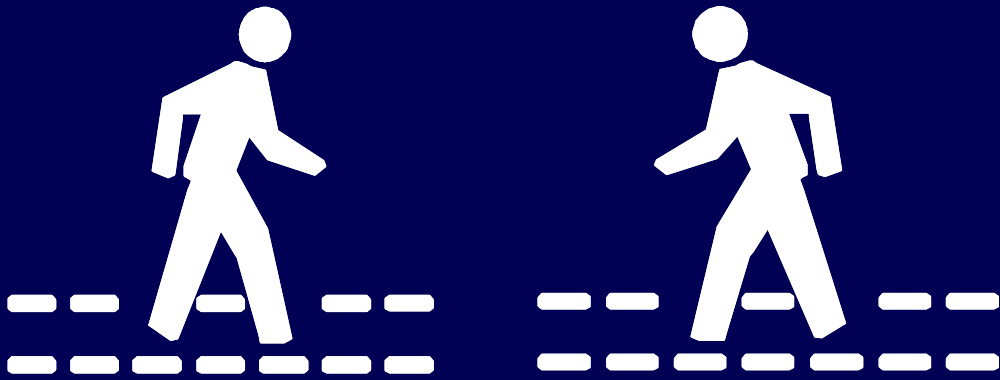


**18th DOE CSG
Training Conference
Seattle**



***Security & Technology:
a Complex Dance***

**John G. O'Leary
Computer Security Institute
April 23, 1996**

Security & Technology a Complex Dance

Abstract


Security and technology are inextricably intertwined. The ways that they interact with each other demonstrate some remarkable choreography. This presentation will examine the interplay of security and technology, noting how the result sometimes appears graceful and synergistic and sometimes resembles the section in front of the stage at a heavy metal concert. There is an escalation of the game, wherein craftier crooks spur us to devise better locks, which, in turn spawn more accomplished thieves. It is easy to find areas where technology augments security and where security advances technology. We'll also discover instances where they are perceived to hinder each other.

One of the most deeply rooted assumptions of the information systems security field is that security is a people problem, not a technical one. Based on this assumption, it has been continually stated that one doesn't need technical expertise to do the security job. We'll examine that supposition in light of today's technological trends and what appears to be in store for the future.

Biography

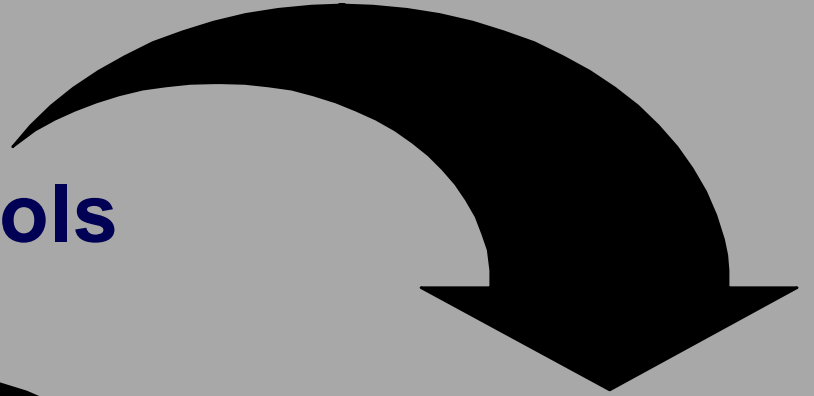
John G. O'Leary is Director of Education for the Computer Security Institute. He has been an active practitioner in computer/information systems security and contingency planning for significant parts of three decades. Mr. O'Leary has designed, implemented, maintained and managed security for networks ranging from single-site to multi-national, LAN to WAN, and including mainframes, minicomputers and micros of varying ilk. John has built, modified and tested recovery plans for a similar range of environments. His background spans programming, systems analysis, auditing, project management, DP operations, troubleshooting, quality assurance, internal and external consulting, training, and user interaction ranging from hand-holding to rancorous altercations. He has never been convicted.

Security & Technology

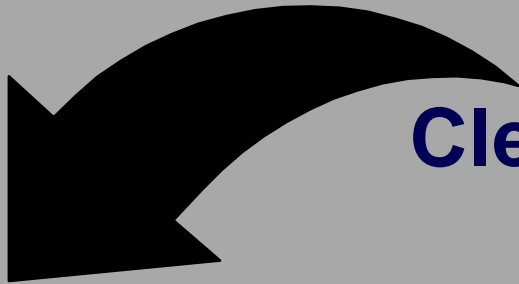
- **Inextricably intertwined**
 - **Movement of one invariably affects the other**
 - **Relationship is not always linear**
- 
- **Sometimes an advancement for both disciplines**
 - **Sometimes one advances at the expense of the other**
 - **A breakdown in one can be devastating to the other**
 - **.....so can an advance**

Escalation of the Game

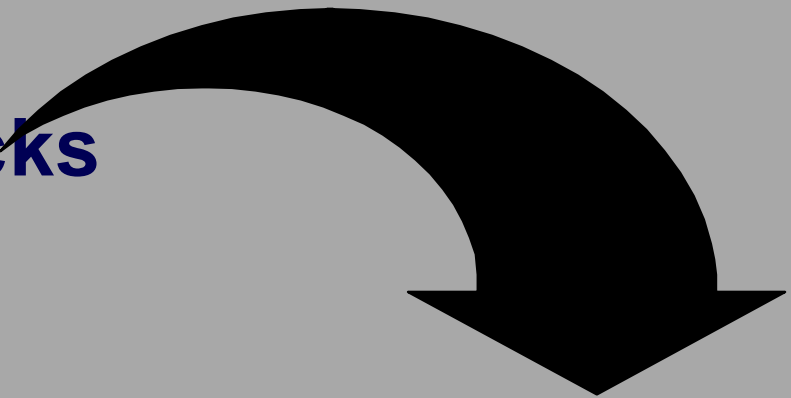
- **Good controls**



- **Clever crooks**



- **Better locks**

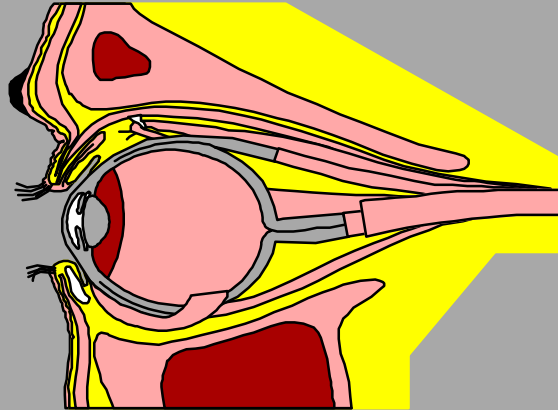


- **More accomplished
criminals**

- **Same problem, but at a higher
level of expertise**

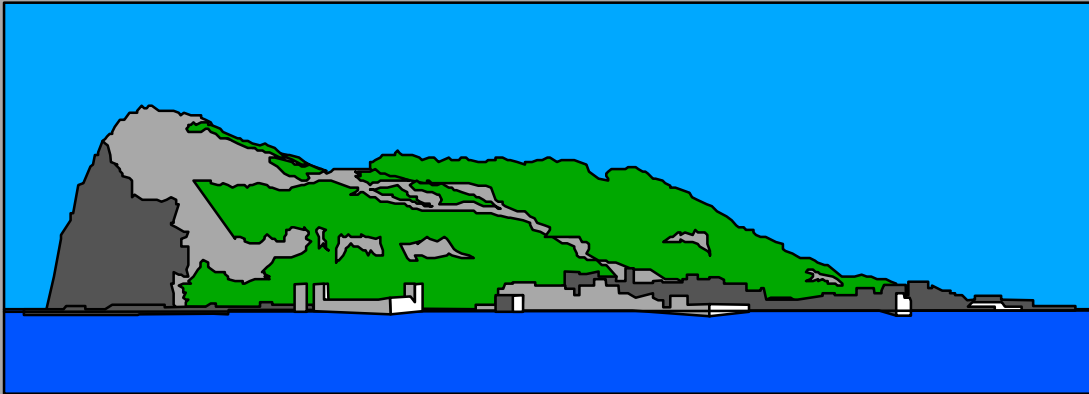
Technology to Augment Security

Biometrics



- **Retina scan**
- **Fingerprints**
- **Voice prints**
- **Hand geometry**
- **Signature analysis**
- **Keystroke pattern**

Technology to Augment Security



Password Augmentation

- One-time passwords
- Smart cards
- "Dongles" or tokens
- KERBEROS implementations

Technology to Augment Security

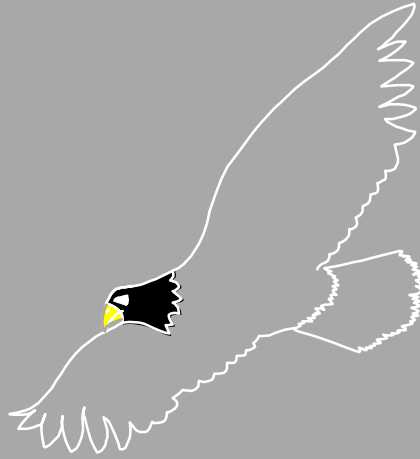
"Vaulting" for DRP



- Partitioned, protected, specifically allocated storage at backup site
- Electronic link
- Timely mirroring of critical updates
- No fetching backups
- Up and running quickly

Technology to Augment Security

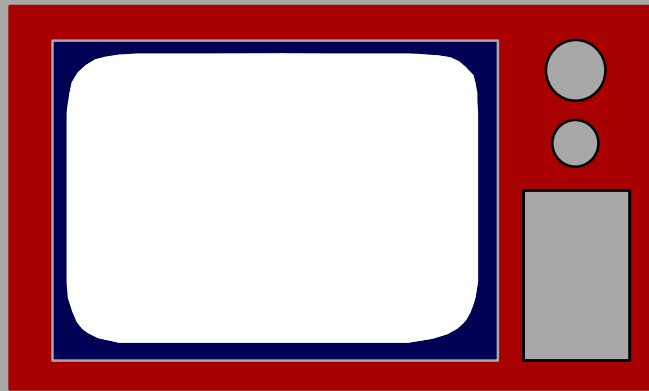
RAID Arrays



- **Striping to prevent total reliance on one particular storage device**
- **Ability to shift data when encountering problems**
- **Protection for critical information**

Technology to Augment Security

Fiber optic cable



- Tougher to tap
(but not impossible)
- No electronic interference
- High speed data transfer
- Transmission quality
- Costs coming down

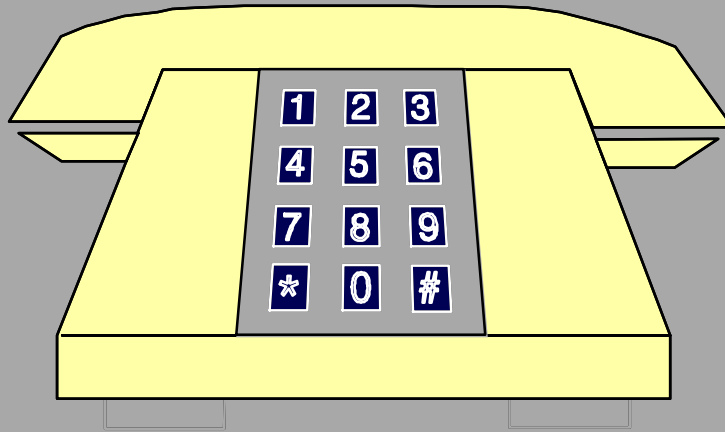
Technology to Augment Security *Spread Spectrum*



- For wireless transmission
- Multiple frequencies within a predefined range
- Non-sequential
- Time-based jumping
- Defense from frequency scanning

Technology to Augment Security

Caller ID



- For some protection from local, amateur hackers
- Screening out nuisance calls
- Investigating criminal calls
- Civil liberty issues

Technology to Augment Security

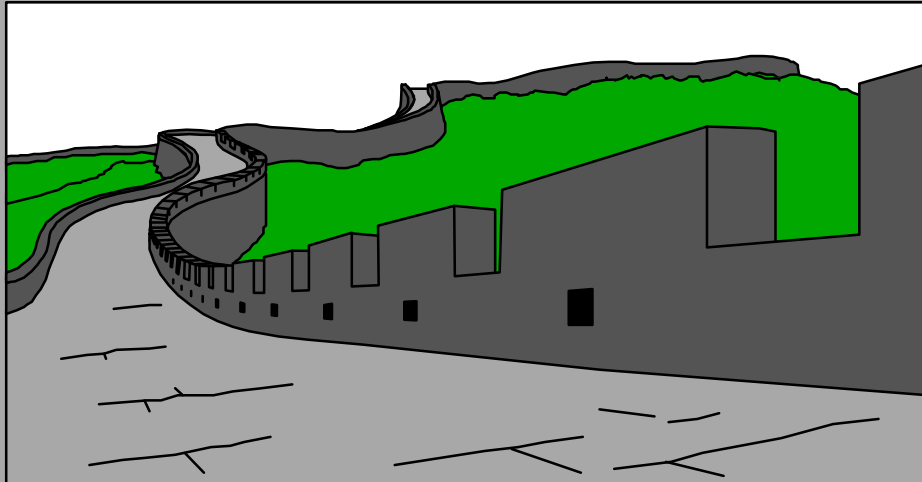


Telco Tech



- Dial Number Recorders to catch phone fraud
- Directional antennae to locate source of cellular calls (Shimomura, Telco & FBI finding Kevin Mitnick)
- But "on" cell phones broadcast their identity number regularly (Cloning happens)

Technology to Augment Security *Internet Firewalls*



- **Hardware/ software combinations**
- **Placed in "DMZ"**
- **Filter inbound and outbound packets**
- **Control point for Net access**

Technology to Augment Security

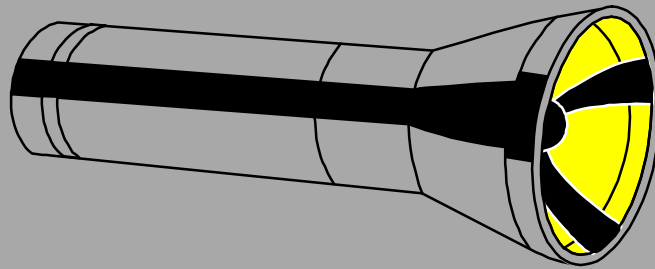
Public Key Cryptography



- Truly a revolutionary advance in mathematics
- An idea before its time in 1977
- Networks, especially LANs make it very relevant
- Secrecy, message authentication
- Product offerings multiplying

Technology to Augment Security

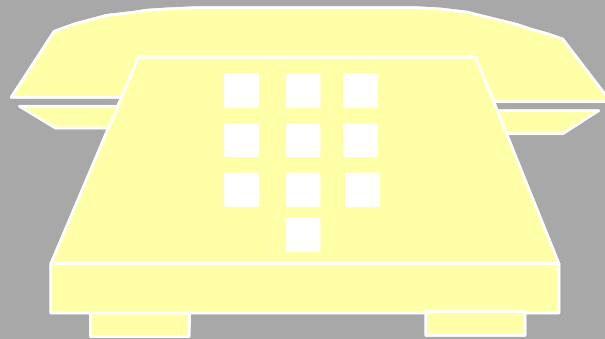
Penetration Tools



- Shine light on weak points
- Exposures recognized by the product or technique
- SATAN, Crack, etc
- You still must close the identified holes

Technology to Subvert Security

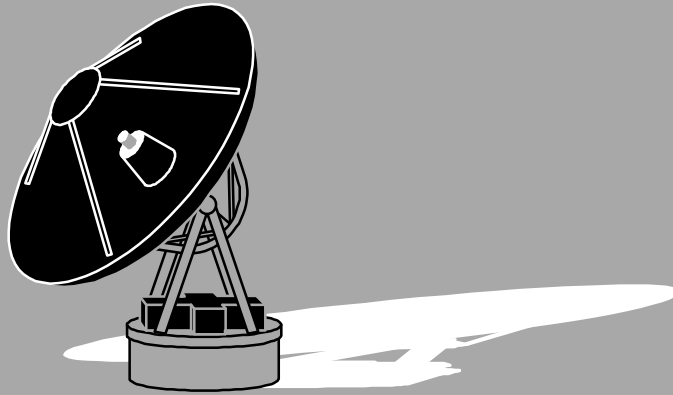
Blue Boxes



- **Tone generators**
- **Supervisor state**
- **Bypass billings**
- **Apple connection**
- **Circuit diagrams available on hacker BBS**
- **First step for fledgling computer criminals**

Technology to Subvert Security

Signal Interception



- **Wiretap**
twisted pair or coax
- **Internal or external**
- **At junction box**
- **In beam path for wireless**
- **In "footprint" for satellite**
- **Passive interception can be undetectable**

Technology to Subvert Security

"Tunneling" past Firewalls



- Encapsulated packets
- Knowledge of screening at firewall
- Need way to rebuild packets once past firewall
- One reason why firewalls, while necessary, are not sufficient

Technology to Subvert Security

"LISTSERV" Attacks



- Denial of service



- Add target's name (Limbaugh) every "Listserv" you find

- Thousands of messages daily

- Obscure topics & content

- Screening through for real messages excessively time-consuming, if possible

Technology to Subvert Security

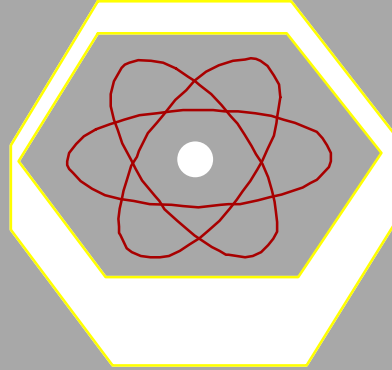
Internet Factoring



- **Lenstra in 1995**
- **Used multiple internet sites and computers**
- **Partitioned computational tasks**
- **Factored a 119 bit RSA key in 6 weeks**

Technology to Subvert Security

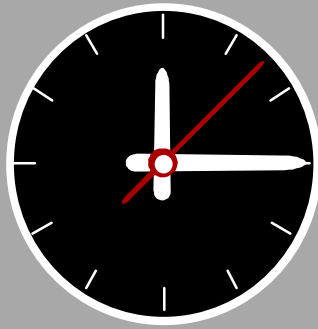
Mathematics vs Cryptography



- Quadratic sieve
- General number field sieve
- Ways to lessen the work in factoring the product of primes
- Make the solution space smaller

Technology to Subvert Security

Timing Attacks



- Precise measurements of time to go through the public key encryption process
- Clues to the size of numbers used as modulus
- Limits the range of potential primes

Technology to Subvert Security

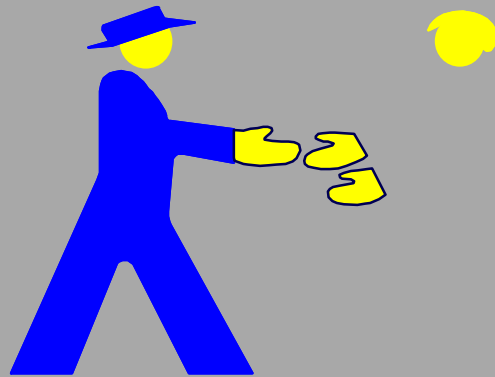
Malicious Program Code



- Viruses
- Logic Bombs
- Worms
- Trojan Horses
- War Dialers
- Password Catchers
- etc., etc., etc.

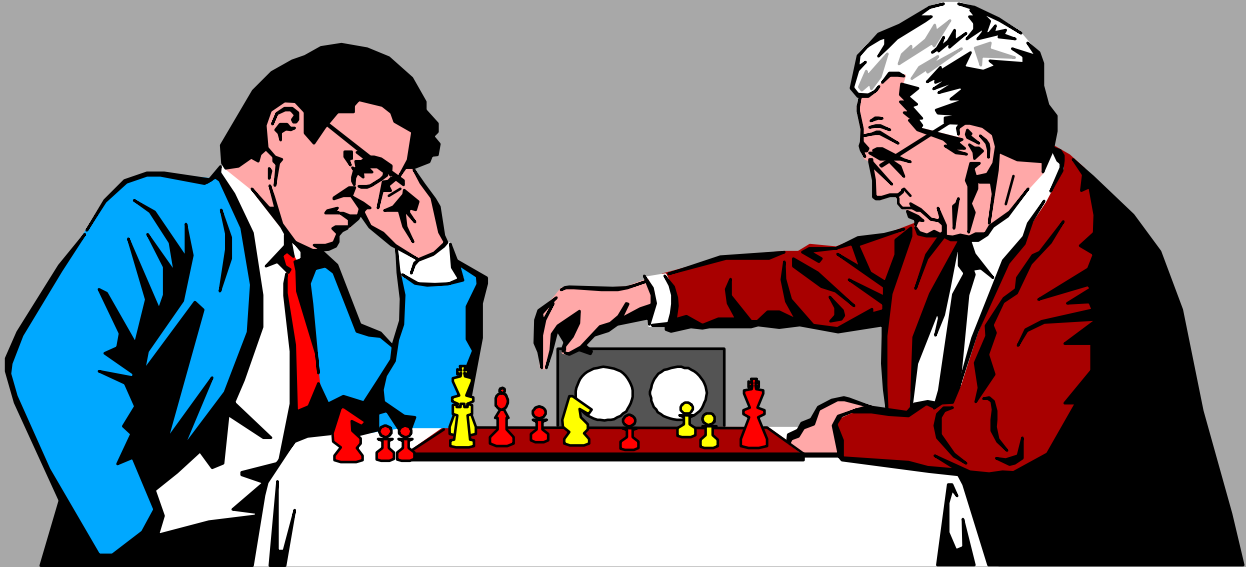
Technology to Subvert Security

Social Engineering



- Hacker specialty
- Sounding knowledgeable
- Prey on those who want to help
- Some technical knowledge makes it even more effective
- Rampant

Technology to Subvert Security



- Ongoing chess game
- Do not underestimate the technical prowess or the dedication of your adversary
- Don't make a deity out of him or her either
- Wait for the mistake
- Keep your defense solid

Security as a Non-technical Job



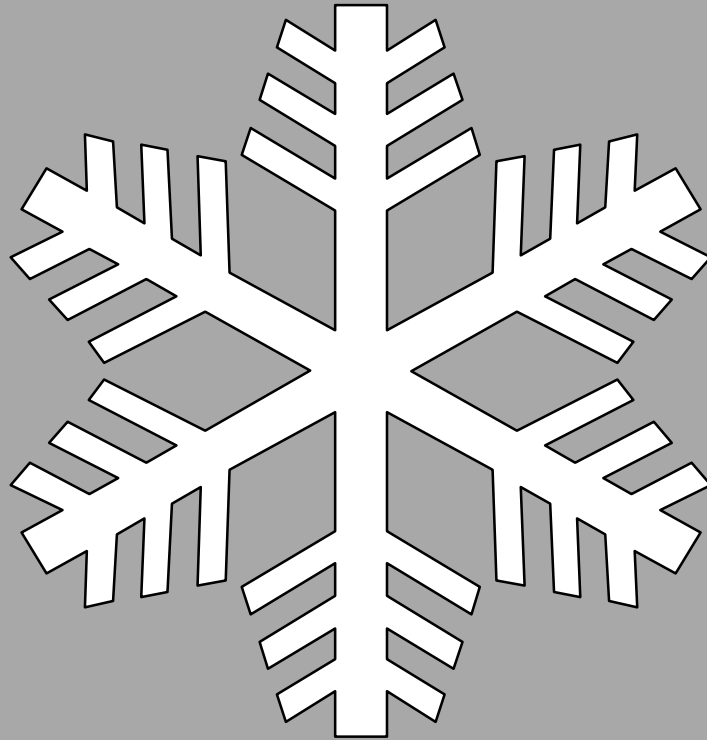
- People skills
- People problem
- Knowledge of the organization
- Audit mind-set
- Controls orientation
- Security knowledge

Security as a Technical Job



- **Subtle exposures**
- **Validity of controls**
- **Performance impact**
- **Explain to management what really happened, or what might happen**

Security as a Technical Job

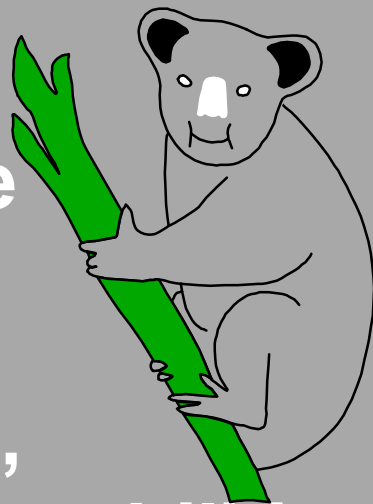


- **Screen out the snow**
- **Avoid foolish statements
(maintain credibility)**
- **Design workable solutions**
- **Produce realistic DR plans**
- **Clarify for judges & juries**

Security as a Technical Job

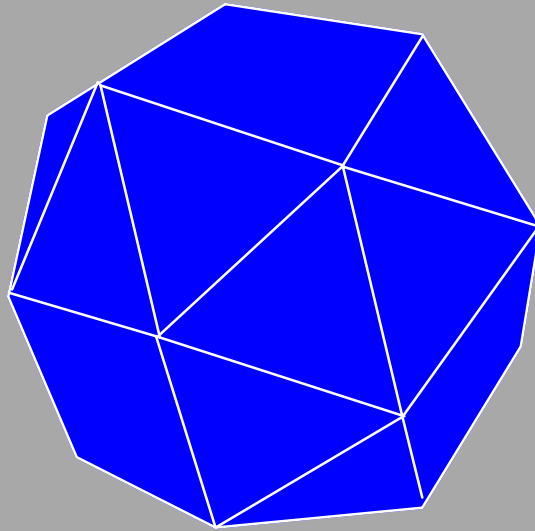
Technical knowledge required to do security today

- NOS capabilities
- Mainframe package operation
- Database structure, schemas, search capabilities
- "Object" technology & concepts
- Firewall filtering actions
- Encryption algorithm strength
- Implementation strategies



Future Trends

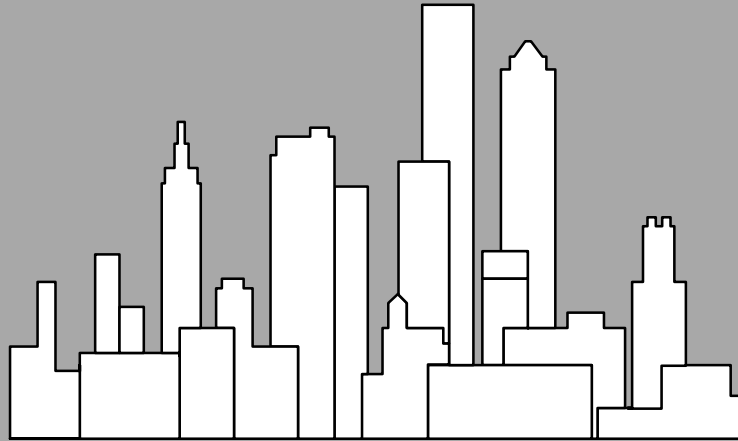
Faster Change



- **18 month lifespan for new technology**
- **More connections**
- **Cheaper, easier to obtain technology**
- **Security trying to play "catch up"**

Future Trends

More Stress Points



- Dial up
- Internet
- Massive workstation storage
- Flood-like flow
(cable modems)
- Instant events
(faster processors)

Technology and Security

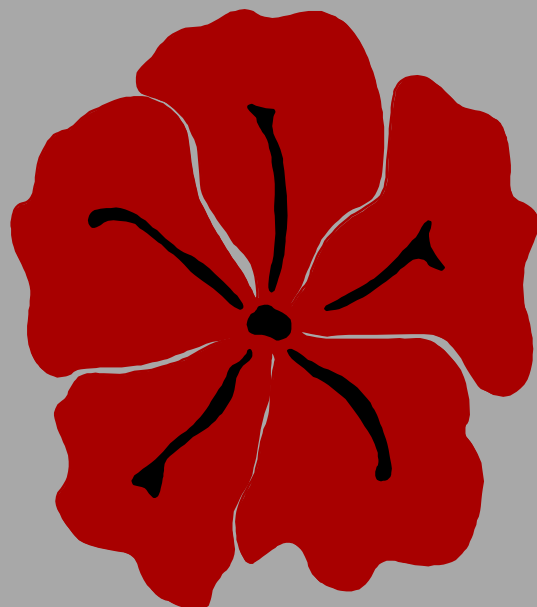


- Energetic dance
Lots of action
Changes in direction
- Must anticipate partner
- Room for improvisation,
if coordinated
- Fun to watch, fun to do.....
when it's done right

Words of Encouragement

By its very nature, computer security involves complex and sensitive issues.

Such situations are not always fun, but they are challenging; and challenges make you grow.



Words of Encouragement

Learn a lot about a lot

Deep but narrow knowledge
will break when confronted
with a new situation.

You can't be a technical
illiterate and do the job well.

You can't deal only with
machines or programs.

"Wetware" is part of
the network.

Words of Encouragement

Your job is truly important

The networks you are
protecting are instrumental
in the production of goods
and services worldwide.



Words of Encouragement

*Focus on the real needs
of the organization.*

**Security supports the
business, not vice-versa.**

Look to the future.

**Weave your way through
technological promises
and pipe dreams.**

Words of Encouragement

*Empathize with the
other person.*



**They're trying to do their
job, just like you.**

**They probably don't quite
understand all the technical
aspects of the network, but
they know it's supposed to
"augment their productivity."**

Words of Encouragement Stress your own professionalism.



**Learn, don't fake it.
"I don't know" can be
a legitimate answer.**

Be evenhanded.

**Do your best with what
you get, even when your
solution was better.**

No whining.