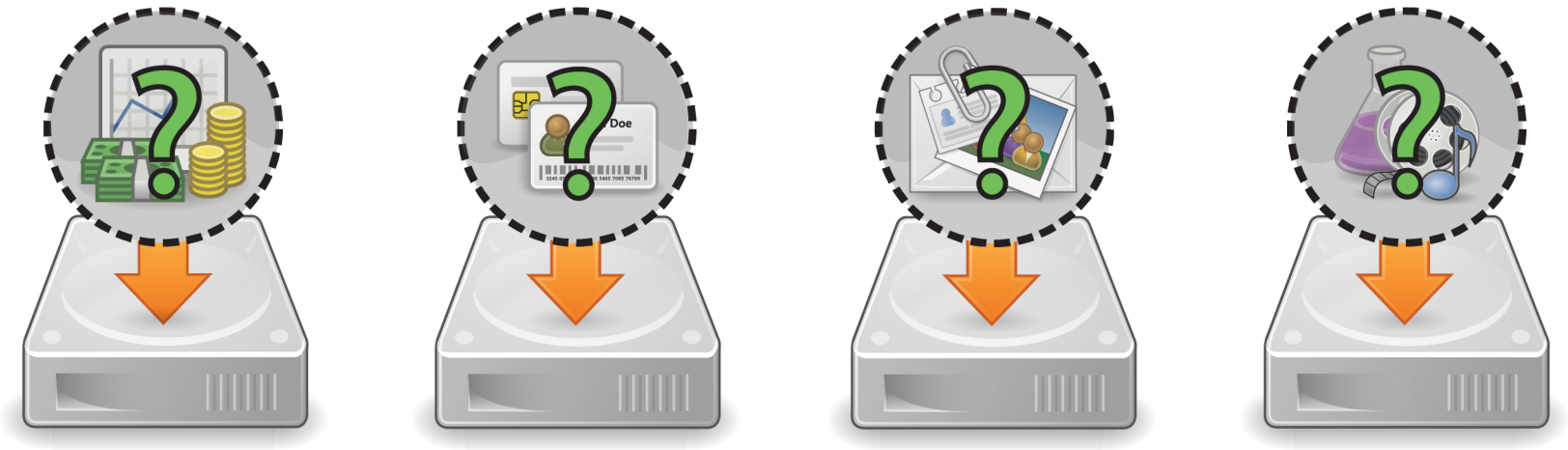
[digital asset drives]



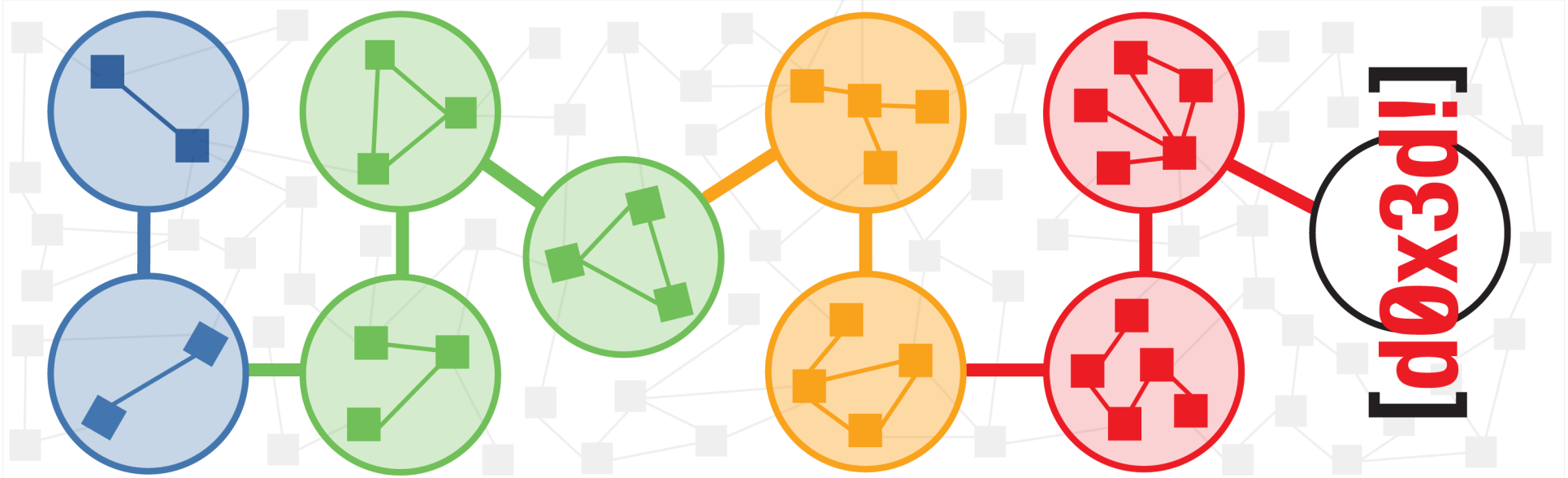
financial data

authentication credentials

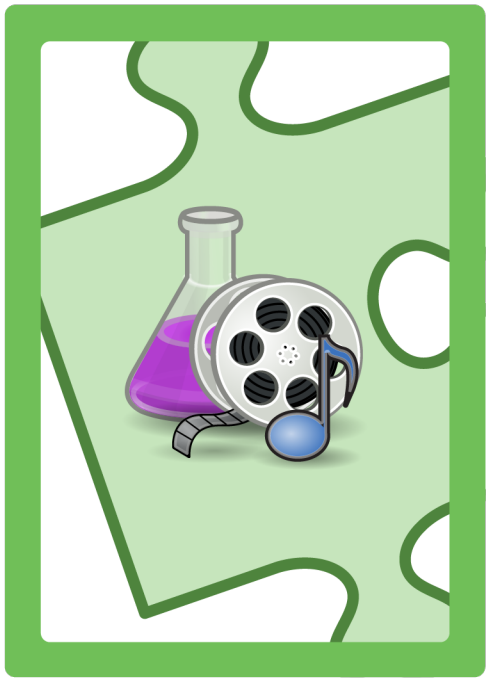
personally identifiable information

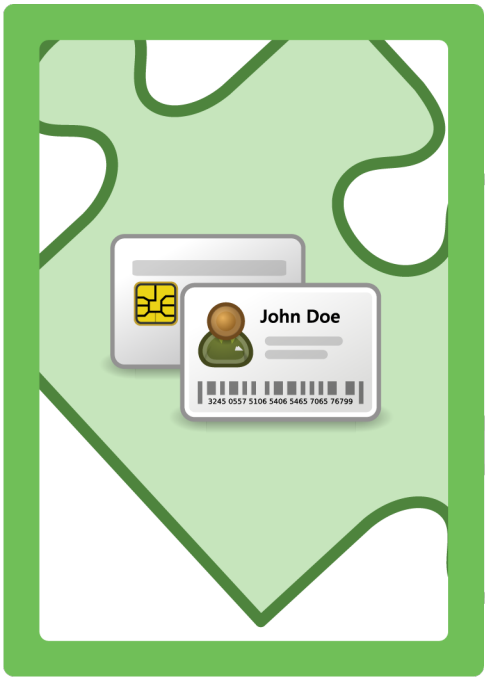
intellectual property

[patch 2] [patch 3] [patch 4] [patch 5] [you got d0x3d!]



infocon 5 infocon 4 infocon 3 infocon 2 infocon 1





[intrusion detected]: Raise the **[infocon]** level.

[honeypot audit]: Immediately draw a **[patch!]** card. If the pictured **[node]** is compromised, raise the **[infocon]** level.

[check]: The hand limit is five cards. Every card in excess of the hand limit must be discarded. You may play **[zero-day exploits]** before discarding them.

[patch] situations:

- Any **[lo0t!]** cards left on a **[node]** being patched are discarded.
- If a player is on a node being patched, she must **[move]** to a compromised node (obeying normal movement rules), then **[decommission]** the node and its **[patch!]** card.
- **[zero-day exploits]** can be used to prevent all **[patch]** effects.

order of play

1. [action]
   Take up to 3 actions:
   [move], [compromise], [drop], [give], [exchange], [pickup], [recover]
2. [loot]
   Draw 2 **[lo0t!]** cards. Resolve **[intrusion detected]** and **[honeypot audit]** cards.
3. [patch]
   Draw and resolve **[patch!]** cards, as indicated by the **[infocon]** level.
4. [check]
   Discard, to obey the hand limit.

[intrusion detected]: Raise the **[infocon]** level.

[honeypot audit]: Immediately draw a **[patch!]** card. If the pictured **[node]** is compromised, raise the **[infocon]** level.

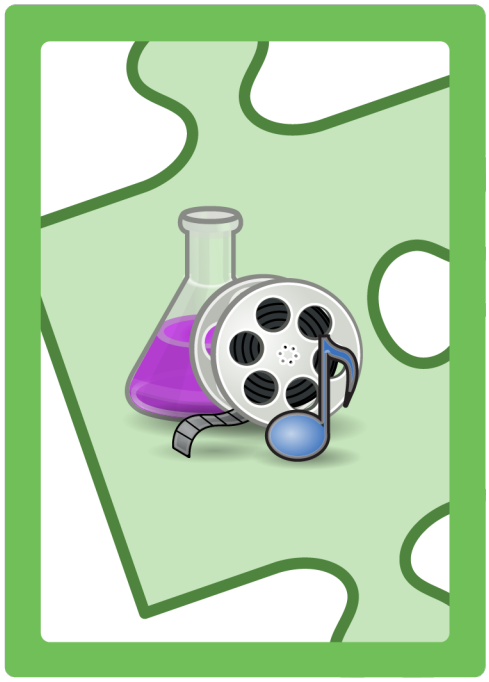
[check]: The hand limit is five cards. Every card in excess of the hand limit must be discarded. You may play **[zero-day exploits]** before discarding them.

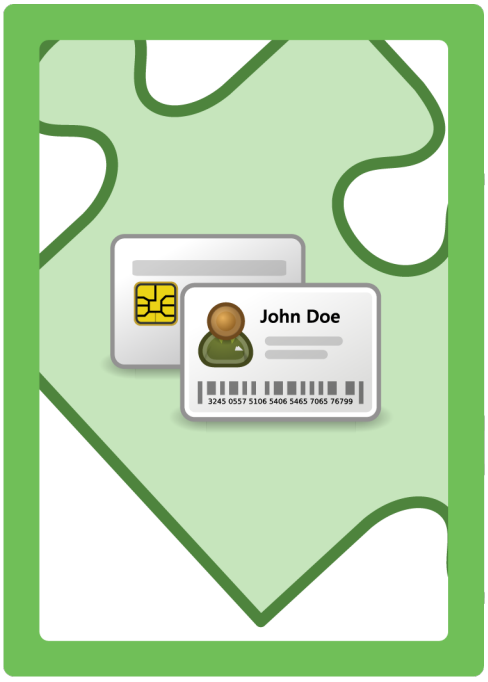
[patch] situations:

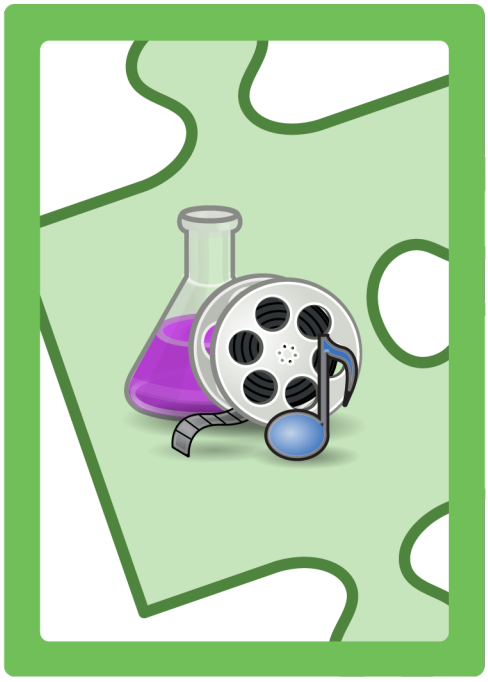
- Any **[lo0t!]** cards left on a **[node]** being patched are discarded.
- If a player is on a node being patched, she must **[move]** to a compromised node (obeying normal movement rules), then **[decommission]** the node and its **[patch!]** card.
- **[zero-day exploits]** can be used to prevent all **[patch]** effects.

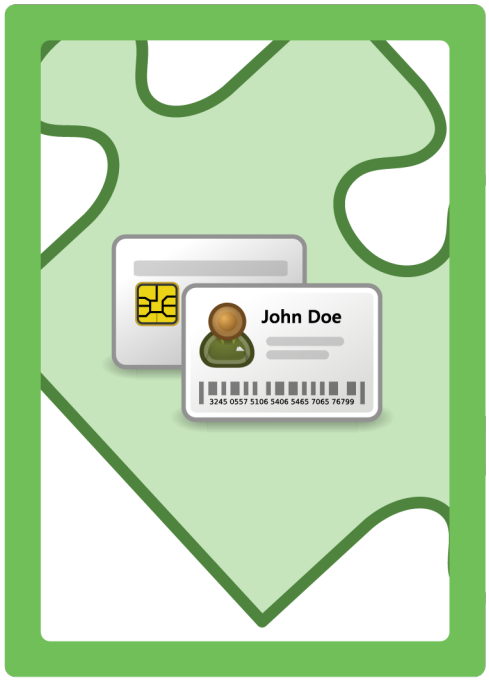
order of play

1. [action]
   Take up to 3 actions:
   [move], [compromise], [drop], [give], [exchange], [pickup], [recover]
2. [loot]
   Draw 2 **[lo0t!]** cards. Resolve **[intrusion detected]** and **[honeypot audit]** cards.
3. [patch]
   Draw and resolve **[patch!]** cards, as indicated by the **[infocon]** level.
4. [check]
   Discard, to obey the hand limit.




John Doe
3245 0557 5106 5406 5465 7065 76799




John Doe
3245 0557 5106 5406 5465 7065 76799

wireless router

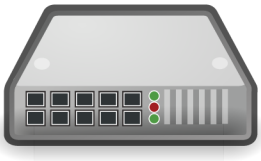
web server

VPN gateway

VoIP server

single sign-on service

VLAN switch



SMTP server

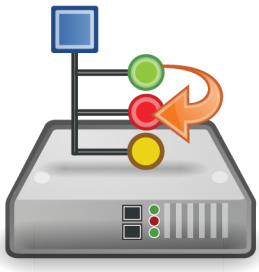
secondary DNS server

sales database

primary DNS server

network file server

NAT device

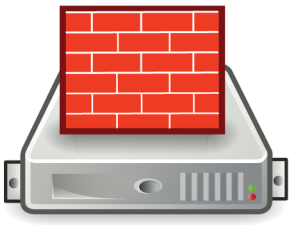


intrusion detection system

internet gateway

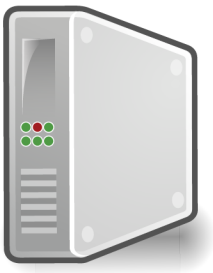
IMAP server

firewall



customer database

client



client

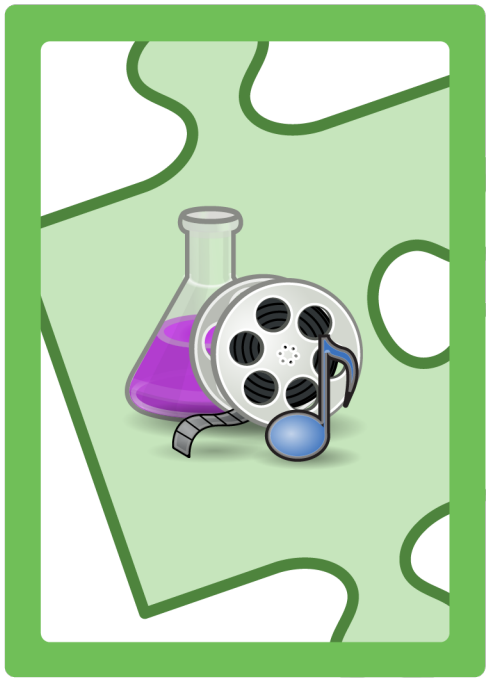
client

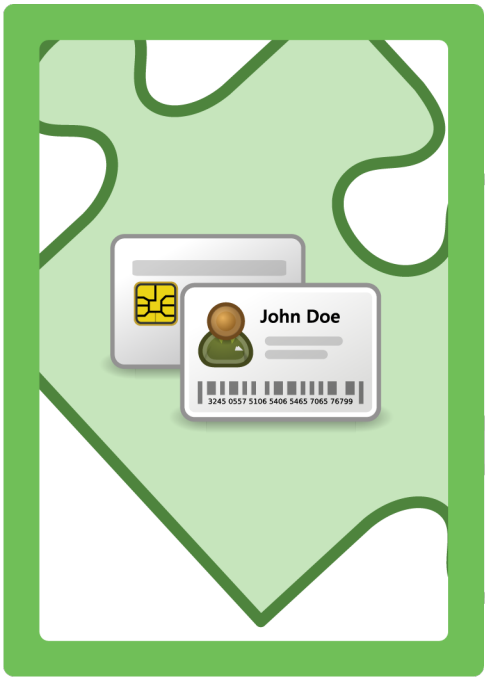
client

chat server

certificate services

backup file server





[zero-day exploit]

buffer overflow

compromise any node and move any hacker to that node

[zero-day exploit]

trojan horse

compromise any node and move any hacker to that node

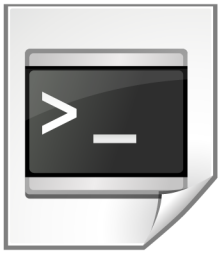
[zero-day exploit]

logic bomb

compromise any node

[zero-day exploit]

integer overflow



compromise any node

[zero-day exploit]

format string vulnerability

compromise any node

[botmaster]

Special Ability:

As one action, [give] or [exchange] **two** cards.

[cryptanalyst]

Special Ability:

As one action, [move] or [compromise] **diagonally**.

[the insider]

Special Ability:

As one action, [compromise] **two** adjacent tiles.

[malware writer]

Special Ability:

As one action, [move] across **two** compromised tiles.

[social engineer]

Special Ability:

As one action, [move] to **any** compromised tile.

[war driver]

Special Ability:

As one action, [give] or [exchange] a card to a player **anywhere** on the network.

[intrusion detected]

virus signature matched

[intrusion detected]

network anomaly observed

honeypot audit

wireless router

wireless router

web server

web server

VPN gateway

requires two actions
to compromise

VPN gateway

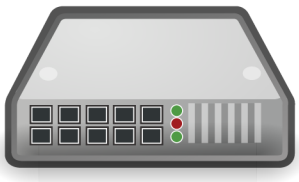
requires two actions
to compromise

VoIP server

VoIP server

VLAN switch

VLAN switch



single sign-on service

single sign-on service

SMTP server

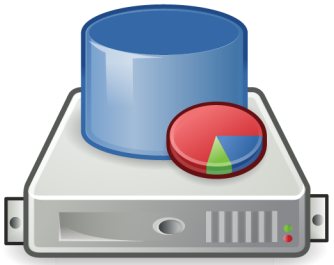
SMTP server

secondary DNS server

secondary DNS server

sales database

sales database



primary
DNS server

primary
DNS server

network
file server

network
file server

NAT device

NAT device

intrusion detection system

requires two actions to compromise

intrusion detection system

requires two actions to compromise

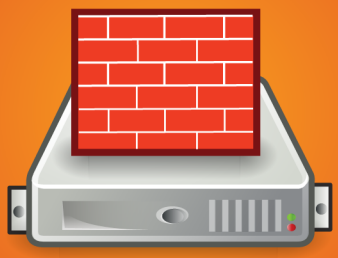
internet gateway

internet gateway

IMAP server

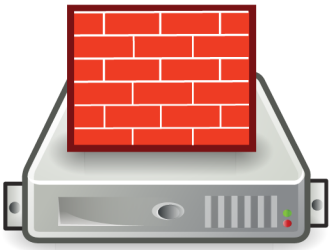
IMAP server

firewall



requires two actions
to compromise

firewall



requires two actions
to compromise

customer database

customer database

client

client

client

client

client

client

client

client

chat server

chat server

certificate services

certificate services

backup file server

backup file server