Global Uni-Docs Corporation
P.O. Box 7123
Dallas, TX 75209-0123

GUD

FTC RFID Consumer Privacy and Data Security Commnets

Fundamental inadequacies in network security have led to the emergence of centralized authentication authorities. These centralized authorities (CAs) are used to authorize access to data, authenticate exchange participants, and to administer network encryption keys and user passwords. However, CAs come at a high cost. Aside from direct costs, administrators are required to maintain secure directories and administer data trust classifications, log-ins, passwords, and encryption keys; all of which constantly change and increase the total cost of ownership.

CAs introduce risk as well as cost. Security and privacy breaches are inevitable because existing approaches separate electronic content from authentication controls. This creates three fundamental vulnerabilities: the manipulation of data before it is exchanged; the modification of content after an authenticated session has been established; and the risk of authorized insiders acting as rogue actors.

Every day, we learn of private and public entities with compromised electronic files, many of which include highly sensitive data. The Pentagon's network infrastructure diagram was exposed after P2P file downloads were inadvertently published. Citigroup had banking records stolen after attackers manipulated the electronic manifest and redirected the delivery. Cyber attackers recently hijacked computer systems and disrupted the power grid in Estonia. All of these breaches are traceable to the separation of electronic content from security controls. Additional information layers, such as RFID identification methodology, do not remove these vulnerabilities and may exacerbate risk.

Identifying an asset using RFID tags, molecular markers, or other means may create additional risk because the underlying data may be separated from the "tag". All one needs to do is disassociated the asset from the data to impugn the system. The same is true of authentication methodologies that are dependent upon centralized authorities.

Current data authentication approaches require extensive key management, such as Public Key Infrastructure (PKI). However, once content is distributed, there are no effective enforcement controls. Not only that, PKI is often administered using third parties that weaken how authentication procedures are executed once content is archived.

IT security spending has reached over $70 billion per year, yet the number of successful attacks, the sophistication of the attackers, the cost to remedy the breaches, and the value of the compromised data continues to grow at alarming rates suggesting that existing alternatives are not working exceptionally well.

Now is the time to consider a different approach: Content-Centric Security (CCS). CCS content is self-governing after distribution and facilitates secure exchanges between users or devices. CCS transforms the way we think of secure data because the content itself, through embedded rule-sets, determines who, when, where, what, and how it is to be used.

As more participants, requiring various trust levels, using multiple devices, exchange increasing amounts and types of content, enterprises face enormous risk. The number and scale of attacks is increasing with competitors, rogue nation-states, terror groups, and organized crime all executing increasingly sophisticated cyber attacks. Dependency upon centralize authorities to authenticate participants and ensure that content has not been manipulated will not work efficiently in a wireless environment due to the lack of architectural robustness. Content-Centric Security (CCS) solves these problems by providing a game-changing technology that creates “smart” self-governing security controls tightly bound to content. Now is the time to consider Content-Centric approaches to security.

David Shaw, President
Global Uni-Docs Corporation