FEATURE ARTICLE

Leading the COMSEC Revolution

The STU-III Secure Telephone

JOHN C. NAGENGAST

A quiet revolution has begun in US telecommunications, one that will dramatically change how we secure our classified and sensitive communications from potential adversaries. The ultimate result will be better and considerably less expensive communications security, readily available at an affordable price to anyone in the US who needs it.

Leading the revolution is the STU-III Program. Known as the Future Secure Voice System project, the National Security Agency sponsored this major initiative in partnership with the telecommunications industry to develop and deploy a new family of telephone security equipment which went far beyond the capabilities of anything previously available.

For the first time, a secure telephone that looks and operates just like a regular telephone can be installed by the user in minutes. The new secure telephone replaces the standard unit and does not need to be locked in a vault for the night. In its basic form, it will be available at a price under $2,000 and even a choice of colors. Most important, the realization of this new secure phone is anticipated within a timeframe previously unheard of for Government communications security equipment.

INCEPTION OF THE STU-III

In 1983, the National Security Agency began to take a hard look at US COMSEC in general and at telephone security in particular. NSA assessed the situation in one word, "dismal." The existing secure telephone system for the US Government was the aging AUTOSEVOCOM system which used equipment built in the 1950s and 1960s and relied on expensive leased circuits. Furthermore, AUTOSEVOCOM served only a very limited number of users, a number that was actually shrinking because of the obsolescence and expense of the system.

Although development of the STU-II secure telephone had begun in 1975, delivery of the equipment was just beginning in 1983. The price of the STU-II was on the order of $12,000, and installation and maintenance costs were considerable. Also, the STU-II was designed for a projected user population of only 10,000. A quick analysis of the requirements for secure telephones for the mid-1980s put the figure for the Federal Government and for related users closer to half a million.

In addition, NSA and other key planners were beginning to realize that a solution for telephone security could not just address the traditional Government community of COMSEC users. Many areas of the private sector deal with sensitive information which can affect our national well-being in both the short and long term.

As a hypothetical example, consider a telephone call between the president of a large US oil company and one of its officials in a Middle East country, in which they discuss sensitive negotiations being conducted to avert a potential embargo of crude oil shipments to the US. An eavesdropper with hostile intentions towards the US could exploit this information to the detriment of our national interests.

It quickly became obvious that a whole new initiative was needed in telephone security — one that would address the entire spectrum of needs, and at an affordable cost. Moreover, the solution was needed quickly. A traditional acquisition program, with a long development and test cycle, was out of the question. With this perspective, a radically different approach began to take shape.

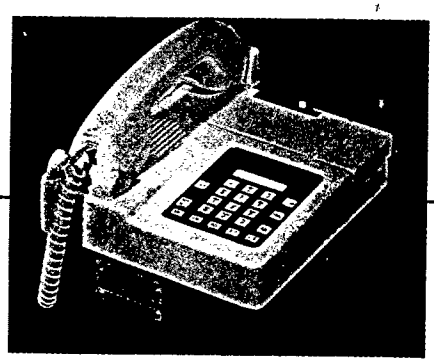
THE PROGRAM STRATEGY

It became clear that to do what was needed, NSA was going to have to use the same kind of approach industry would use in bringing a product to the commercial marketplace. This approach would have to provide considerable incentive to the developers of the secure telephone and create competition among a number of suppliers to insure getting the best product at the best price.

At the same time, NSA recognized that there were unique requirements for secure telephones for specialized uses, such as command and control. It was not necessary or economical to provide these features in every secure telephone. The majority of secure telephone users simply do not need them. Thus, the STU-III was conceived as a family of equipment: The STU-III/Low Cost Terminal would be designed for the regular users, with low price of ownership being a primary goal. The STU-III/Command and Control (C^2) Terminal would provide flexible multifunction capabilities with unique features for special applications.

NSA was already developing a compact version of the STU-II for mobile radio telephone applications. After careful examination, it was decided that this equipment could serve as the basis for the STU-III/C^2. It was an approach which capitalized on existing development with the

[Continued on page 20]



STU-III/C² being developed by RCA.

added benefit of providing an equipment, no bigger than a shoebox, which would be compatible with the STU-II.

For the STU-III/LCT, however, NSA was essentially starting from scratch, and a way had to be found to quickly bring the product from the conceptual stage to fruition. First, the idea had to be converted into specific concepts and a functional definition, combining NSA's knowledge of cryptography with the capabilities and experience of the telecommunications industry. Second, NSA had to establish a competitive, multivendor base for large-volume production at a low price.

In order to achieve this rather tall order, a two-phased approach was laid out. The first phase, lasting six months, would be a competitive concept definition study among the top companies in the field. Then, the winners of the concept definition would enter a two-year, integrated development and initial production phase, with continued competition among the participants for the initial production.

THE CONCEPT DEFINITION PHASE

Early in 1984, after an extensive review of US telecommunications/electronics companies and their capabilities, NSA selected five firms to participate in a competitive concept definition for the STU-III/LCT. The companies were AT&T, GTE, ITT, Motorola and RCA.

The ground rules for the study were straightforward. At the end of the six-month study phase, NSA would pick at least two companies for the actual development. NSA would specify only the minimum performance and security requirements; the companies would be free to propose the best design concept and how they would begin volume production two years from the start of the development. Finally, the winners would share in an initial large purchase by NSA and would also sell their product directly to the US marketplace, including the Government and private sectors.

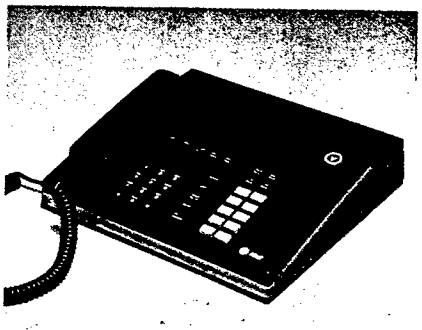
A unique feature of the competition was that the resulting independent designs all had to be able "to talk to each other" (as well as to the STU-III/C²). Considerable time and effort was spent by NSA and the participating companies during the concept definition to hammer out an interoperability specification. This stage created some interesting moments, with five companies in heated competition being forced to come together in one room and agree on something which would have considerable impact on their own design. To the credit of all involved, the overall success of the program took precedence over the individual interests, and agreement was reached.

THE DEVELOPMENT/INITIAL PRODUCTION PHASE

The concept definition phase was completed on schedule in November 1984, with each company submitting a detailed Concept Definition Report. After an extensive evaluation, development contracts were awarded in March 1985 to AT&T, Motorola, and RCA. A fourth company, GTE, was chosen to develop central system management facilities which would provide automated capabilities for ordering and distribution of cryptographic key (a sequence of random numbers which control the encryption and decryption process) for the STU-III and other functions indigenous to a large-scale secure telephone system.

The total cost to the Government for these developments is expected to approach ninety million dollars. In addition, in order to be in the best possible competitive position, the three LCT developers are investing a significant amount of their own resources in the program.

Each of the three developers is required to demonstrate prototype units to NSA at Month 12 of the development/initial production phase. NSA will award the initial production contracts shortly thereafter, basing each vendor's share on price, equipment function and features, and performance in completing the prototype units. At Month 15, each vendor will deliver forty units for an extensive field test by the Government.



AT&T STU-III LCT.

The prototype equipments will first be evaluated in a formal system testbed to verify proper operation, including interoperability

[Continued on page 22]

of the various vendors' equipments. The equipment will then be placed in the hands of a variety of users worldwide to evaluate its performance under actual field conditions. The vendors will be required to correct any deficiencies identified during the prototype testing prior to their delivery of the first production units. Finally, at Month 24, the actual production will begin.

Each participating company has planned a fully automated production capability for the STU-III/LCT, with capacity to build in excess of 10,000 units a month.

THE STU-III FROM A USER'S PERSPECTIVE

What does all this mean to the user? First of all, the user will have a choice. He can select the version that best fits his needs or the type of service plan a particular vendor may offer. It will also be possible for the user to request a special feature or a custom interface to meet the requirements of his PBX.

Next, the STU-III will be easy to install. The normal interface is the common, garden-variety modular jack, so that the STU-III can be plugged in anywhere an ordinary phone can. For office installations with multiline phones, i.e. those with five-line select and hold buttons, an optional version will be available that mates with the standard 1A2 connector used in these installations. If a custom installation is required, the user can arrange it with the STU-III vendor of his choice. And, unlike previous secure telephones, the STU-III will operate over a single standard phone line.

The real test is when the STU-III is in place and ready for that first phone call. A secure call is placed just like a regular call. In fact, until the secure button is pressed, it is a regular call using normal dialing procedures and going over the telephone network in standard fashion. When the other party answers, either one can press the secure button initiating an authentication procedure between the two telephones lasting no more than twelve seconds. The two parties can then converse without fear of being overheard by anyone along the transmission path.

Motorola STU-III terminal.

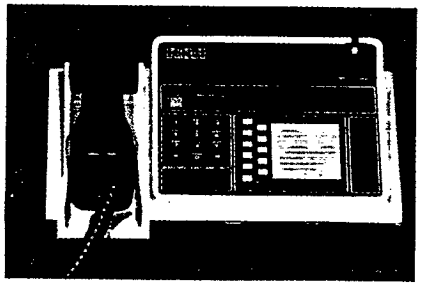
The various STU-III telephones will all offer a number of modern telephone features, such as one-button speed dialing for frequently called numbers and all the units include a feature called the Crypto Ignition Key, or CIK for short.

The CIK serves two fundamental purposes. When it is removed, the STU-III becomes unclassified and no special storage area or vault is necessary. Also, without the CIK, the STU-III cannot be used in the secure mode, preventing unauthorized use, even though it will continue to serve as a regular phone to place or receive nonsecure calls. In addition, the STU-III will incorporate a display which, when in the secure mode, tells the user who he is talking to and what the authorized classification level for the conversation is, based on the security clearances of the participating parties. The display also prompts the user if he makes a mistake, such as attempting to go secure when he has forgotten to insert the CIK.

FUTURE EVOLUTION OF THE STU-III

An important consideration for the future is how the STU-III family will evolve to cover new requirements and keep pace with rapidly changing telecommunications technology. NSA will continue its involvement with the vendors to insure the security of the product, but it will be up to the vendors to develop newer, more flexible versions of the equipment.

Additions to the product line could include models for mobile or hand-held cellular radio applications, or a unit which provides wideband capabilities for use in the coming Integrated Services Digital Network (ISDN). Also, the vendors will be able to incorporate new technology, such as sub-micron level VLSI to produce a smaller, lower cost STU-III in the years to come. Finally, other vendors will be able to build STU-III compatible products to compete with the original three on the basis of more features, better service or lower price. What this means is that the STU-III will be an evolving product — one that gets better as time goes on.



RCA's STU-III.

John C. Nagengast, *is currently the Deputy Chief of the Future Secure Voice System Special Project Office (FSVS SPO), the National Security Agency.* ■