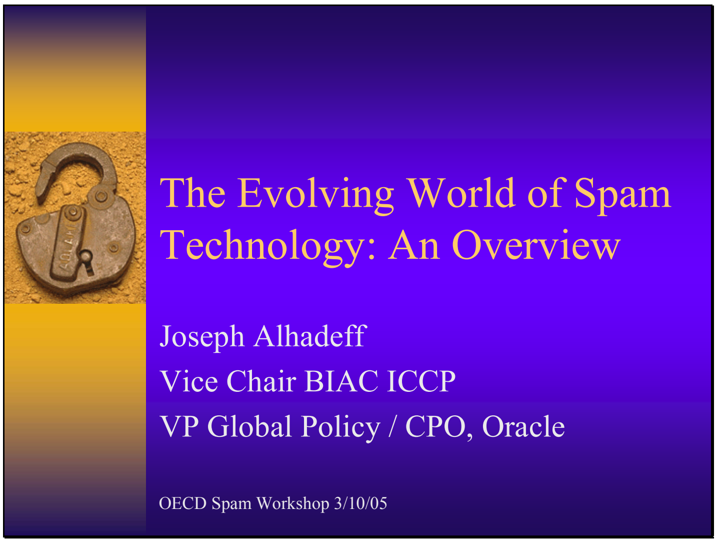


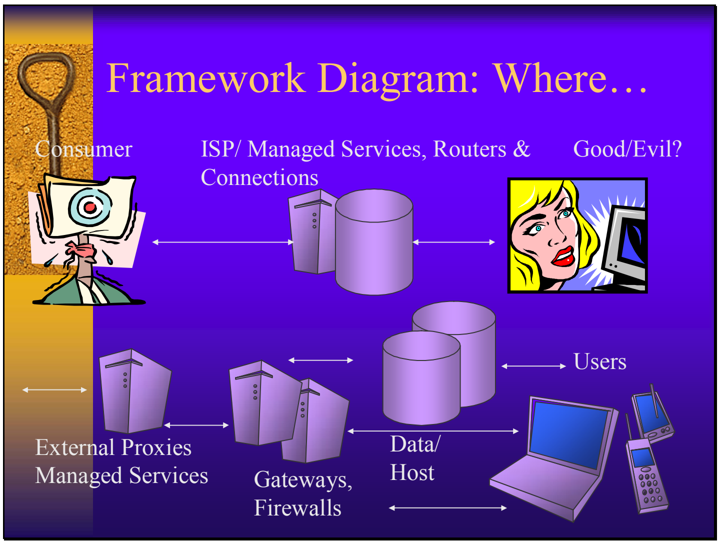
The Evolving World of Spam Technology: An Overview

Joseph Alhadeff

Vice Chair BIAC ICCP

VP Global Policy / CPO, Oracle

OECD Spam Workshop 3/10/05



Framework Diagram: Where…

Consumer

ISP/ Managed Services, Routers & Connections

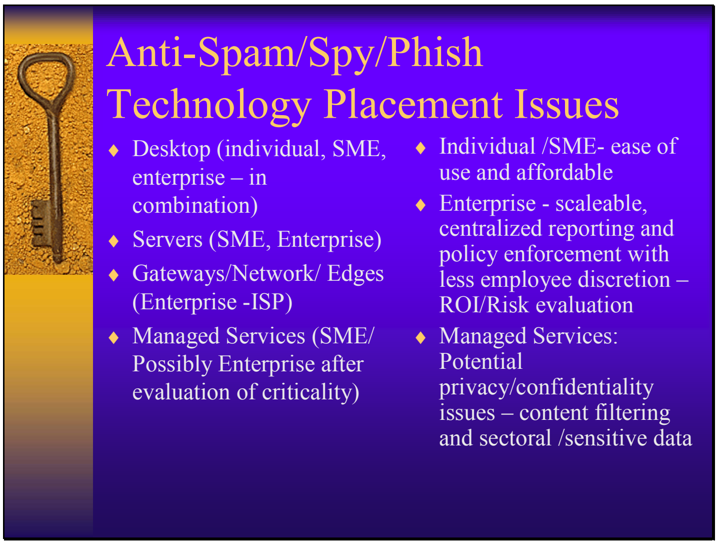
Good/Evil?

Users

External Proxies Managed Services

Gateways, Firewalls

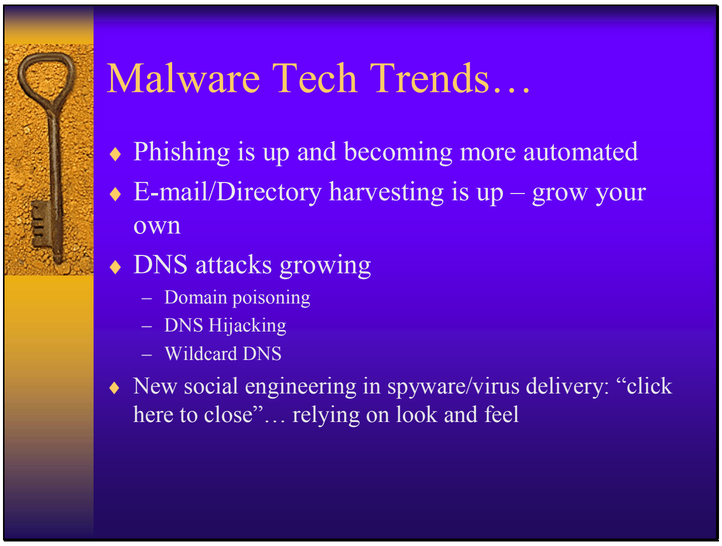
Data/ Host



Anti-Spam/Spy/Phish Technology Placement Issues

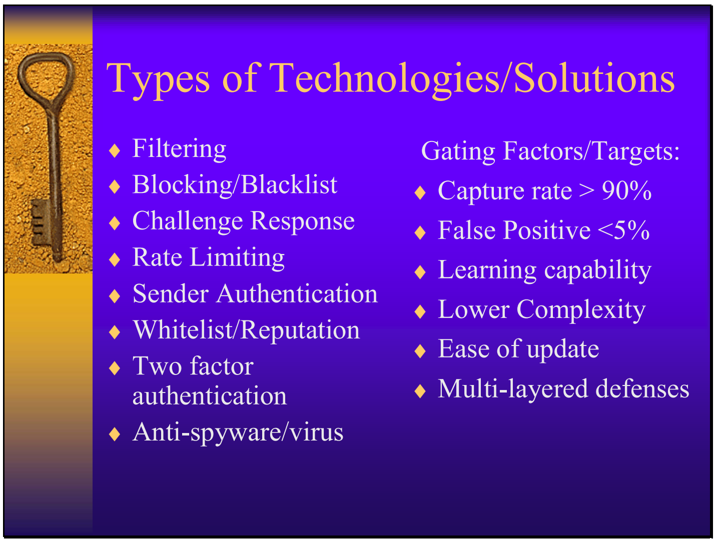
- Desktop (individual, SME, enterprise – in combination)
- Servers (SME, Enterprise)
- Gateways/Network/ Edges (Enterprise -ISP)
- Managed Services (SME/ Possibly Enterprise after evaluation of criticality)

- Individual /SME- ease of use and affordable
- Enterprise - scaleable, centralized reporting and policy enforcement with less employee discretion – ROI/Risk evaluation
- Managed Services: Potential privacy/confidentiality issues – content filtering and sectoral /sensitive data



Malware Tech Trends…

- Phishing is up and becoming more automated
- E-mail/Directory harvesting is up – grow your own
- DNS attacks growing
  - Domain poisoning
  - DNS Hijacking
  - Wildcard DNS
- New social engineering in spyware/virus delivery: “click here to close”… relying on look and feel

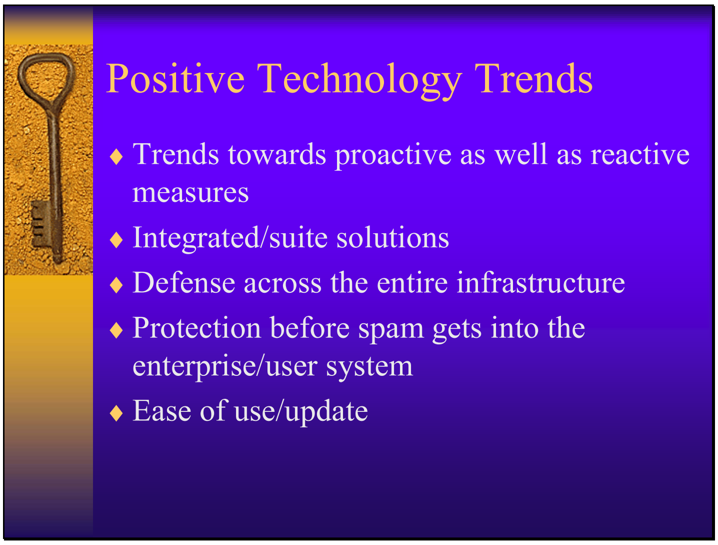


Types of Technologies/Solutions

- Filtering
- Blocking/Blacklist
- Challenge Response
- Rate Limiting
- Sender Authentication
- Whitelist/Reputation
- Two factor authentication
- Anti-spyware/virus

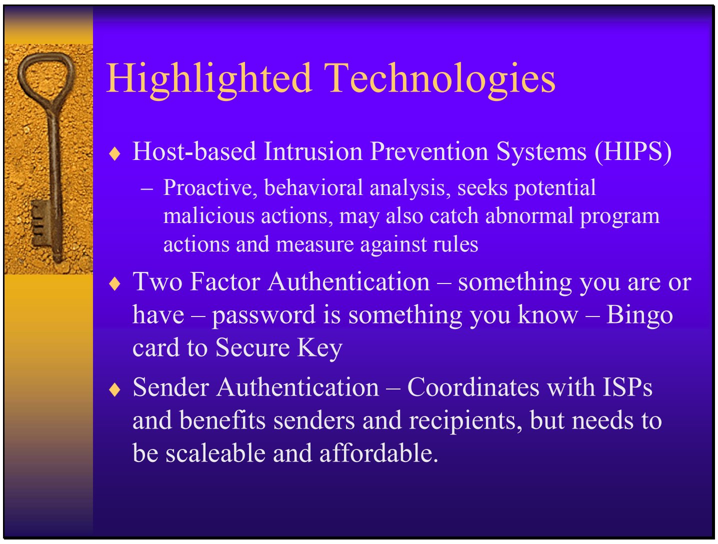
Gating Factors/Targets:

- Capture rate > 90%
- False Positive <5%
- Learning capability
- Lower Complexity
- Ease of update
- Multi-layered defenses



Positive Technology Trends

- Trends towards proactive as well as reactive measures
- Integrated/suite solutions
- Defense across the entire infrastructure
- Protection before spam gets into the enterprise/user system
- Ease of use/update

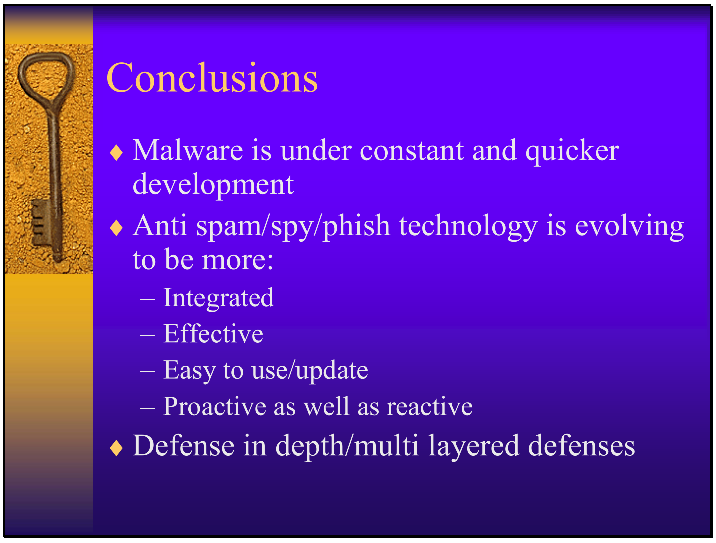


Highlighted Technologies

- Host-based Intrusion Prevention Systems (HIPS)
  - Proactive, behavioral analysis, seeks potential malicious actions, may also catch abnormal program actions and measure against rules
- Two Factor Authentication – something you are or have – password is something you know – Bingo card to Secure Key
- Sender Authentication – Coordinates with ISPs and benefits senders and recipients, but needs to be scaleable and affordable.

Anti Spam / Filters

- Lexical analysis –phrases/words/Header/keyword
- Signature – additive; effective for know spam
- Bayesian – Algorithm of attributes – probability of spam
- Natural Language Processing – context-based correlates text and categories of meanings
- Collaborative/Community – group decision making and posting on spam
- Heuristics – more proactive, rules of analysis
- Toolkit – blend of the above



Conclusions

- Malware is under constant and quicker development
- Anti spam/spy/phish technology is evolving to be more:
  - Integrated
  - Effective
  - Easy to use/update
  - Proactive as well as reactive
- Defense in depth/multi layered defenses