This set includes a number of games that can be incorporated into lectures or used as study aids. The purpose of these card games is to help students see the mechanics of various security topics in a simplified model, without the baggage of a full programming framework and memory model.

Because of the broad nature of the subject matter, we divide the topics into multiple largely disjoint card sets. Some of these topics are focused on binary data, and in particular on a toy computing architecture; these will share a single set of cards. Another set focuses on a networked application framework, which comprises a second set. A third set focuses on the network infrastructure.

We divide the games into a number of sections, dealing with specific topics. Not all courses will cover all of the sections included here, and doubtless there will be topics not included in these games. The section order here corresponds to the order of topics covered in the University of Maryland course CMSC 414: Computer and Network Security.

Each game should take 5 to 10 minutes in a classroom setting. Where appropriate, we provide variations that might take longer for use in studying. The games are designed for 4 to 6 players.

In addition to the contents of the game set, you might find paper and writing instruments helpful for some of the games.

1 Low-Level Programming Errors

These games cover topics like stack layout, buffer overflows, and some mitigation techniques. We will work in a pseudoassembly environment for a very simple architecture. Specifically, our architecture will have 4-bit bytes, which we will refer to as quartets (in comparison with 8-bit octets).

describe a card layout
1.1 Introducing the Game Set

1.2 Stack Organization

1.3 Writing to a Buffer

1.4 Overflowing a Buffer

1.5 Preparing Shellcode

1.6 Executing Shellcode

1.7 Metamorphic Executable Code

I'm putting this here, because it's not enough for its own section, and more or less fits thematically.

2 Web-Based Attacks

multiple players is more relevant here, since we can split up client, server, attacker, and victim — not every game will have all of these, and this is still less than a full table's worth

the cards will be somewhat generic, so some of these will look very similar

need generic terminator for all injections

need supplied-field

need document/interface framing cards

need server response cards (like search, echo, etc.)

do we need data flow cards? (eg, client -¿ server, attacker -¿ victim, ...)

need attack effects: insertion, extraction, modification; composite with other actions (redirect, etc)

2.1 SQL Injection

2.2 SQLi Prevention

this will just have one or two extra cards for players to use
2.3 Man-in-the-Middle

2.4 Remote File Inclusion

2.5 Stored Cross-Site Scripting

2.6 Reflected Cross-Site Scripting

2.7 Cross-Site Request Forgery

2.8 Defending Against XSS and CSRF

this will just have one or two extra cards for players to use