



(1) Browser

Spoofed – requests to (2) (maybe phishing)
 Repud. - forge a regular user's ID (2)

(2) Process, (3) External dll

Spoofed – create widget command (2)
 Spoofed – response to (1)
 Spoofed – write to Db (4)
 Tamper - Malware manipulates data
 Repud. - ID forged for DB interactions
 Info Disc – Data for DB/Browser session
 Deny – Crash process
 Escalate - Malicious Browser Request
 Escalate - Malicious code from DLL

(4) Database

Tamper – MitM to read data(5)
 Info Disc - Net Eavesdropping(5),(6)
 Deny – Network DDos(4)

(5) Read

Tamper – MitM to read data
 Info Disc - Net Eavesdropping
 Deny – Network DDos

(6) Write

Tamper – MitM to write data
 Info Disc – Net Eavesdropping
 Deny - Network DDos

(7), (8) (Create) Widget

Tamper – Malicious widget to (2)
 Info Disc – Widget functions
 Deny – Move dll

(9) Request

Tamper – MitM to request
 Info Disc - Net Eavesdropping
 Deny - Network DDos

(10) Response

Tamper - MitM to response
 Info Disc - Net Eavesdropping
 Deny - Network DDos

Mitigation

Spoof	To authenticate principals: <ul style="list-style-type: none">-Windows authentication (NTLM)-Kerberos authentication-Windows or Live ID authentication-PKI systems such as SSL/TLS and certificates-IPsec-Digitally signed packets	To authenticate code or data: <ul style="list-style-type: none">-Digital signatures-Message authentication codes-Hashes
Tamper	<ul style="list-style-type: none">-Discretionary Access Control Lists-Mandatory Integrity Controls	<ul style="list-style-type: none">-Digital signatures-Message authentication codes
Repudiation	<ul style="list-style-type: none">-Strong authentication-Secure logging and auditing-Digital signatures	<ul style="list-style-type: none">-Time stamps-Trusted third parties
Information Disclosure	<ul style="list-style-type: none">-Encryption	<ul style="list-style-type: none">-ACLs
Denial of Service	<ul style="list-style-type: none">-Discretionary Access Control Lists-Filtering	<ul style="list-style-type: none">-Quotas and rate limits-Authorization-High-availability designs
Elevation of privilege	<ul style="list-style-type: none">-Windows Discretionary Access Control Lists-Group or role membership	<ul style="list-style-type: none">-Privilege ownership-Permissions-Input validation