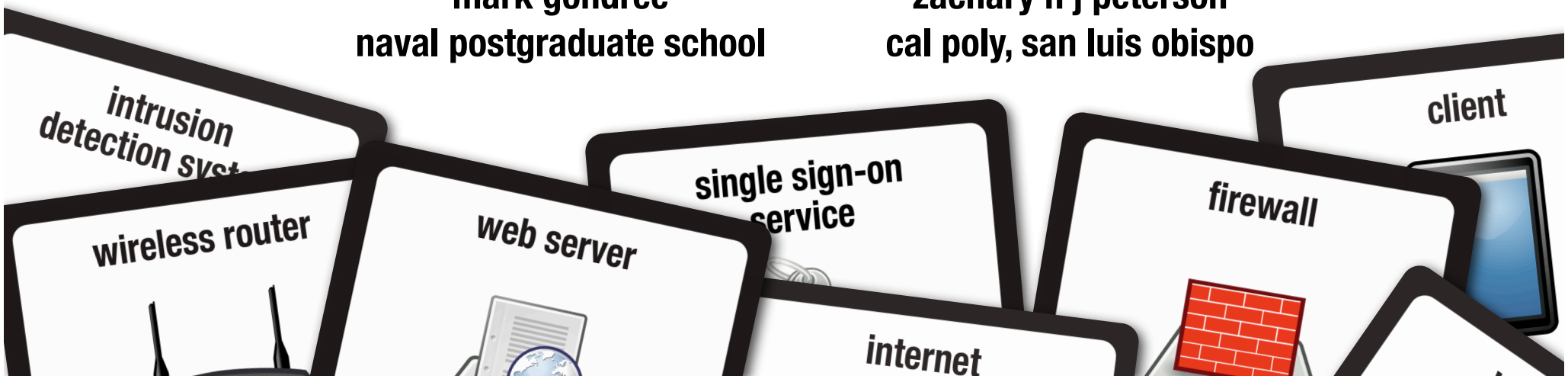
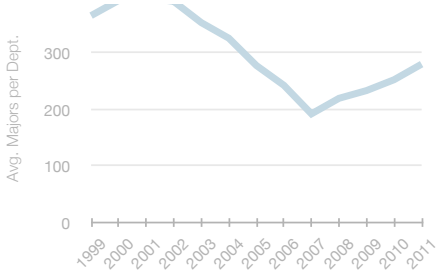
valuing security by getting [d0x3d!]

experiences with a network security board game

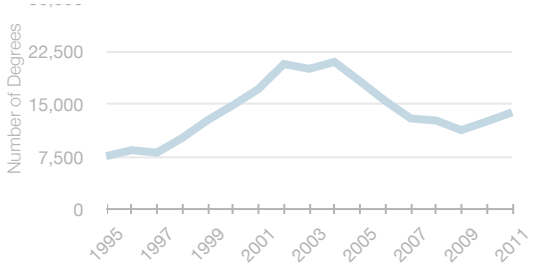
mark gondree
naval postgraduate school

zachary n j peterson
cal poly, san luis obispo

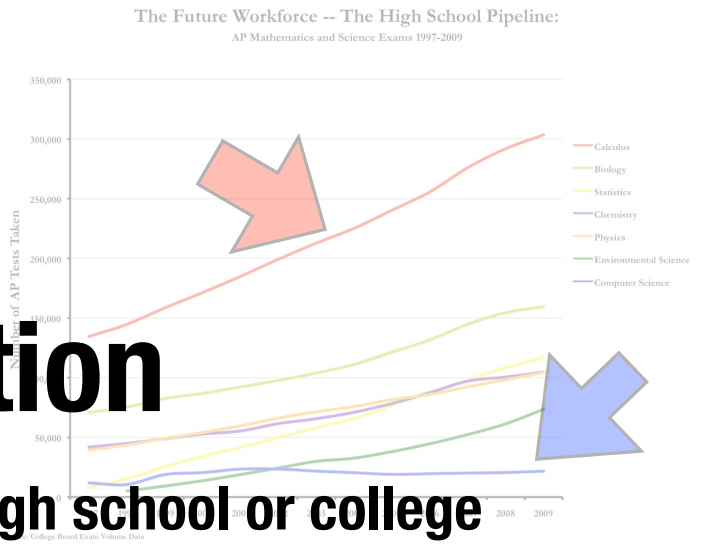




Source: Table 6: Total Bachelor's Enrollment by Department Type



Source: Table 3: Bachelor's Degrees Awarded by Department Type



CS enrollment

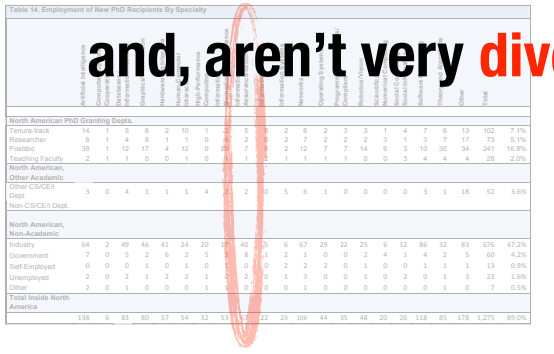
CS graduates

cybersecurity education

students not pursuing (or offered) CS in high school or college

of those that do, don't pursue **security**

and, aren't very **diverse**



67/1275 (5%) of CS PhDs pursued security

Male	7,983	88.3%
Female	1,057	11.7%
Total Known Gender	9,040	
Gender Unknown	246	
Grand Total	9,286	

Nonresident Alien	524	7.0%
Amer Indian or Alaska Native	39	0.5%
Asian	1,115	14.8%
Black or African-American	274	3.6%
Native Hawaiian/Pac Islander	22	0.3%
White	5026	66.9%
Multiracial, not Hispanic	104	1.4%
Hispanic, any race	409	5.4%
Total Residency & Ethnicity Known	7,513	
Resident, ethnicity unknown	741	
Residency unknown	1032	
Grand Total	9,286	

BS

Male	4,968	75.4%
Female	1,623	24.6%
Total Known Gender	6,591	
Gender Unknown	20	
Grand Total	6,611	

Nonresident Alien	3,332	56.7%
Amer Indian or Alaska Native	12	0.2%
Asian	753	12.8%
Black or African-American	96	1.6%
Native Hawaiian/Pac Island	19	0.3%
White	1533	26.1%
Multiracial, not Hispanic	8	0.1%
Hispanic, any race	119	2.0%
Total Residency & Ethnicity Known	5,872	
Resident, ethnicity unknown	320	
Residency unknown	419	
Grand Total	6,611	

MS

Male	1,154	81.6%
Female	261	18.4%
Total Known Gender	1,415	
Gender Unknown	41	
Grand Total	1,456	

Nonresident Alien	634	48.1%
Amer Indian or Alaska Native	2	0.2%
Asian	171	13.0%
Black or African-American	16	1.2%
Native Hawaiian/Pac Islander	4	0.3%
White	465	35.3%
Multiracial, not Hispanic	3	0.2%
Hispanic, any race	22	1.7%
Total Residency & Ethnicity Known	1,317	
Resident, ethnicity unknown	43	
Residency unknown	96	
Grand Total	1,456	

PhD

but, why?

causes are generally unknown

increasingly structured curricula

realities, perceptions & stigmas



a non-digital, computer security board game

to address the shortage of cybersecurity and other STEM professionals

used to easily incorporate security into any curriculum

[d0x3d!] is: accessible, collaborative, fun



[setting]

bad guys have stolen your data, and hidden them in their network

you and your teammates take on the role of an elite hacking syndicate



each player assumes a [hacker] role

[objective]

their mission is to infiltrate the network, and as a team, recapture four

[digital assets]



authentication credentials



financial data



personally identifiable information



intellectual property

[game play]

on their turn, a player:

[action] takes up to three actions

[loot] draws two lo0t! cards

[patch] draws patch! cards

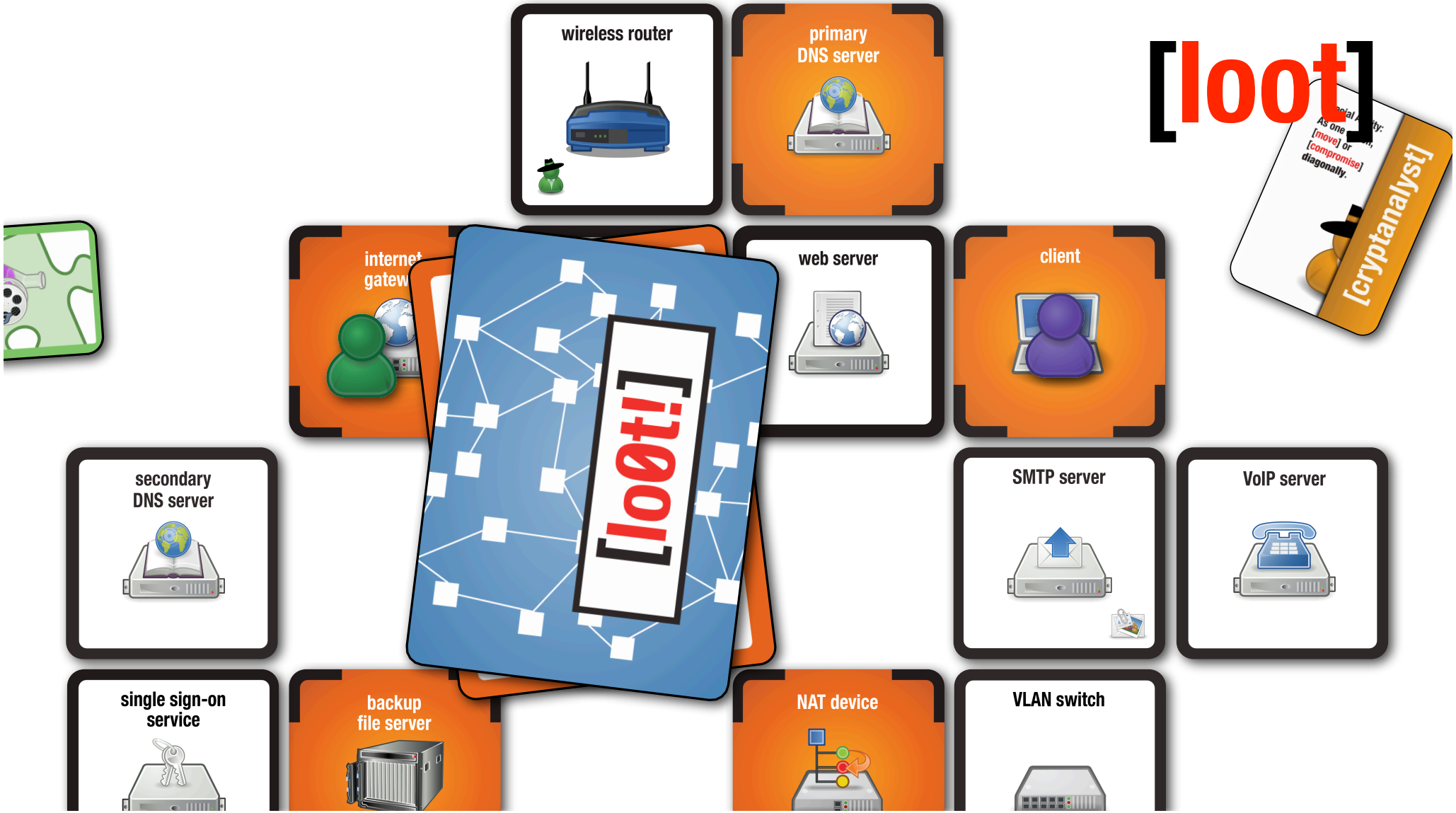

[action]
[move] or
[compromise]
diagonally.
[cryptanalyst]

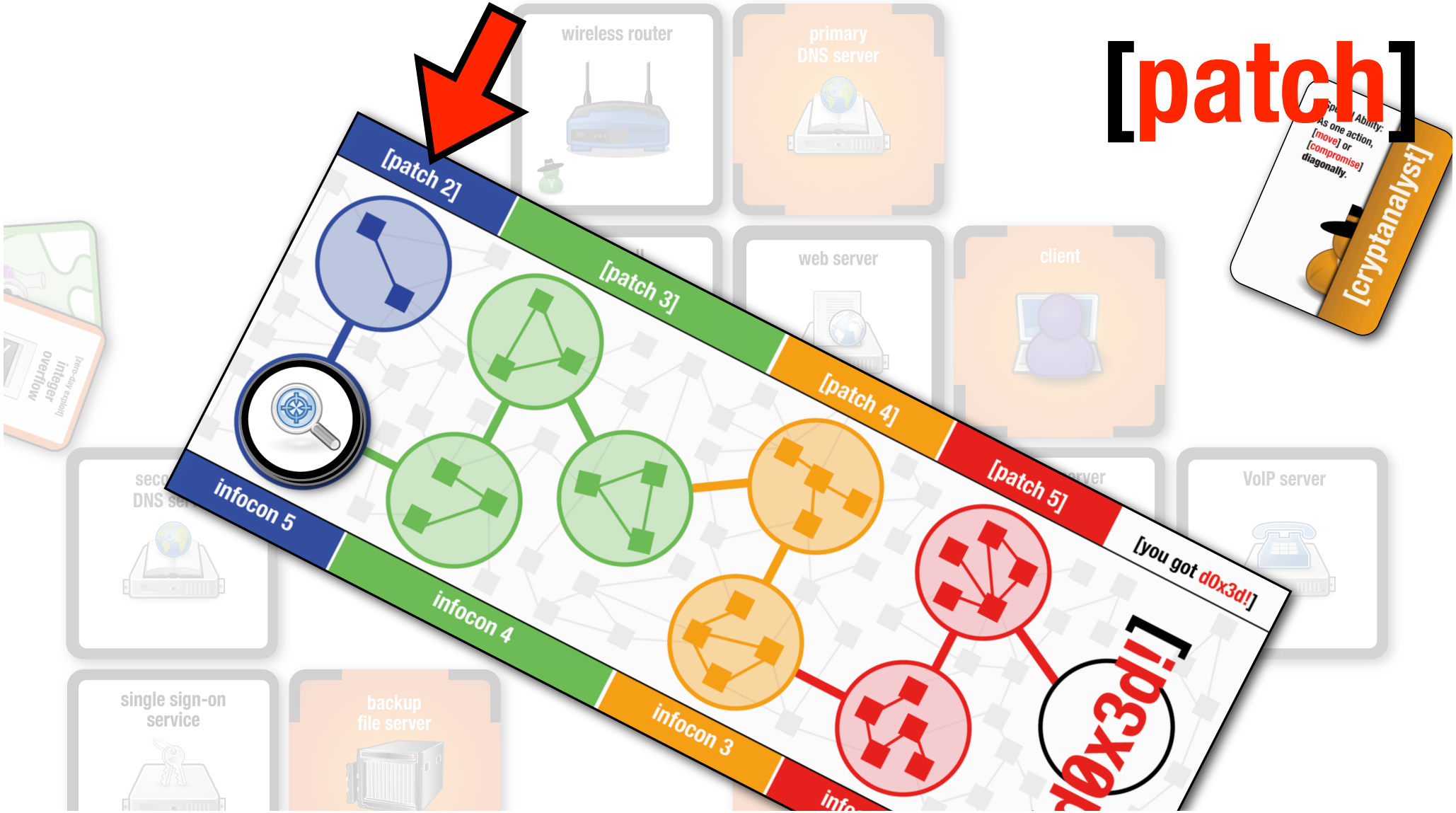

wireless router
primary DNS server
[action]
[cryptanalyst]
internet gateway
firewall
requires two actions to compromise
web server
client
secondary DNS server
client
SMTP server
VoIP server
single sign-on service
backup file server
NAT device
VLAN switch

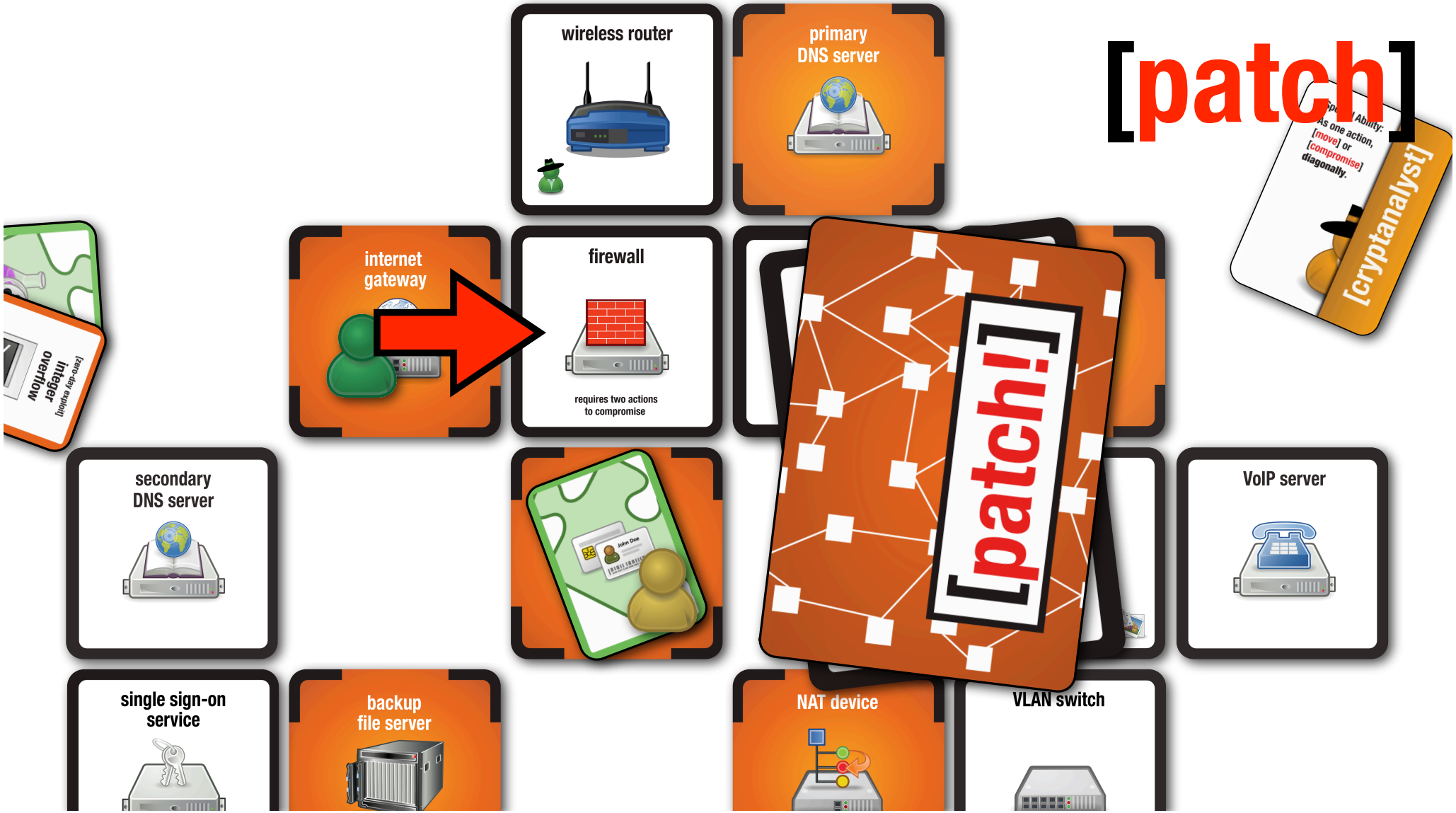

wireless router
primary DNS server
[action]
internet gateway
firewall
requires two actions to compromise
web server
client
[cryptanalyst]
[move] or [compromise] diagonally.
secondary DNS server
client
SMTP server
VoIP server
single sign-on service
backup file server
NAT device
VLAN switch

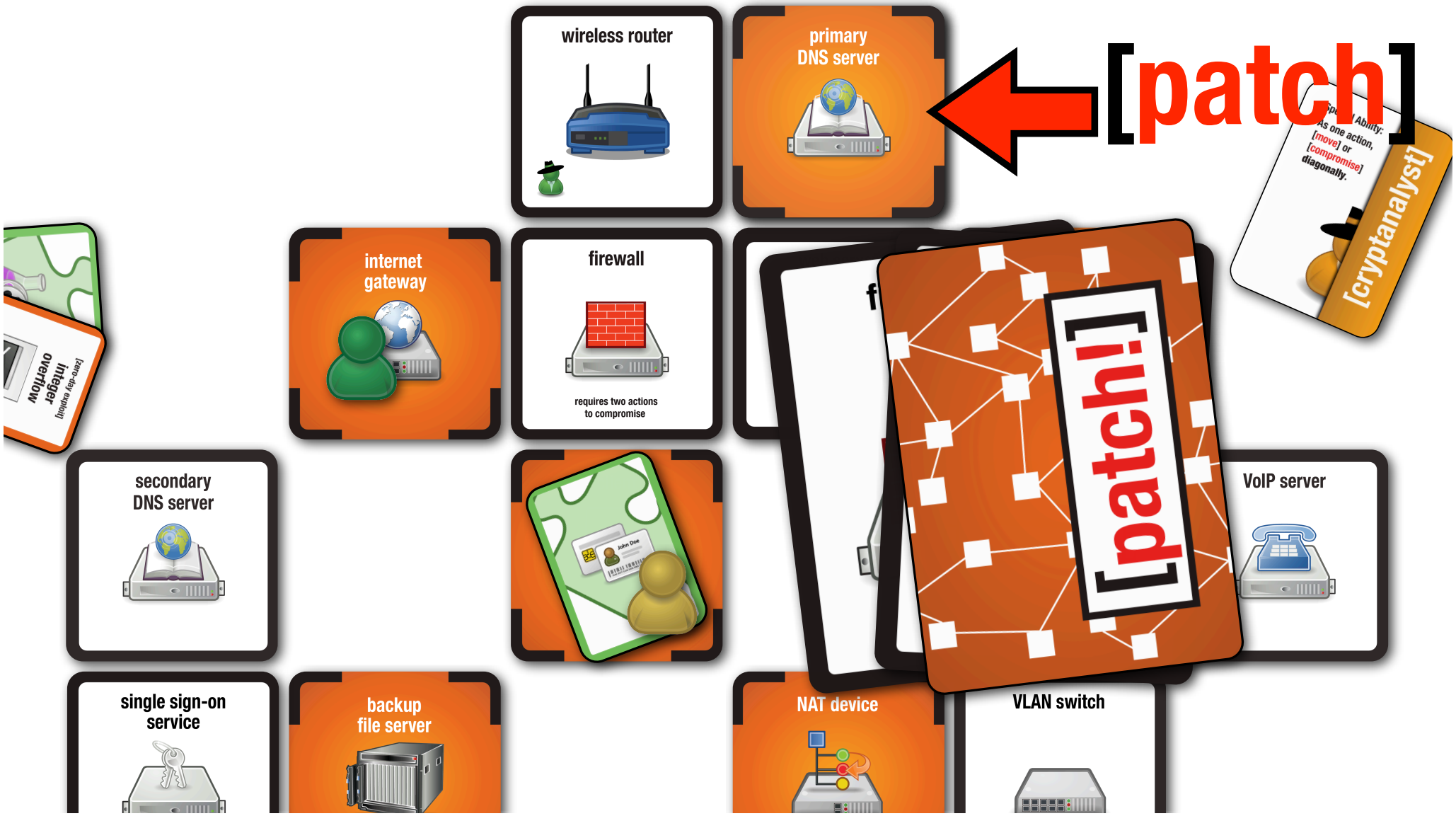

wireless router
primary DNS server
[action]
internet gateway
firewall
requires two actions to compromise
web server
client
[cryptanalyst]
[move] or [compromise] diagonally.
secondary DNS server
SMTP server
VoIP server
single sign-on service
backup file server
NAT device
VLAN switch


wireless router
primary DNS server
internet gateway
client
secondary DNS server
SMTP server
VoIP server
single sign-on service
backup file server
NAT device
VLAN switch
[loot]
[cryptanalyst]


wireless router
primary DNS server
[loot]
internet gatew
web server
client
[cryptanalyst]
secondary DNS server
SMTP server
VoIP server
single sign-on service
backup file server
NAT device
VLAN switch


[patch]
wireless router
primary DNS server
web server
client
VoIP server
single sign-on service
backup file server
integer overflow
[patch 2]
[patch 3]
[patch 4]
[patch 5]
infocon 5
infocon 4
infocon 3
[you got d0x3d!]
[cryptanalyst]


wireless router
primary DNS server
[patch]
internet gateway
firewall
requires two actions to compromise
[cryptanalyst]
integer overflow
secondary DNS server
VoIP server
single sign-on service
backup file server
NAT device
VLAN switch


wireless router
primary DNS server
[patch]
internet gateway
firewall
requires two actions to compromise
integer overflow
[cryptanalyst]
[patch!]
secondary DNS server
VoIP server
single sign-on service
backup file server
NAT device
VLAN switch

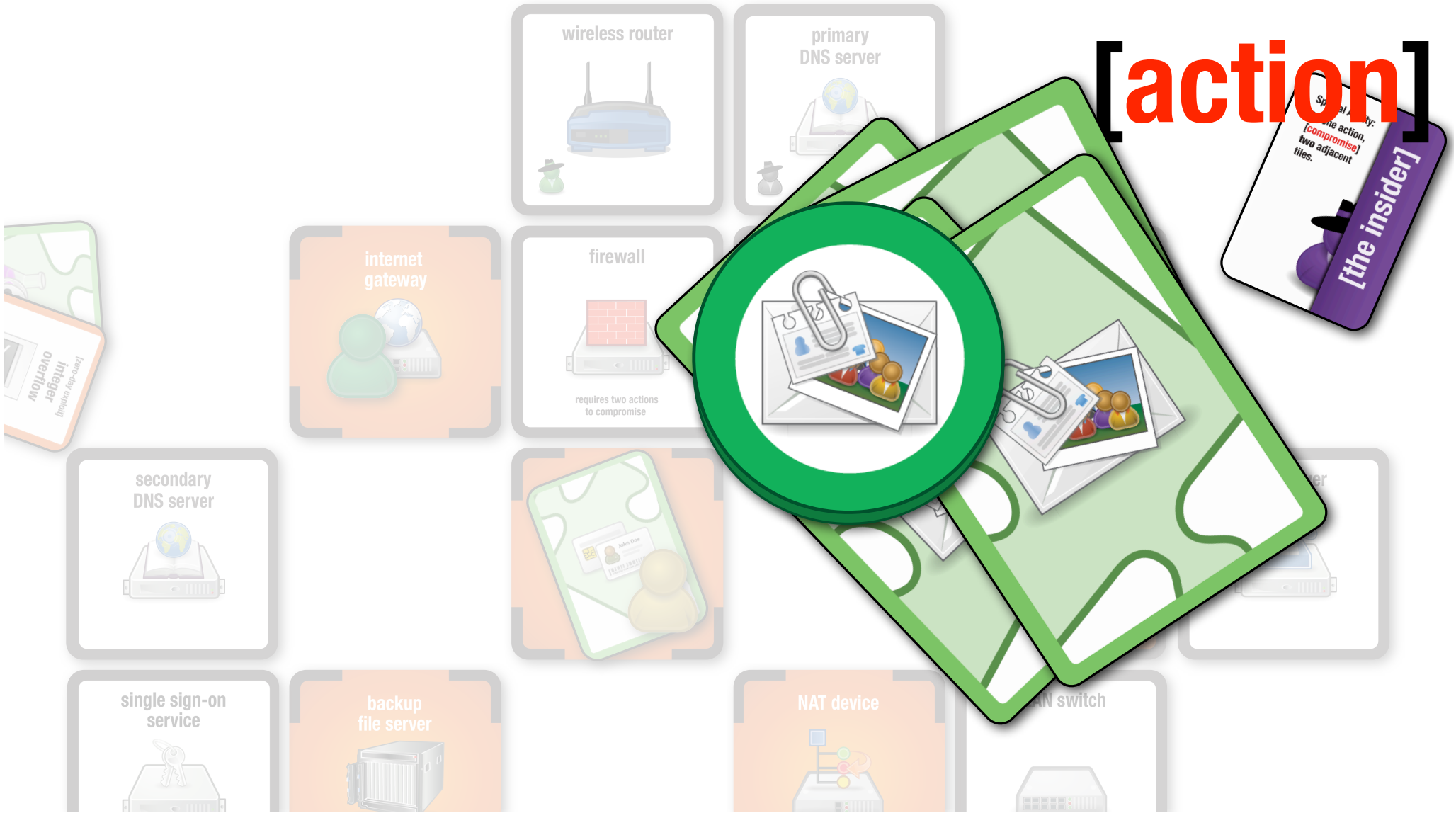
now it’s [the insider]’s turn

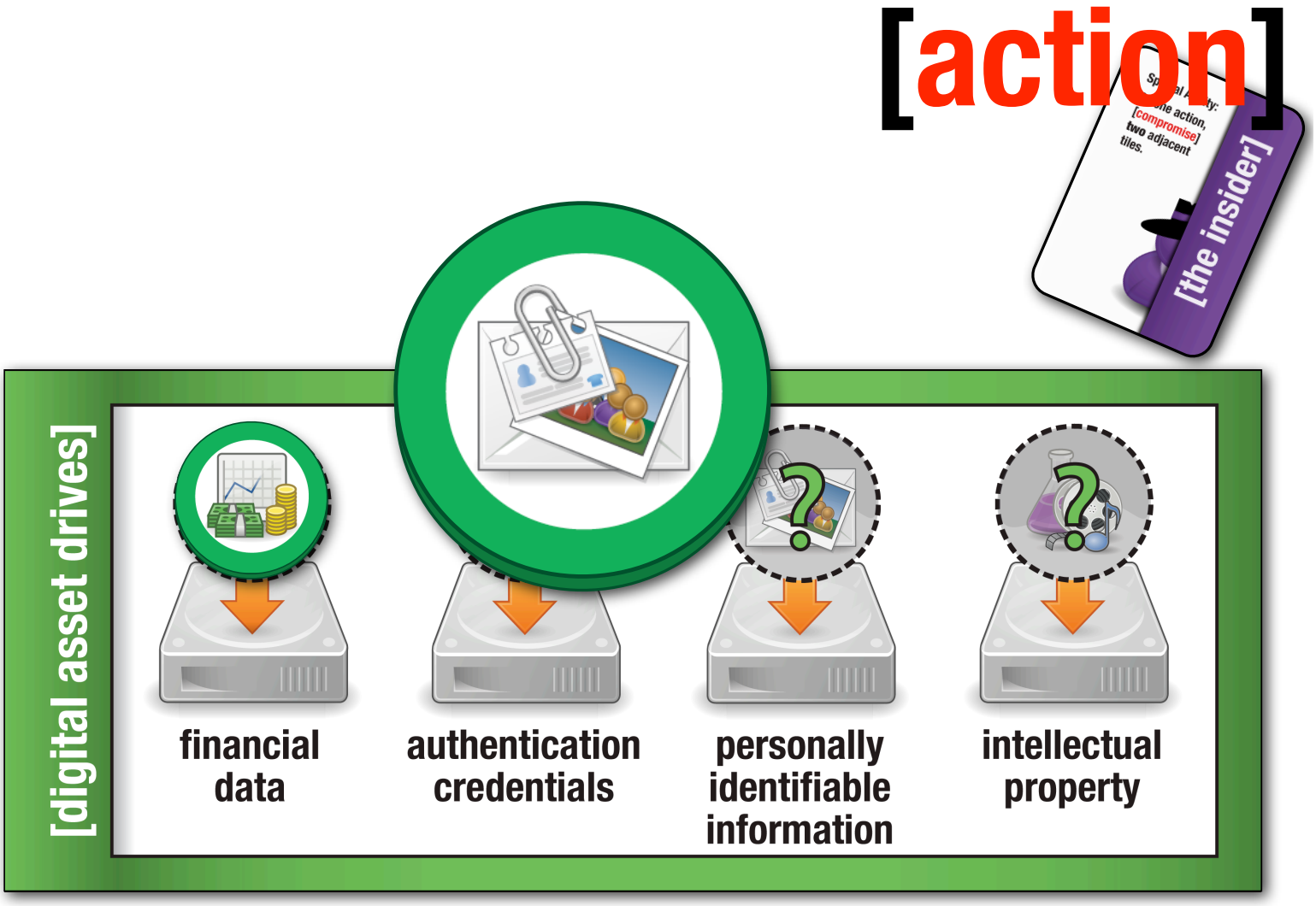



[action]
[compromise]
two adjacent
tiles.
[the insider]


wireless router
primary DNS server
[action]
[the insider]
integer overflow
internet gateway
firewall
requires two actions to compromise
web server
client
secondary DNS server
SMTP server
VoIP server
single sign-on service
backup file server
NAT device
VLAN switch


wireless router
primary DNS server
[action]
[the insider]
integer overflow
internet gateway
firewall
requires two actions to compromise
web server
client
secondary DNS server
SMTP server
VoIP server
single sign-on service
backup file server
NAT device
VLAN switch

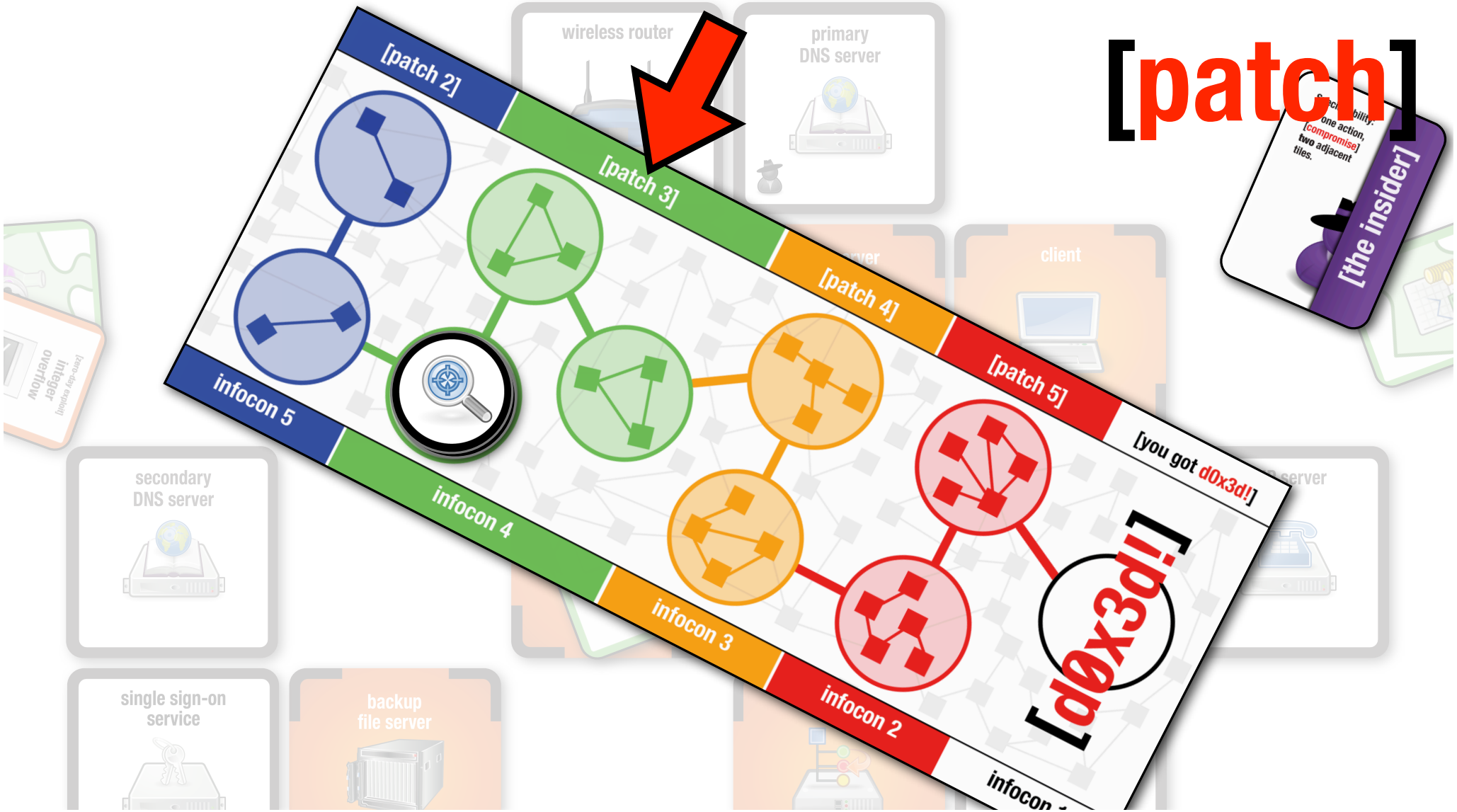

wireless router
primary DNS server
internet gateway
firewall
requires two actions to compromise
secondary DNS server
single sign-on service
backup file server
NAT device
[action]
[the insider]


[action]
[compromise]
two adjacent
tiles.
[the insider]
[digital asset drives]
financial data
authentication credentials
personally identifiable information
intellectual property

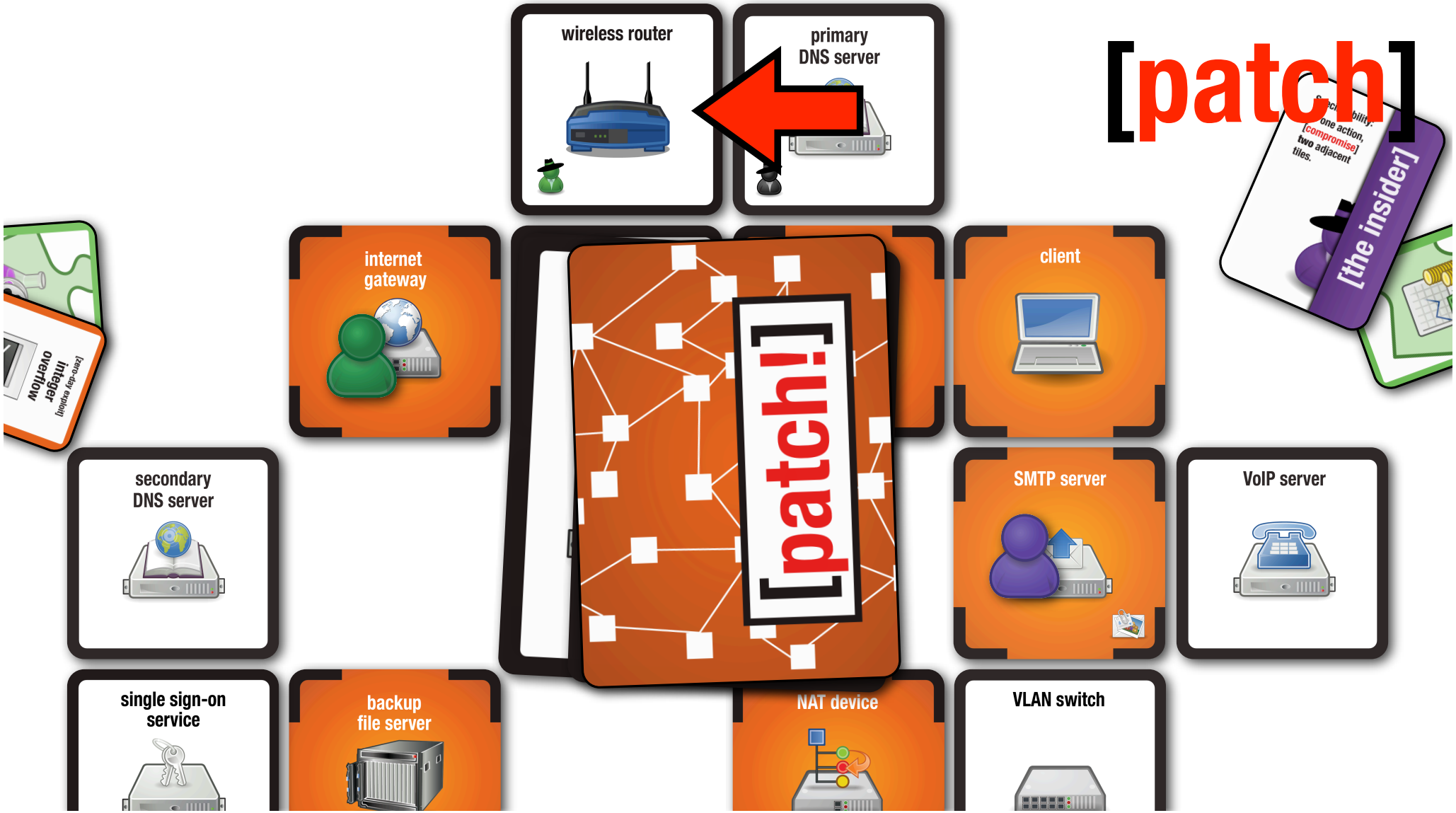

wireless router
primary DNS server
[loot]
internet gateway
firewall
requires two actions to compromise
integer overflow
secondary DNS server
VoIP server
single sign-on service
backup file server
NAT device
VLAN switch
[loot!]
[the insider]

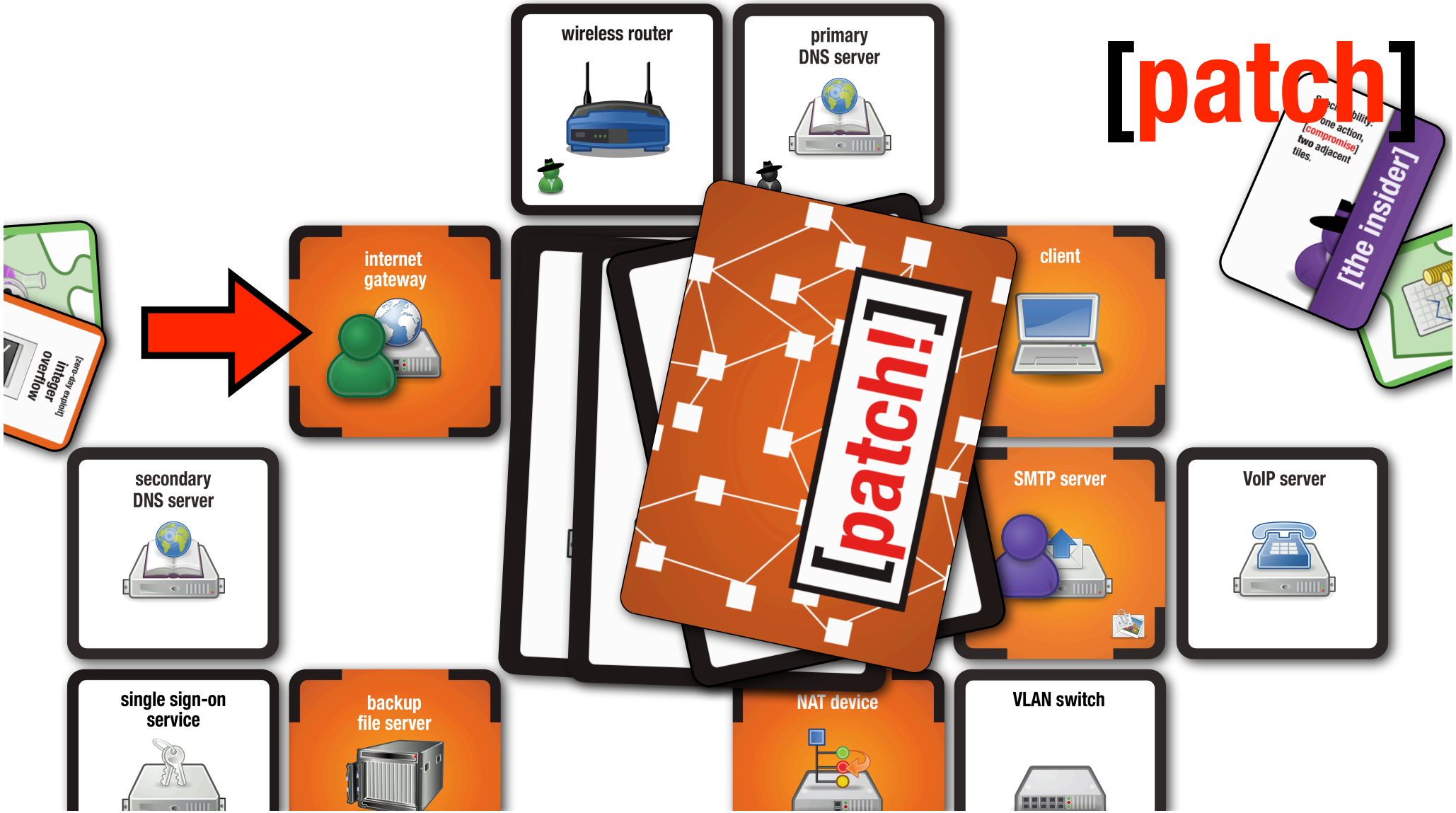

wireless router
primary DNS server
[loot]
internet gateway
firewall
requires two actions to compromise
secondary DNS server
VoIP server
single sign-on service
backup file server
NAT device
VLAN switch


[loot]
[the insider]
[patch 2]
[patch 3]
[patch 4]
[patch 5]
infocon 5
infocon 4
infocon 3
infocon 2
[you got d0x3d!]
[d0x3d!]
wireless router
primary DNS server
secondary DNS server
single sign-on service
backup file server
integer overflow


[patch]
[patch 2]
[patch 3]
[patch 4]
[patch 5]
infocon 5
infocon 4
infocon 3
infocon 2
[you got d0x3d!]
[d0x3d!]
[the insider]
wireless router
primary DNS server
client
secondary DNS server
single sign-on service
backup file server


wireless router
primary DNS server
[patch]
internet gateway
client
secondary DNS server
SMTP server
VoIP server
single sign-on service
backup file server
NAT device
VLAN switch
integer overflow
[the insider]
[compromise]


wireless router
primary DNS server
[patch]
internet gateway
client
[patch!]
secondary DNS server
SMTP server
VoIP server
single sign-on service
backup file server
NAT device
VLAN switch
integer overflow
[the insider]


wireless router
primary DNS server
[patch]
internet gateway
client
secondary DNS server
SMTP server
VoIP server
single sign-on service
backup file server
NAT device
VLAN switch
[patch]
[the insider]
integer overflow


wireless router
primary DNS server
[patch]
[zero-day exploit]
integer overflow
compromise any server
internet gateway
client
[the insider]
secondary DNS server
SMTP server
VoIP server
single sign-on service
backup file server
NAT device
VLAN switch

[goals]

intended for a young, non-CS audience

introduce security terminology & raise awareness

stimulate adversarial and analytical thinking

provide opportunities for discussion

be fun, informal and accessible

[design & development]

inspired by Forbidden Island

cooperative play

dynamic game board

meaningful mechanics, iconography & terminology

language neutral

[limitations]

digital assets are arbitrary, overly general

network is simplistic and misrepresents adjacency

we have used these limitations as opportunities for post-game discussions & curriculum modules

[observations]


[hartnell]


[hartnell]


[cyberadventurers]


[cyberadventurers]



[ISSA InfoSecCon]


[NSF SFS Symposium]


[EPIC]

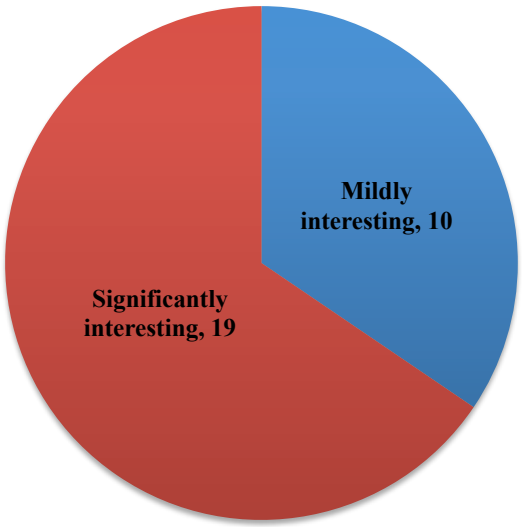

[EPIC]
[the insider]
[social engineer]
[lobby asset token]
[lobby3d]
[lobby]

[observations]

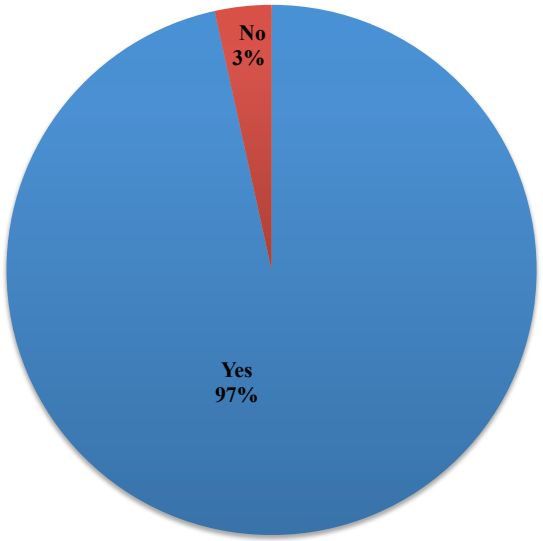




[observations]



what value did you take from the game?



do you recommend we use the game next year?

[IRB: challenges to assessment]

are games experiments or lessons?

Common Rule Exemption exists, but are games “normal educational practices?” Are after-school programs a “commonly accepted educational setting?”

assessing activities at primary & secondary schools

may require: institutional agreement, background checks, parent approval of materials

assessing games involving the use of minors & military

minors have special status and require consent; are college IRBs qualified to determine harm? Military students are also a vulnerable population, complicating participation

[status]

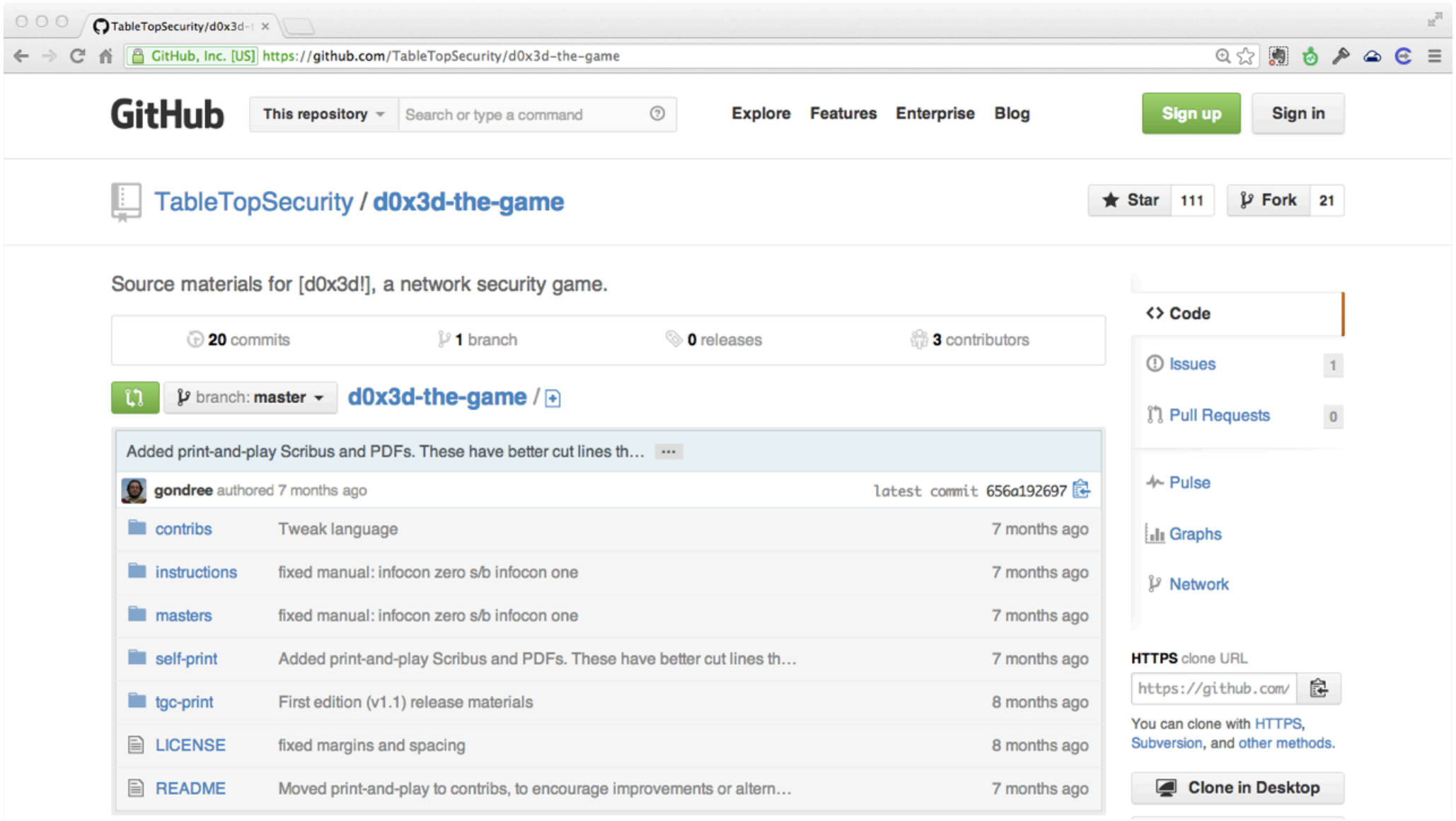
released open-source: download, print and remix

promotional & instructional videos

three follow-on exercises and curriculum modules

opportunities for a variety of student research

www.d0x3d.com


TableTopSecurity/d0x3d-t
GitHub, Inc. [US] https://github.com/TableTopSecurity/d0x3d-the-game
GitHub
This repository
Search or type a command
Explore
Features
Enterprise
Blog
Sign up
Sign in
TableTopSecurity / d0x3d-the-game
Star 111
Fork 21
Source materials for [d0x3d!], a network security game.
20 commits
1 branch
0 releases
3 contributors
branch: master
d0x3d-the-game /
Added print-and-play Scribus and PDFs. These have better cut lines th…
gondree authored 7 months ago
latest commit 656a192697
contribs Tweak language 7 months ago
instructions fixed manual: infocon zero s/b infocon one 7 months ago
masters fixed manual: infocon zero s/b infocon one 7 months ago
self-print Added print-and-play Scribus and PDFs. These have better cut lines th… 7 months ago
tgc-print First edition (v1.1) release materials 8 months ago
LICENSE fixed margins and spacing 8 months ago
README Moved print-and-play to contribs, to encourage improvements or altern… 7 months ago
Code
Issues 1
Pull Requests 0
Pulse
Graphs
Network
HTTPS clone URL
https://github.com/
You can clone with HTTPS, Subversion, and other methods.
Clone in Desktop

Home Connect Discover Me Search

Iván Sánchez Ortega
@RealIvanSanchez

Follow

Finally, my printed-at-home @dox3d set is ready for play. :-)
pic.twitter.com/wdVW5hhO

Reply Retweet Favorite



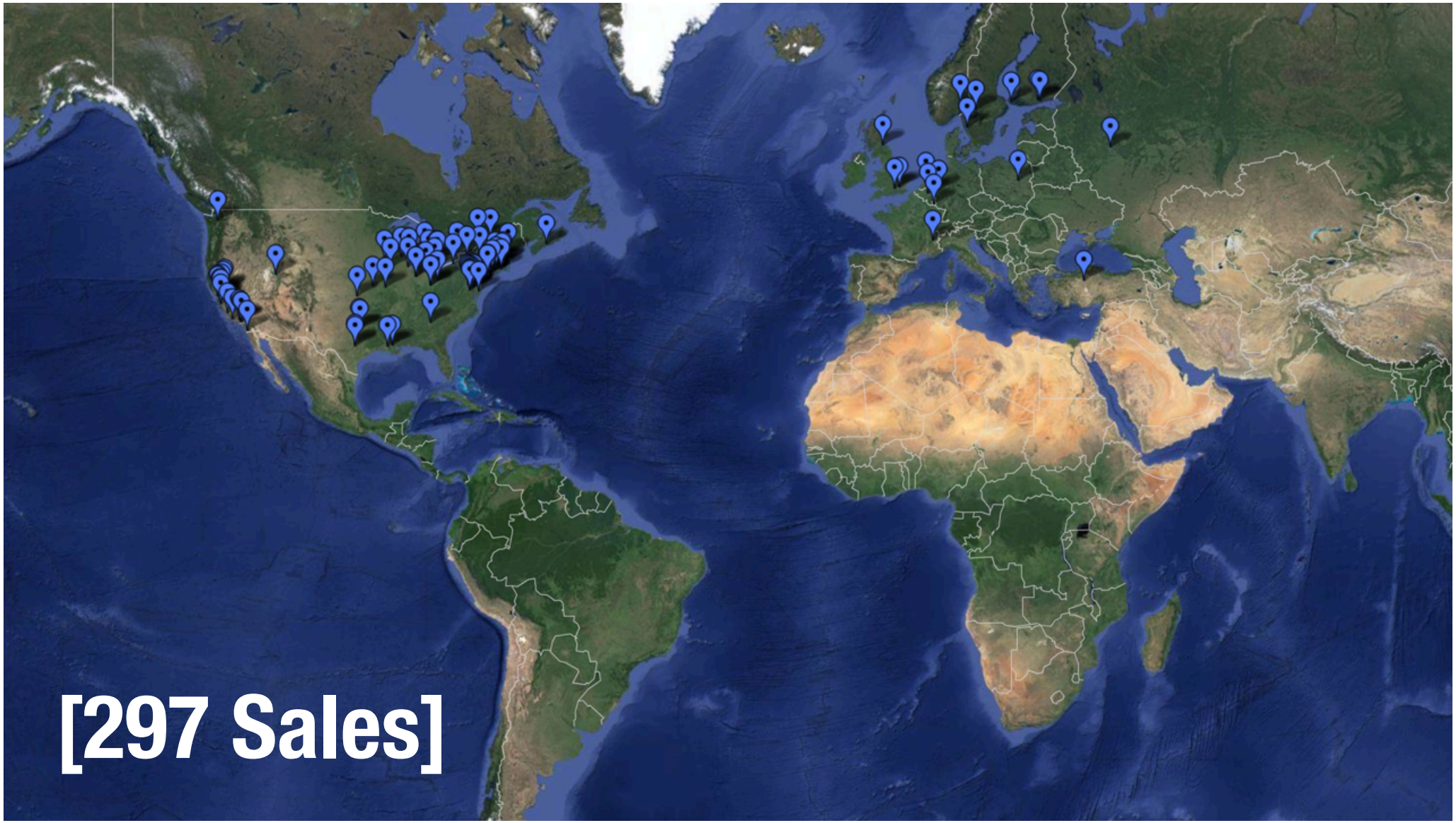
12:41 AM - 12 Jan 13 · Embed this Tweet

Flag media

Reply to @RealIvanSanchez @d0x3d

Javier Cantero @jcantero 12 Jan
@RealIvanSanchez ¿Lo has imprimido en alguna copistería o con una impresora casera?
Details

Iván Sánchez Ortega @RealIvanSanchez 12 Jan
@jcantero En una impresora láser color normalilla. Luego es cuestión de marcar dobleces con cuchilla y cortar con


[297 Sales]

[future work]

[d0x3d!] v2.0: new hacker roles, abilities, game board

building assessment tools

online card creator

workshop

www.d0x3d.com @d0x3d

[th4nks!]

mgondree@nps.edu
@mgondree

znjp@calpoly.edu
@znjp