Improving Security of Handheld IT Devices

August 29 2005

Handheld devices such as personal digital assistants are becoming indispensable tools for today's highly mobile workforce. Small and relatively inexpensive, these devices can be used for many functions, including sending and receiving e-mail, storing documents, delivering presentations and remotely accessing data.

While their small size can be an advantage, it also can be a disadvantage since handheld devices can be easier to misplace or to steal than a desktop or notebook computer. If they do fall into the wrong hands, gaining access to the information they store can be relatively easy. The National Institute of Standards and Technology (NIST) has recently issued two reports aimed at making it harder for unauthorized users to access information from these devices.

Proximity Beacons and Mobile Device Authentication (NISTIR 7200) describes how two different kinds of location-based authentication mechanisms that use signals from wireless beacons can be used to authenticate handheld device users. If the user is in an unauthorized location or a location outside a defined boundary, access will be denied or an additional authentication mechanism must be satisfied before gaining access.

While many organizations use smart cards for security, they require a card reader that can be nearly as large as the handheld device. Smart Cards and Mobile Device Authentication (NISTIR 7206) describes two types of smart cards that use standard interfaces supported by handheld devices, avoiding the use of more cumbersome, standard-size smart card

readers.

Both reports describe these innovative authentication mechanisms and provide details on their design and implementation. The reports are available at csrc.nist.gov/publications/nistir/index.html.

Source: NIST