



HIGHTOWER

The Evolution of Threats and their Impact upon Technology

Interop 2008

Las Vegas, Nevada

E. Eugene Schultz, PhD., CISSP, CISM
Chief Technology Officer & Chief Information
Security Officer

High Tower Software
gschultz@high-tower.com

Copyright 2008 High Tower – All Rights Reserved



About information security-related threats

- Formal definition of threat—” An expression of an intention to inflict pain, injury, evil, or punishment. An indication of impending danger or harm.”
- In information security—threats are sources of potential or actual security-related compromise, damage, disruption or loss
 - Must be thoroughly evaluated and understood if a risk analysis is to be valid and meaningful
 - Usually evaluated in terms of type, nature and extent
 - Subject to sudden and drastic change

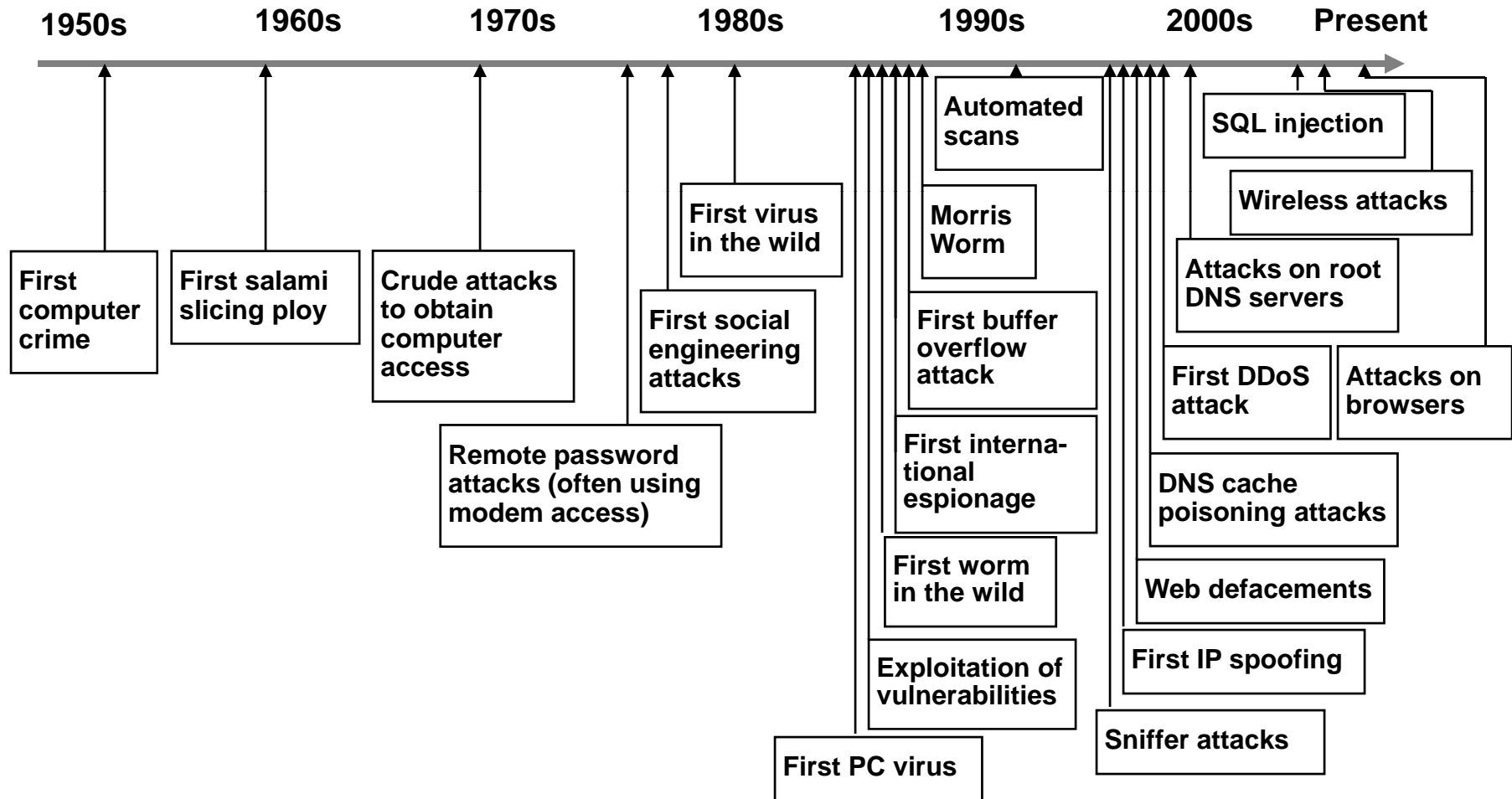


About information security-related technology

- A wide range of technology, all of which is purported to be able to very effectively mitigate security-related risk, exists
- How does one even start in evaluating all of this technology?
- Major issues to be addressed in this presentation include
 - Has security technology provided sufficient control over threats that have surfaced over the years?
 - Which security technologies have in general worked worst/best and why?

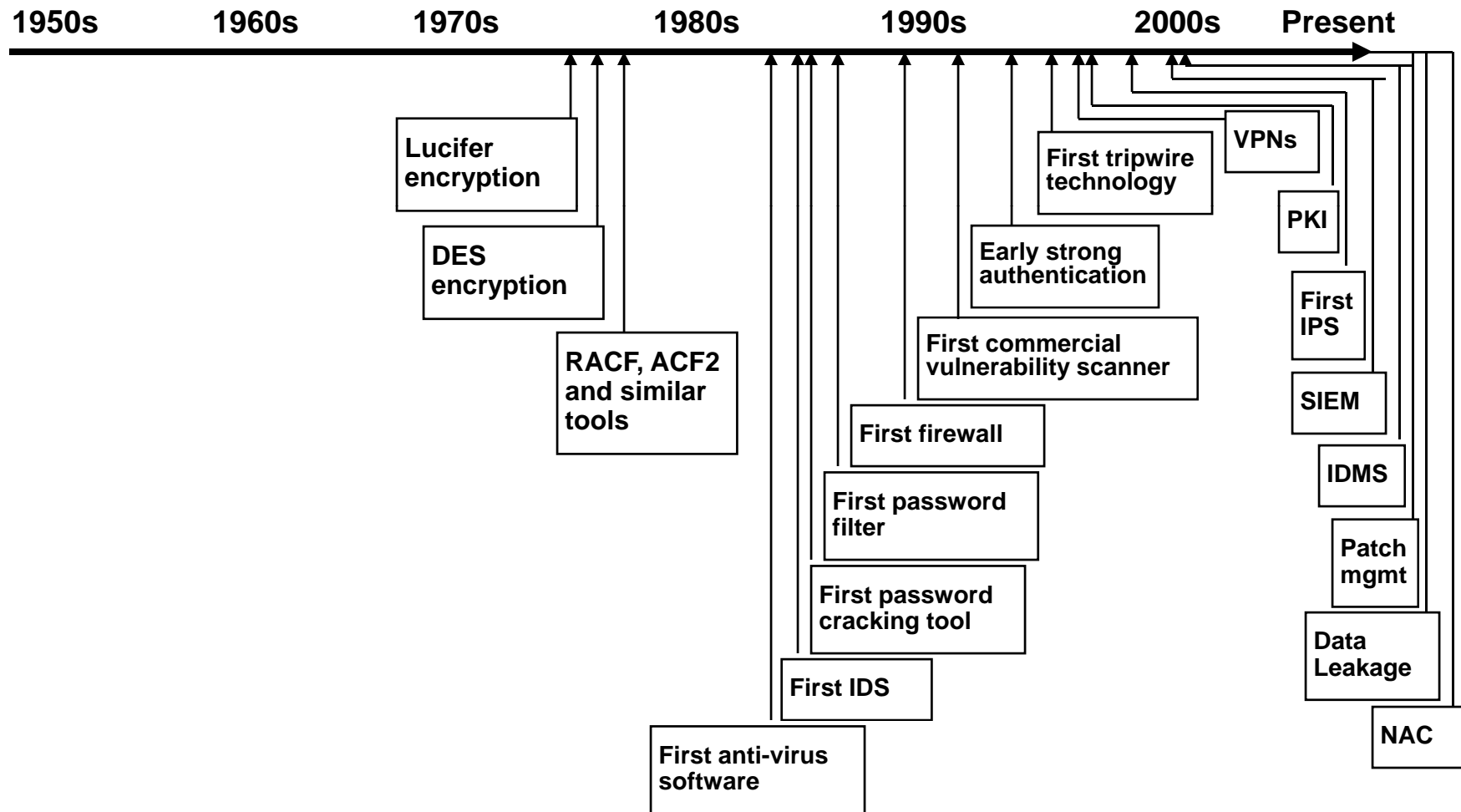


A threat timeline





A security technology timeline





Has security technology provided sufficient control over threats?

- No amount of technology, no matter how good, can solve the whole problem
 - There will always be residual risk
- New technology invariably lags behind new threats
- BUT—*security risks have proliferated and have become so technical in nature that they are now not manageable without suitable security technology*
 - Insufficient human resources available
 - Speed of response needed not possible with humans
 - Potentially prohibitive costs
 - Lack of necessary skills and knowledge



A comparison of certain security technologies

LESS ADEQUATE	MUCH MORE ADEQUATE
<ul style="list-style-type: none">• Password filters• PKI• Network Access Control (NAC)• Some types of intrusion prevention	<ul style="list-style-type: none">• Tripwire tools• Identity management tools• Patch management tools• Security Information/Event Management (SIEM) tools



Some technologies have proven useful, but are starting to show their age

- Firewalls
- Intrusion detection systems
- Anti-virus software



Why some technologies work better than others

- Some are more conducive to mitigating particular types of risk resulting from threats than others
- Cost versus benefit ratios are higher for some types of technology
- Some technologies have proven more flexible and adaptive than others
- Some are more strategic and long lasting than others
- Some solve both security and non-security needs (the “two-in-one” benefit)



Conclusion

- Security threat has evolved to the point that security technology is now more of a necessary component of every security practice than ever before
- Information security staff need to recognize where each given technology fits into a basic prevention-detection-response framework
- Obtaining information about the probable longevity of any security technology is essential while the technology is being evaluated



Conclusion

- Understanding the amount of residual risk and the implications after technology is deployed is also necessary
- No matter how automated any technology is, there is still a critical need for humans in the loop
- Ultimately, any security technology is successful only to the degree that it produces a favorable cost-benefit ratio
 - Metrics must be developed and used to determine whether technology controls are meeting their objectives

Continued

The background of the slide is a solid black color. On the left side, there are several overlapping, flowing, curved lines in various shades of red, ranging from a deep, dark red to a bright, almost white-red. These lines create a sense of movement and depth, resembling smoke or liquid in motion. The lines are most prominent on the left and fade out towards the right.

Questions?