ERCOT'S

Defense in Depth Strategy

Director, Corporate Security

Chris Uranga

ERCOT IT

Cyber Security Actions

- *Conducted a three day "White Hat" attack on ERCOT's infrastructure. Attempt was to be complete and penetrating, but not endangering the production environments or uptime.*

- *Completed a six week cyber assessment to be more comprehensive and to clarify and prioritize risks.*

Email-borne Threats at ERCOT

September 2003

Trojan Horse
A program that neither replicates nor copies itself, but causes damage or compromises the security of the computer. Typically, an individual emails a Trojan Horse to you-it does not email itself-and it may arrive in the form of a joke program or software of some sort.

Worm
A program that makes copies of itself; for example, from one disk drive to another, or by copying itself using email or another transport mechanism. The worm may do damage and compromise the security of the computer. It may arrive in the form of a joke program or software of some sort.

Virus
A program or code that replicates; that is, infects another program, boot sector, partition sector, or document that supports macros, by inserting itself or attaching itself to that medium. Most viruses only replicate, though, many do a large amount of damage as well.

Hacktools: Programs that are used by hackers for various purposes.

Computer viruses are among the most frustrating challenges faced by IT organizations today.

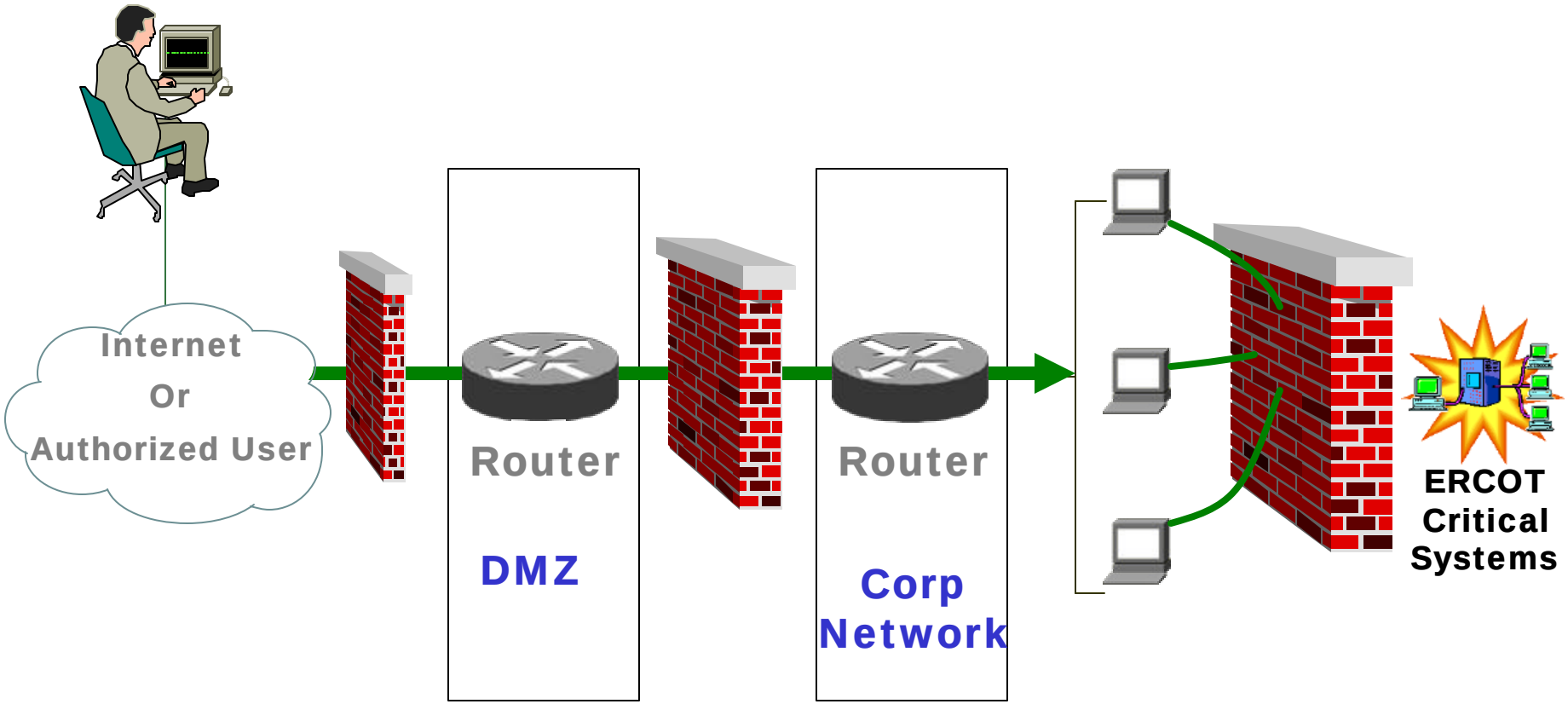
They rob workers of productivity, divert IT personnel from more strategic corporate concerns, and can even jeopardize your company's information security.

Multiple Layer Defense Strategy

- Several “filtering” processes are employed
- First allows appropriate access from Internet
- More restrictive filters are employed from the internet to an intranet connection
- Applications are buffered from access through use of a DMZ

Defense in Depth Strategy

September 2003



Questions?

Contact Chris Uranga
512.248.3092
curanga@ercot.com