

The Internet



An expensive shared resource

Casey Schaufler

Manager, Trust Technology

casey@sgi.com



Back in the old days



Computers were expensive

Only a government could afford one

Even then you had to share it



No one likes taking turns

sgti™



sgti

Time Sharing

sgti™

*Pretend it's always your turn
You're idle most of the time anyway
You'll do your task and leave*

sgti

Computers got cheap

sgi™

Not so cheap you got your own

Cheap enough to support boredom

Looking about became economical

sgi

Access Controls

sgi™

You don't know the name

Dismount the pack

Task Associations

sgi

Convenient Access Controls

sgi™

Discretionary Access Controls

Mandatory Access Controls

Time based Access Controls

Tickets, Tokens, Cookies

sgi

Computers got even cheaper

sgi™

So cheap, you can have your own

No need for access controls

You'll do your task, then turn it off

sgi

Sharing became difficult

sgi™

300 Baud Modems

SneakerNet, TapeNet

8 inch Floppies

sgi

EtherNet™

sgi™

Thick Yellow Cable

Connect with your compatriots

All Machines are peers

Doesn't leave the building

sgi

High Speed Modems

sgi™

Extend the yellow cable

Connect to more compatriots

All sites are peers

It's still under control

sgi

Protocol Explosion

sgi™

TCP, UDP

FTP, TFTP

SNMP

YP (NIS, NIS+), DNS

RFS, NFS, AFS, PCNFS

telnet, rlogin, rcmd, rexec

sgi

The Internet

sgi™

Connection to the internet was expensive

Policy of no commercial use

But then came ...

sgi

The World Wide Web

sgi™

Valuable assets globally accessible

Intellectual property

Graphical images

Credit card numbers

sgi

eCommerce



Point to point communications

Specific limited protocols

Virtual Private Networks (VPN)



Everyone Knows



Security = Cryptographic Authentication

Data encryption goes beyond secure

A good firewall protects servers

Nothing else matters



Security Professionals Know



The InterNet provides communications

The InterNet has no security policy

Attribute information is not shareable

The other guy can't be trusted anyway



User Identification on the InterNet



Identification by VISA Number

- MasterCard, American Express, Discover

Authentication by expiration date

Limited facilities available

Assurance by the bank

- Threats of credit card fraud
- Refusal of payments



E-Commerce Protection Profile



BuyStuff.com as a reference monitor

Always invoked

- Server supports limited protocols

Not circumventable

- Server not programmed to do other things

Small enough to be analyzed

- Large set of public objects
- Small set of user objects



Strong Access Control?



Solved problem on a single system

- Single administrative domain
- Controlled security parameter

Depends on sufficient authentication

Limited by assurances

Not a solution on simple systems



Clusters



Strap all those little guys together

Create one big system

Access Control!



Cluster Protocols



Need Access Control Support

Proprietary Scheme

IPSEC



IPSEC



Opportunity for strong access control

No current activity

No TSIg equivalent group



The Point



SAC is of limited use

SAC is important to some

SAC is solved on a single system

Internet use of SAC is limited

SAC will go nowhere without

- Standard internet support
- Increased sharing of compute resources



Thank You

sgt[™]

sgt