Inside Risks ??? (*CACM ??,* ??, Jan 1999)
Our Evolving Public Telephone Networks
Fred B. Schneider and Steven M. Bellovin

The public telephone network (PTN) in the U.S. is changing—partly in response to changes in technology and partly due to deregulation. Some changes are for the better: lower prices with more choices and services for consumers. But there are other consequences and, in some ways, PTN trustworthiness is eroding. Moreover, this erosion can have far-reaching consequences. Critical infrastructures and other networked information systems rely today on the PTN and will do so for the foreseeable future.

Prior to the 1970's, most of the U.S. telephone network was run by one company, AT&T. AT&T built and operated a network with considerable reserve capacity and geographically diverse, redundant routings, often at the explicit request of the federal government. Many telephone companies compete in today's market. So cost presures have become more pronounced. Reserve capacity and rarely-needed emergency systems are now sacrificed on the altar of cost. And new dependencies—hence, new vulnerabilities—are introduced because some services are being imported from other producers.

Desire to attract and retain market share has led telephone companies to introduce new features and services. Some new functionality (such as voice menus within the PTN) relies on call-translation databases and programmable adjunct processors, which introduce new points of access and, therefore, new points of vulnerability. Other new functionality is intrinsically vulnerable. CallerID, for example, is increasingly used by PTN customers, even though the underlying telephone network is unable to provide such information with a high degree of assurance. Finally, new functionality leads to more-complex systems, which are liable to behave in unexpected and undesirable ways.

You might expect that having many phone companies would increase the capacity and diversity of the PTN. It does, but not as much as one would hope. To lower their own capital costs, telephone companies lease circuits from each other. Now, a single errant backhoe can knock out service from several different companies. And there is no increase in diversity for the consumer who buys service from many providers. Furthermore, the explicit purchase of diverse routes is more difficult to orchestrate when different companies must cooperate.

In addition, the need for the many phone companies to interoperate has itself increased PTN complexity. Second, competition for local phone service has necessitated creating databases (updated by many different telephone companies) that must be consulted in processing each call, to determine which local phone company serves that destination.

The increased number of telephone companies along with an increased multiplexing of physical resources has other repercussions. The cross connects and multiplexors used to route calls depend on software running in operations support systems (OSSs). But information about OSSs is becoming less proprietary, since today virtually anybody can form a telephone company. The vulnerabilities of OSSs are thus accessible to ever larger numbers of attackers. Similarly, the SS7 network used for communication between central office switches was designed for a small, closed community of telephone companies; deregulation thus increases the opportunities for insider attacks (because anyone can become an insider by becoming a telephone company). Security by obscurity is not the solution: network components must be redesigned to provide more security in this new environment.

To limit outages, telephone companies have turned to newer technologies. Synchronous Optical Network (SONET) rings, for example, allow calls to continue when a fiber is severed. But despite the increased robustness provided by SONET rings, using high-capacity fiber optic cables leads to greater concentrations of bandwidth over fewer paths, for economic reasons. Failure (or sabotage) of a single link is thus likely to disrupt service for many customers—particularly worrisome, because the single biggest cause of telephone outages is cable cuts.

Today's telephone switches—crucial components of the PTN—are quite reliable. Indeed, a recent National Security Telecommunications Advisory Committee study found that procedural errors, hardware faults, and software bugs were roughly equal in magnitude as causes of switch outages. Reducing software failure to the level of hardware failures is an impressive achievement. But switch vendors are coming under considerable competitive pressure, and they, too, are striving to reduce costs and develop features more rapidly, which could make matters worse.

Fred B. Schneider (Cornell University) and **Steven M. Bellovin** (AT&T Labs Research) served on the NRC Computer Science and Telecommunications Board committee that authored *Trust in Cyberspace*. Chapter 2 of that report (see www2.nas.edu/cstbweb/index.html) discusses the eroding trustworthiness of the PTN. See *Inside Risks 101* (Nov. 1998) for a summary of the report.