

Seguridad de las Computadoras

¿El Talón de Aquiles de la Fuerza Aérea Electrónica?*

TENIENTE CORONEL ROGER R. SCHELL, USAF

El oficial de la KGB se dirigió al grupo selecto de oficiales soviéticos con el acostumbrado tono secreto pero con un aire de excitación inusual:

Camaradas, hoy les hablaré de uno de los descubrimientos más significativos de recopilación de inteligencia desde que se “descifraron” los códigos “indescifrables” japonés y alemán en la SGM—la penetración de la seguridad de las computadoras estadounidenses. Prácticamente (incluso literalmente) no hay ningún secreto importante de defensa nacional de EE.UU. que no esté guardado en una computadora, en algún lugar. Al mismo tiempo, hay pocas computadoras (de haberlas) en su sistema de defensa nacional que no sean accesibles en teoría, e incluso en la práctica, a nuestra curiosidad. Y lo que es aún mejor, no tenemos que esperar a que envíen esa información particular que deseamos para que podamos interceptarla; podemos solicitar y obtener materiales de interés específicos para nosotros, sin prácticamente ningún riesgo para nuestros agentes.

Los estadounidenses han desarrollado una tecnología de “núcleo de seguridad” para resolver su problema, pero no necesitamos preocuparnos—recientemente discontinuaron el trabajo en esta tecnología. Son conscientes del potencial de un problema de seguridad informático, pero con su descuido habitual decidieron no corregir el problema hasta que se verificaran ejemplos de nuestra explotación activa. Nosotros, por supuesto, no les debemos dejar encontrar estos ejemplos.

Su primera reacción a esta situación puede ser, “¡absurdo!” Pero antes de rechazarla de inmediato, reconozcamos que sabemos que puede pasar. La pregunta es la siguiente: ¿aplicaremos una tecnología y una política firmes antes de que ocurra esto? Para asegurarnos de ello, hay cosas que no sabemos sobre la probabilidad de éxito de un esfuerzo de ese tipo, pero podemos evaluar racionalmente los factores de control más sobresalientes:

- La gran *vulnerabilidad* de las computadoras contemporáneas se ha indicado claramente en la experiencia del autor con una penetración sin detectar mecanismos de seguridad. Además, las debilidades de seguridad están documentadas en informes militares y civiles.
- La *capacidad* de los soviéticos (o de cualquier grupo hostil importante) para lograr la penetración requerida es bastante evidente. De hecho, no se requieren destrezas particulares más allá de las de los profesionales informáticos normalmente competentes.
- La *motivación* de dicha actividad de recopilación de información es aparente evidentemente a primera vista. Con frecuencia se informa del gran alcance y de la gran intensidad de los esfuerzos de inteligencia soviéticos en áreas como la interceptación de comunicaciones.
- El *daño* potencial de la penetración aumenta con la cada vez mayor penetración de información sensible en computadoras y la interconexión de estas computadoras en redes grandes. Mediante la penetración en computadoras un enemigo podría, por ejemplo, arriesgar planes de empleo de aviones caza tácticos o arriesgar planes de operación y determinar objetivos para misiles nucleares.
- La *oportunidad* de una explotación hostil de estas vulnerabilidades está aumentando cada vez más debido al mayor uso de computadoras y a la falta de una política de seguridad significativa que controle su uso. En nombre de la eficiencia se permite a muchas más perso-

*Reprinted from *Air University Review* 30, no. 2 (January–February 1979): 16–33.

nas con menos (o ninguna) autorización un acceso más sencillos a los sistemas de computadoras clasificados.

Tenemos un problema y una solución a mano. El examen detallado de la capacidad y motivación de una nación hostil (por ejemplo, Unión Soviética) en esas áreas está debidamente en el campo del analista de inteligencia y en gran medida fuera del alcance de este artículo. No obstante, trazará los límites del problema de seguridad de la computadora y mostrará cómo el método del núcleo de seguridad cumple los requisitos para una solución factible—aunque la terminación reciente ha cortado de raíz un trabajo muy prometedor hacia una solución.

¿Qué es lo que hace que las computadoras sean un problema de seguridad?

Aunque es necesaria una cierta apreciación de sutileza para entender los detalles del problema de seguridad informática, nuestro objetivo aquí es iluminar los temas básicos fundamentales. Para entender estos temas, examinaré no solamente las capacidades y limitaciones de las computadoras mismas sino también sus usos.

En primer lugar, damos por sentada la necesidad fundamental de proteger debidamente contra los riesgos la información militar sensible clasificada. Desde hace mucho tiempo, se ha reconocido la seguridad como uno de los principios bélicos básicos, y a través de la historia, la seguridad o su falta han sido un factor importante en el resultado de batallas y guerras. Podemos y controlamos estrictamente la información cuando la diseminación es teórica. Por lo tanto, no es lógico hacer caso omiso del hecho de que las computadoras puede diseminar la misma información a cualquiera que sepa cómo pedirla, omitiendo completamente los costosos controles que ponemos en la circulación de documentos.

En segundo lugar, debemos apreciar que la “explotación del crecimiento fenomenal de las ciencias informáticas es un área importante de énfasis tecnológico dentro del DoD”.¹ Actualmente, carecemos de una superioridad cuantitativa (o incluso paridad) en varias áreas de niveles de fuerzas, y las computadoras parecen proporcionar la superioridad cualitativa que debemos tener. La necesidad de estas capacidades es clara cuando nos damos cuenta de que las buenas capacidades “C³ [comando, control y comunicaciones] pueden duplicar o triplicar la eficacia de la fuerza; por el contrario, una C³ ineficaz ciertamente pone en peligro o niega el objetivo buscado”.² De hecho, nos hemos convertido en un sentido muy real en una “Fuerza Aérea electrónica”³ con computadoras como base.

Por último, necesitamos reconocer que algunas vulnerabilidades importantes pueden acompañar a las ventajas sustanciales de la tecnología informática. La mayoría de las personas que toman decisiones no pueden permitirse el tiempo de mantener un entendimiento completo de una tecnología informática que se desarrolla de forma muy veloz. Pero aún menos pueden permitirse el lujo de ignorar lo que la computadora puede hacer y también sobre cómo puede fallar. En particular, un comandante responsable de la seguridad debe asegurarse de que los controles de diseminación se extiendan a las computadoras. Debe poder hacer las preguntas siguientes—para hacer aflorar la vulnerabilidad potencial para efectuar un examen crítico y sin sesgo.

Lecciones históricas en tecnología de emergencia

No es nuevo encontrar que una tecnología emergente tiene sus ventajas y desventajas. En particular, la amenaza a la que se enfrentan las computadoras se ilustra hoy en la evolución de las comunicaciones eléctricas militares—una tecnología revolucionaria anterior. Nuestro riesgo de seguridad de comunicaciones del Eje fue fundamental para el desenlace de la SGM, y las com-

putadoras ofrecen ahora a nuestros enemigos la oportunidad de dar un giro de 180 grados a la situación.

Los especialistas de comunicaciones militares reconocieron pronto la vulnerabilidad de la transmisión eléctrica a la interceptación, por ejemplo, mediante micrófonos ocultos o escuchas clandestinas de señales de radio. Las soluciones fueron sencillas y efectivas pero drásticas: restringir la transmisión solamente a información relativamente poco importante (es decir, sin clasificar) o rutas de transmisión vigiladas físicamente y protegidas contra la intrusión. Igualmente, durante varios años, la Fuerza Aérea restringió el uso de computadoras a datos sin clasificar o a una computadora protegida especializada en usuarios autorizados (aprobados). En ambos casos, las soluciones de seguridad limitaron el uso de la tecnología donde más se necesitaba: para obtener información importante en situaciones potencialmente hostiles, como asistencia en el campo de batalla.

Las restricciones de seguridad de comunicaciones dieron lugar a diversos dispositivos criptográficos. Estos dispositivos iban a codificar información en una forma ininteligible y por tanto sin clasificar de modo que no se requería la protección de toda la ruta de transmisión. No obstante (de importancia suprema para nosotros aquí) esto cambió dramáticamente la propia naturaleza del problema de seguridad propio: desde una cuestión de protección física a una pregunta de eficacia técnica. Se discutió la eficacia de los dispositivos criptográficos, basada no en un análisis técnico cuidadoso sino en una ausencia aparente de una forma conocida para contrarrestarlos. En el presente, la tecnología informática está en una posición análoga con un argumento similar por su eficacia contra el acceso no autorizado a datos informáticos. En ambos casos, los argumentos parecen ofrecer un riesgo aceptable a pesar de tener una base técnica de hecho débil.

Los dispositivos criptográficos técnicamente débiles encontraron un uso militar amplio debido a la falsa confianza y a la urgente necesidad operacional de las comunicaciones eléctricas. Un ejemplo notable fue la máquina Enigma usada por los alemanes durante la SGM. Su red de mando y control nacional de alto nivel usada para la seguridad de comunicaciones durante la guerra. Como indica *el secreto Ultra*, “los alemanes consideraban que su código era completamente seguro”.⁴ No obstante, antes de que empezara realmente la guerra, los británicos habían “resuelto de hecho el rompecabezas de Enigma”.⁵ La Fuerza Aérea está desarrollando una dependencia similar con cada decisión (formal o de hecho) para acreditar controles de seguridad informáticos. En cualquier caso, las decisiones políticas permiten que una debilidad técnica se convierta en una vulnerabilidad militar.

Los ejemplos durante la SGM muestran cómo la tendencia a defender decisiones anteriores (aceptar y usar técnicas más plausibles) aseguran al enemigo disponer de oportunidades de explotación. En Europa las señales descifradas de Enigma (llamadas Ultra) “no solo daban la fuerza completa y la disposición del enemigo, sino que mostró que los aliados [sus tropas] podían lograr una sorpresa táctica”.⁶ De hecho, el General Dwight Eisenhower afirmó que “Ultra fue decisivo”.⁷ El libro titulado *The Codebreakers (Los descifradores)* describe una confianza similar equivocada de los japoneses y observa que los criptoanalistas estadounidenses “contribuyeron enormemente a la derrota del enemigo, acortaron considerablemente la guerra y salvaron muchos miles de vidas”.⁸ Desde luego, los alemanes “deben haberse sorprendido por nuestros conocimientos de las posiciones de sus submarinos, pero afortunadamente no aceptaron el hecho de que habíamos descifrado Enigma”.⁹ De forma similar, los japoneses “estaban hipnotizados con la ilusión de que sus códigos nunca corrieron un riesgo serio”.¹⁰ Parece que las autoridades del Eje no reconocían su debilidad de seguridad sin la confirmación directa de la contrainteligencia—y esto solo salió a la luz después de que perdieran la guerra. En lo que se refiere a la seguridad informática de la Fuerza Aérea, la ausencia de guerra ha excluido su explotación definitiva; sin embargo, la falta de contrainteligencia firme en la explotación ya se ha ofrecido como evidencia de seguridad efectiva.

Aunque los esfuerzos técnicos llevaron a estas vulnerabilidades devastadoras, fueron sin embargo expertos técnicos como William Friedman los que proporcionaron una base técnica firme: “Sus estudios teóricos, que revolucionaron la ciencia, fueron correspondidos por sus soluciones reales, que la asombraron [la comunidad científica].”¹¹ Hoy, nuestras fuerzas armadas hacen un uso amplio de dispositivos criptográficos con confianza. Para las computadoras, al igual que para las comunicaciones, el quid de la cuestión es la eficacia del mecanismo de seguridad. El trabajo riguroso lógicamente reciente ha producido una tecnología de núcleo de seguridad. No obstante, el DOD no está aplicando aún esta tecnología.

El empuje de esta revisión histórica se recoge en la máxima, “Aquellas personas que no pueden recordar el pasado están condenadas a repetirlo”. Los paralelos históricos se resumen en la Tabla I. La lección principal que hay que aprender es esta: no confíe la seguridad a la tecnología a menos que la tecnología sea demostrablemente fiable, y la ausencia de riesgo demostrada no es absolutamente una demostración de seguridad.

Comunicaciones eléctricas		Computadoras electrónicas
	Uso limitado	
rutas protegidas solo sin clasificar		instalación especial solo sin clasificar
	Seguridad plausible	
tecnología criptográfica crucial para la seguridad sin contrainteligencia conocida base técnica débil		seguridad interna controles cruciales sin penetración conocida base técnica débil
	Dependencia in justificar	
confianza falsa en la criptografía aceptación política		confianza falsa en controles internos aceptación política
	Enemigo subestimado	
intercepción repetida y sin detectar los defensores exigen contrainteligencia		acceso repetido, sin detectar y selectivo los defensores exigen contrainteligencia
	Tecnología adecuada	
teoría de información		núcleo de seguridad

Tabla I. Evolución comparativa de los problemas de seguridad

Distinción entre cálculo y protección

La computadora dada de una instalación puede procesar datos sensibles de forma segura, y una máquina idéntica puede ser totalmente insegura en otra instalación. La clave para entender el problema de seguridad informático es distinguir cuándo la computadora solamente calcula y cuando debe proporcionar también seguridad. Estos son dos casos muy distintos.

En el primer caso, llamada comúnmente “modalidad especial”, la computadora y todos sus usuarios están dentro de un solo perímetro de seguridad establecido por guardas, perros, cercas, etc. Mediante el uso de comunicaciones seguras, este perímetro puede ampliarse geográficamente a terminales remotas. Solamente se requieren estos controles de seguridad externos para mantener la seguridad del sistema. El uso de la computadora está restringido de modo que en cualquier momento todos los usuarios, remotos o locales, son un acceso autorizado a todos los datos informáticos. Un atacante potencial debe sortear los controles externos y penetrar en el círculo del personal autorizado. La computadora solo calcula; ningún fracaso ni subversión de la computadora misma puede poner en riesgo la seguridad debido al entorno protegido.

En el segundo caso, llamado comúnmente “modalidad de niveles múltiples”, la computadora misma debe distinguir internamente múltiples niveles de sensibilidad de información y autorización del usuario. En particular, la computadora debe proteger cierta información de ciertos usuarios. Para la modalidad de múltiples niveles, los controles de seguridad internos de equipos y programas de computadoras deben asegurarse de que cada usuario pueda tener acceso solo a la información autorizada. Para la seguridad de niveles múltiples, la computadora misma debe proteger claramente así como calcular. Para el atacante potencial, simplemente bastará obtener acceso a los usuarios periféricos de la computadora—si se puede penetrar en los controles internos.

Los controles de seguridad de múltiples niveles funcionan de forma análoga a un dispositivo criptográfico; su eficacia es esencial para la seguridad de la información. Debido a la estructura inherente de las computadoras, una debilidad de seguridad de múltiples niveles invita a una explotación repetida. Además, esas fallas de seguridad interna de la computadora casi nunca se detectan. Contrariamente a las comunicaciones donde el acceso del enemigo al tráfico importante es un asunto de probabilidad, en una computadora penetrada se tiene un acceso selectivo, no solamente para la extracción sino también para la modificación de información a su elección. Lo que es peor, el poder de procesamiento de las computadoras modernas proporciona esta información de modo rápido y completo.

Si estamos preocupados por la protección de nuestros códigos criptográficos, entonces ciertamente no tiene sentido abandonar nuestras computadoras. Debemos darnos cuenta de que la modalidad de múltiples niveles puede ayudar al atacante a menos que los controles internos de la computadora misma proporcionen una protección fiable.

Evidencia de controles de seguridad débiles

La cuestión crítica entonces es esta: ¿nos atrevemos a confiar en los controles de seguridad interna de programas de computadora y hardware? La experiencia del autor con debilidades de seguridad indica que las computadoras contemporáneas no proporcionan una protección fiable. Se comprobaron las computadoras propuestas como suficientemente seguras para proteger información sensible en caso de deficiencias de seguridad. Un equipo de expertos técnicos sancionado formalmente vio debilidad en estas computadoras supuestamente seguras. (Para mayor precisión, los ejemplos se limitarán a esas evaluaciones en las que el autor participó personalmente).

El equipo de expertos técnicos operó como un usuario legítimo con acceso limitado a una pequeña parte de la información en el sistema. El objetivo del equipo era penetrar en los controles de seguridad internos y demostrar que se podría obtener el acceso no autorizado. En todos los casos de la experiencia del autor, se descubrieron debilidades de seguridad graves después de solo unas cuantas horas o días de esfuerzo.

Contraseñas para pedir. Un elemento común de protección es una contraseña o clave secretas que el usuario debe proporcionar para recibir servicios o información. Para ser efectiva, el secreto de las contraseñas debe conservarse. Una computadora IBM 370 con la opción de reparto de tiempo (TSO) tenía terminales remotas en diversas áreas descontroladas; las contraseñas se-

cretas restringían el acceso del usuario. Esta computadora particular contenía información sensible de selección de fuentes de adquisición de la Fuerza Aérea con una diseminación muy controlada. Los miembros del equipo de expertos técnicos averiguaron que meramente tenían que preguntar por nombre el archivo de las contraseñas para que imprimieran las contraseñas de todos los usuarios de TSO—sin traza de que habían corrido riesgo. Los diseñadores no se habían fijado en la relación entre la seguridad y la capacidad para imprimir un archivo.

La buena publicidad no es suficiente. En el Pentágono, un sistema de General Electric llamado “GCOS” proporcionó un cálculo clasificado (secreto) para el Estado Mayor del Aire y otros con terminales remotas protegidas en lugares seleccionados. El fabricante llevó a cabo una campaña publicitaria sobre su seguridad. Los defensores de la Fuerza Aérea propusieron crear un sistema de niveles múltiples añadiendo terminales remotas desprotegidas, para usos sin clasificar, a fin de lograr mayor coordinación y eficiencia. Nuevamente, las contraseñas iban a proteger la información sensible. Cuando un usuario presentó su contraseña a la computadora, GCOS comprobó una lista de contraseñas para verificar la legitimidad del usuario. Para hacer esta comprobación, GCOS copió parte de la lista en su memoria principal. Entre otros defectos, el equipo de expertos técnicos averiguó que GCOS dejó esta copia de las contraseñas donde pudieran imprimirse fácilmente y sin trazas. Los diseñadores habían pasado por alto la posibilidad de un uso indebido deliberado de una función de computadora necesaria.

Los diseñadores del gobierno no son perfectos. Después de la penetración en el Pentágono, algunos defensores afirmaban que los diseñadores del gobierno con un mayor conocimiento de seguridad podrían evitar dichos defectos. Una organización que procesaba datos de inteligencia sensible hicieron uso de un esfuerzo sustancial “arreglando” básicamente el mismo sistema GCOS. Tenían confianza de que podrían mantener la seguridad de modalidad de niveles múltiples. El equipo de expertos técnicos averiguó que estos “arreglos” podrían evitarse fácilmente. En este caso no solo podría cualquier usuario obtener cualquier información en el sistema sino que también podría tener acceso a información clasificada en computadoras conectadas en una red con esa computadora.

Un contrato no puede dar seguridad. Básicamente se seleccionó el mismo sistema GCOS para un sistema de mando y control importante. Los defensores aseguraron a los usuarios que estaría protegido en múltiples niveles porque la seguridad era requerida por el contrato. Una amplia evaluación del equipo de expertos técnicos dio a conocer que había muchos defectos de seguridad profundos y complejos que desafiaban la reparación práctica—se opinó que la computadora no solo finalmente no protegía sino que no se podía proteger.

La mejor seguridad no es suficientemente buena. Honeywell Information Systems, con patrocinio del DOD, modificó la computadora GCOS en un esfuerzo para mejorar sustancialmente varias áreas, incluida la seguridad. El resultante servicio Multiplexed Information and Computing Service (Multics) fue muy alabado por su seguridad. El equipo de expertos técnicos usó una computadora de laboratorio de la Fuerza Aérea para evaluar Multics como computadora de protección potencial de múltiples niveles para el Pentágono. Aunque tenía el mejor diseño de seguridad de todos los sistemas encontrados, el equipo de expertos técnicos halló varios defectos de implementación.¹² En un caso, Multics comprobó primero una posible autorización del usuario para acceder a la información y, cuando la solicitud demostró ser válida, ejecutó la solicitud. No obstante, el usuario pudo cambiar la solicitud después de la comprobación de validez pero antes de la ejecución; Multics ejecutó después la solicitud cambiada, permitiendo un acceso sin autorización. Esta penetración de Multics provino de un atajo de implementación para mejorar la eficiencia.

Contraseñas codificadas recuperadas. El sistema Multics codificó internamente su lista de contraseñas de modo que incluso impresas, las contraseñas no eran ininteligibles. Cuando un usuario presentó su contraseña, se codificó y después se comparó con la lista codificada. El equipo de expertos técnicos usó el método de penetración desarrollado en la computadora del laboratorio

para acceder a la lista de contraseñas codificadas de una universidad grande y después descifró el código para obtener todas las contraseñas.

Trampilla instalada. El equipo de expertos técnicos penetró en Multics y modificó la copia maestra del fabricante del sistema de operación Multics mismo instalando una trampilla: las instrucciones de la computadora para omitir deliberadamente los controles de seguridad normales y asegurar así la penetración incluso después de haber arreglado el defecto inicial. Esta trampilla era pequeña (menos de 10 instrucciones de 100.000) y requería una contraseña para usarla. El fabricante no pudo encontrarla, incluso cuando sabía que existía y cómo funcionaba. Además, desde que se insertó la trampilla en la copia maestra de los programas del sistema de operación, el fabricante distribuyó automáticamente esta trampilla a todas las instalaciones Multics.

Registro de auditoría destruido. Algunos han discutido que una necesidad de computadora no impide siempre un acceso no autorizado siempre que se mantenga un registro de auditoría de dichos accesos. El sistema Multics mantenía un registro de auditoría protegido de acceso, y se registraron los accesos sin autorizar del equipo de expertos técnicos. No obstante, el registro de auditoría estaba por sí mismo sujeto a un acceso sin autorizar. El equipo de expertos técnicos modificó meramente el registro para borrar todas las trazas de sus acciones, como la inserción de la trampilla.

Incluso los arreglos tienen defectos. Honeywell produjo una nueva computadora Multics que corrigió todos los defectos de implementación informados por el equipo de expertos técnicos. Este equipo usó la computadora nueva de Honeywell en su fábrica de Phoenix, Arizona, y penetró nuevamente en el sistema de seguridad.¹³ ¡Este nuevo defecto fue debido a cambios hechos para corregir los cambios anteriores! Se iba haciendo cada vez más claro que proporcionar una computadora segura a múltiples niveles era realmente difícil.

El caballo troyano no está muerto. Aunque algunos habían reconocido el problema, los defensores que pertenecían al Estado Mayor Aéreo alababan una instalación por su solución de seguridad de niveles múltiples en otra computadora. La solución consistía en programas para segregar la información en clasificada y sin clasificar. No había terminales remotas, pero los usuarios podían enviar trabajos sin clasificar a la computadora sin controles de seguridad. A partir de un trabajo sin clasificar, el equipo de expertos técnicos penetró en el sistema fundamental de computadoras y modificó la solución en un caballo troyano, un programa aparentemente útil que ocultaba capacidades perjudiciales. El caballo troyano ocultó una copia invisible de trabajos clasificados. Un trabajo posterior sin clasificar recuperó la información oculta, poniendo en riesgo la seguridad. Así pues, la solución de seguridad no solamente era ineficaz sino que realmente acentuaba el problema de seguridad.

La moraleja evidente. Pocos o ningún control de seguridad de computadora contemporáneo han impedido a un equipo de expertos técnicos un acceso fácil a cualquier información buscada. Estos ejemplos no son completos de ninguna manera; no deben usarse para inferir la predominancia de ciertos defectos o asociar debilidades particulares con tan solo unos pocos fabricantes. Otros tienen problemas de seguridad comparables.

Futilidad de evaluación por penetración

La Fuerza Aérea, en un sentido muy real, ha sido afortunada de que la seguridad sea tan deficiente en las computadoras actuales—el mayor peligro vendrá cuando parezca plausible el argumento de que una computadora es segura porque los equipos de expertos técnicos no pudieron penetrar en ella. De hecho, la evaluación de controles de seguridad de computadoras internas es un reto muy difícil. Como en el caso de la criptografía, hay básicamente dos métodos.

Si los controles de seguridad se basan en una tecnología firme cuidadosamente formulada, entonces pueden estar sujetos a un análisis racional de su eficacia. Como ya se ha observado, esto

no es generalmente cierto en las computadoras contemporáneas. También se tratará el método del núcleo de seguridad, que está sometido a un análisis técnico tan metódico.

De forma alternativa, un defensor puede simplemente buscar formas de penetrar en los controles de una computadora; al no poder penetrar, puede discutir plausiblemente que no hay forma de penetrar, ya que no conoce ningún método. Si se encuentra una falla de seguridad, primero puede parchearse antes de discutir de la seguridad. Evidentemente, este argumento tiene muchas dificultades teóricas y prácticas.

En principio, uno podría probar todos los programas posibles para encontrar uno que permita una penetración en el sistema de seguridad. Este método de agotamiento sería efectivo pero está muy lejos de ser viable. ¡Para cualquier computadora sustancial esto llevaría tanto tiempo que antes de acabar la evaluación el sol se habría consumido! Así pues, una evaluación realizable por agotamiento debe ser tan incompleta como ridícula.

De hecho, el esfuerzo hecho en penetrar y parchear produce un retorno marginal deficiente en términos de seguridad. Los ejemplos de equipos de expertos técnicos indican algunas de las dificultades:

En primer lugar, la experiencia muestra que los nuevos perpetradores tienden a encontrar nuevos defectos—incluso después de que equipos anteriores hayan encontrado todo lo que pudieron. Parece poco probable que un atacante real no involucre a nuevas personas.

En segundo lugar, los defectos no son producto generalmente de una estupidez general sino que se deben a descuidos humanos al tratar un problema de diseño difícil. Así pues, los arreglos mismos probablemente tengan defectos.

En tercer lugar, no se requiere un experto muy especializado para penetrar en el sistema de seguridad. Es cierto que la mayoría de los profesionales informáticos no conocen formas de penetrar en los sistemas que usan; desean hacer un trabajo, no interferir con él. No obstante, cuando se les da la asignación, incluso los profesionales menos experimentados e inexperimentados han tenido éxito uniformemente en penetrar en el sistema de seguridad.

En cuarto lugar, la exposición al ataque es frecuentemente mucho mayor que simplemente la procedente de usuarios conocidos del sistema. Las conexiones telefónicas comerciales con sistemas militares están aumentando y permiten el acceso desde todo el mundo. Las interceptaciones de comunicaciones también permiten el acceso a conexiones directas sin asegurar; las interceptaciones de microondas por parte de los soviéticos en EE.UU., como reveló recientemente la Casa Blanca, demuestran esta capacidad. La falta de control de seguridad estricta en el envío de trabajos de computadora permite ataques en nombre de un usuario legítimo incluso para computadoras sin terminales remotas. La interconexión con otras computadoras puede añadir también un grupo grande de usuarios desconocidos.

En quinto lugar, los ataques pueden desarrollarse y perfeccionarse en otras computadoras menos en la computadora objetivo. Una computadora similar propiedad o accedida legítimamente por el atacante pueden usarse para minimizar el riesgo de detección. Una vez perfeccionado, los métodos de ataque pueden aplicarse a la computadora objetivo.

Por último, para un penetrador hostil, los métodos de trampa y caballo troyano son probablemente los más atractivos, y estos defectos creados deliberadamente en programas informáticos son las más difíciles de detectar. La mayoría de los equipos de expertos técnicos se concentran en defectos accidentales que nadie podría encontrar, pero los defectos deliberados están latentes hasta que son activados por un atacante. Estos errores pueden colocarse prácticamente en cualquier lugar y diseñar cuidadosamente para escapar la detección. No obstante, la mayoría de los sistemas militares incluye programas no desarrollados en un entorno seguro, y algunos incluso se desarrollan en el extranjero. De hecho, algunos sistemas pueden ser subvertidos por un técnico remoto anónimo sin una función legítima en el desarrollo del sistema. Estos errores pueden activar esencialmente cualquier interfaz externa—desde un telegrama sin clasificar a una situación única establecida para la detección por un sistema de vigilancia.

En resumen, la penetración y el parche de controles internos no es una técnica de seguridad prometedora. Incluso sin la posibilidad de trampillas y caballos troyanos y sin demandas de seguridad militares, “las compañías privadas han tratado siempre de parchear defectos en los llamados sistemas de computadoras [seguros], y después de millones de dólares y años de esfuerzo, cedieron antes el fracaso”.¹⁴ Este método es poco más que un juego de inteligencia en el que el diseñador debe tratar de encontrar (y parchear) *todos* los defectos mientras el enemigo necesita encontrar (y explotar) todo menos un defecto restante—una contienda bastante desequilibrada.

El “resultado final” es simple. El comandante responsable de la seguridad en un sistema informático necesita una respuesta inequívoca a una pregunta crucial: ¿depende la seguridad de los controles internos? Es decir, ¿hay alguna falla o subversión de la computadora misma que podría degradar la seguridad? Si es así, con las computadoras contemporáneas tiene una falta de uniformidad radical en la laxitud sobre la seguridad de computadoras dentro del entorno militar que normalmente tiene controles estrictos sobre la diseminación de información sensible.

Alternativas de seguridad de computadoras

Hemos visto que en las computadoras contemporáneas los controles internos no solo son ineficaces sino que también desafían la evaluación. No obstante, evidentemente podemos seguir la ruta de la experiencia criptográfica alemana y japonesa—subestimar la explotación enemiga de la debilidad técnica. Esta es el riesgo que hemos corrido en cada una de las diversas decisiones de la Fuerza Aérea para operar computadoras contemporáneas en una modalidad de múltiples niveles.

Si perdemos esta apuesta, el daño depende de qué está protegiendo la computadora. Puede variar desde la violación de la privacidad personal hasta el fraude, daños en el campo de batalla o ataque sorpresa preventivo. Por ejemplo, se ha propuesto que la Fuerza Aérea cambie dinámicamente los objetivos de sus misiles balísticos estratégicos; esto apoya la política nacional de respuesta flexible y permitiría la aplicación de armas de represalia para los objetivos militares lucrativos. Sin embargo, las computadoras están en el centro de esta capacidad; si fueran penetradas, un enemigo podría cambiar los objetivos de los misiles para que impacten en objetivos de poco valor o incluso en objetivos amigos como parte de un ataque por sorpresa.

No trataremos de explorar las numerosas posibles situaciones de dependencia de las técnicas débiles, pero nos fijaremos en soluciones alternativas. Comprenden asuntos técnicos y de política. Básicamente, la Fuerza Aérea tiene dos alternativas además de hacer caso omiso del problema: limitar el uso de computadoras o usar la tecnología adecuada disponible para hacer que los controles internos sean más fiables.

Evite la dependencia de los controles internos

La alternativa evidente es restringir de forma deliberada el uso de computadoras a una modalidad especial de modo que los controles internos no puedan afectar la seguridad. Hay tres formas comunes de evitar la dependencia en los controles internos.

En primer lugar, se puede dedicar una computadora separada a cada nivel de información clasificada. Esto es particularmente atractivo para un sistema en línea o de tiempo real donde la información debe ser inmediatamente accesible. Este método puede conducir a computadoras duplicadas o usadas de modo ineficaz.

En segundo lugar, cada nivel de información clasificada puede programarse para usar la computadora para un período diferente. Esto requiere purgar información de toda la memoria del sistema al final de un período programado. Este procedimiento manual normalmente engorroso carece de capacidad de respuesta y desperdicia los recursos informáticos mientras se completa el nivel de clasificación.

En tercer lugar, se pueden procesar varios niveles de clasificación juntos. Todas las líneas de comunicación deben protegerse, y todos los usuarios necesitarían ser un acceso autorizado a toda la información. Como los controles internos no son fiables, todo el producto del sistema está clasificado temporalmente como del máximo nivel. Para obtener información con una menor clasificación, una autoridad competente debe revisar manualmente la salida de contaminación y rebajarla antes de descargarla en el nivel inferior.

Estas restricciones de uso son compatibles con una buena seguridad, pero resultan en una degradación sustancial de capacidad en una computadora moderna.

Gastos adicionales. Estas restricciones de seguridad aumentan considerablemente el costo. Se necesitan medidas de seguridad de comunicación adicionales, y mano de obra adicional para la revisión manual de la salida. Existe también el costo de las investigaciones de aprobación de seguridad para los usuarios cuya información la computadora podría contaminar con información de una clasificación más elevada. Otros costos incluyen aquellos para equipos duplicados y la capacidad adicional para compensar los recursos desperdiciados. Por ejemplo, cuando un sistema de computadoras importante no provea la seguridad prometida de niveles múltiples, los sitios principales de la Fuerza Aérea tenían que aprobar a muchos usuarios y hacer compras de múltiples millones de dólares de equipos adicionales.

Mayor riesgo. En la práctica la modalidad especial conduce a un aumento importante en la exposición de información. La falta de controles internos destruye efectivamente la división en compartimientos prevista para limitar el daño de la subversión. El mayor número de personas que requieren aprobación aumenta la probabilidad de dar acceso a un individuo en el que no se puede confiar. Los procedimientos de purga manuales tienen tendencia a errores que dejan residuos de memoria clasificada que pueden ser extraídos por usuarios no autorizados. Además, la revisión manual de grandes volúmenes de salida de computadora puede ser de hecho una argucia burocrática para transferir responsabilidad de seguridad de los diseñadores a los usuarios; el revisor tiene poca probabilidad de detectar información clasificada sin autorizar que haya estado incluida de forma accidental o incluida de forma deliberada en la salida.

Capacidades inevitables. Dichas restricciones de seguridad pueden limitar seriamente la capacidad de operación de los sistemas de apoyo en el campo de batalla. Las armas modernas exigen sistemas de mando y control con un acceso rápido a una base grande de información actual y exacta. Esta base de datos (necesariamente compartida e integrada) contendrá típicamente información que va de sin clasificar a muy secreta. Como muchas personas que mantienen la información menos clasificada tienen autorizaciones limitadas, y el volumen de información requiere el uso de computadoras, tenemos el problema de seguridad clásico de múltiples niveles. Los controles internos de la computadora son cruciales para proteger la información, y evitar la dependencia en los controles internos limitará seriamente las capacidades del sistema.

El problema se acentúa por la interoperabilidad con su red interconectada de computadoras con una comunidad de usuarios grande, diversa y geográficamente dispersa. Las redes de computadoras de sistemas de mando y control son un ejemplo importante. No obstante, un oficial militar observó que debido a la seguridad deficiente de las computadoras internas en una de dichas redes, sus computadoras 35 de gran escala de uso general nunca se usarían verdaderamente para la finalidad para la que se compraron. El problema se agrava aún más por la mayor necesidad de fusión de información de inteligencia seleccionada (sin arriesgar fuentes sensibles) con información de operaciones tácticas.

En resumen, la modalidad especial evita muchos problemas de seguridad de la computadora pero no satisface las necesidades de operación de una fuerza militar moderna. Estas necesidades solo se pueden satisfacer mediante la protección eficaz de múltiples niveles en la computadora misma.

Aplique una tecnología adecuada

El desarrollo y la aplicación de seguridad de computadoras internas fiables no son sencillos ni imposibles. Aunque frecuentemente se reconoce la necesidad de una operación de múltiples niveles, las fuerzas armadas han prestado solamente atención al desarrollo de la tecnología requerida. De hecho, la Fuerza Aérea dirigió recientemente la terminación de su programa de desarrollo de seguridad de múltiples niveles, el mayor en el Departamento de Defensa.¹⁵

Antes de que examinemos el avance tecnológico que se ha hecho, debe resultar instructivo identificar parte del razonamiento que afloró en la terminación reciente de la Fuerza Aérea. La pauta de ideas refleja que la seguridad de computadoras no es actualmente un foco importante.

- La posibilidad de que la industria resuelva el problema de seguridad de las computadoras se ha sobrestimado al llegar a la conclusión de que la industria tiene el mismo problema de seguridad que las fuerzas armadas. No obstante, la analogía de comunicaciones indica una dificultad. En el sector civil, las violaciones de seguridad de comunicaciones están sometidas a legislación, no a prevención; los micrófonos ocultos son ilegales, y hay un resarcimiento legal para la pérdida. Por el contrario, las fuerzas armadas deben acudir a la prevención (por ejemplo, criptografía aprobada por los militares), ya que no podemos llevar a juicio a la KGB. La situación de las computadoras es similar; hay impulsos legislativos pero un éxito comercial limitado para lograr controles internos demostrablemente efectivos. La espera de soluciones espontáneas para la industria es probable que sea larga, y es poco probable que cumplan con las normas de seguridad militar en áreas como la protección contra la subversión deliberada.
- La financiación inadecuada de la investigación y del desarrollo (I+D) se asignó para continuar un elemento del programa a un nivel óptimo. No obstante, hay partes del programa con fondos disponibles que también se terminaron. Se completaron con éxito ocho millones de dólares de EE.UU. de trabajo. Quedaron unos 10 millones de dólares de EE.UU. de trabajo en más de cuatro años para completar el desarrollo de un prototipo completo y la base general asociada para efectuar compras competitivas. Varias estimaciones indican que los costos de desarrollo pueden recuperarse evitando las sanciones de la modalidad especial—sin mencionar la mayor capacidad de seguridad y operación.
- La amenaza se minimiza buscando contrainteligencia que no está prácticamente disponible, por ejemplo, ejemplos reales de agentes enemigos sorprendidos en el acto. El enemigo puede parecer demasiado ignorante para la penetración, no interesado en secretos militares, o incapaz de una subversión y explotación planificadas. Una cuantificación de un solo número de la probabilidad de amenaza puede suponer implícitamente un incidente aleatorio en vez de una actividad de penetración planificada. Esto puede indicar un riesgo sin un criterio objetivo de aceptabilidad. Estas percepciones no se basan generalmente en métodos de inteligencia profesional con “ejemplos trabajados” (por ejemplo, de seguridad de comunicaciones) de la metodología.
- El interés en desarrollar soluciones está limitado por una falta clara de responsabilidad de la eficacia de controles internos. Las oficinas de estado mayor y política pueden dar recomendaciones, guiar e incluso aprobar mecanismos de seguridad informáticos sin responsabilidad por cualquier riesgo de seguridad que pueda resultar. Por otra parte, la prueba de seguridad y los esfuerzos de evaluación y las asesorías económicas de comandantes individuales están en gran medida sin relacionar con la protección real del sistema. Esto es claramente contrario a la seguridad de comunicación militar donde los expertos técnicos son responsables de certificar los mecanismos de seguridad.

- El problema de seguridad informática es difícil de reconocer cuando la política no distingue claramente los casos donde la computadora simplemente proporcione cálculo y donde la computadora proporcione protección interna. Dicha política se concentra en el desarrollo de controles de seguridad que “no son necesariamente certificablemente perfectos”—un objetivo bastante ambiguo. En dicha estructura de política, los análisis no identificarán la necesidad de controles internos. De hecho, una computadora podría satisfacer bien todos los reglamentos y seguir siendo muy vulnerable.
- La confianza en controles débiles aumenta debido a la suposición de que el gasto en recursos de seguridad la mejorará sustancialmente. De hecho, el esfuerzo puede ser simplemente ineficaz, como en el caso del interminable penetrar y parchear. La política actual enumera características de diseño de computadoras para la seguridad interna que no son ni necesarias ni suficientes para la seguridad.
- La atención a los trucos de seguridad hace que no nos fijemos en debilidades importantes. Hay muchos mecanismos de eficacia mínima para mejorar los controles de seguridad interna—analizadores de escritura a mano, codificación de datos internos, memoria de solo lectura para información de seguridad, etc. Cierta guía ha animado a los programas de computadora que clasifican y etiquetan productos por nivel de seguridad. La evaluación de estos programas se concentra en resultados esperados con usuarios amigos en vez de la subversión deliberada de los programas o la penetración del sistema fundamental. Llevar a cabo dichos esfuerzos aislados frecuentemente es peor que no hacer nada, ya que da un falso sentido de seguridad.

Estas clases de problemas hicieron que la Fuerza Aérea considerara su programa de desarrollo de la División de Sistemas Electrónicos (recientemente terminado) como “controvertido”. Pero nuestro examen previo del problema hace claro que la operación a múltiples niveles sin una tecnología adecuada es una apuesta de alto riesgo. Como mucho, es extrañamente poco coherente con las normas establecidas en otras áreas (por ejemplo, comunicaciones) de seguridad militar que hacen una hipótesis de una amenaza hostil deliberada, competente y motivada y responde con contramedidas efectivas. Lo más probable es que anule las demás medidas de seguridad, permitiendo un daño limitado solo por la imaginación del enemigo.

Tecnología del núcleo de seguridad

Afortunadamente, la I+D militares—en particular el programa de la Fuerza Aérea recientemente terminado,¹⁶—ha logrado un avance sustancial hacia la tecnología adecuada para lograr una seguridad de múltiples niveles. Un paso importante hacia la solución fue la introducción en 1972 de la tecnología del núcleo de seguridad¹⁷, que proporcionó una base científica demostrablemente eficaz de los controles de seguridad internos. Aunque una explicación de los detalles técnicos va más allá del alcance de este artículo, un informe técnico resume el método del núcleo de esta forma:

El método para obtener un sistema seguro comprende primero definir los requisitos de seguridad y después crear un diseño conceptual que pueda mostrarse para proporcionar la protección requerida (es decir, un modelo). El modelo define formalmente un sistema ideal (en nuestro caso uno que cumpla con los requisitos de seguridad militar), y proporciona una base para probar una implementación subsiguiente. Una vez que se haya implementado [un núcleo de seguridad] que cumpla con los requisitos descritos anteriormente, se habrá logrado la seguridad de las computadoras. Del software en el sistema, solamente el núcleo de seguridad . . . necesita corregirse . . . El sistema operativo propio o el software de aplicación pueden contener desperfectos introducidos de forma inadvertida o trampillas maliciosamente plantadas sin arriesgar la seguridad.¹⁸

Según el programa de la Fuerza Aérea el núcleo demostró su viabilidad técnica, independientemente de cualquier vendedor de computadoras particular o política de seguridad. El núcleo también ha establecido considerablemente su aceptabilidad operacional, con evidencia específica para una amplia funcionalidad, buena eficiencia, capacidad de certificación de seguridad y compatibilidad. Además, los requisitos técnicos básicos del núcleo se han incorporado con éxito a las especificaciones de compras militares para una computadora comercial a gran escala y una computadora de sistemas de armas empotrada. En pocas palabras, la tecnología básica está muy a mano.

Fundamento científico

Un núcleo de seguridad es un pequeño conjunto de instrucciones de programas de computadora y equipos asociados que controla todo el acceso por parte de los usuarios (es decir, a través de sus programas) a la información. Un núcleo de seguridad dado es normalmente exclusivo de una computadora particular. Un núcleo de seguridad para computadoras es de muchas maneras conceptualmente análogo a un dispositivo criptográfico para las comunicaciones.

El diseño del núcleo de seguridad se deriva directamente de esa especificación precisa (es decir, un modelo matemático) de su función. (El modelo de núcleo es análogo al algoritmo que define la función matemática de un dispositivo criptográfico). Este modelo matemático es una formulación precisa de reglas de acceso basadas en atributos del usuario (autorización, necesidad de saber) y atributos de información (clasificación). Los parámetros del sistema controlan el uso específico de una instalación (por ejemplo, para la política de clasificación del DOD, protección de privacidad, etc.).

La característica de distinción fundamental (de ahí su nombre) del concepto de núcleo de seguridad es que un núcleo representa un perímetro de seguridad interno distinto. En particular, esa porción del sistema responsable de mantener la seguridad interna se reduce desde esencialmente toda la computadora hasta principalmente el núcleo. Así pues el núcleo es análogo a un dispositivo criptográfico que elimina la mayor parte de una ruta de comunicación de la consideración de seguridad. Para ser un poco más técnico y concreto, un núcleo de seguridad típico tiene varios (digamos que de diez a veinte) programas de computadora pequeños (es decir, subrutinas) que pueden ser invocadas por otros programas (por ejemplo, el sistema operativo y los programas de aplicaciones de usuario individuales). El núcleo, y solo el núcleo, controla y gestiona todos los componentes de hardware que almacenan y acceden a información. Los demás programas (es decir, no nucleares) deben invocar el núcleo (es decir, llamar a sus subrutinas) para tener acceso a la información—el núcleo comprueba el usuario y los atributos de información y permite solo acceso que esté autorizado. Sin embargo, a pesar de estas comprobaciones, existe un impacto mínimo del usuario. La Figura 1 ilustra conceptualmente esta estructura.

El avance técnico significativo fue el descubrimiento de un conjunto de funciones de modelos y condiciones que son probablemente suficientes para impedir riesgos a todos los posibles programas de computadora que no sean de núcleo. Cada función del modelo determina el diseño de un programa de núcleo. Además, el modelo impone condiciones de seguridad que el diseño debe cumplir. Se han demostrado teoremas de seguridad que muestran que el núcleo (al seguir precisamente el modelo) no permitirá un riesgo, sea cual sea el programa que lo use o cómo lo use. Es decir, el diseño del núcleo es a prueba de penetraciones—en particular a todos esos ataques inteligentes que nunca tuvieron en consideración los diseñadores de núcleos.

Esta base de plenitud matemática sube el nivel del diseño del núcleo y del proceso de evaluación por encima de un mero juego de ingenio con un atacante; esto es análogo a la teoría de información como base de un criptoanálisis moderno. Un efecto dramático es que el núcleo facilita la evaluación objetiva de seguridad interna. El evaluador no necesita examinar el casi ilimitado número de posibles intentos de penetración; solamente necesita verificar que el modelo

matemático esté correctamente implementado por el núcleo. En otras palabras, el núcleo proporciona los controles internos verificablemente fiables necesarios para la seguridad de múltiples niveles.

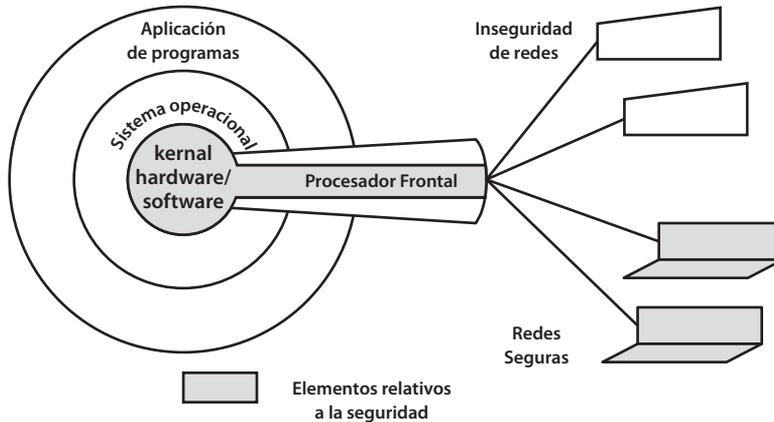


Figura 1. Sistema de computadora seguro

Viabilidad de ingeniería

Para ser útil, el concepto de núcleo no debe ser solamente matemáticamente firme sino también viable de implementar. La implementación satisfactoria se basa en tres principios de ingeniería:

Plenitud. Se debe invocar un núcleo de seguridad cada vez que se acceda a datos en la computadora.

Aislamiento. Se debe proteger un núcleo de seguridad y su base de datos contra la modificación no autorizada.

Capacidad de verificación. Un núcleo de seguridad debe ser suficientemente pequeño y simple de modo que su función pueda probarse y verificarse completamente.

Un núcleo de seguridad de laboratorio para una minicomputadora comercial (Digital Equipment Corporation modelo PDP-11/45) mostró tener viabilidad en 1974. El hardware de “memoria virtual” de esta computadora era una ayuda significativa para asegurar la plenitud y el aislamiento del núcleo. Este núcleo en funcionamiento constaba solo de unas 1000 instrucciones de computadora. El experimento también estableció que es mucho más fácil introducir el concepto de núcleo en un diseño inicial que modificarlo más adelante.

La base del diseño (es decir, modelo de núcleo) se verificó matemáticamente. Como con los dispositivos criptográficos, la verificación de la implementación correspondiente se basaba más en un diseño de ingeniería cuidadoso y pruebas extensas que en matemáticas formales. Las pruebas automáticas y las técnicas de verificación de programas indicaban que la implementación del núcleo correspondía al diseño. Este prototipo de laboratorio confirmó la viabilidad pero no estaba orientado hacia la evaluación de rendimiento y eficiencia. De pasada, es interesante observar que un equipo de expertos técnicos trató de penetrar su seguridad pero no pudo.

Rendimiento

Se examinó el rendimiento en un sistema de computadoras más grande. Se experimentó una degradación muy pequeña del rendimiento (menos de un 1 por ciento) cuando se modificó el Multics comercial (para la gama 6000 de Honeywell) al modelo de núcleo. Esta versión de Multics no se implementó como un verdadero núcleo, es decir, los controles se distribuyeron en vez

de recopilarse en una entidad pequeña verificable; no obstante, esta versión hizo todos los controles de seguridad requeridos en un núcleo y así confirmó que el núcleo no era inherentemente ineficiente.

Las buenas características de seguridad del hardware del núcleo fueron un auxiliar importante para el rendimiento, y estas características eran independientes del vendedor. La versión tuvo tanto éxito que Honeywell incluyó el Mecanismo de Aislamiento de Acceso resultante en ofertas comerciales Multics para la protección de la privacidad y la información comercial. Este sistema se usó como base del prototipo de Fuerza Aérea terminado; el desarrollo prototipo fue implementar un núcleo verdadero verificable.

Funcionalidad

Un núcleo de seguridad fuerza al usuario de la computadora a pensar en la seguridad pero no degrada gravemente las capacidades de la computadora. Esto se demostró claramente cuando se instalaron con éxito las modificaciones de Multics para esos usuarios exigentes en el Pentágono: las limitaciones del diseño del núcleo tenían un impacto adverso mínimo en los usuarios. Así como la criptografía permite el uso seguro de equipos de comunicación comerciales, el concepto de núcleo permite el uso seguro de equipos y programas de computadora comerciales estándar. La instalación del Pentágono con su procesamiento clasificado confirmó los conceptos de apoyar una computadora basada en núcleo en un contexto de seguridad total del sistema.

La utilidad operacional del núcleo se demostró adicionalmente con el prototipo de minicomputadora inicial. Una demostración mostró la interfaz de operaciones segura y sistemas de inteligencia para la fusión de la información táctica del campo de batalla. Además, varios esfuerzos militares de I+D en varias etapas de terminación han usado elementos importantes de la tecnología del núcleo de seguridad: una red de mando y control, un controlador criptográfico, un sistema de comunicación digital nacional, un sistema “monitor de máquinas virtual” a gran escala, un sistema operativo de minicomputadora general y una minicomputadora militarizada segura (basada en el Nivel 7 Honeywell comercial). Aunque confirman la utilidad del núcleo de seguridad, ninguno de esos esfuerzos de I+D conducirá a disponibilidad y uso operacional generales.

Política de seguridad

Aunque el concepto de núcleo de seguridad no contradice la política actual, la política futura debe reconocer y aprovechar las características del núcleo. La política debe reconocer que el modelo matemático proporciona una forma de traducir las reglas de seguridad tipo papel y lápiz en términos informáticos. Además, una política significativa para la modalidad de múltiples niveles reflejaría las realidades tecnológicas: o todo el sistema debe ser correcto (no viable actualmente) o se debe usar el núcleo de seguridad.

En lo que respecta a dispositivos criptográficos, el núcleo debe protegerse contra la subversión (por ejemplo, inserción de una trampa) durante su desarrollo. Pero proteger el núcleo ciertamente involucra a muchas menos personas y a un entorno más controlado que tratar de proteger todos los programas de computadora del sistema; así pues, en contraste con los sistemas contemporáneos, el núcleo hace que sea tratable proteger contra la subversión. Además, la evaluación (para la certificación) de controles internos de seguridad de computadoras es una tarea técnica difícil. El método del núcleo para el diseño y la implementación hace viable dicha certificación, pero esta evaluación sigue requiriendo expertos técnicos muy capaces—así como la evaluación de dispositivos criptográficos.

Este método conceptualmente se asemeja a la criptografía militar moderna. (Vea la Tabla II). Sin embargo, se debe reanudar el desarrollo y se deben hacer ajustes de política si se va a poner a disposición en general en cualquier momento en un futuro inmediato. Para estar seguros, hay demandas que compiten en recursos. El desarrollo de armas empleables directamente (como

aviones caza) puede tener siempre una mayor prioridad que el desarrollo de seguridad de computadoras, pero según lo explicó un observador: “¿Cómo serían de efectivos esos aviones caza si los planes para su empleo fueran conocidos por adelantado por un adversario que hubiera penetrado en la computadora que contenía esos planes?”¹⁹ El núcleo de seguridad es claramente la única tecnología disponible en la actualidad que puede proporcionar las capacidades de seguridad y operacionales que debemos tener.

Tabla II. Puntos comunes en tecnología de seguridad

	Mecanismo criptográfico	Núcleo de seguridad
amenazas negadas..... en vez de ilegalizadas	micrófonos ocultos	penetración
elementos comerciales..... estándar preservados	circuitos de comunicación	computadoras y programas
porciones limitadas sensibles a la seguridad	principalmente el cripto	principalmente el núcleo
base fundamental formulada de forma precisa	algoritmo criptográfico	modelo matemático
evaluación de diseño..... criterios definidos	teoría de información	teoremas de seguridad
implementación que cumple..... exactamente el diseño	ingeniería metódica	programas verificados
subversión controlada..... por seguridad física	fabricación	programación
expertos diestros necesarios..... para la certificación	criptoanalistas e ingenieros	científicos informáticos

La seguridad a menudo requiere opiniones subjetivas, y algunas personas pueden diferir con el autor sobre puntos específicos. En general, parece evidente que un usuario que confíe ciegamente en la protección proporcionada por computadoras para obtener información militar sensible pondrá en peligro seriamente la seguridad. De hecho, la mayoría de las computadoras no incluyen ni siquiera las características nominales para apoyar un sistema de seguridad militar. Incluso cuando lo hacen, la esencia del problema de seguridad de la computadora es la eficacia técnica de los controles internos, y la evidencia es clara de que la mayoría de los controles internos no son fiables.

Por otra parte, la limitación del uso de computadoras para evitar este problema es costosa y nos priva de la capacidad operacional vital. El dilema de eficacia en comparación con la eficiencia genera presión para subestimar la amenaza y el exceso de confianza de controles de seguridad internos. Desgraciadamente, estas presiones han conducido a la Fuerza Aérea a una dependencia perturbadora y en aumento sobre los controles de seguridad débiles incluso en ausencia de evidencia de eficacia.

La Fuerza Aérea terminó recientemente el único programa de DOD importante para proporcionar controles internos científicamente firmes—controles basados en el concepto de núcleo de seguridad. El desarrollo del pasado ha demostrado claramente la viabilidad, el rendimiento y la utilidad de esta tecnología. No obstante, debido a la carencia de un entendimiento técnico y

una política significativa, existe en la actualidad poco apoyo oficial para el desarrollo de esta capacidad prometedora.

Se deben tomar tres medidas básicas para controlar el impacto del adversario de nuestra debilidad de seguridad de computadora:

- Promulgar una política clara que distinga entre dependencia en controles externos (modalidad especial) y controles internos (modalidad de múltiples niveles). No debe ser posible satisfacer la política sin proporcionar una seguridad de forma genuina. La modalidad de múltiples niveles sin una base técnicamente firme debe estar expresamente prohibida.
- Incorporar controles de seguridad militarmente explícitos en sistemas de procesamiento clasificados. Deben estar basados en una especificación precisa de las funciones requeridas (como en el modelo de núcleo para Multics del Pentágono). Este paso es crucial para la futura introducción de seguridad de múltiples niveles sin un rediseño de sistema completo. (Entretanto, esto puede ayudar a proteger la privacidad y los recursos valiosos).
- Reanudar el desarrollo del núcleo de seguridad para proporcionar seguridad de múltiples niveles técnicamente firme. Como en el programa anterior de la Fuerza Aérea, esto debe orientarse hacia el proceso de adquisición militar competitivo. Al mismo tiempo, la política debe cambiarse para facilitar el uso operacional de la tecnología de núcleo.

No es fácil hacer que un sistema de computadoras sea seguro, pero tampoco es imposible. El mayor error es no hacer caso al problema—un error fatal que evidentemente permite que sigan sin usarse soluciones disponibles. El error en esta área crítica introduce un talón de Aquiles en nuestros sistemas de apoyo del campo de batalla—la piedra angular de la Fuerza Aérea electrónica moderna.

*Escuela Naval de Posgraduados
Monterey, California*

Notas

1. Malcolm R. Currie, "Electronics: Key Military 'Force Multiplier' " (Sistemas electrónicos: multiplicador de las fuerzas militares clave), *Air Force Magazine*, julio de 1976, p. 44.

2. Edgar Ulsamer, "How ESD Is Building USAF's Electronic Eyes and Ears" (Cómo el ESD está formando los ojos y oídos electrónicos de la USAF), *Air Force Magazine*, julio de 1977, p. 40.

3. La importancia de la electrónica de la Fuerza Aérea se indica en "The Electronic Air Force" (La fuerza aérea electrónica), *Air Force Magazine*, julio de 1977, p. 29, que observa que este es el séptimo ejemplar anual de la revista dedicado principalmente a este "problema fundamental de la Fuerza Aérea".

4. F. W. Winterbotham, *The Ultra Secret (El secreto Ultra)* (New York: Harper and Row, 1974), p. 11.

5. *Ibid.*, p. 15.

6. *Ibid.*, p. 107.

7. *Ibid.*, p. 191.

8. David Kahn, *The Codebreakers (Los descifradores)*, (New York: Macmillan Co., 1967), p. 67.

9. Winterbotham, p. 85.

10. Kahn, p. 591.

11. *Ibid.*, p. 392.

12. Thomas Whiteside, "Dead Souls in the Computer" (Almas muertas en la computadora), *The New Yorker*, 29 de agosto de 1977, pág. 59-62.

13. Tom Alexander, "Waiting for the Great Computer Rip-off" (Esperando el gran timo de la computadora), *Fortune*, Julio de 1974, p. 143.

14. Bonnie Ginzburg, "Military Computers Easily Penetrable, AF Study Finds" (Computadoras militares fácilmente penetrables, averiguaciones de un estudio de la FA), *Washington Post*, 8 de agosto de 1976, p. A6.

15. En agosto de 1976, el Mando de Sistemas de la Fuerza Aérea dirigió la terminación del Programa de Seguridad del Sistema de ADP de la División de Sistemas Electrónicos. La terminación se completó en septiembre de 1977, deteniendo el desarrollo (que iba bien) de un prototipo general seguro para demostrar completamente la aceptabilidad operacional y el desarrollo asociado de especificaciones, recomendaciones de política y criterios de evaluación para uso general.

16. Lawrence Curran, "Air Force 'Kernel' Attains Computer Security Using Existing Technology" (El 'núcleo' de la Fuerza Aérea logra la seguridad de las computadoras usando una tecnología existente), *Electronics*, 30 de septiembre de 1976, pág. 59, 61.

17. El autor hizo una hipótesis inicial sobre el concepto de núcleo de seguridad y su base matemática. La investigación patrocinada de forma subsiguiente en la MITRE Corporation completa la formulación detallada, según se describe en *1976 Computer Security Developments Summary (Resumen de desarrollo de seguridad de computadoras de 1976)* de ESD, MCI-76—2, División de Sistemas Electrónicos, Base de la Fuerza Aérea Hanscom, Massachusetts, enero de 1977.

18. W. L. Schiller, *The Design and Specification of a Security Kernel for the PDP-11/45 (El diseño y la especificación de un núcleo de seguridad para el PDP-11/45)*, ESD—TR-75-69 (Bedford, Massachusetts: MITRE Corporation, mayo de 1975), p. 9.

19. "Computer Security: A Case of Priorities" (Seguridad de computadoras: un caso de prioridades), *Electronics*, 30 de septiembre de 1976, p. 10.

El progreso tecnológico nos ha proporcionado meramente medios más eficientes para retroceder.

Aldous Huxley

Teniente Coronel Roger R. Schell, USAF (Doctorado, Massachusetts Institute of Technology) es un Oficial de Intercambio de USAF/USN como Profesor Asistente de Ciencias Informáticas en la Escuela Naval de Posgraduados, Monterey, California. La mayor parte de su servicio ha sido en desarrollo y adquisiciones de sistemas de armas. Sirvió como ingeniero y gerente de software de computadoras, y durante varios años fue gerente del Programa de Seguridad de Sistemas ADP de la Base de la Fuerza Aérea de Hanscom, Massachusetts. Se graduó de la Escuela Superior de Comando y Estado Mayor y de la Escuela Superior de Guerra Aérea, Base Aérea Maxwell, Alabama.