#	Organization	Commentor	Type	Page #	Line #	Section	Comment (Include rationale for comment)	Suggested change
		Russell Davis					In general, there is a lack of security engineering discussed. In particular, most computers today do not start from a known good state. Instead, there is a reliance on patch management and other approaches to mitigate risk after the fact. Researchers may recall the success of early boot sector infectors because the rogue code loaded before security software. If a machine does not start from a known good state, there is no basis for security. Moreover, even though CPUs have bounds registers, we still see buffer overflow errors. The detail at the boot and OS level requires much work. Coupled with corruption of semiconductor supply chain, the risk to computing systems is greater. How many products were rushed to market only later to discover unanticipated security vulnerabilities?	Include security engineering.