Export Controls on "Recoverable" Products under the Export Administration Regulations: Alliance for Network Security's Report to the Interagency Working Group on Encryption Washington, D.C. ~ June 23, 1999

Background

The Alliance for Network Security ("ANS") was formed in 1998 to engage in a dialog with the law enforcement and intelligence communities concerning the impact of recoverable products on their missions and to make recommendations regarding export controls on "recoverable" products under the Export Administration Regulations ("EAR"). The members of ANS are 3Com, Ascend, Cisco, Hewlett-Packard, Intel, Lucent, Microsoft, NetScreen, Network Associates, Nortel, Novell, RedCreek, Secure Computing and Sun Microsystems. In the first half of 1999, ANS members have conducted an analysis of the market for recoverable products and a study of the cost of compliance with encryption export controls. The results of these studies, and ANS' recommendations with respect to the export controls on recoverable products under the EAR, are summarized in this document.

Market Analysis

ANS contracted with Datamonitor, Europe's leading independent research-based consulting firm in the information technology industry, to conduct a survey concerning the impact of export controls on recoverable products, as a part of its comprehensive study of the security industry. Datamonitor determined that American companies dominate the market for recoverable products, today. Using several different methodologies, Datamonitor estimates that relaxation of export controls as advocated by ANS would result in a revenue increase of approximately $1/3 billion and an increase in market share of approximately 10% for American companies over the next five years. In addition, and perhaps just as important, American companies could expect commensurate increases in service and management contracts and new infrastructure business.

American dominance of the market for recoverable products is based on a number of assumptions. The most important assumption is that American companies will successfully compete in the new era of converged (voice and data) networks. Historically, local companies dominated national markets for circuit switching networks. More recently, American companies dominated the worldwide market for data networks. As voice and data networks converge, this new market will be contested by both local companies specialized in circuit switching networks and American companies specialized in data networks. There are two "nightmare" scenarios for ANS members.

In the "Jaws" scenario, a foreign competitor emerges and dominates the market for converged networks, crushing its American rivals by offering high quality networking equipment combined with a "best of breed" security product. A merger between a traditional network equipment supplier like Alcatel, Ericsson or Siemens and Checkpoint, which is the leading vendor of firewall-based virtual private networks ("VPN"), could produce such a scenario.

In the "Chickens" scenario, not one but many foreign competitors emerge and dominate their local markets for converged networks. American rivals would not be crushed, but the net effect of such a balkanized market would be that the American companies get pecked to death, by chickens.

Cost of Compliance Survey

ANS conducted a survey, sampling three large networking companies and three smaller network appliance companies. Results show that the large companies are spending in excess of $10 million per year each, and smaller companies are spending approximately 10% of the total revenues per year each, to comply with encryption export controls. This cost reduces profits significantly, making it difficult to compete with foreign firms.

ANS Recommendations

ANS respectfully recommends that the Administration's export policy for recoverable products be expanded and that the Commerce Department's Bureau of Export Administration amend the provisions of the EAR governing recoverable products in the following respects:

1. Authorize Exports under License Exception

Datamonitor's research shows that the majority of recoverable products are sold via distribution channels, rather than directly to end-users, because sales through distributors require less staff, language and cultural understanding, and permits faster growth. Efficiencies of the distribution channels permit U.S. firms to bring products to market rapidly, in high volumes, and at competitive prices. Distribution channels include consultants, system integrators, value added resellers, resellers, service providers and outsourcers. By authorizing exports under License Exception, rather than Encryption Licensing Arrangements ("ELAs"), BXA would accomplish three goals. First, it would permit distribution channel partners to use the same License Exception, thus facilitating the delivery of recoverable products to the market. Second, it would reduce duplicate ELA requests from the entire distribution channel for some products that have already been reviewed. Third, it would shift responsibility for compliance with the EAR from the manufacturer to the distribution partner, who is better positioned to evaluate the bona fides of a particular end-user.

2. Authorize Telco/ISP Deployments for Subscriber Use

Datamonitor's research also shows that approximately half of VPN sales today are to service providers, such as Telco/ISPs, who deploy them for subscriber use, because the complex nature of VPN products requires expertise that the Telco/ISPs are well positioned to provide. The outsourcing of communications and security services is a common business practice.

3. Eliminate End-user Reporting

End-user reporting is burdensome, because so few sales are made directly to end-users. Distribution partners are reluctant to disclose their customers to manufacturers, for competitive reasons. As a possible compromise, ANS recommends authorizing exporters to report sales to distribution partners, and require distribution partners to report separately their re-exports to end-users.

4. Authorize Secure Extranets

Datamonitor reports that, whereas electronic commerce in the United States is mostly business to consumer (B2C) using client-server products implementing SSL, electronic commerce in Europe is mostly business to business (B2B) using peer-to-peer products, implementing IPSec. The condition that recoverable products are "limited to internal use" inhibits use of recoverable products in B2B electronic commerce. This limitation will preclude business partners from communicating with each other and is a "showstopper" for many potential exports of recoverable products.

5. Authorize Exports to Additional Countries

Datamonitor reports that the market outside the United States will grow faster than the market inside the United States, and that "rest of world" will grow faster than Europe. Therefore, the fastest growing markets are not authorized under current ELAs. ANS recommends that sales be authorized to all countries (except embargoed/terrorist countries).

6. Authorize Sales to Certain Governments

Datamonitor did not break out sales to governments vs. other end-users. The informal view of Datamonitor representatives is that government VPN sales are growing. Civilian government agencies are likely to deploy commercial off-the-shelf recoverable products rather than design their own (like civilian U.S. government agencies). As a possible compromise, ANS recommends approval of sales to civilian government agencies. ANS notes that even with such a compromise, U.S. vendors will remain at a disadvantage vis-à-vis local competitors that generally are the preferred suppliers to local governments.

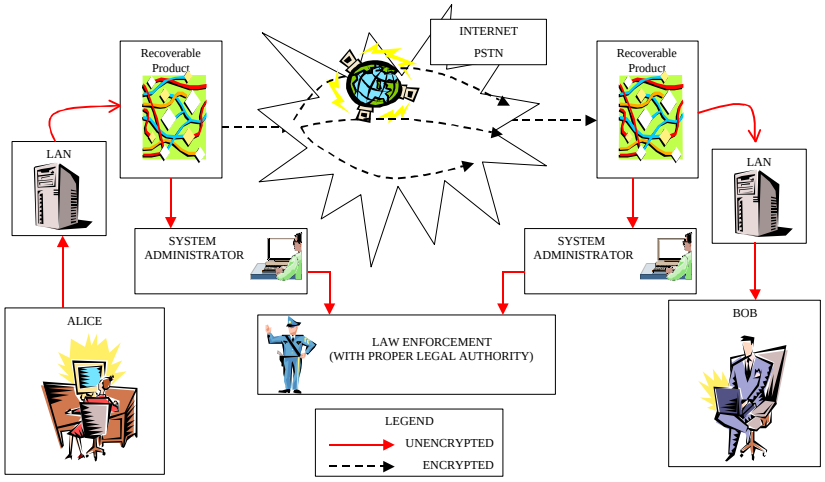
7. Change "Recoverable" to "Administrator-Controlled"

The public is confused by the similarity between "recovery" products and "recoverable" products. Therefore, ANS recommends that the term "recoverable" be changed to "administrator-controlled".

Conclusion

Customers like administrator-controlled products because they can obtain strong cryptography without the vulnerability of key escrow. Law enforcement likes administrator-controlled products because it can obtain access to plaintext using existing practices. The intelligence community would prefer an encryption-free world, but that is no longer an option. Administrator-controlled products are no more (or less) useful to the intelligence community than key escrow products. Not permitting U.S. companies to compete in these markets with their administrator-controlled products simply gives away foreign market share to foreign competitors, thus also impacting the intelligence community. If American companies are allowed to export administrator-controlled products, then intelligence community also obtains a "home field" advantage by understanding the products, which they have said is important. For these reasons, among others, the recommendations suggested by the ANS should be published in the form of a new interim rule with request for comments at the earliest opportunity.

Administrator-Controlled Intermediate Systems



Administrator-Controlled Remote Access Systems