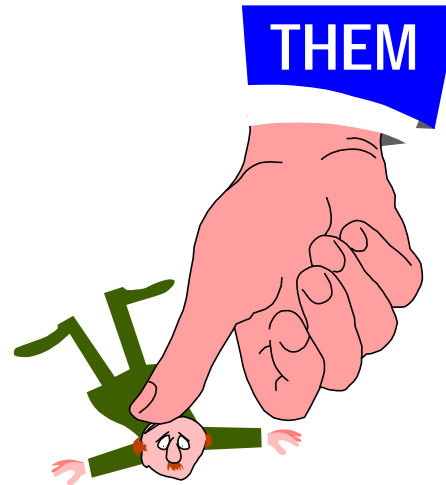
Secure Communications over Open Networks

(A Handbook for Paranoids)

Disclaimer

- Security requires a paranoid mindset
 - If you're going to play then you need to look at the big picture
 - This tutorial is intended to give a background on communications security
 - You could spend your life doing this stuff and still make mistakes
- ***Nothing*** is secure

**Just because you're paranoid
doesn't mean "they" aren't out
to get you.**



The Elusive “They”

- During this tutorial, I will refer to “them” a lot
 - You decide who “they” are -- every paranoid has different enemies
 - Hackers / Industrial Spies
 - Thought police
 - KGB / SMERSH / UN
 - CIA / IRS / ATF / NSA / NRA / U.N.C.L.E.
 - Orbital Mind Control Lasers / Illuminati / etc.

Before You Start

- Risk Assessment:
 - What are you trying to hide?
 - How much will it hurt if “they” find it out?
 - How hard will “they” try?
 - How much are you willing to spend?
“spend” means a combination of:
 - Time
 - Pain
 - Money

Why Secure Communications?

- To carry out a business transaction
 - E-Commerce
- To coordinate operations (Command and Control)
 - Remote management
- To protect information
 - Privacy
 - Confidentiality

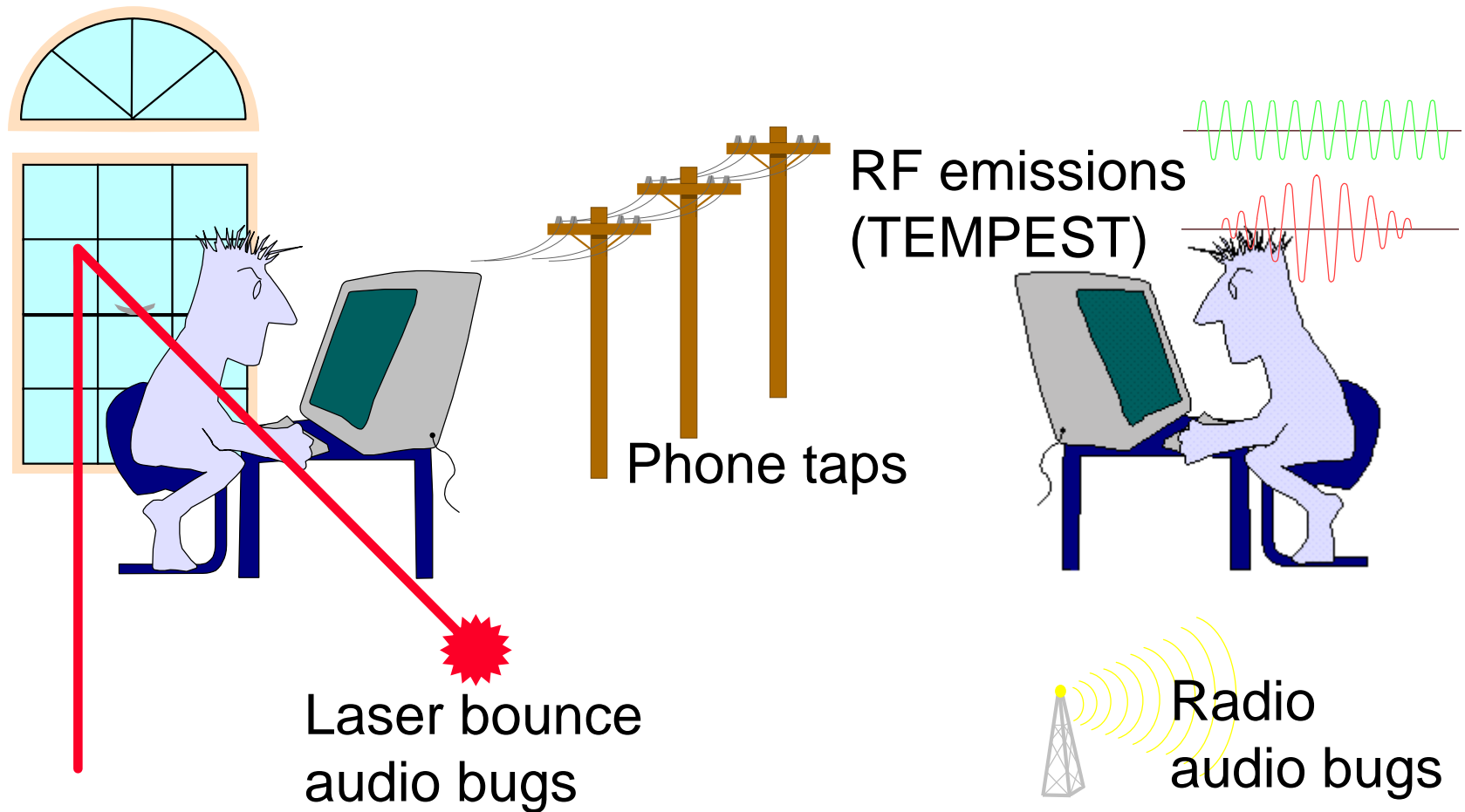
The Environment

- Communications security is the land of cost/benefit analysis
 - Make getting your data too expensive for the attacker and they may not even try
 - Make protecting your data too expensive for yourself and you may be unable to operate

Target Analysis

- Target analysis is the (hypothetical) art of analyzing a target's communications security to identify the weakest link
- You'd better do it, because "they" will do it, too

Target Analysis



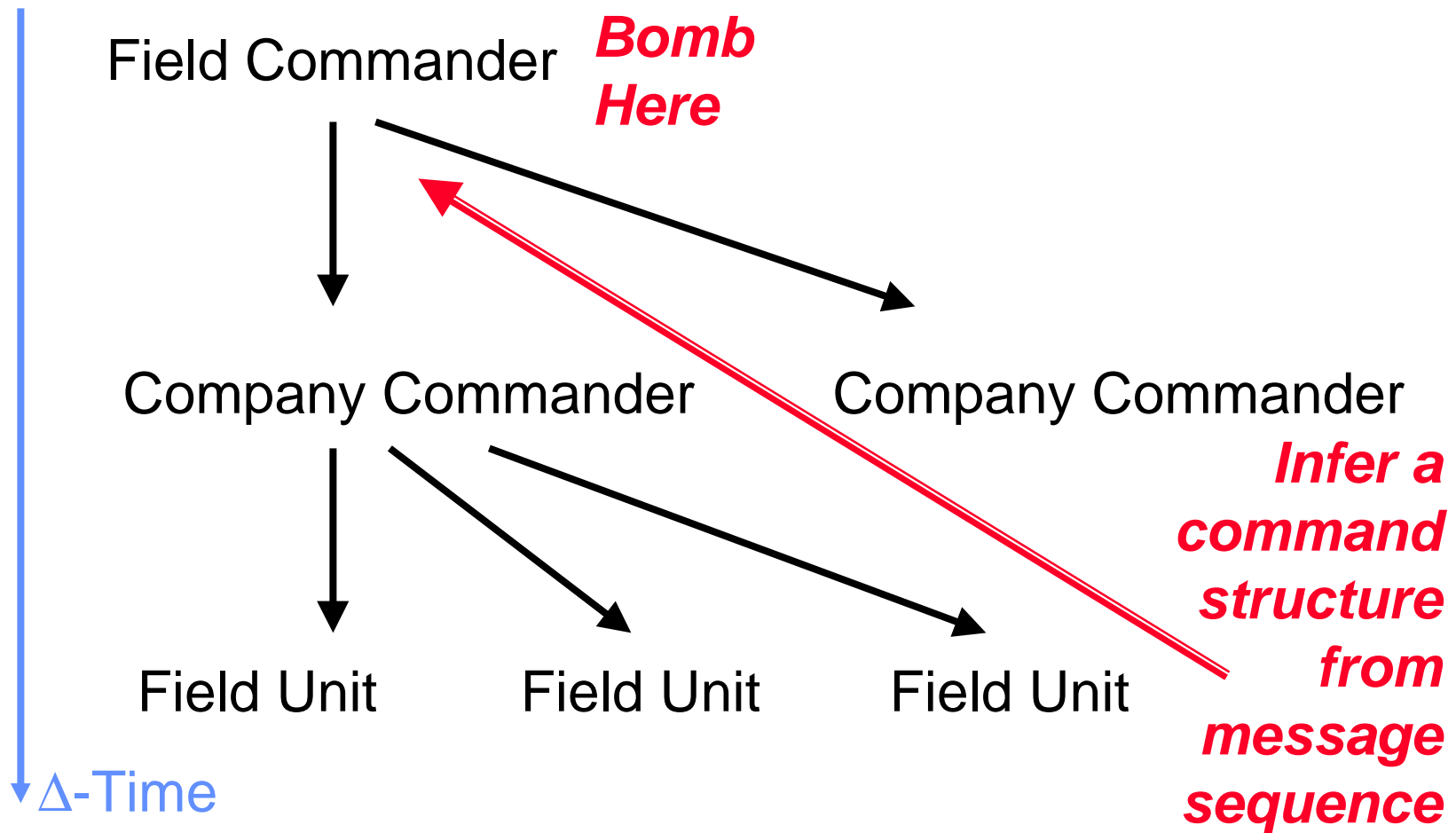
Target Analysis

- Sweep your computer for bugs
 - Work only inside a metal cage w/no windows
 - Store the computer in a safe
 - Don't use the local power grid to power your crypto systems
- ...etc. -- it's all cost/benefit analysis

Traffic Analysis

- The art of ***inferring*** about contents of communications by ***analyzing the pattern*** of communications
 - Density of data
 - Occurrence and timing of connections
 - Duration of connection
 - Sequence of connection

Traffic Analysis



Traffic Analysis in Open Networks

- In open networks the majority of traffic is in the clear (unsecured)
... Therefore securing it becomes a dead giveaway to the traffic analyst!
- Ideally your secure communications will somehow look like unsecure communications or get lost in the noise

Traffic Analysis in Open Networks

- Incidentally, US law enforcement appears to be building an argument around a mindset that “if it’s encrypted that indicates that someone is probably doing something they shouldn’t”
 - I.e.: **Honest** people don’t **need** secure communications

Traffic Analysis: Example

- Terrorist hit in Paris*
- French intelligence agency correlates
 - All payphone calls near kill zone
 - Calls within “time window” of kill
 - Calls to another payphone that makes a call outside of France within a 20 minute period
 - Iranian agent in south of France is caught

*Amazingly, this was reported in Time magazine

Traffic Analysis: Internet

- Identify software pirates by correlating file download activity
 - Large size files
 - Download rate
 - Frequency of particular files
 - Correlate file sizes/volumes across networks and you can backtrack users*

*Almost nobody keeps good enough logs to do this

Covert Channels

- Low data-rate communications encoded and hidden within another communication
 - Computers are great for this because they are patient!
- Example: Let's say we agree that if I hit your web site within an hour, it's a 1. If not it's a 0. I can send 24 bits/day.

Covert Channels *(cont)*

- Signal theory applies to covert channels
 - data rate == signal strength
 - Noise reduction techniques can be applied to detect and potentially recover the signal
- The more data your covert channel carries the less covert it is*
 - The happier that makes a traffic analyst

*Note that this applies to “stealth scans” and denial of service

Covert Channels *(cont)*

- Implication:
 - If you are setting up a covert channel hide where there is already a high noise level:
 - AOL instant messenger (more on this later)
 - The firewalls mailing list :)
- Hidden does not mean secured
 - It just means that they have 2 problems to solve instead of one: finding your communications and then cracking them

TEMPEST

(Transient Electromagnetic Pulse Standard)

- TEMPEST is a defense, not an attack
 - The attack is “Van Eck monitoring”
(<http://jya.com/emr.pdf>)
- CRTs and electronic devices emit electromagnetic frequencies which may be monitored
 - Claims vary from short distances (10m) to longer (300m+)

TEMPEST *(cont)*

- Peter Wright describes in *Spy Catcher*:
 - A German intelligence office...
 - British spies attempting to bug it by sneaking in along buried power lines...
 - Discover to their surprise that there is a signal on the power line...
 - The signal is generated by code machines and can be decoded into teletype output!

TEMPEST (cont)

- If you think They are going to come after you with Van Eck monitors, you're in deep trouble
 - Use battery powered laptops
 - Work **quickly** in electronically dead rooms underground
 - Run your TV and blender while you are encoding and decoding :)

Cryptanalysis

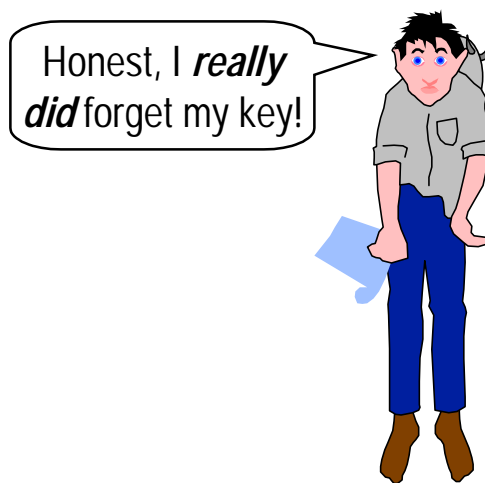
- Code-breaking is very time-consuming and requires highly specialized skills
 - It's a **very** expensive form of attack
 - Affordable by well-funded government agencies and research scientists
 - Outside the scope of “ordinary” hacking activity

Cryptanalysis *(cont)*

- Usually it's cheaper to exploit other flaws:
 - Bad key generation
 - Key storage / host security
 - Buffer software flaws in surrounding code
 - Error conditions that reveal data
- Use well-known and tested algorithms
- Worry about the other stuff instead

Rubber Hose Cryptanalysis

- If your communications security is so good They can't break it...
...the only thing left for Them to break is ***you***



Key Purchase Attack*

- There is no castle so strong that it cannot be overthrown by money
- *Cicero*

... How valuable is your data?

*Dan Geer

Erasing Magnetic Media

- Deleting files permanently is actually much harder than it seems - especially if they can get the physical disk media
 - Even overwriting data repeatedly doesn't work 100%: disk heads do not always align the same way on a track*
 - Commercial de-gaussers are not strong enough -- co-incidentally

*See Peter Gutmann's article at www.cs.auckland.ac.nz/~pgut001

Advanced Paranoia

- Hopefully by now you are convinced that you're helpless

...Against a sufficiently funded and motivated attacker, you may be...

But at least be ***expensive*** to attack!

Goofy Comsec Stories: 1

- Peter Wright tells of Egyptians using a Hagelin rotor-based cipher machine
 - British agents place a bug in the code room, posing as telco workers
 - Whenever the Egyptians change their keys the British listeners count the *>click<* sounds of the rotors being set
 - Reduces the strength of the cipher to a few minutes' guesswork

Goofy Comsec Stories: 2

- Peter Wright tells of British embassy staff using one time pads in a secured code room
 - Russians plant an audio bug in the room
 - British cipher clerk reads the message aloud as another enciphers it one letter at a time
 - An unbreakable cryptosystem is completely sidestepped

Goofy Comsec Stories: 3

- Soviet agents subvert an NSA employee whose job it is to destroy classified documents
 - Since the documents are to be destroyed there is no audit trail for further access
 - Instead of destroying them he sells them

Spycraft 101

- Is this stuff useful?
 - Probably not, hopefully
- Very very very hard to find information about tradecraft

Spycraft

- The actions of a secret agent are very similar to those of a criminal
 - But with a higher price if caught
 - Most captures are a result of sloppiness or external compromise
 - Spy's controller or cut-out is compromised
 - Spy's communications are detected
 - Spy lives inconsistent lifestyle / breaks cover (Aldrich Ames)

Spycraft *(cont)*

- “Legitimate Cover”
 - Individual hiding within a legitimate role
 - Co-workers and surrounds don’t know he’s a spy
- “Organizational Cover”
 - Entire organization is a front operation
 - Everyone is a spy
 - Can re-enforce actions / cover each other

Spycraft *(cont)*

- Choosing a cover:
 - Use the least fictional material possible - a “legitimate cover”
 - I.e.: if you are a pro-quality photographer, use that as a cover
 - If you don’t write good English, don’t pose as a school grammar teacher :)
 - Successful deep cover agents have only one lie about their cover: who they work for

Spycraft *(cont)*

- Good covers for the high tech age:
 - A security consultant
 - A conference lecturer
 - A developer in Microsoft's NT kernel group
 - A computer repair person
 - A telephone repair person
 - A member of the FBI computer crime squad

Spycraft *(cont)*

- In large-scale operations, infiltrate agents into the countermeasures forces of the opposition
 - E.g.: Kim Philby at MI6 and Aldrich Ames at CIA
 - DC drug dealers had cover agents in DC police force communications dispatch office!
 - Such agents can payoff quickly!

Spycraft *(cont)*

- Traditionally deep cover agents have a “controller” or cut-out who manages them and feeds messages to home
 - This is one of the important purposes of national embassies (e.g.: the US Embassy in Moscow, and the Soviet Embassy in DC)
 - This reduces the amount of data the agent must transmit
 - No need for powerful transmission system

Spycraft *(cont)*

- Generally a spy and controller arrange communication protocols and drops in isolation
 - Maintain a few ways of getting in contact in the event that the controller is compromised or hit by a car
 - (But if the controller is caught the spy is in trouble)
 - Typically a dead drop message broadcast

Spycraft *(cont)*

- Set up 2 or 3 contact re-establishment protocols
 - Don't use them except in an emergency
 - “if you ever see an ad in the NYT ‘lonely hearts section’ for a phlegmatic philatelist in search of...”
 - “love” == meet me at location #1
 - “romance” == meet me at location #2
 - “hot sex” == get out of town fast!

Spycraft *(cont)*

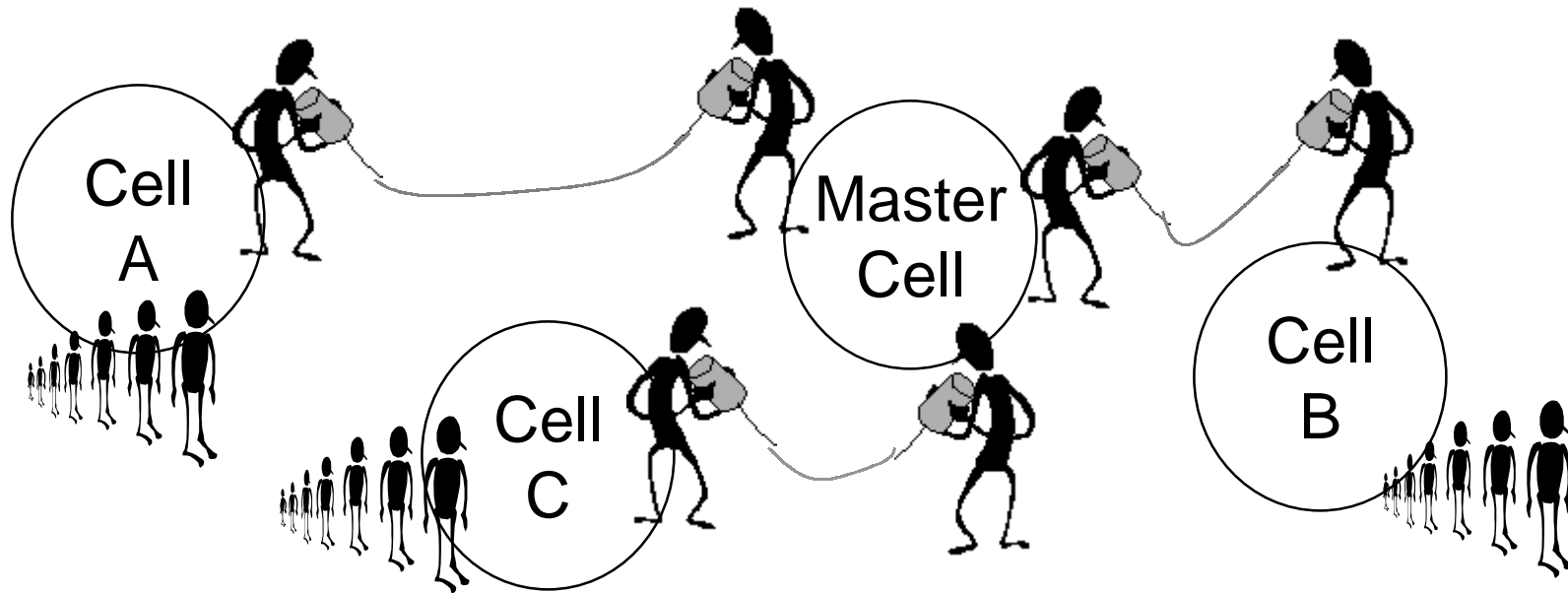
- Deniability
 - Consider maintaining a front cover that would provide a plausible explanation
 - I.e.: pretend to be a pervert or drug user - it's common enough and gives a good excuse for being sneaky
 - Only James Bond can survive getting caught sneaking around with a silenced gun and 2-way satellite radio

Cells

- Terrorists / guerillas organize into cell structures (rather than centralized hierarchies like government intelligence agencies)
 - Cells are small working groups that have cut-outs to other cells
 - Team of 5, one team leader who knows how to contact another team of 5, etc.

Cells *(cont)*

- Central authority / coordination is done by master cells in which each member has a contact to another cell



Dead Drops

- A “dead drop” is a location where a message can be left:
 - A hollowed bolt used in a park bench
 - A soda can thrown out of a moving car
 - A paper bag taped under a washroom sink
 - A scratch on a painted wall
 - An ad in a newspaper
 - A song request on a radio station

Internet Dead Drops

- The Internet is the ultimate hiding spot for dead drops! :)
 - A USENET posting
 - A “mistaken” URL hit on a web site (the mistake gleaned from logs later)
 - A “bounced” E-mail message
 - A spam E-mail message
 - A SATAN scan / hacking attempt

High Tech Meetings

- 2 people in an airport waiting lounge are waiting for flights
 - They never speak
 - They are 30 feet apart
 - One is using a laptop
 - One is looking at his pocket scheduler
 - They are using their IRDA ports to synchronize (encrypted) files

Crypto Engines

- All cryptosystems use a key (a secret) to process a message into a reversible form that is (hopefully) unreadable
 - The algorithms may be simple or complex
 - The algorithms may be strong (DES) or junk (Caesar shift, AKA ROT-13)
- Don't write your own unless you're willing to devote your life to cryptology

Key Management

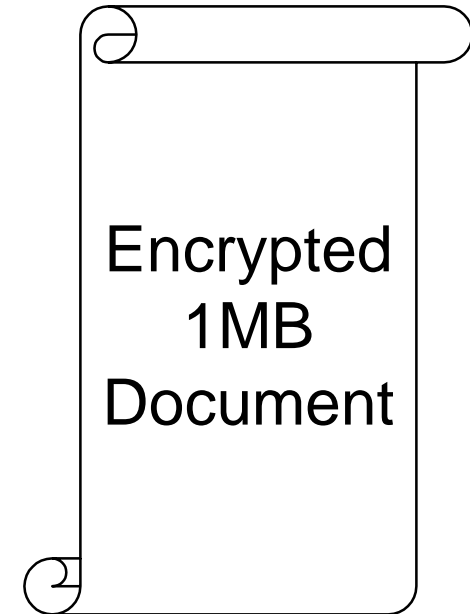
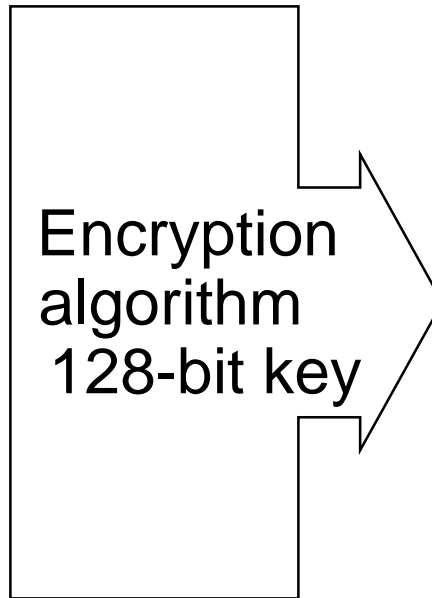
- Key management is an extremely difficult problem
 - If you give the key to a computer it can be stolen from the computer
 - The human brain is used as “secure” offline storage
 - Key management, and by extension cryptography, is about bootstrapping small secrets into bigger ones

Key Management *(cont)*

5-char password
in user's head



“plugh”



Small Secret
in “secure”
storage

Larger Secret
in less secure
storage

Big Secret
ready to
transmit publicly

Key Management *(cont)*

- One key per communicating pair
 - Pro: harder to compromise
 - Con: expensive to set up and update keys
 - May not work in battlefield conditions
- One key per “network” of pairs
 - Pro: cheaper to set up and update keys
 - Con: easier to compromise
 - Works in battlefield conditions

Secret Key

- Assumes that a pre-arranged key is exchanged out-of-band
- Key is stored as safely as possible
- Key is replaced periodically
- Does not scale to large installations
 - Same key between all partners --or--
 - Many keys to exchange and keep track of

Public key

- Use clever mathematical tricks to exchange a key with another party over an insecure link
 - Diffie-Hellman key exchange
 - RSA key exchange
- Eavesdropper cannot access key
- Knowing you exchanged the key with the *right partner* is still tricky

Public Key *(cont)*

- Public key (RSA) can also be used in non-interactive exchanges
 - One party publishes a public half of a key pair keeping the other half of the key pair secret
 - The other party generates a message to the first party based on their published half which can only be decoded by the holder of the secret half

Public Key *(cont)*

- Public key pairs may be used to “sign” a message by encrypting it with the secret key
- Recipient can check signature by decrypting with the public key
 - Usually instead of encrypting the entire document a cryptographic hash function is applied and the result is encrypted

Public Key Certificates

- A “certificate” is a copy of someone’s public key (along with other information) that has been signed by a Certification Authority (CA)
- CA’s certificates signed by other CAs, etc. forming a Certification Hierarchy
 - Global hierarchy still sorting itself out and probably will never happen

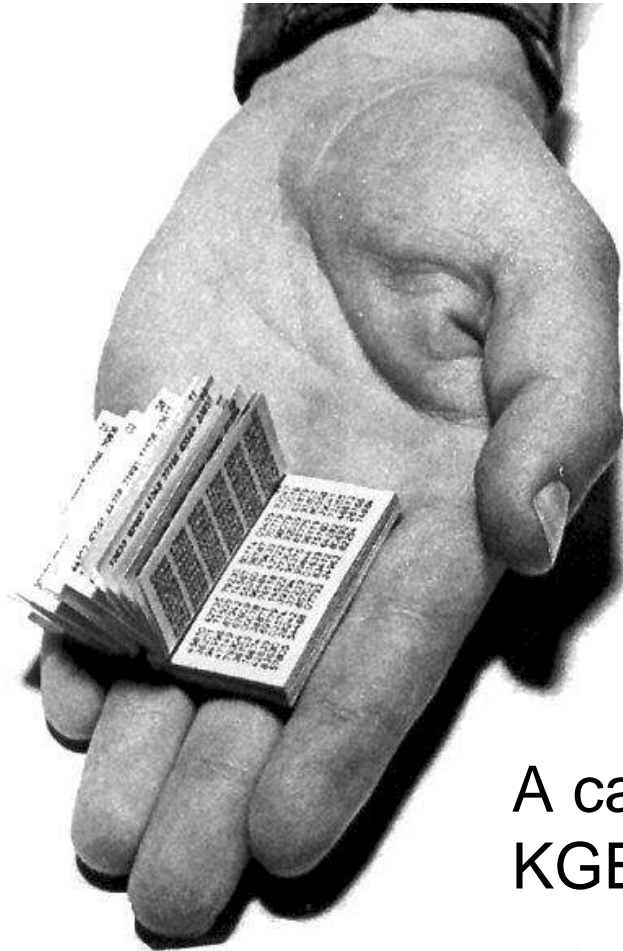
Problems w/Public Key

- Attacker can substitute certificates in transit (if a CA is not being used)
- How strong/how much do you trust the CA's security?
- Attacker can compromise the secret part of a public key pair and impersonate one of the participants
 - There are still secrets to keep

How Public Key Usually Used

- Public key used to exchange a random session key for link-level encryption
- Public key used to exchange a random message key for an individual message
- Public key used to sign a transaction by encrypting a cryptographic hash of the message

One Time Pads



A captured
KGB one time pad

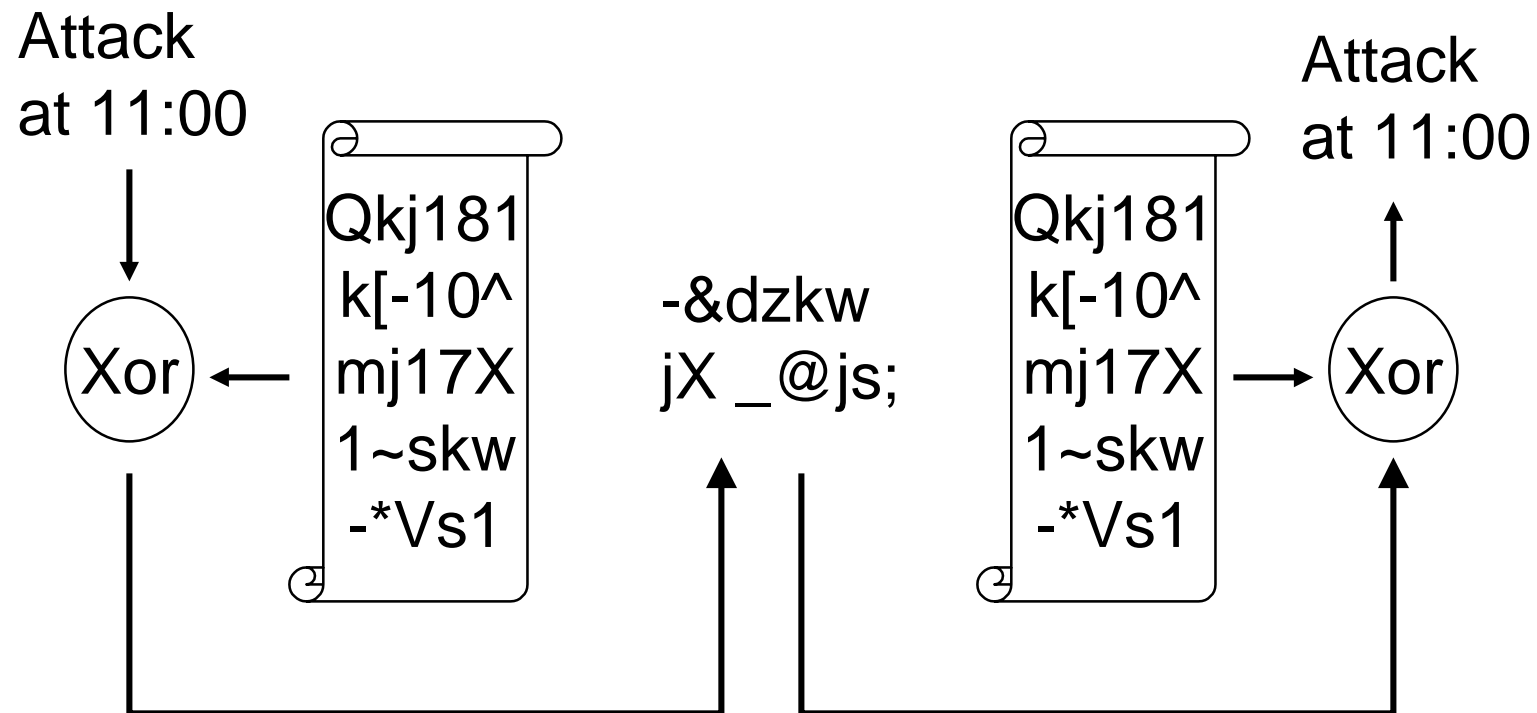
One Time Pad: Principles

- Vernam's Cipher: ***use a key size equal to the size of your document***
- Theoretically and provably unbreakable
 - Practically, it is very very difficult to use
 - Key management is hellaciously difficult
- Ideally suited to deep-cover moles or individuals with low bandwidth requirements

One Time Pad: Principles *(cont)*

- Make a bunch of random data on a CDROM
- Give each party a copy; they go their separate ways
- To encode, Xor the message with the “pad” and send the result
- To decode, Xor the result with the “pad” and you’ll get the original message

One Time Pad: Principles *(cont)*



One Time Pad: Randomness

- One Time Pads data must be completely random to be secure
 - Do NOT use output of DES, a music CD, etc.
 - Do use:
 - radioactive decay
 - MD5 output of a series of video-capture frames of a lava lamp in action
 - amplified background noise, sampled

One Time Pad: Exchanging Pads

- The tricky part is exchanging the pad
 - If you are caught with a one time pad it is prima facie evidence of espionage
 - If the pad is copied then you're completely compromised
 - Peter Wright tells of breaking into soviet spies' houses and copying their pads then reading their messages
 - Make sure you give it to the right person!

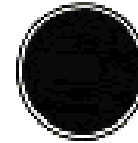
VENONA

- Soviets use one time pads to operate deep cover moles
 - Duplicates of pads were printed
 - Duplicates accidentally are used to secure communications for shipboard monitoring
 - A British code clerk recognizes patterns
 - For several years the British are able to piece together tantalizing bits of KGB communications

VENONA (Cont)

VENONA

~~TOP SECRET~~



USSR

Ref. Date: [REDACTED] (of 14/5/1964)

Issued: 18/10/1962

Copy No.: 301

MESSAGE

"DANAN", "LAD", SOURCE: INSTIGATORS FOR CONTACT AND CORRESPONDENCE (1942)

From: NEW YORK

To: MOSCOW

No.: 216

24th June 1942

To: VENONA(1)

In reply to com. 2301(a) and 2105(b).

"DANAN" (11) is at the present time in the company of his family which is in a hotel in BURENO ALIAS where open contacts

[3 groups unrecovered]

to get in touch with collaborators of the FELLOWCOUNTRYMEN[REDACTED] (111) [4 groups unrecovered] "LAD" (14) also in [CN ARGENTINA]. His home address is:

[Continued overleaf]

DES

- National Bureau of Standards Data Encryption Standard
 - 56-bit encryption algorithm
 - Now obsolete against devoted attackers
 - Still not too bad
 - Many many implementations available
 - Has withstood public scrutiny for 20+ years

DES modes

- ECB (Electronic CodeBook) - each block always encrypted the same way
- CBC (Cipher Block Chaining) - each block encrypted with information from previous block or initialization vector
- CFB (Cipher FeedBack) - stream mode
- OFB (Output FeedBack) - chaining stream mode

Basic DES Blocks

```
des_cblock          kblock;
des_keyschedule    ksched;
char                kp[512];
char                jnk[8], ojnkn[8];
/* no error checking - this is an example */
fprintf(stderr, "? ", );
fgets(kp, sizeof(kp), stdin);
strcpy(jnk, "spamit!");
des_string_to_key(kp, k);
des_set_key(kblock, ksched);
des_ecb_encrypt(jnk, ojnkn, ksched, DES_ENCRYPT);
```

3-DES

- Use DES to repeatedly encipher with different keys
- Significantly improves over the strength of plain DES
- Encrypt with Key1
- Decrypt with Key2
- Encrypt with Key3

IDEA

- International Data Encryption Algorithm
- 128-bit encryption designed to be fast on modern processors
- Has been available for 8+ years no cracks yet
- Has similar modes to DES

Hashes & One-Way Functions

- Cryptographic hashes take input and “fold” it into an irreversible (we hope) large number based on the total information contained in the message
- Ideally a single bit change in the message will result in a complete randomization of the hash code
 - I.e., 50% of the hash code’s bits will flip

MD5

- MD5 is very popular cryptographic hash function
 - High performance
 - Freely available
 - Beginning to be replaced with SHA-1 (secure hash algorithm 1) which is better
 - Very easy to use

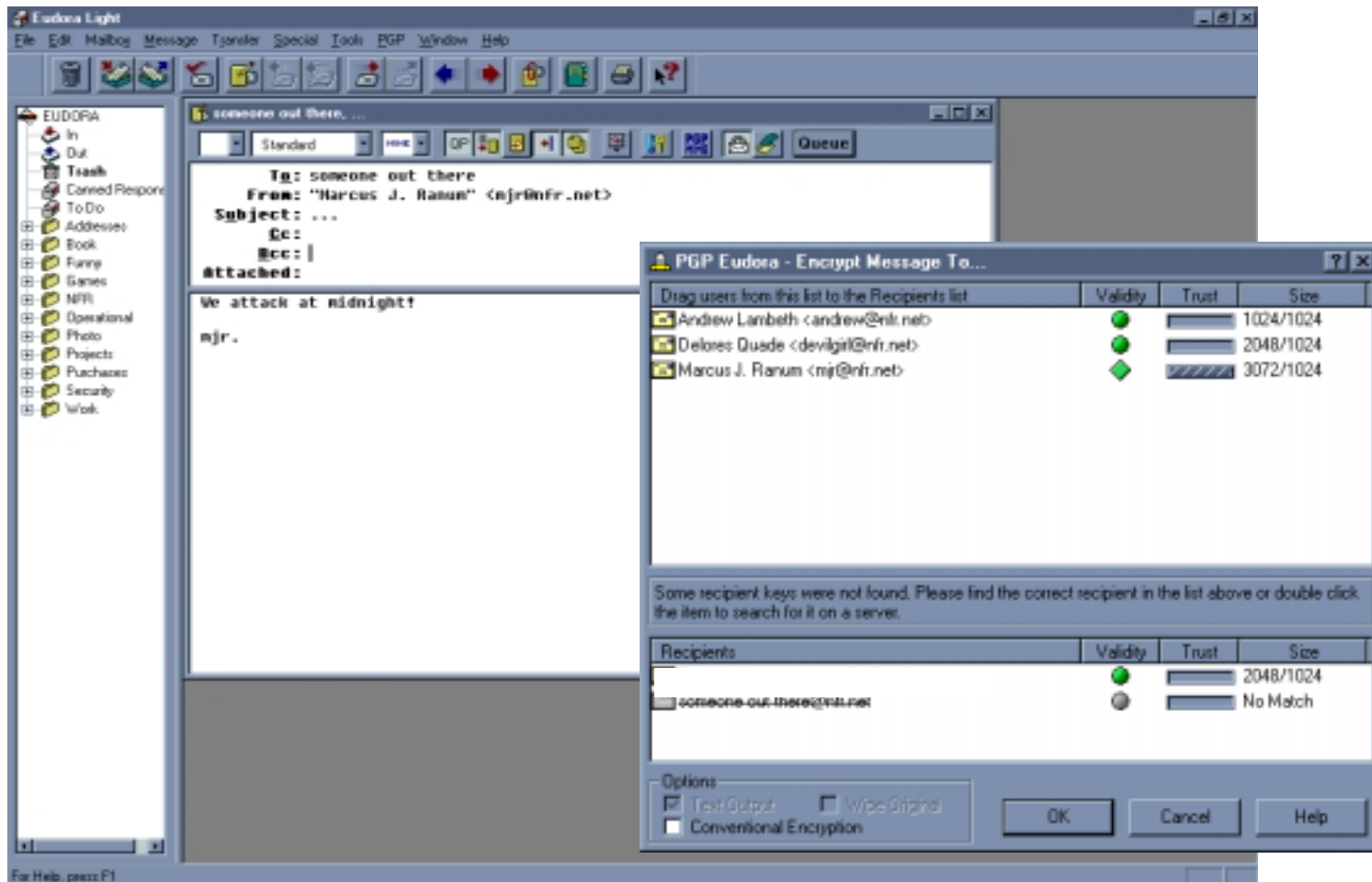
MD5 In Action

```
MD5_CTX      ct;  
char         out[16];  
  
extern char *hex(char *);  
  
foo(char *s) {  
    MD5_INIT(&ct);  
    MD5_Update(&ct,s,strlen(s)+1);  
    MD5_Final(out,&ct);  
    printf("MD5(\"%s\") is %s\n",s,hex(out));  
}
```

PGP

- Pretty Good Privacy
 - Widely used and widely available file/Email encryption software
 - Has been integrated into a number of Email packages as a plug-in
 - Very easy to use
 - Just click to encrypt!
 - There is no excuse for not using it

PGP / Mailer Integration



PGP messages

- PGP messages combine many algorithms:
 - IDEA for message body encryption
 - MD5 for message body hash/integrity check
 - RSA for key exchange of message body IDEA key
 - RSA for signature of MD5 hash code

PGP: Creating a public key

```
C:\mjr\ARCHIVES\old-bin> pgp -kg  
Pretty Good Privacy(tm) 2.6 - Public-key encryption for the masses.  
(c) 1990-1994 Philip Zimmermann, Phil's Pretty Good Software. 23 May 94  
Distributed by the Massachusetts Institute of Technology. Uses RSAREF.  
Export of this software may be restricted by the U.S. government.  
Current time: 1998/06/04 10:50 GMT  
Pick your RSA key size:  
  1)  512 bits- Low commercial grade, fast but less secure  
  2)  768 bits- High commercial grade, medium speed, good security  
  3) 1024 bits- "Military" grade, slow, highest security  
Choose 1, 2, or 3, or enter desired number of bits: 3  
Generating an RSA key with a 1024-bit modulus.
```

You need a user ID for your public key. The desired form for this user ID is your name, followed by your E-mail address enclosed in <angle brackets>, if you have an E-mail address.

For example: John Q. Smith <12345.6789@compuserve.com>

Enter a user ID for your public key:

foo@bar.com

PGP: Signing Someone's Key

```
C:\mjr\ARCHIVES\old-bin> pgp -ks
```

```
[...]
```

```
A user ID is required to select the public key you want to sign.
```

```
Enter the public key's user ID: jds@math.okstate.edu
```

```
A secret key is required to make a signature.
```

```
You specified no user ID to select your secret key,  
so the default user ID and key will be the most recently  
added key on your secret keyring.
```

```
Looking for key for user 'jds@math.okstate.edu':
```

```
Key for user ID: Jennifer Smith <jds@math.okstate.edu>
```

```
512-bit key, Key ID 54BD8EE3, created 1994/03/30
```

```
READ CAREFULLY: Based on your own direct first-hand knowledge, are  
you absolutely certain that you are prepared to solemnly certify that  
the above public key actually belongs to the user specified by the  
above user ID (y/N)? Y
```

PGP: Adding New Keys

```
C:\mjr\ARCHIVES\old-bin> pgp \tmp\ciac_pgp
```

```
[...]
```

```
File contains key(s). Contents follow...
```

```
Key ring: '\tmp\ciac_pgp.$00'
```

Type	bits/keyID	Date	User ID
pub	1024/6CCB7419	1995/02/06	CIAC <ciac@llnl.gov>
sig	2334DE91		(Unknown signator, can't be checked)
sig	5BE1616D		(Unknown signator, can't be checked)
sig	8395C749		(Unknown signator, can't be checked)
sig	FC0C02D5		(Unknown signator, can't be checked)
sig	4C33BA15		(Unknown signator, can't be checked)
sig	07567455		(Unknown signator, can't be checked)
sig	8015A109		(Unknown signator, can't be checked)
sig	6CCB7419		CIAC <ciac@llnl.gov>

```
1 matching key found.
```

```
Do you want to add this keyfile to keyring 'c:\mjr\archives\old-bin\pub  
(y/N)? Y
```

PGP: Signing documents

```
C:\mjr\ARCHIVES\old-bin> pgp -s foo
```

```
[...]
```

```
A secret key is required to make a signature.
```

```
You specified no user ID to select your secret key,  
so the default user ID and key will be the most recently  
added key on your secret keyring.
```

```
You need a pass phrase to unlock your RSA secret key.
```

```
Key for user ID "Marcus J. Ranum Laptop/Military Grade Key <mjr>"
```

```
Enter pass phrase: [XXXXXXXXXXXXXXXXXXXXXXX]
```

```
Pass phrase is good.
```

```
Key for user ID: Marcus J. Ranum Laptop/Military Grade Key <mjr>
```

```
1024-bit key, Key ID 9ACE2239, created 1994/09/16
```

```
Key is disabled.
```

```
Just a moment....
```

```
Clear signature file: foo.asc
```


PGP: Signing documents *(cont)*

```
C:\mjr\ARCHIVES\old-bin>type foo.asc
```

```
-----BEGIN PGP SIGNED MESSAGE-----
```

```
this is a test
```

```
-----BEGIN PGP MESSAGE, PART 01/00-----
```

```
Version: 2.6
```

```
iQCVAwUBNXaDgBLOs56aziI5AQELAgQAwgej6copoQBingUi5dY6q5kbNnSus4TL  
2Q5Vh+hhD+z/M1dVAK9JIZ/nRcxSXI+VezjIA/HHbU3zITqejmvAoA6bi+2l/rsT  
oC5TgM/Os+n9JyQnxR89L41K7aq8pR0a/dbDVJyixU2/+s8dwlTW5m8UAx2psLuv  
bxIoIyIiW1U=
```

```
=GZXF
```

```
-----END PGP MESSAGE, PART 00/00-----
```

```
C:\mjr\ARCHIVES\old-bin>
```

PGP: Encrypting documents

```
C:\mjr\ARCHIVES\old-bin> pgp -team bar.txt jds@math.okstate.edu  
Pretty Good Privacy(tm) 2.6 - Public-key encryption for the masses.  
(c) 1990-1994 Philip Zimmermann, Phil's Pretty Good Software. 23 May 94  
Distributed by the Massachusetts Institute of Technology. Uses RSAREF.  
Export of this software may be restricted by the U.S. government.  
Current time: 1998/06/04 11:29 GMT
```

```
Recipients' public key(s) will be used to encrypt.  
Key for user ID: Jennifer Smith <jds@math.okstate.edu>  
512-bit key, Key ID 54BD8EE3, created 1994/03/30  
.  
Transport armor files:
```

PGP: Encrypting Documents

(cont)

```
C:\mjr\ARCHIVES\old-bin>type bar.asc
```

```
-----BEGIN PGP MESSAGE, PART 01/00-----
```

```
Version: 2.6
```

```
hEwDDTkpflS9juMBAgChWIN/2t8jyjUDmF83eGanyRXuxmxkmafniCCplm/yaql  
mOobEYJv7TK3ROTraf+J2CcgVLZvvKWDDrz2GqT7pgAAADdqIIY/VsnSumzn1CLz  
J3II3IOVdQfWT+RXxIl68XJJJgEDuBqIltPAnp7i5+nQHGIImKMWyeIag  
=b6MP
```

```
-----END PGP MESSAGE, PART 00/00-----
```

```
C:\mjr\ARCHIVES\old-bin>
```

PGP: Decrypting Documents

```
C:\mjr\ARCHIVES\old-bin> pgp foo.asc
```

```
Pretty Good Privacy(tm) 2.6 - Public-key encryption for the masses.  
(c) 1990-1994 Philip Zimmermann, Phil's Pretty Good Software. 23 May 94  
Distributed by the Massachusetts Institute of Technology. Uses RSAREF.  
Export of this software may be restricted by the U.S. government.  
Current time: 1998/06/04 11:41 GMT
```

```
File is encrypted. Secret key is required to read it.  
Key for user ID: Marcus J. Ranum Laptop/Military Grade Key <mjr>  
1024-bit key, Key ID 9ACE2239, created 1994/09/16
```

```
You need a pass phrase to unlock your RSA secret key.  
Enter pass phrase: [XXXXXXXXXXXXXXXXXXXXX]  
Pass phrase is good. Just a moment.....
```

```
This message is marked "For your eyes only". Display now (Y/n)?  
[...]
```

PGP: File Encryption

```
C:\mjr\ARCHIVES\old-bin> pgp -c foo.txt  
Pretty Good Privacy(tm) 2.6 - Public-key encryption for the masses.  
(c) 1990-1994 Philip Zimmermann, Phil's Pretty Good Software. 23 May 94  
Distributed by the Massachusetts Institute of Technology. Uses RSAREF.  
Export of this software may be restricted by the U.S. government.  
Current time: 1998/06/04 11:32 GMT
```

```
You need a pass phrase to encrypt the file.  
Enter pass phrase: [XXXXXXXXXXXXXXXXXXXX]  
Enter same pass phrase again: [XXXXXXXXXXXXXXXXXXXX]  
Just a moment....  
Transport armor files:  
C:\mjr\ARCHIVES\old-bin>
```

```
C:\mjr\ARCHIVES\old-bin>
```

PGP: Creative Uses

- PGP can be used to create self-checking high-integrity message-grams
 - Use for remote management
 - Email to address which calls a script that checks a PGP signature on a document
 - If the document signature is OK then execute the command (or just use the message body as shell input!)

Cryptographic File System

- CFS is a user-mode NFS server for UNIX that overlays cryptographic services onto the file system
- Works on most versions of UNIX (Solaris, BSD, etc.)
- Includes utility programs for attaching and detaching, manipulating directories, etc.

Using CFS

- Typically in system startup:

```
if [ -x /usr/local/etc/cfsd ]; then
    /usr/local/etc/cfsd && \
        /etc/mount -o port=3049,intr localhost:/null /crypt
fi
```

- This starts the daemon and then NFS mounts it via the loopback interface
- Then attach filesystems with `cattach`

Secure File System

- Dos/Windows filesystem driver by Peter Gutmann
 - www.cs.auckland.ac.nz/~pgut001/sfs/index.html
- Creates multiple virtual encrypted volumes on normal media
 - Works with most drives, including floppy disks
 - Includes enhanced SCSI drivers
 - Can quickly unmount and forget cryptokeys for drives by pressing a hotkey

Steganography

- Steganography is a valuable tool for wanna-be spies
 - It's the electronic equivalent of hiding a microdot on a postcard: hide your data within other innocuous data
 - Hide your ciphertext so They don't know you're using cryptography and are therefore a suspect worth watching

Steganography *(cont)*

- Romans used to implement this by shaving a slave's head, tattooing a message on it, letting his hair grow back, and sending him to deliver the "message"
 - Message possibly was pre-enciphered with Caesar shift (ROT-13)



Steganography: Example

```
C:\tmp>type steg.txt
```

In an ideal world we would all be able to openly send encrypted mail or files to each other with no fear of reprisals. However there are often cases when this is not possible, either because you are working for a company that does not allow encrypted email or perhaps the local government does not approve of encrypted communication (a reality in some parts of the world). This is where steganography can come into play.

```
C:\tmp>snow -C -m "attack@11:00" -p "passphrase" steg.txt out.txt
```

```
Compressed by 18.75%
```

```
Message used approximately 69.64% of available space.
```

```
C:\tmp>
```

Steganography: Example *(cont)*

```
C:\tmp>type out.txt
```

In an ideal world we would all be able to openly send encrypted mail or files to each other with no fear of reprisals. However there are often cases when this is not possible, either because you are working for a company that does not allow encrypted email or perhaps the local government does not approve of encrypted communication (a reality in some parts of the world). This is where steganography can come into play.

```
C:\tmp>snow -C -p "passphrase" out.TXT
```

```
attack@11:00
```

```
C:\tmp>
```

Steganography: Example *(cont)*

- In vi it looks like (with “set list”):

```
^I      ^I  ^I^I  ^I   ^I^I  ^I   ^I   $  
In an ideal world we would all be able to openly send ^I  
encrypted mail or files to each other with no fear of ^I  
reprisals. However there are often cases when this is ^I  
not possible, either because you are working for a^I  ^I  
company that does not allow encrypted email or perhaps  
the local government does not approve of encrypted$  
communication (a reality in some parts of the world).$  
This is where steganography can come into play.$
```

Steganography *(cont)*

- Loads of steganographic tools on:
members.iquest.net/~mrmil/stego.html
- Hide data in:
 - .wav files
 - gzip files
 - turn PGP files into “english text”
 - .jpg or .gif
 - and many more!

Steganography *(cont)*

- Very cool JAVA program for steganography!
www.stego.com

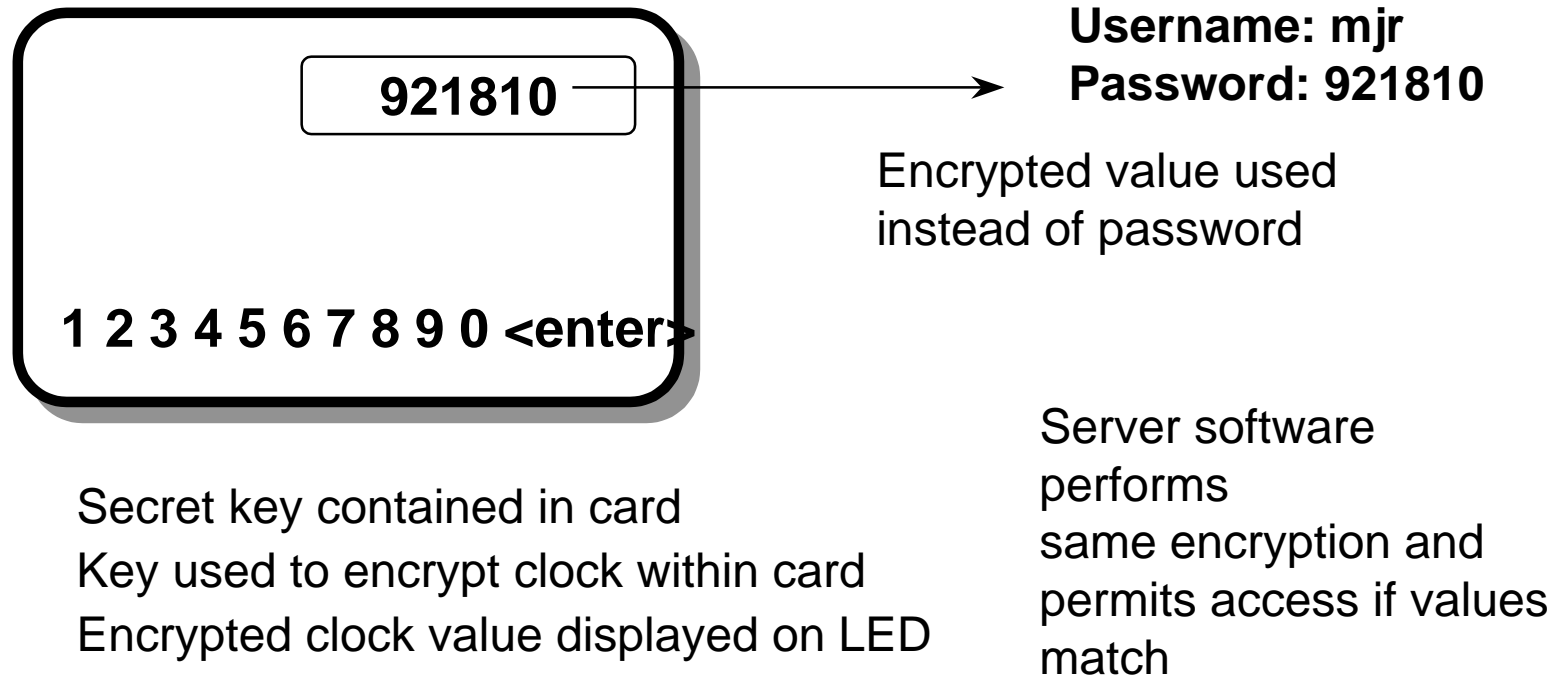
Authentication

- Why?
 - Know who you are dealing with
 - (Normally done in the “login” process)
- Authentication is a huge problem in secure communications
 - ***Who*** are you communicating securely ***with?***

Authentication

- Weak - Trusts the network
- Strong - Relies on protocols that do not require transmitting secrets over the network
- Any authentication worth using should be able to resist an attacker even if the attacker can monitor the entire login
- Passwords are obsolete

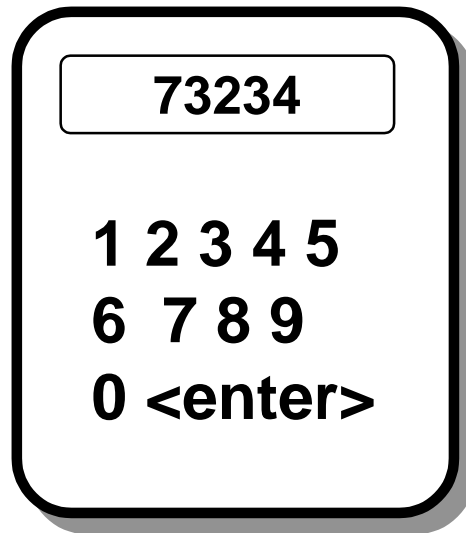
Authentication: Time Tokens



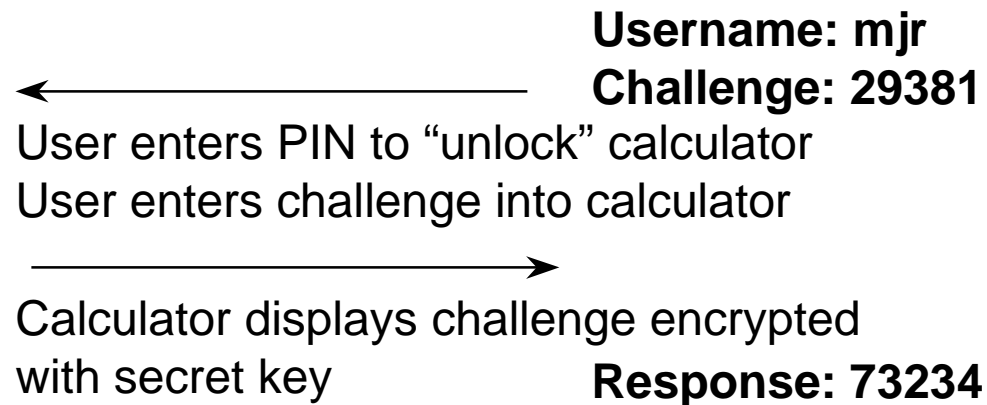
Time Tokens

- You could build your own out of a palm pilot with a minimum of coding
 - Store a secret key
 - Encrypt (time - (time % 60))
 - Transmit that
 - Server has key and time, does comparison
 - Check on both “sides” to adjust clock drift
 - Store clock drift value for best results

Authentication: Challenge/Response



Secret key contained in calculator

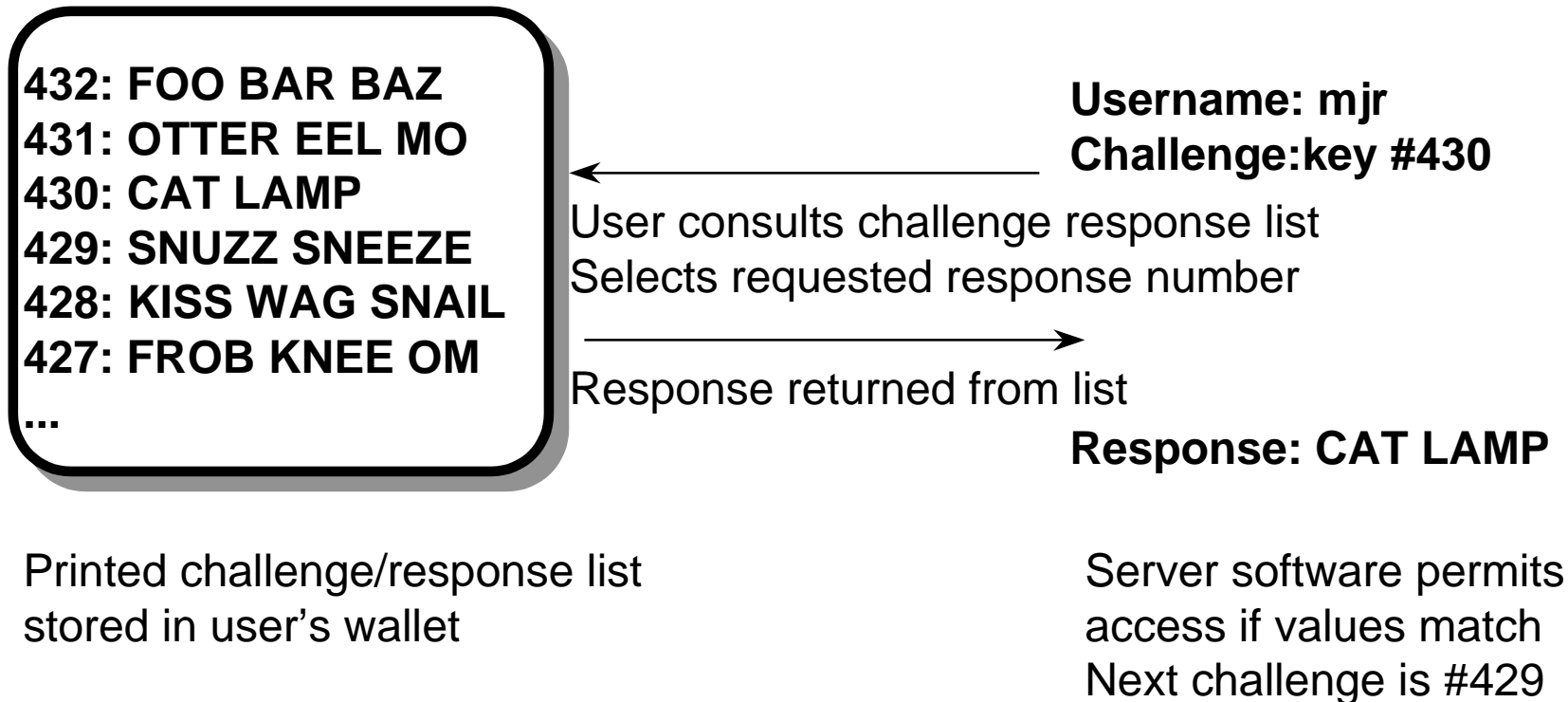


Server software performs same encryption and permits access if values match

Challenge/Response

- Build your own challenge response trivially using a palm pilot
 - Firewall toolkit included authentication module compatible with *assurenets pathways secure net key*

Authentication: Software



Software

- Use OPIE
 - Available from
<ftp://thumper.bellcore.com/pub/nmh/nrl/>
- **WARNING:** S/Key is a pain in the neck to use!!!!

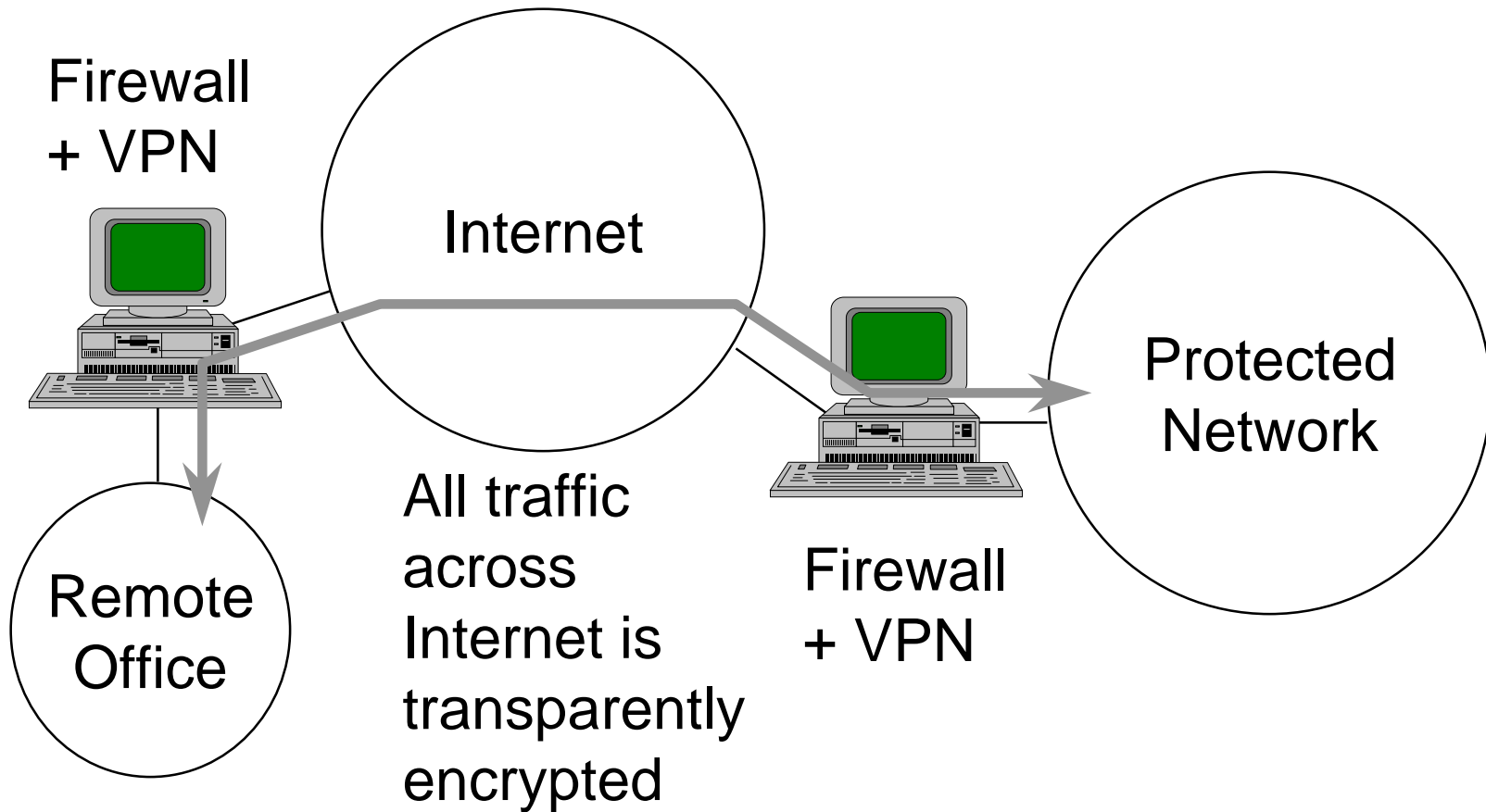
Authentication: Summary

- These days separate authentication (as distinct from encryption / key exchange) is becoming obsolete
 - For ease of use rely on something like ssh or a VPN that integrates authentication behind an apparently simple “Password:” request

Virtual Private Networks (VPNs)

- VPNs treat the Internet as cheap backbone
- Encryption provides integrity and privacy
- Encryption *does not* provide access control
- Encryption *does not* guarantee reliability

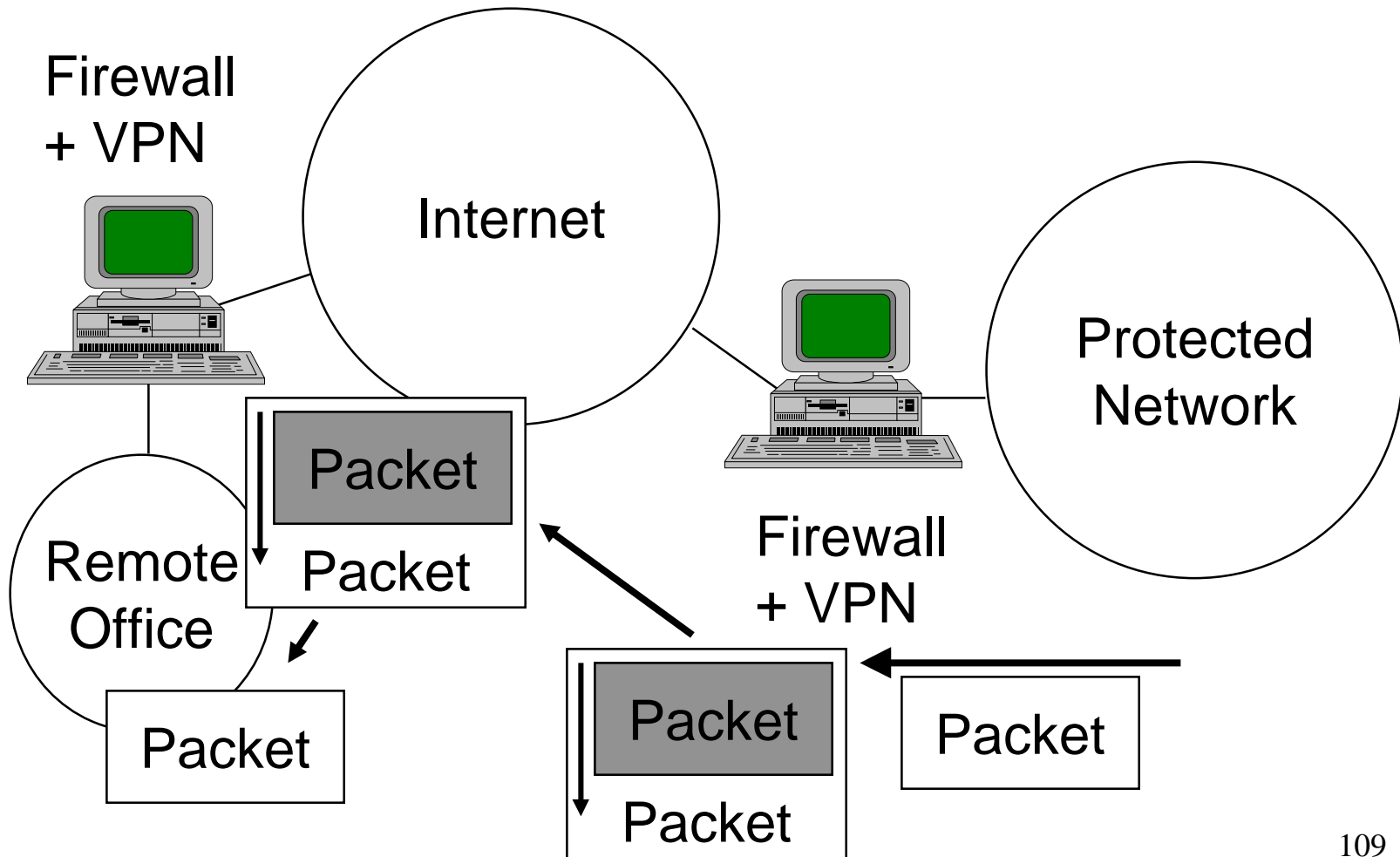
Virtual Private Network



Packet VPNs

- Packet VPNs encode one packet inside another and transmit it to gateway
- Remote gateway verifies packet's integrity then decrypts it and transmits it on the local network
- Application independent
- May be multi protocol

Packet VPN



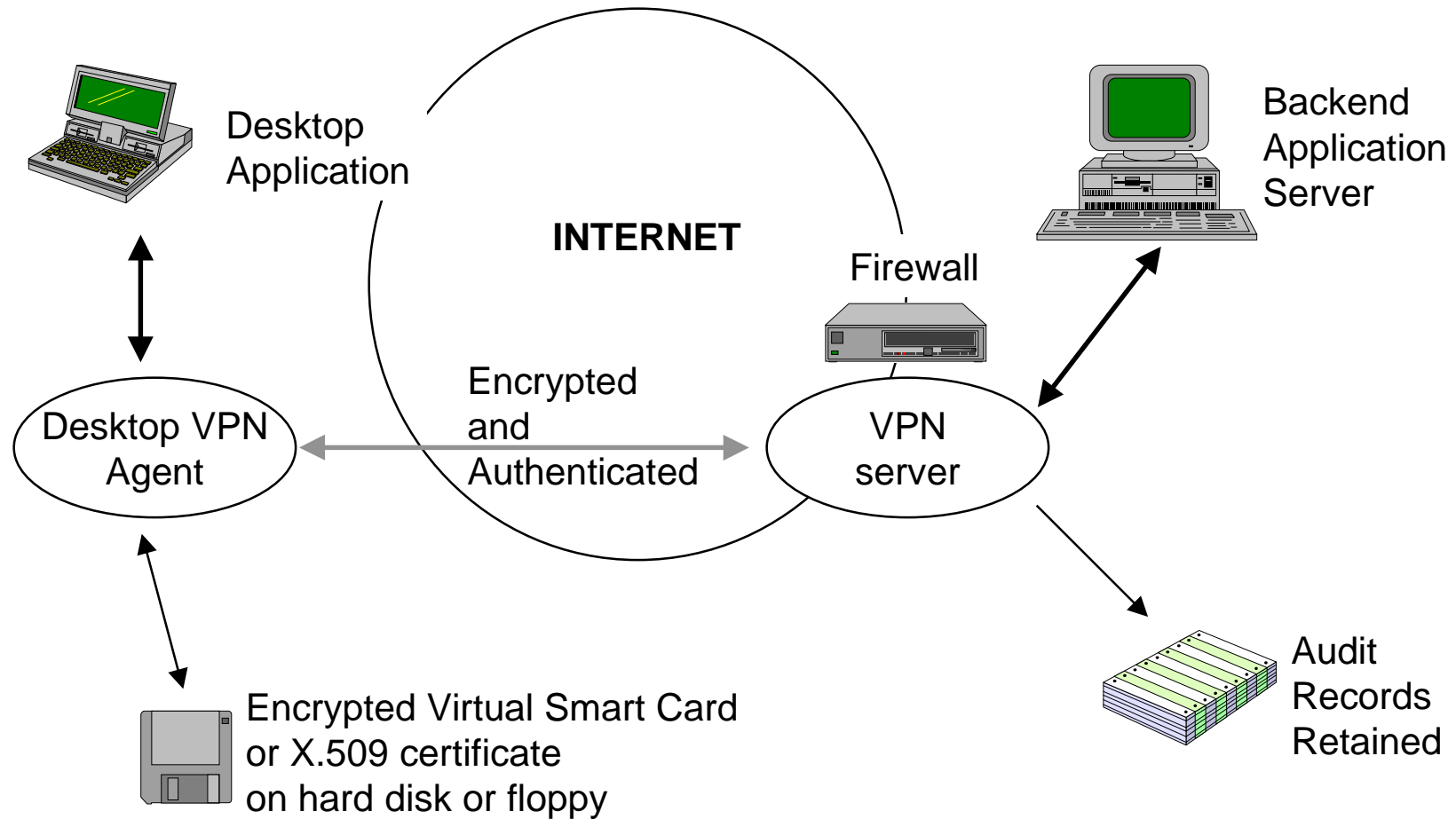
Packet VPNs

- IPSEC
- SKIP
- Jillions of proprietary solutions
 - Alta Vista tunnel
 - Checkpoint VPN-1
 - Raptor Remote
 - Network Systems Corp, “sleeves”
 - ... etc.

Application VPNs

- Like a firewall proxy that has been torn in half
 - One piece runs on desktop and negotiates with a server on the firewall
 - May not work with all applications
 - But does not require modifications to IP stack

Application VPNs



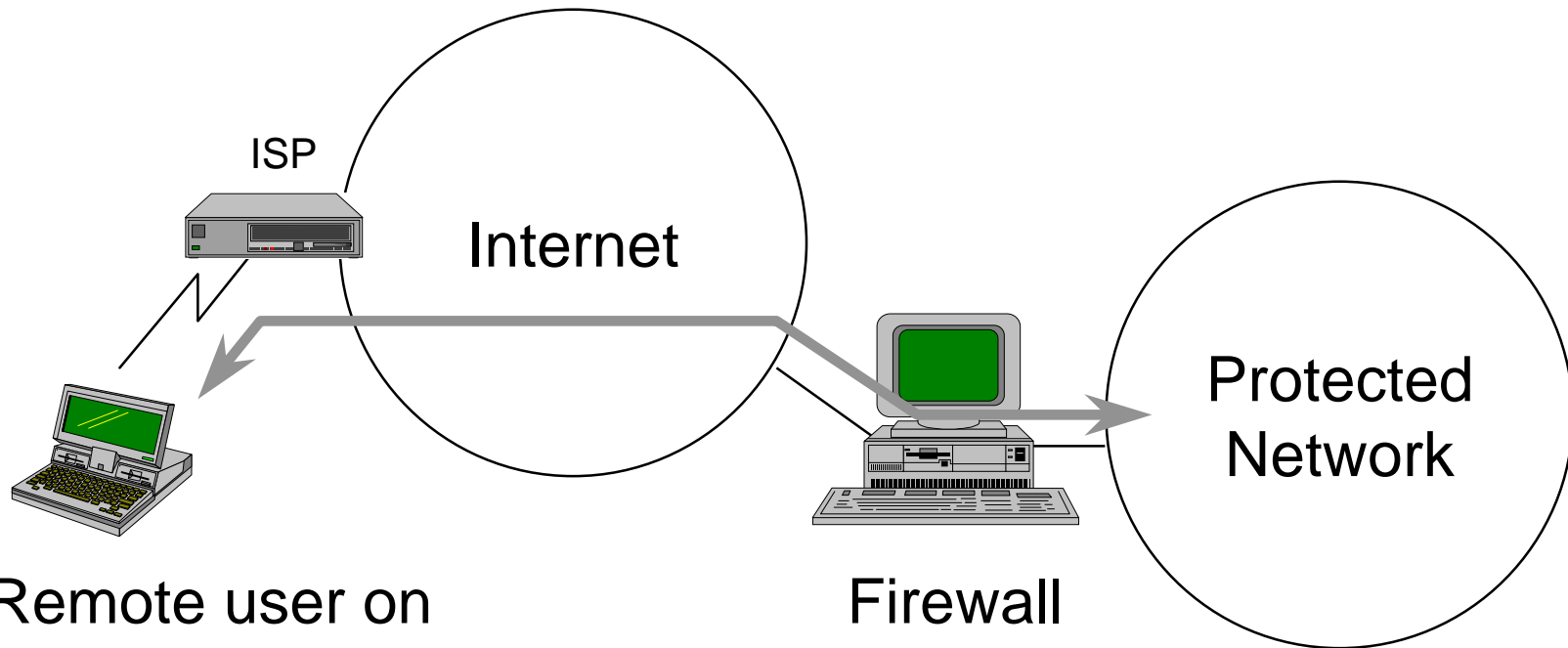
Application VPNs

- Standards Track:
 - SOCKS5
 - SSH
- Jillions of proprietary solutions
 - Timestep
 - V-One Smartgate
 - Microsoft proxy / PPTP
 - ... etc.

Dynamic VPN Membership

- Permit systems to become temporary members of VPN regardless of location
 - Excellent solution for wandering staff/remote access/business partners

Dynamic VPN



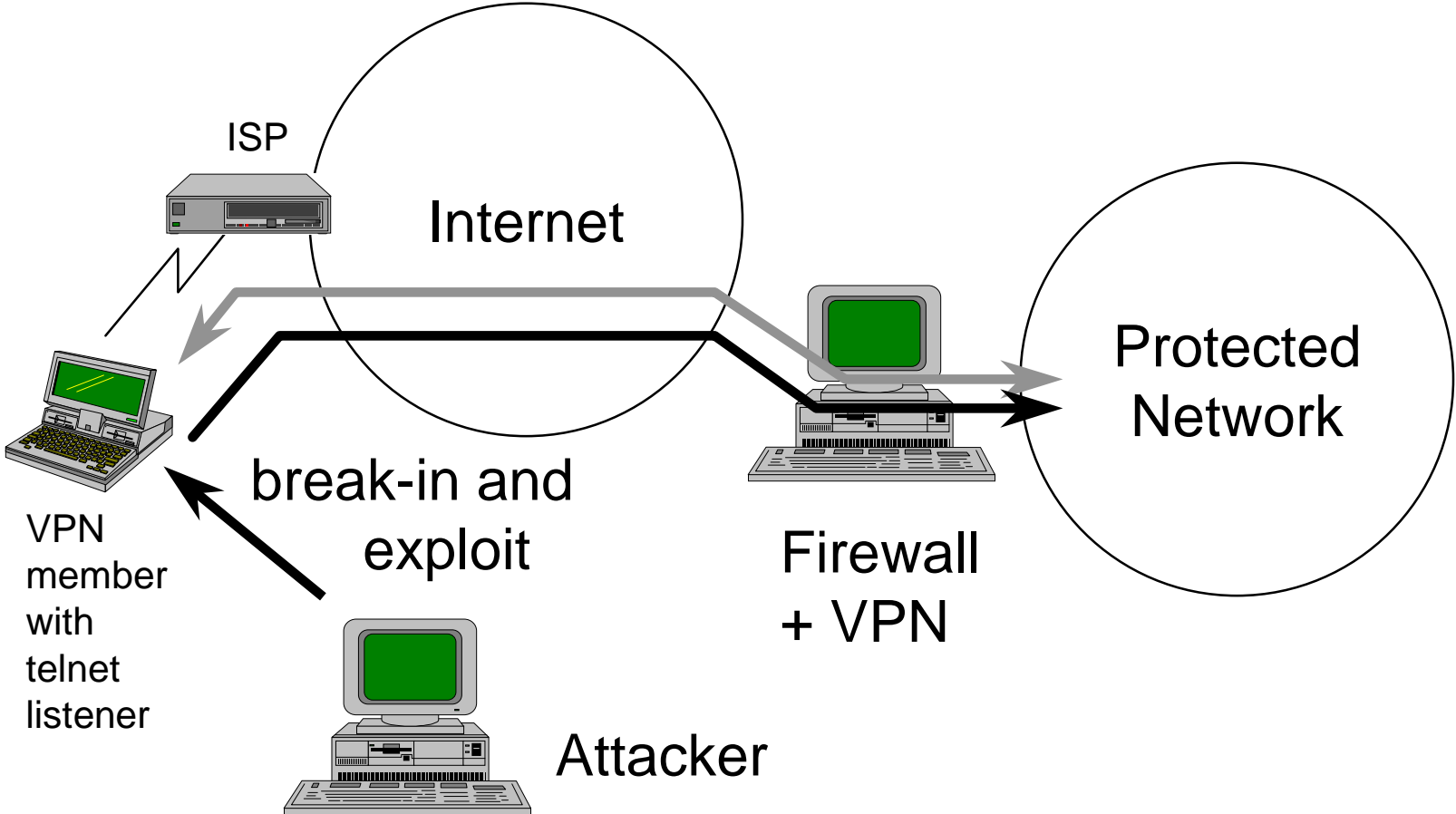
Remote user on laptop becomes a member of VPN through dialup connection

Firewall + VPN

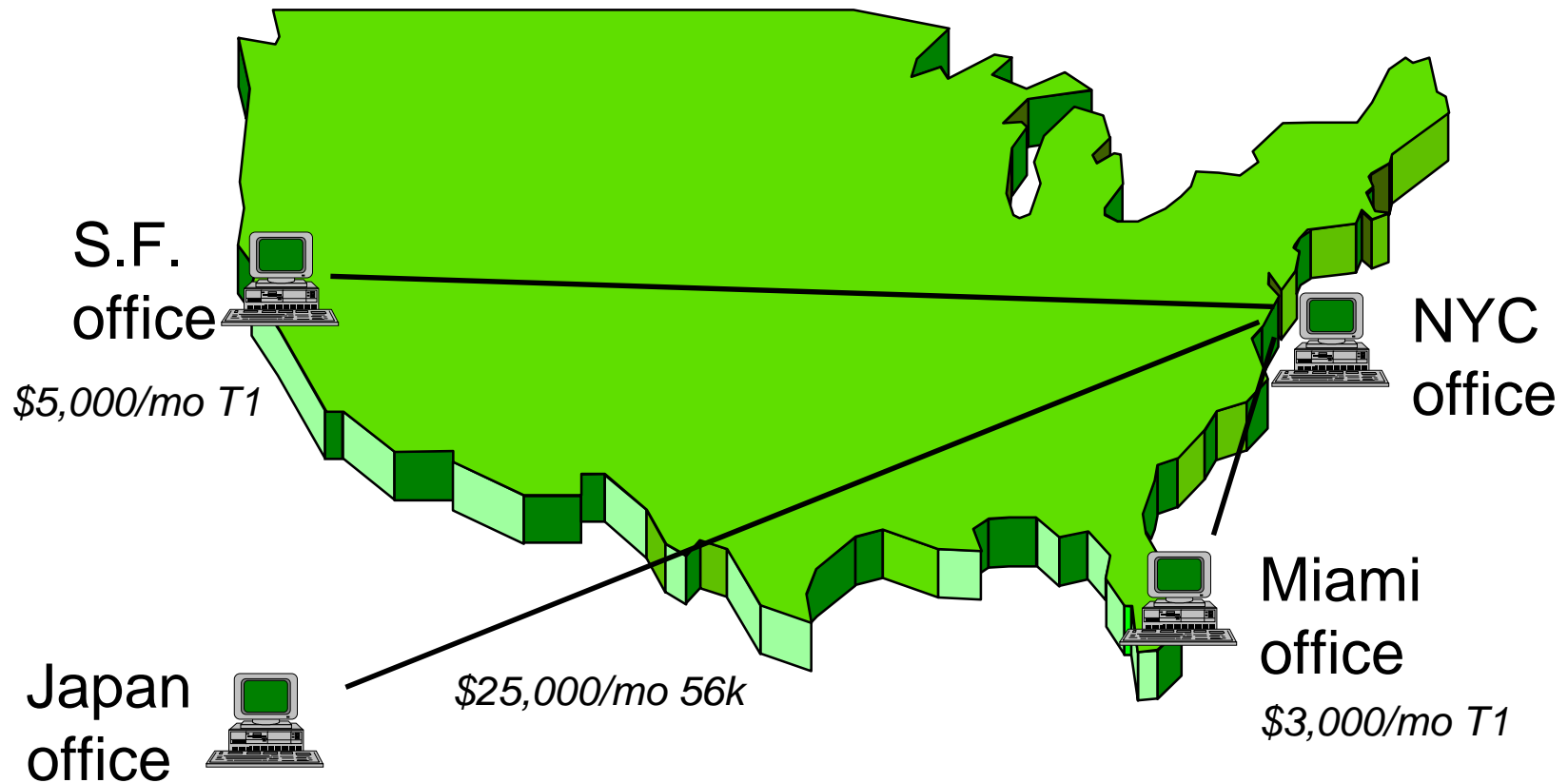
Dynamic VPN Membership *(cont)*

- When establishing remote VPN members it is important that the end-point node is secure enough
 - VPN member may become a jump-off point for attack
 - VPN member may accidentally route traffic into protected network

Dynamic VPN Membership *(cont)*

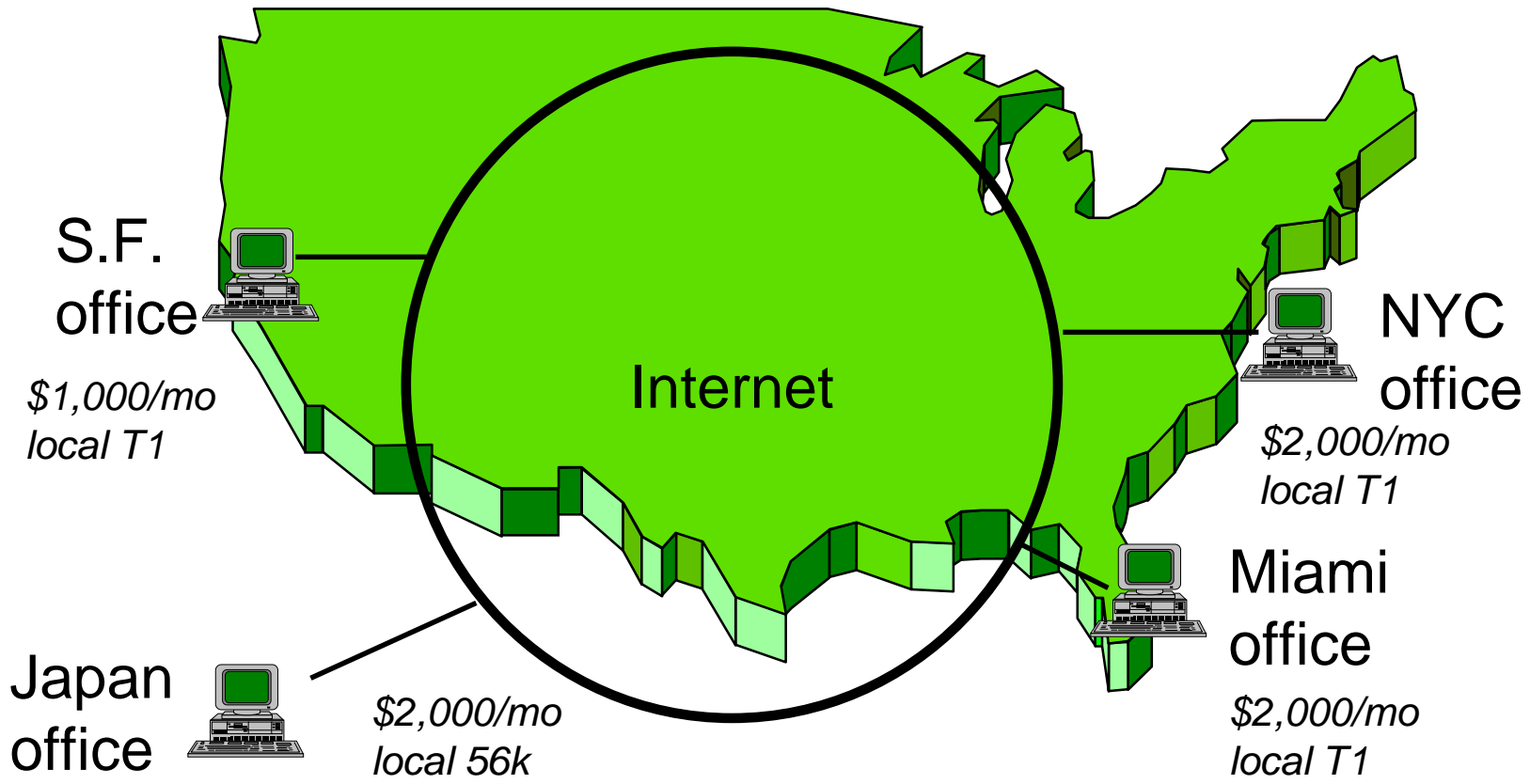


VPN Cost Savings



(All numbers W.A.G.'s)

VPN Cost Savings

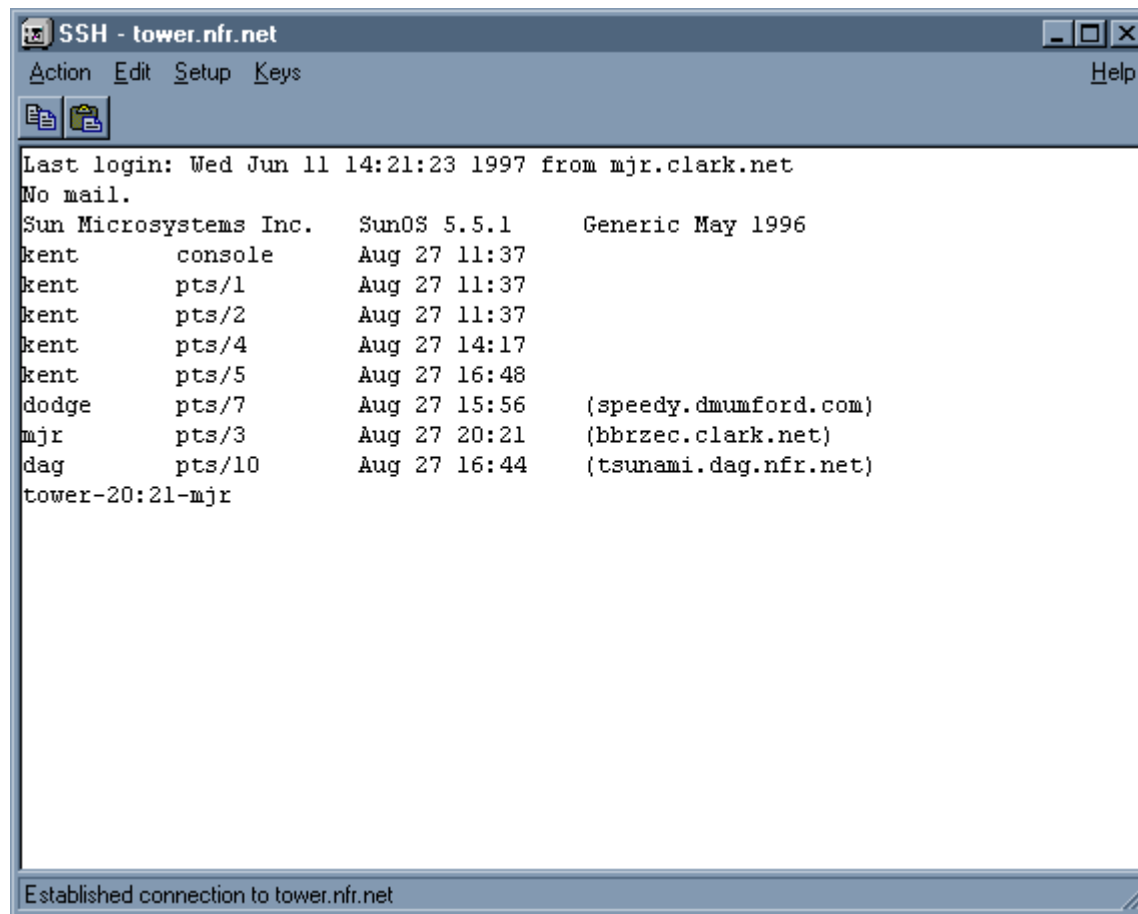


(All numbers W.A.G.'s)

SSH

- SSH is a popular application VPN
 - Source for UNIX and a UNIX server is available for free
 - A Windows client is available for a fee
 - Free windows clients are appearing
 - public.srce.hr/~cigaly/ssh/
 - <http://www.zip.com.cw/~roca/ttssh.html>
 - Can use RSA / certificates for authentication, or passwords

SSH / Win32



```
SSH - tower.nfr.net
Action Edit Setup Keys Help
Last login: Wed Jun 11 14:21:23 1997 from mjr.clark.net
No mail.
Sun Microsystems Inc. SunOS 5.5.1 Generic May 1996
kent console Aug 27 11:37
kent pts/1 Aug 27 11:37
kent pts/2 Aug 27 11:37
kent pts/4 Aug 27 14:17
kent pts/5 Aug 27 16:48
dodge pts/7 Aug 27 15:56 (speedy.dmumford.com)
mjr pts/3 Aug 27 20:21 (bbrzec.clark.net)
dag pts/10 Aug 27 16:44 (tsunami.dag.nfr.net)
tower-20:21-mjr

Established connection to tower.nfr.net
```

Socks

- Socks includes sources for a daemon
 - Driver programs
 - Application side APIs
 - Winsock shims are available
(hummingbird.com
www.hummingbird.com/products/socks/)
- Available from:
<ftp://ftp.nec.com/pub/socks/>

IPSEC

- IPSEC is the IETF's standard for IP encryption and authentication
 - It is not widely adopted
 - It has taken forever to produce
 - Vendors are producing incompatible (or no) versions
 - Only recently it's starting to look viable

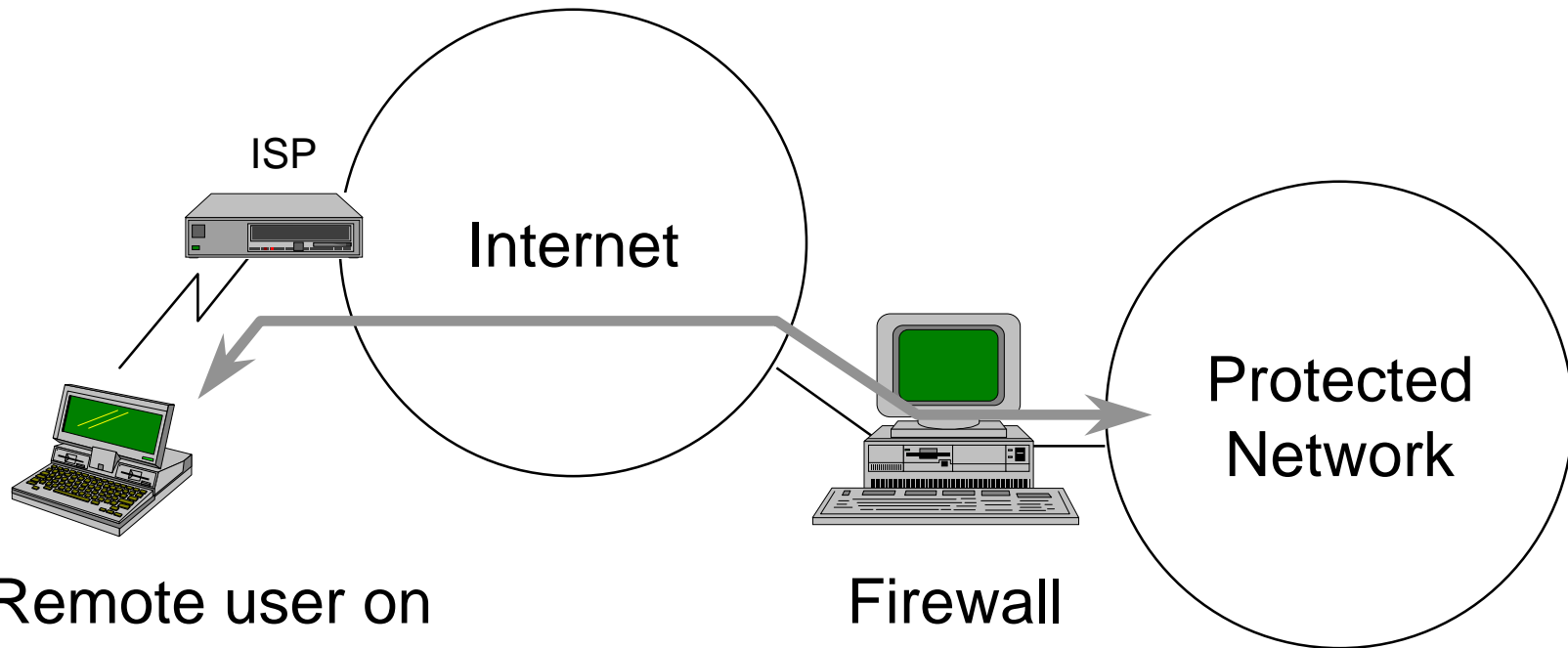
IPSEC *(cont)*

- Right now single-vendor solutions are the only thing that's guaranteed to work
 - This (should) change in the next year or so

Dynamic VPN Membership

- Permit systems to become temporary members of VPN regardless of location
 - Excellent solution for wandering staff/remote access/business partners

Dynamic VPN



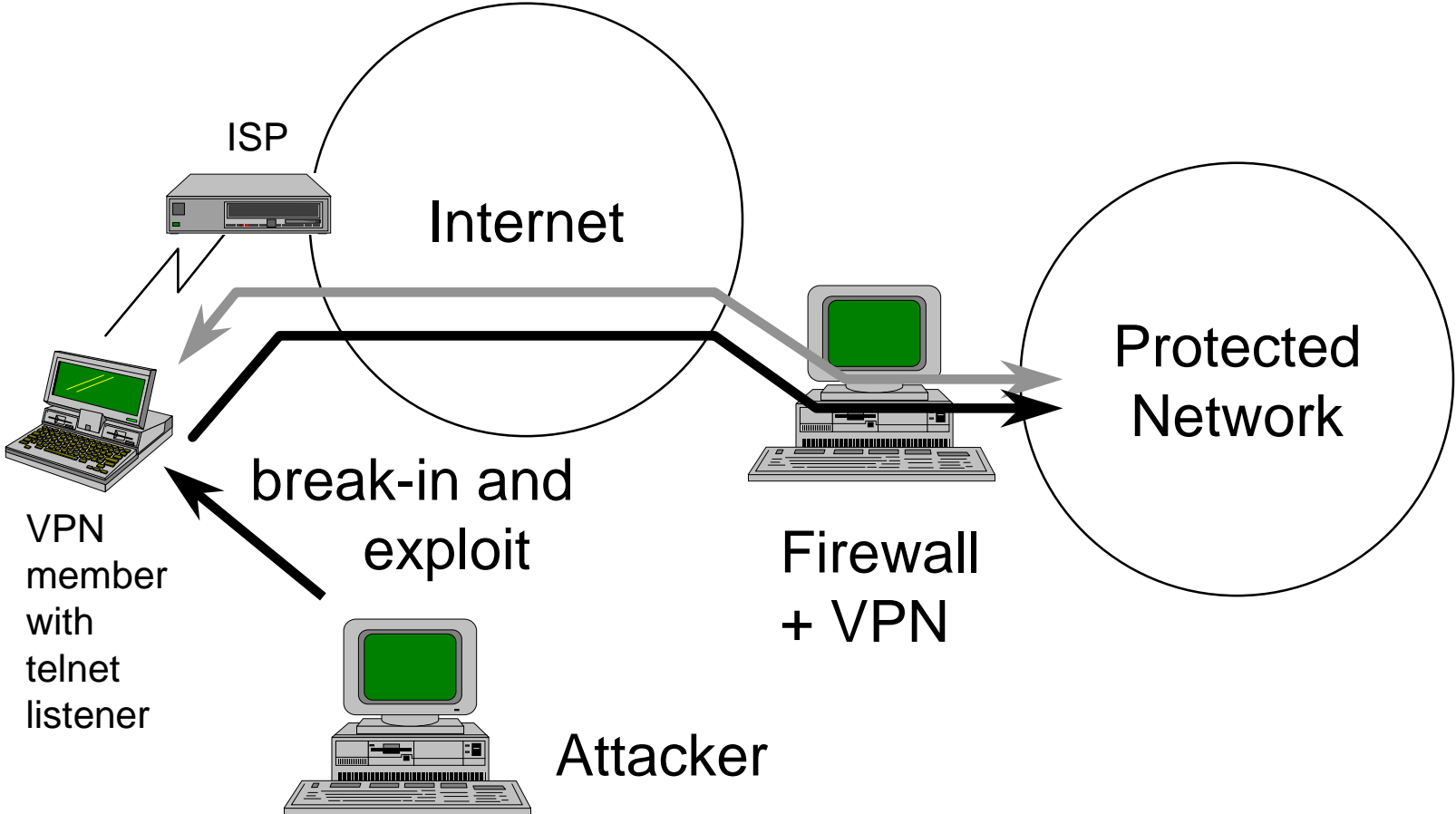
Remote user on laptop becomes a member of VPN through dialup connection

Firewall + VPN

Dynamic VPN Membership *(cont)*

- When establishing remote VPN members it is important that the end-point node is secure enough
 - VPN member may become a jump-off point for attack
 - VPN member may accidentally route traffic into protected network

Dynamic VPN Membership *(cont)*



Building a VPN

- You can build a VPN with scrap systems for under \$450 a site!
 - Capable of handling T1+ speeds
 - Uses imported/exported encryption (SSH)
 - FREE except for the hardware
 - P200mmx w/1gb disk
 - Linux/BSDI/OpenBSD/FreeBSD/whatever
 - Network card

Building a VPN *(cont)*

- This idea appears to have originated with Olaf Titz
 - Subsequent enhancements by Steve Berry and Thor Simon
- This is a simple refinement over early VPNs (ca 1992) that used tunnel IP drivers

Building a VPN* *(cont)*

Pentium 233 running LINUX (appears not to be CPU bound)

Throughput Mb/S

Cypher		Mean
3des[4]		1.43
des	2.38	2.31
blowfish	2.87	2.78
none		3.25
non-VPN		7.90

Percent of
non-VPN

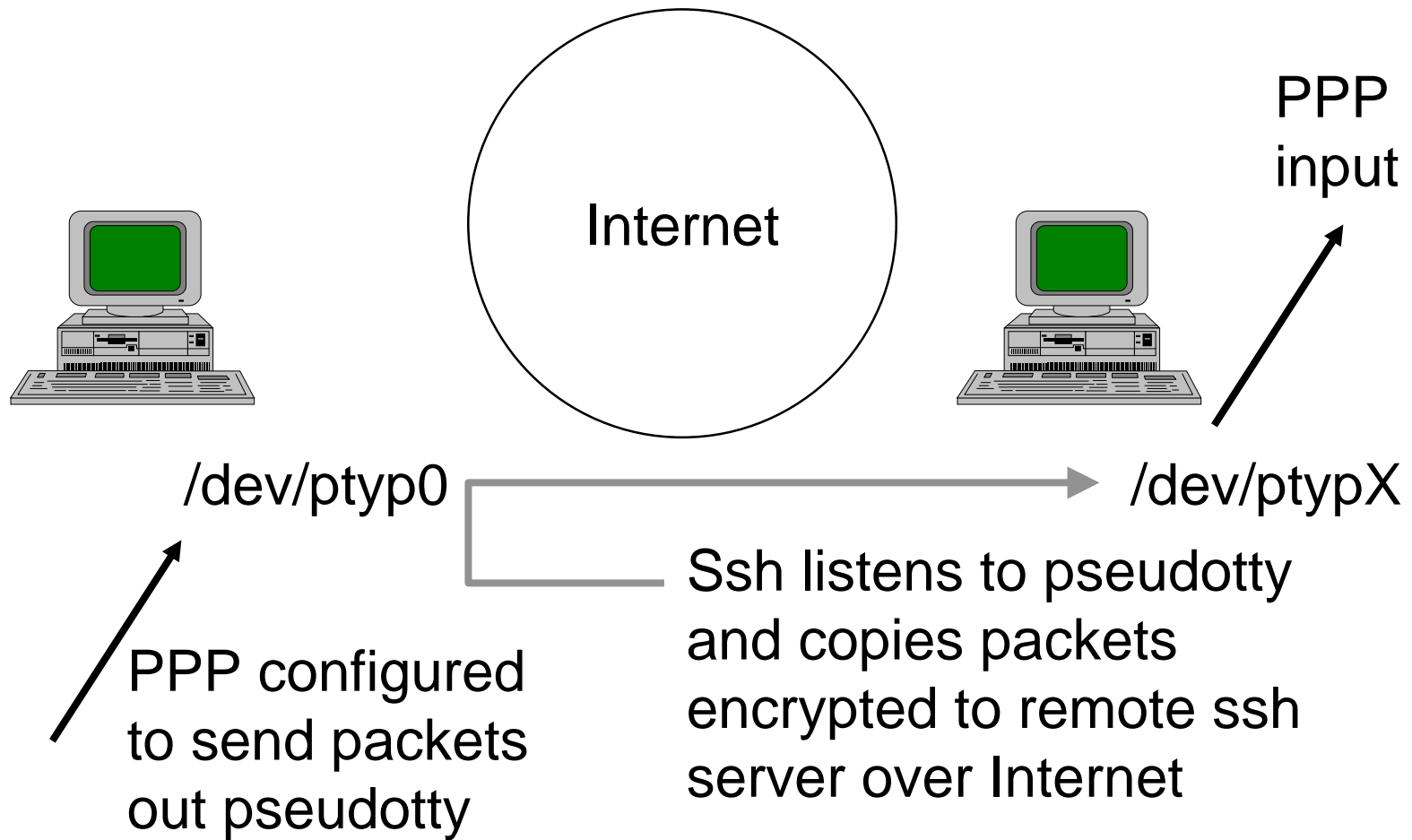
Cypher	Throughput
3des	18.1
des	30.1
blowfish	36.3
none	41.1
non-VPN	100

*Performance measures courtesy Steve Berry

Building a VPN *(cont)*

- The hack:
 - Allocate a pseudoterminal
 - Have a point-to-point crypto program listen to it on one side
 - Run pppd on the other side
 - Then set routing up to make the traffic go through the point-to-point tunnel

Homebrew VPN



Building a VPN *(cont)*

- Sample scripts for LINUX on:
 - www.clark.net/pub/mjr/vpn/
- Sample implementation is in perl
 - Most of the code deals with allocating pseudotys
- Should interoperate transparently between any UNIX systems that run PPP (!)

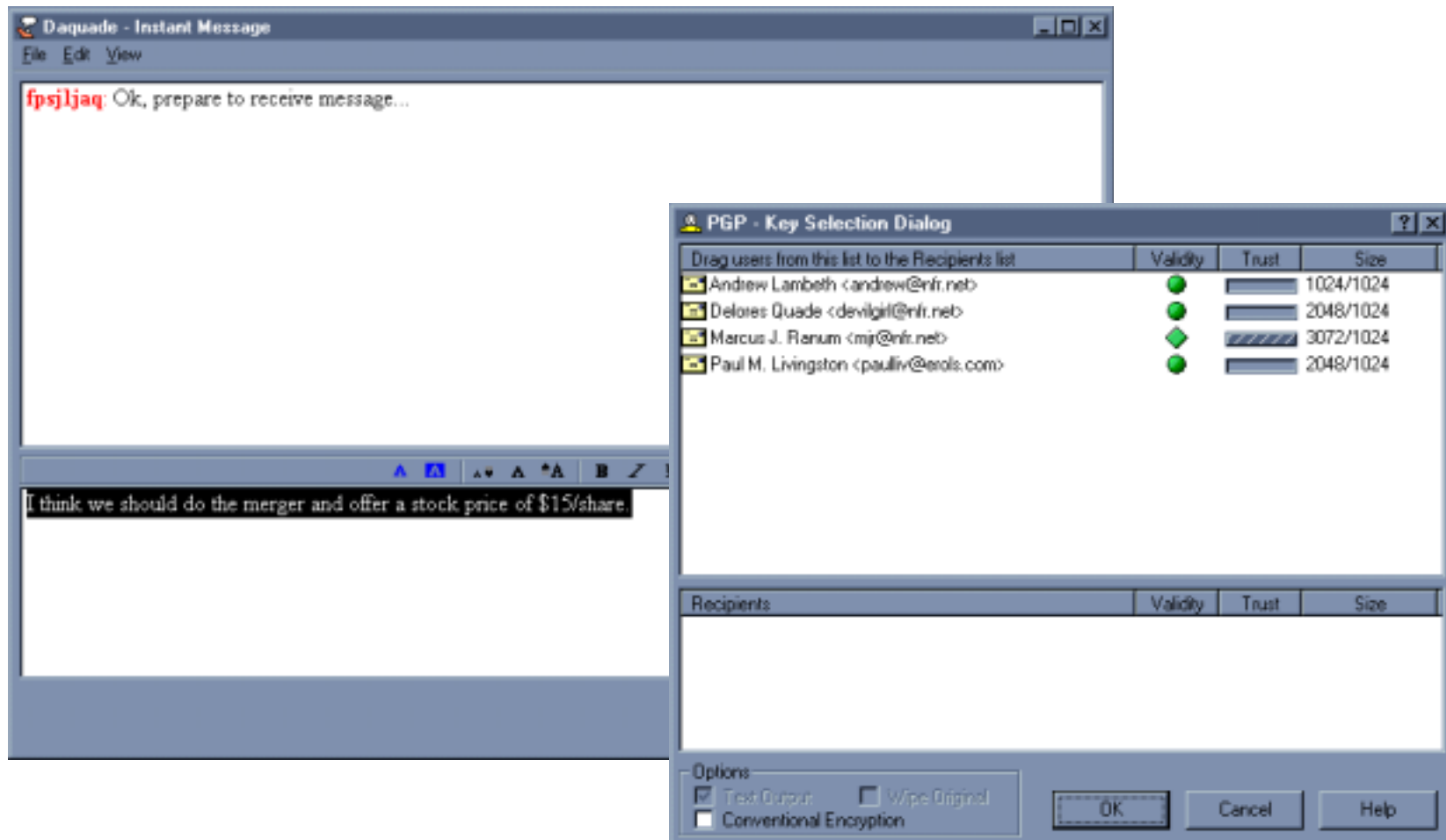
AOL Instant Messenger

- Instant Messenger is a free service that allows multi-way communications using opaque “screen names”
 - No registration required
 - Cannot trivially map screen name to a real person
 - High volume service hard to tap and may defeat traffic analysis

AOL Instant Messenger

... **And** you can use PGP over it, if you're
a spy

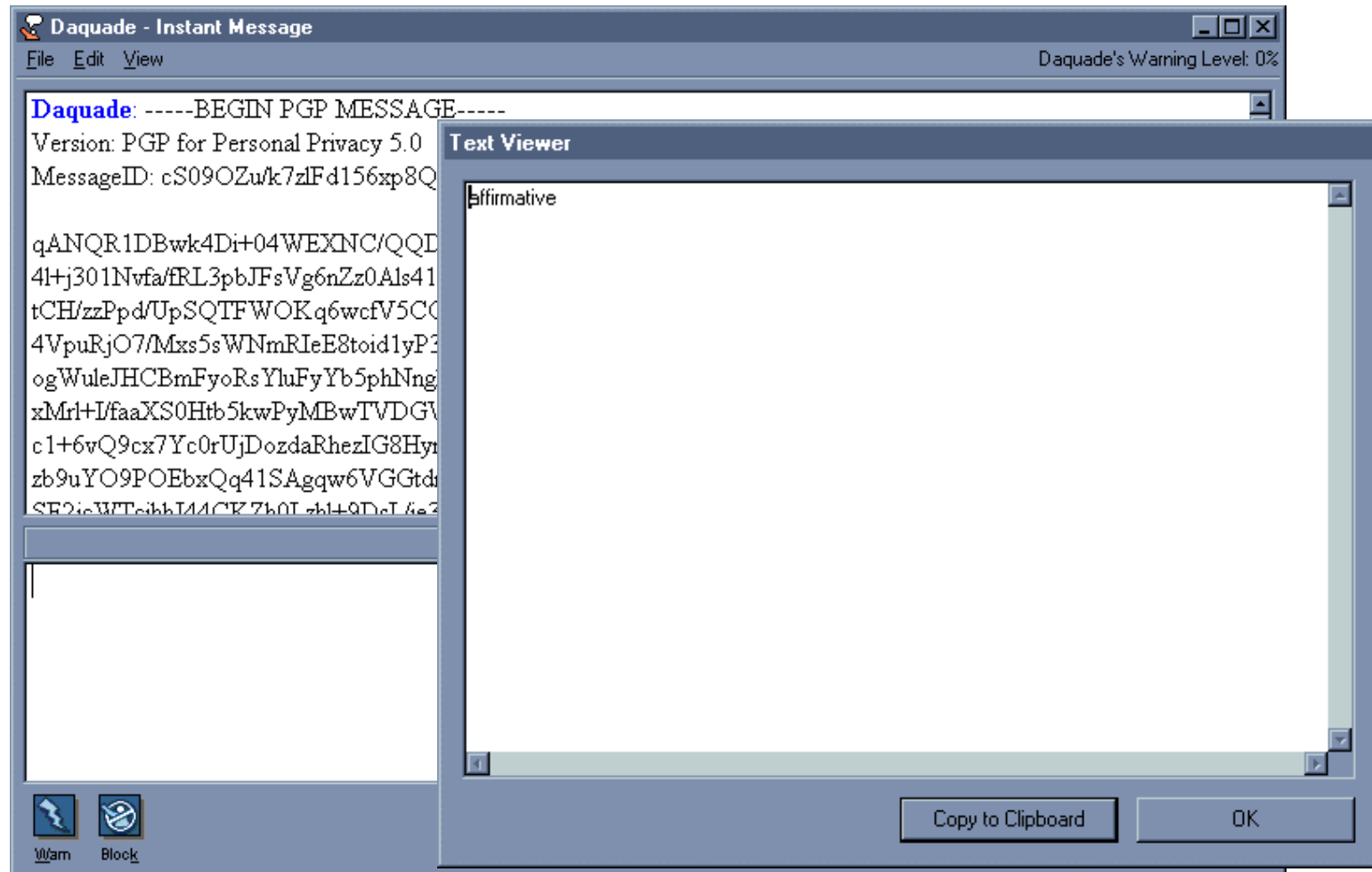
Setting up the message



Sending the message



Getting a message



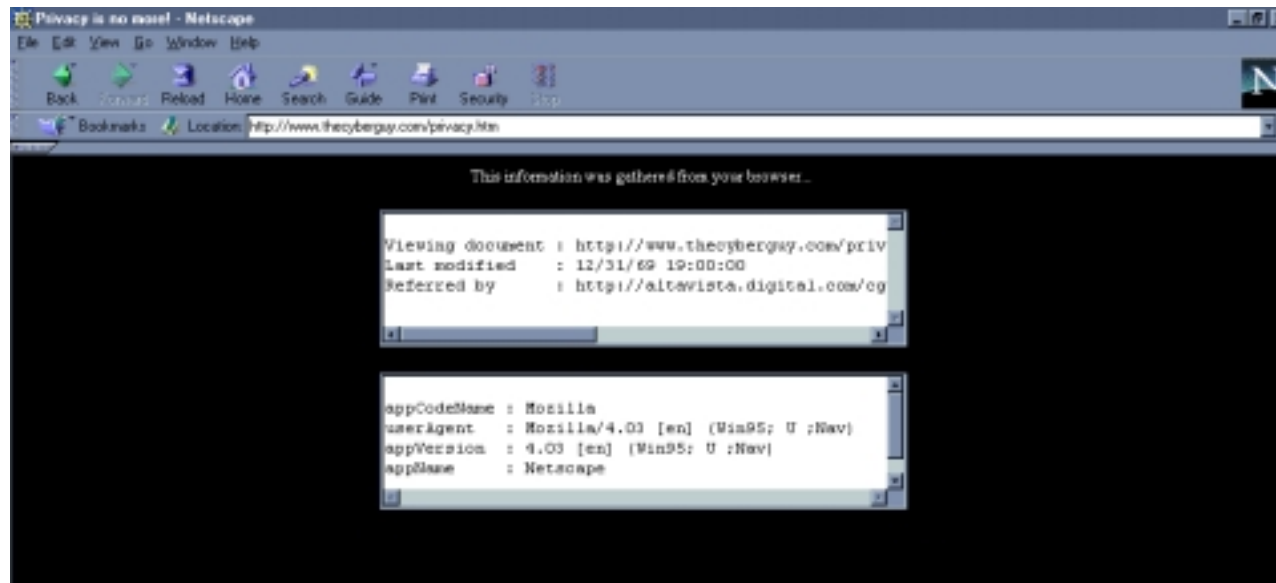
Anonymity and Privacy

- Within the next few years it'll be safe to assume that everything you do on the web will be watched
 - Not necessarily because They will but because marketers will
 - For secure communications anonymity may be a requirement
 - You don't want your browser to tell Them who posted that message to the dead drop BBS!

Ways you lose anonymity on the web

- Browsers cheerfully announce lots of information
 - Who you are
 - Where you came from
- Applications may publish feedback (e.g. “Microsoft Registration Wizard”)
- Query / online sales engines record your interests (e.g.: Amazon.com)

What your Browser Says



Web stings:

- A company has an anonymously run web site devoted to criticizing it:
 - Personnel dept wants to find who from the company goes there
 - Posts to online web-based message board a file with a hyperlink to a “clear” GIF on the human resources server
 - Records accesses to the GIF from systems within company network!

Anonymizing servers

- [Www.anonymizer.com](http://www.anonymizer.com) offers a web anonymity service
 - URLs are forwarded and remapped so the site can't see your IP address or browser information
- Build your own anonymizer service by using someone else's caching proxy
 - Or an AOL account under a fake name :)

Anonymous Remailers

- Anonymous remailers privatize E-mail by hiding the source path and sender
 - Original was anon.penet.fi which was shut down by government intervention
 - Newer remailers are much more sophisticated and don't have a single point of failure

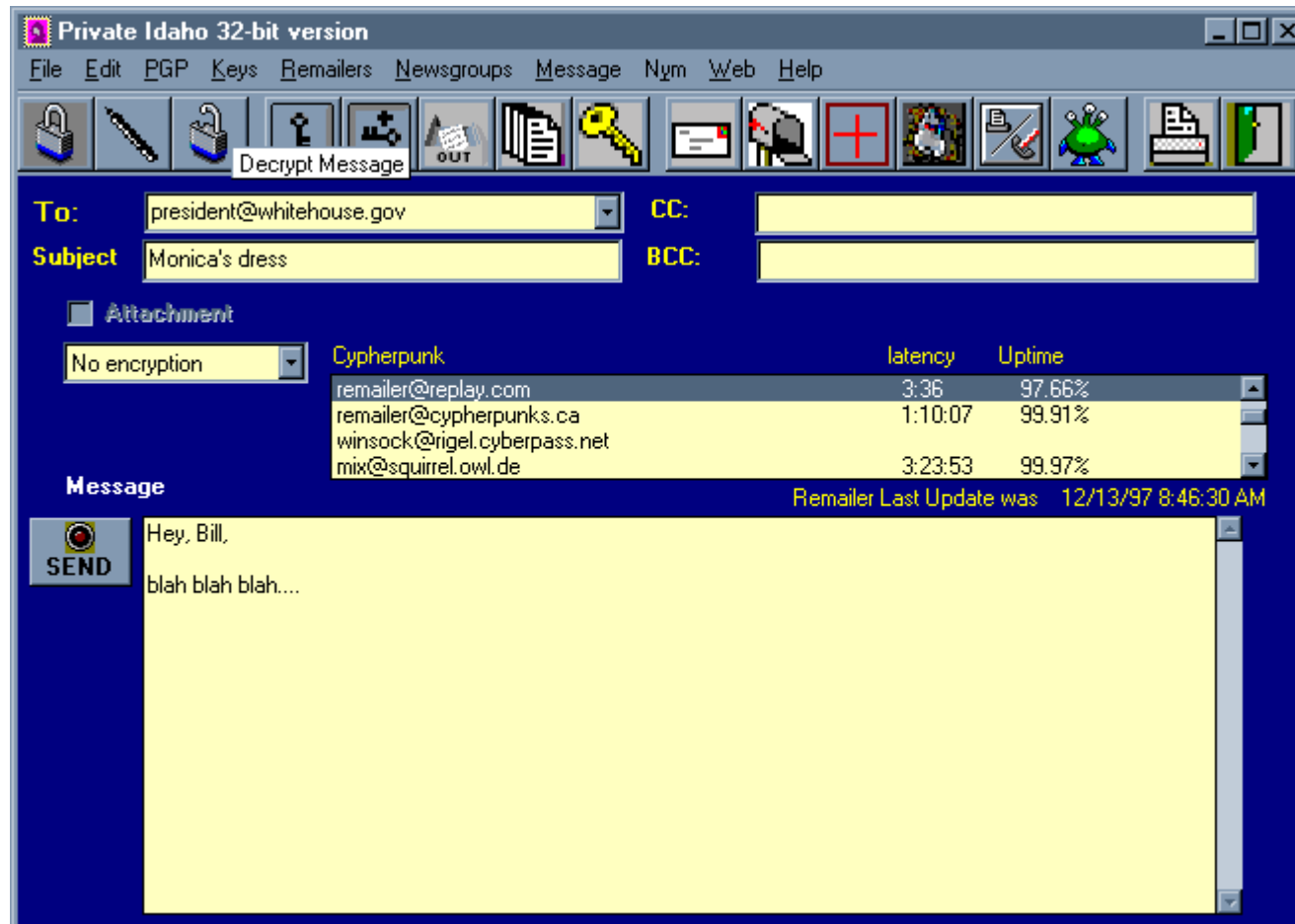
Anonymous Remailers *(cont)*

- There are many free remailers on the 'net:
www.cs.berkeley.edu/~raph/remailer-list.html
- Remailers can be chained
 - Mixmaster remailer messages contain multiple hops each of which is anonymous
 - To compromise a message you'd need to compromise several sites

Using Remailers

- Probably the easiest way to use remailers is via Private Idaho
 - Program that provides an easy interface to remailing
 - www.eskimo.com/~joelm/pi.html
 - wkweb4.cableinet.co.uk/hmartin/pidaho.html
(Win32 version)
 - Supports cypherpunk and mixmaster remailers

Private Idaho Win32



New Technologies

- Unfortunately for Them, new privacy and communication security technologies are always popping up
 - Many of these privacy technologies can be bootstrapped into dead drops or covert channels
- ... Bummer, eh?

The Eternity Server

- A server intended to prevent data from ever being destroyed
 - To foil Scientologists, etc, who want to “un-publish” information
 - Uses PGP signatures to allow anonymous control and posting of documents
 - Web interface includes directory service and searching

The Eternity Server *(cont)*

- The intent of the server is to be censor-proof*
 - Which means a spy could avoid wartime information controls
 - Eternity articles get posted to USENET so They can't even tell who is reading them

*Let's not post illegal material (child porn)

The Eternity Server *(cont)*

- The hope is to eventually have enough eternity servers sharing data that it would be impossible for Them to ever remove it

... Sounds like a great place for a dead-drop!

www.dcs.ex.ac.uk/~aba/eternity

Crowds

- Crowds is a web anonymity tool
 - Requests from many web users are batched together and shuffled
 - The crowds service redirects the requests to the correct user
 - Can go through many levels of crowds server to further shuffle

Crowds *(cont)*

- Crowds sounds like a great way of accessing a dead-drop or running a covert channel
- For more information, see research.att.com

Rivest's Wheat and Chaff

- Instead of encrypting data conventionally, simply break data up into many messages and then use a shared message integrity check code to verify the correct chunks
 - Can be used with arbitrarily large or small chunks of data

Wheat and Chaff *(cont)*

Msg1: attack at, checksum: 118872AF
Msg2: retreat at, checksum: 726A16CD
Msg3: 11:00AM, checksum: A8172BA2
Msg4: 1:00PM, checksum: 52AFFA11



**Generate messages
and checksum them
using pre-arranged key**

Transmit all

Msg1: attack at, checksum: 118872AF
~~Msg2: retreat at, checksum: 726A16CD~~
Msg3: 11:00AM, checksum: A8172BA2
~~Msg4: 1:00PM, checksum: 52AFFA11~~

**Recipient throws away
the ones that don't
checksum as valid**

Wheat and Chaff *(cont)*

- It's not really much different from ordinary encryption
 - There's a shared secret (key)
- Mostly a political dodge to confound export regulators
 - Might be useful for spies
 - Might be useful combined with USENET or Eternity servers

The Regulatory Environment

- Many countries regulate use or export of encryption (more precisely: communication security) technology
 - Some restrict it solely to military use
- Obviously, the stuff is extremely available
 - But restricting it creates an environment in which users paint a target on their backs

The Regulatory Environment

(cont)

- In the US, export of crypto is regulated
 - Crypto using less than 40-bit keys is OK*
 - The rules are deliberately vague in some areas
 - Individual export applications per product
 - Grey area regarding API calls versus plug-ins: is Window's cut&paste a crypto enabler?
 - Intent is to try to delay use of crypto

*Because it's junk

The case for personal secure communications

- Many of us believe we have a right to carry on our legal activities free from surveillance and in private
- Governments have not always been very good custodians of our secrets (do you think your tax returns are private?) and we should not have to trust their diligence

The Feds' case

- Secure communications do pose a vast threat to the powers of government to carry out its military and law enforcement objectives
- With secure communications it is impossible to differentiate a crime in progress from an ordinary message

Sources for crypto

- Peter Gutmann's links page:
www.cs.auckland.ac.nz/~pgut001/links.html
- One of many places to get PGP:
www.csd.uu.se/~d95mno/PGP.html
- Those freedom-loving Finns:
 - [ftp.cs.hut.fi](ftp://ftp.cs.hut.fi)

Technical References

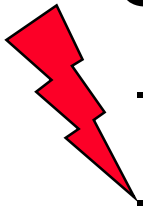
- Applied Cryptography : Protocols, Algorithms, and Source Code in C
 - Bruce Schneier ISBN 0471117099
- Internet Cryptography
 - Rick Smith ISBN 0201924803
- Peter Gutmann's Crypto Links page
www.cs.auckland.ac.nz/~pgut001/links.html

Spy-Tech References

- Spy Catcher
 - Peter Wright ISBN 9991065474
- The Corona Project: America's First Spy Satellites
 - Curtis L. Peebles ISBN 1557506884
- Skunk Works
 - Ben Rich, Leo Janos ISBN 0316743003

Paranoid References

- Janes' Counter-Insurgency catalog
 - Ian V. Hogg(ed.) ISBN 0710611390
- Arsenal of Democracy
 - Tom Gervasi ISBN 0394423283
- An Appraisal of Technologies of Political Control
 - European Parliament / STOA
 - jya.com/stoa-atpc.htm



No Comment Needed...

Back in 1984, it emerged that US export regulations even had special customs codes for such items as 'specially designed instruments of torture' (US Department of Commerce, 1984). There was even some suggestion (in para 376.14) that the US government could distance itself from human rights violations through 'judicious use of export controls'. (US Department of Commerce, 1983). Concerned by the possible scale of the trade in such technologies and the possibility they could be exported on via Europe which has much laxer arms export controls and transparency than the US, the UK human rights organisation, the Omega Foundation, sought comprehensive US export trade statistics. A Freedom of Information request was put down on Omega's behalf by the Federation of American Scientists (FAS).

What emerged was that the new category codes in the export administration regulations have if anything been extended to include, inter alia:

- * 'saps, thumbcuffs, thumbscrews, leg irons, shackles and handcuffs, specially designed implements of torture, straight jackets etc. (OA82C)' and
- * 'stun guns, shock batons, electric cattle prods and other immobilization guns (OA84C)' (United States Department of Commerce 1994).

The statistics of the export licences of such repressive equipment show that from September 1991 to December 1993, the US Commerce Department approved over 350 export licences under commodity category OA82C. The further category OA84C aggregates together data on electric shock batons with shotguns and shells. Over 2000 licences were granted from September 1991 to December 1993. (See Chart 13) As feared, the list names many EU Member States including Austria, Belgium, France, Germany; Iceland, Ireland, Italy, The Netherlands, Spain and the United Kingdom. While the licenses represent a snapshot of permissions for the sale to go forward, they do not indicate actual delivery, nor are they comprehensive since countries in NATO, such as Turkey, do not require a licence (Arms Sales Monitor, 1995). FAS has pointed out that aggregating data in this way, by lumping noncontroversial data on equipment such as those on helmets with controversial data on equipment often used for torture such as shock batons, effectively frustrates public oversight. Given the nature of some of the recipients - Saudi Arabia for example, where Amnesty has already recorded instances of Iraqis being tortured with electric shock batons (Amnesty International, 1994), many observers feared the worst.¹⁶⁶ Pressure to desegregate such categories in the US eventually proved successful but there remains a lack of effective checking and some items which should be in the amended category, are still slipping through.¹⁶⁷

Paranoid Web

- www.nsa.gov:8080
 - The National Security Agency
 - Includes the VENONA intercepts
- www.nro.odci.gov
 - The National Reconnaissance Organization
 - Includes Corona satellite images

1967 Corona Satellite Imagery



Corona VS SPOT (commercial satellite)

Corona,
1971



SPOT,
today

Site is Israel's Dimona nuclear reactor dome

Russian Satellite Imagery



World Trade Center, NYC

SR-71 Imagery



Cam Ranh, Vietnam 1978 w/Soviet Aircraft

KH-12 IMPROVED CRYSTAL



Lockheed “Sea Shadow”

**This is the boat they claim was ‘cancelled’;
presumably this is just a computer rendering...**



Jane's Co-In Catalog

- Out of print, published in 1993, Editor Ian V. Hogg; now (understandably) rare
 - Contains antiterrorist (or antipopulation) tools
 - Surveillance tools
 - Communications monitoring tools
 - ISBN# 0 7106 0868 3

Toys from Jane's

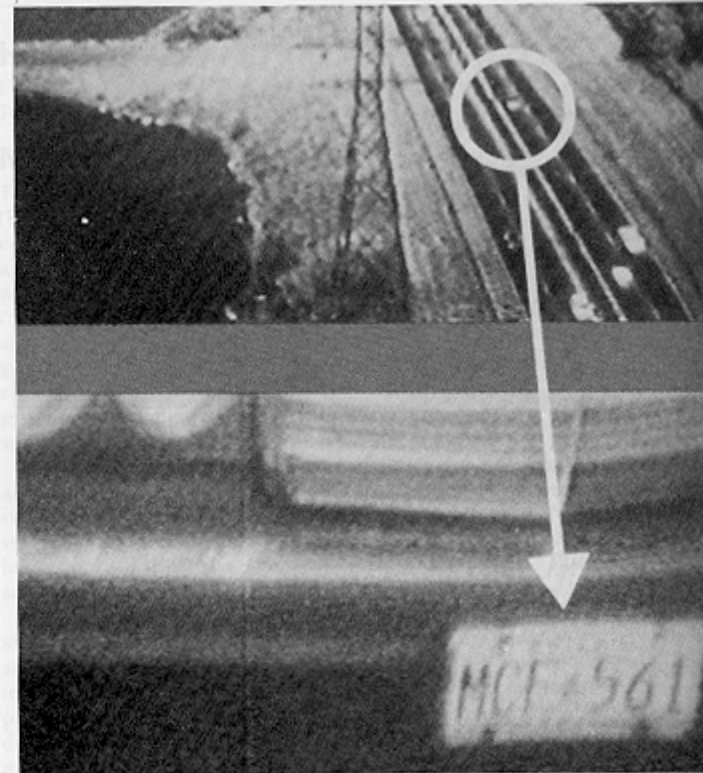
Istec Inc.

Istec Inc., 1810C Highway No.6 N, Hamilton, Ontario L9J 1H2

Wescam stabilised camera mount

The Wescam mount is a remotely-controlled, fully-stabilised mounting unit which can be used to carry virtually any type of camera or sensor mounted on an aircraft, boat or vehicle. For security and surveillance tasks, the use of the Wescam mount allows close control of borders and sensitive installations, speed in search and rescue missions, ease of identifying traffic, unobtrusiveness in observing smuggling operations, and the ability to make a visual record for future reference. With Wescam it is possible to maintain a discreet distance and yet obtain close-up detail for intelligent evaluation.

The standard Wescam mount can accept many different sensors, and sensors can be readily interchanged or integrated into one package for flexible use. Modular design is the key to this flexibility. Mounts are available for many helicopters and RPVs and can be adapted to any type of vehicle. Steering is accomplished by a joystick control, and the system is capable of revolving continuously through the full 360° and of elevating up 30° or down 90° from the horizontal. Both steering sensitivity and direction can be altered from the control console. A dome enclosure for the sensors, with a tracking flat optical glass porthole window, provides environmental protection and crystal clear imaging.



Actual video tape image, using Wescam mount, showing vehicle license read at distance of 1 km and speed of 160 km/hr

Toys from Jane's *(cont)*

Communications Devices Ltd

Communications Devices Ltd, 6 Riverside Park, Dogflud Way, Farnham, Surrey GU9 7UG

Telephone monitoring system

This system has a capacity of from ten to several hundred lines. Unique features include target number surveillance and automatic busy indication; simultaneous speech, day/time and called number recording; ring counter; date/time, called number and target number search and playback; variable speed playback; interactive CRT touch-screen controls with CRT display of date/time recording actually made on playback; high performance three-motor tape drives with microprocessor speed and tape motion control. The system can be provided with either one recorder per line or in a cost and space effective switching matrix configuration with a reduced number of recorders.

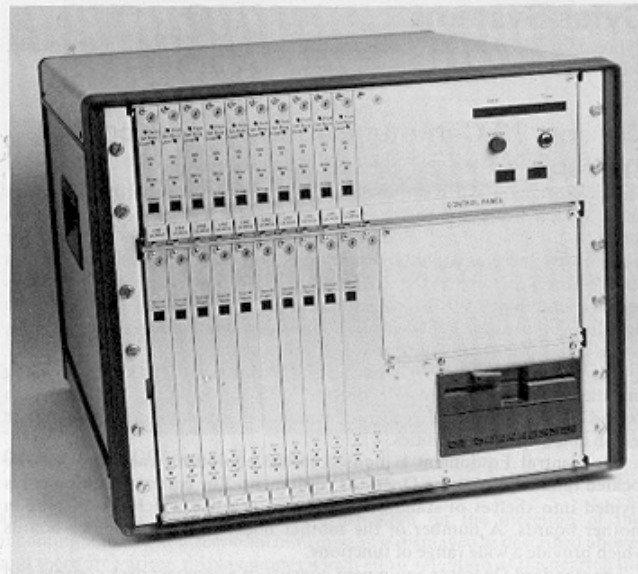


Telephone monitoring system

Facsimile monitoring system

This system continually monitors ten telephone lines and provides the intelligence and national security authorities with an exact printed copy of all received and transmitted facsimile messages. Indication is provided to show when the lines are idle and when they are being used for telephone or facsimile transmission.

Facilities are provided to monitor the audio signal, for remote control of an external tape recorder, and to cut off unauthorised facsimile transmissions. Options include hard and soft disc storage for subsequent cryptoanalysis, four-wire intercept, and a cost- and space-effective line concentrator.



Facsimile monitoring system

Telex monitoring system

This system simultaneously monitors ten telex or twx lines and records the intercepted communications on a high-speed printer. The printer provides a precise record of incoming and outgoing calls, including the number called

Model 300 countersurveillance receiver

The Model 300 is a compact portable system specifically designed for Technical Surveillance Countermeasures (TSCM) applications. The wide frequency band covers mains carrier intercoms at one end to microwave transmitters at the other. It provides the ultimate degree of flexibility through the use of the Z80 microprocessor and expressly engineered software. The Z80 recognises individual Electronic Signature Sound Sources, which can be placed in strategic locations throughout a surveyed area. This unique method of electronic discrimination speeds the search for a transmitting device by up to 75%. By incorporating a sensitive directional homing device the Model 300 will pinpoint the exact location within inches.

The Model 300 lends itself to a variety of control capabilities that provide local or remote automatic, as well as local manual control. The dedicated keypad and selectable resolution tuning provides full control over all operations. Detection modes are selected by single keypad controls covering individual or simultaneous demodulation. Computer selected IF bandwidths can be manually overridden at the operator's discretion. In the automatic tuning mode the Model 300 provides the option of a full spectrum scan or selectable programmed frequency scans, through any of the three sectors provided.

DATA

Operating modes: AM, FM, WBFM, USB, LSB, DSB, CW, SC, tuned subcarrier and carrier current

Frequency range: 1 kHz to 2.5 GHz

IF Bandwidths: 1 fixed, 7 automatic, with manual override

Attenuation control: better than 40 dB in 7 steps

Receiver sensitivity: better than $5\mu\text{V}$ at 10 dB S+N/N

Power supply: 110/240 V AC 50/60 Hz; 12 - 14 V DC

Dimensions: 480 × 507 × 207 mm

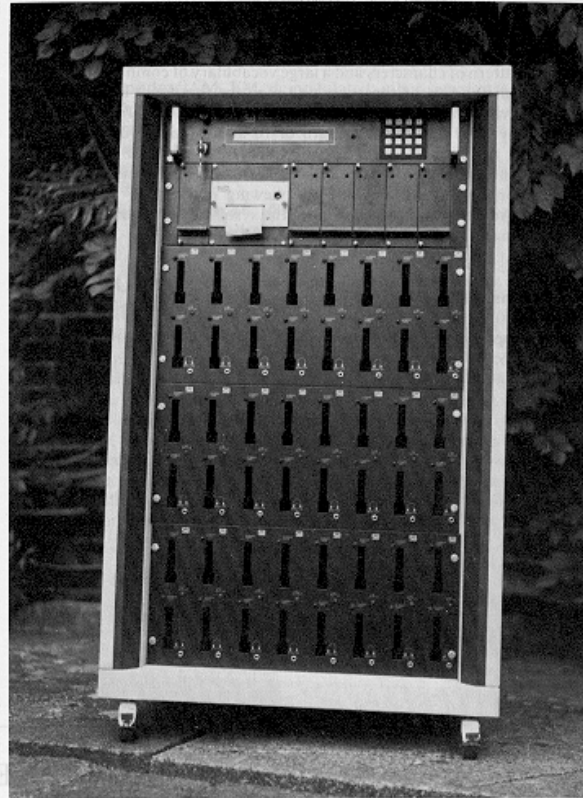
Weight: 22.15 kg



Winkelmann Model 300 countersurveillance receiver

Model 4000 computerised telephone monitoring system

The Model 4000 telephone line monitoring equipment can be used to monitor and record telephone conversations. It will give a printout of start and finish times of calls, numbers dialled (if outgoing) and the lines the calls are made



Winkelmann Model 4000 telephone monitoring system

from. It is fully expandable to meet the needs of the customer. This flexibility has been achieved by the use of standard 19-inch rack units and distributed processing throughout.

The basic configuration for the equipment is one Master sub-rack unit (2U high), any number of slave sub-rack units (3U high) and the corresponding number of cassette drive units (2 × 5U high per slave unit). The Master controls data input/output and provides a real-time clock for the system. The Master 'talks' to the various slave units by cable link and can be situated remotely (up to 3 km away). The slave unit consists of a power supply card, logging printer card (logs up to 16 lines), slave processor card, and up to four telephone interface cards (four lines per card). Each cassette drive unit consists of 16 stereo cassette mechanisms, two cassettes per line monitored; thus for the full 16 lines available in one slave unit two cassette drive sub-racks are required. A separate power supply is required for each complete (two units) cassette drive - this will be incorporated in the Model 4000 unit.

The Master unit has a keypad data entry and a 40-character alpha-numeric display. Functions available from the unit are time of day display, master logging, special numbers facility; associated numbers facility, password facility, self-test routines and status display. A full RS232 compatible port is available, enabling a dumb terminal or a computer to be used as a supervisor console. All the Master programme functions are available from this console.

Toys from Jane's *(cont)*

Master/Slave Receiving and Monitoring System

The master/slave receiving and monitoring system makes use of a master receiver (designated R-3510) and from 1 to 7 slave receiver chassis units (designated R-3511).

The system operates from 20 to 720 MHz. The master receiver provides spectrum sweep and channel scanning capabilities and allows for automatic or

manual hand-off of a signal when it has detected energy above a preset threshold. These signals are handed off to one of seven slave chassis units, each of which contains six monitoring receivers. An IEEE-488 bus controls the system.

Each receiver in the system, including the one in the master chassis and each of the six in the slave chassis units, is composed of five individually shielded modules. These modules are identical for all receivers. In addition to these five modules, each chassis contains an RF signal distribution module.

Modes are AM and FM and resolution is 1 kHz.

Synthesiser lock time is 30 ms maximum and AGC range and threshold is $3\mu\text{V}$ in the 25 kHz bandwidth over an 80 dB minimum dynamic range.

The system meets MIL-STD-810D for shock and vibration and various requirements of MIL-E-5400R and MIL-STD-461. The master and slave dimensions are 483 mm rack mounting utilising 133 mm of space with 508 mm of depth. The master chassis weighs < 13.5 kg and the slave < 24.75 kg.

Manufacturer

Cubic Communications, San Diego.

Modular Receiver Subsystems

The modular receiver subsystem is a variable design subsystem composed of plug-in modules used to achieve a desired functional configuration. Form factors are compatible with ATR and 483 mm rack-

mounted drawers. Available configurations are currently fully militarised and include FFT processors for fast acquisition as well as built-in test. Frequency ranges available are 1 kHz to 2 GHz. Configurations are available for both wideband and narrowband applications.

The MRS-8000 has a frequency range of 20 to 500

MHz and a tuning resolution of 1 Hz (VHF). It has a noise figure of 14 dB and a receiver tuning time of 100 ms. Second order intercept point is +45 dBm maximum, and third order +5 dBm maximum.

Manufacturer

Magnavox Electronic Systems Co. Fort Wayne, Indiana.

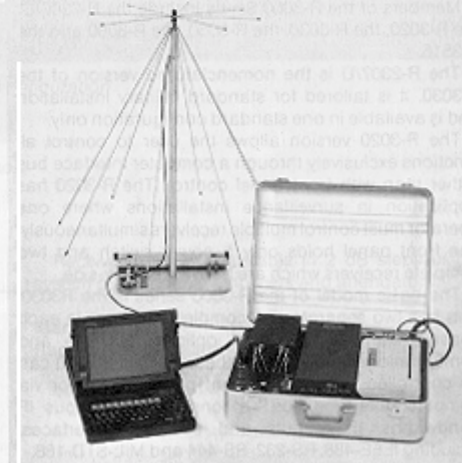
MSS-1200 Transportable Surveillance System

The MSS-1200 offers signal detection, collection and analysis over the frequency range 10 kHz to 1200 MHz at a maximum scan rate of 1.5 MHz/ms. Dual independent receivers permit simultaneous collection and analysis of detected signals. The system can be manually operated

or set in automatic mode to provide a response when particular criteria are met. IF bandwidths are 3, 8, 15, 50, 300 kHz and the IF output is 21.4 MHz. The system is portable, weighs less than 20 kg and measures 279 x 381 x 58 mm. It is able to operate from 115/220 V AC or from 28 V DC.

Manufacturer

Rockwell International, Collins Avionics and Communications Division, Cedar Rapids, Iowa.



Toys from Jane's *(cont)*

CCS Communication Control Inc

CCS Communication Control Inc, 160 Midland Avenue, Port Chester NY 10573

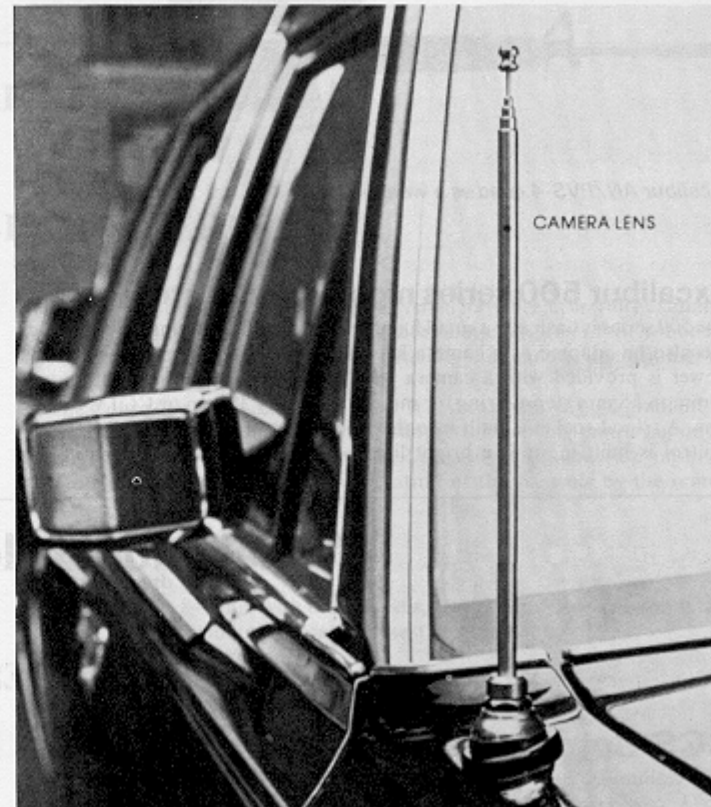
Covert video surveillance system Series 2000

This is a series of disguised CCTV cameras which permit surveillance to be carried out in factories, offices and elsewhere. Each unit consists of a camera and transmitter capable of sending video and audio signals to a nearby receiver where the pictures can be studied and recorded. Type CVS2010 has the camera disguised as a fire extinguisher; CVS2020 as a leather-bound book; CVS 2030 as an attaché case; CVS 2040 as a picture frame; CVS 2050 as a stereo radio set; and CVS 2060 as a decorative wall clock. Each will provide high-resolution images and transmit them up to 8 km away, depending upon conditions. The camera has a wide-angle lens and automatic iris, and a special high-sensitivity camera can be used for low light levels. The camera can be activated by remote control or by magnetic, acoustic or other types of sensor to suit particular requirements.

Antenn-Eye AE60 surveillance system

The AE60 resembles a standard telescoping car antenna, but inside is a micro-miniature lens system. Beneath the car's fender, in the place where the antenna mechanism would normally fit, is the camera and transmitter unit, both entirely concealed from view. There are four antenna units; three have lenses covering 10°, 45° and 60° fields of vision and the fourth is a dummy, to be inserted when the unit is not in use. When observing, the antenna shaft rotates continuously to give a full 360° view of the surveyed area.

It is, of course, possible to adapt this unit to other localities; for example one could mount the unit inside a portable TV or radio set and use the set's antenna for observing; other applications will doubtless come to mind.



Toys from Jane's *(cont)*

Goodbye

...and good luck!