the cost-effectiveness of an investment can be highly
dependent on others’ investment decisions. Another
recent application of the IDS model is on container
shipping transportation [Gkonis and Psaraftis, 2010].
They use the IDS model to study the effect of invest-
ment decision on container screening of ports have on
their neighboring ports.

In this work, we build on the literature in IDS games.
In particular, we adapt the model to situations in
which the abstract “bad event” results from the de-
liberate action of an attacker. The “internal agents”
(e.g., airlines and computer network users), whom we
also often refer to as “defenders” or “sites,” have the
voluntary choice to individually invest in security to
defend themselves against a direct or indirect offensive
attack, modulo, of course, the cost-effectiveness to do
so. A side benefit of explicitly modeling the attacker,
as we do in our model, is that the probability of an
attack results directly from the equilibrium analysis.
Building IDS games can be hard because it requires a
priori knowledge of the likelihood of an attack. At-
tacks of this kind are considered rare events and thus
notoriously difficult to statistically estimate in general.

Related Work. Johnson et al. [2010] and Fultz
and Grossklags [2009] independently developed non-
cooperative game models similar to ours. Johnson
et al. [2010] extend IDS games by modeling uncer-
tainty about the source of the risk (i.e., the attacker)
using a Bayesian game over risk parameters. Fultz and
Grossklags [2009] propose and study a non-graphical
game-theoretic model for the interactions between at-
tackers and nodes in a network. In their model, each
node in the network can decide on whether to con-
tribute (by investment) to the overall safety of the
network and/or to individual safety. The attackers
can attack any number of nodes, but with each at-
tack there is an increased probability that the attacker
might get caught and suffer penalties or fines. Hence,
while their game has IDS characteristics, it is tech-
nically not within the standard IDS game framework
introduced by Heal and Kunreuther.

Most of the previous related work explore the realm
of information security and are application/network
specific (see Roy et al. [2010] for a survey on game
theory application to network security). Past litera-
ture has largely focused on two-person (an attacker
and a defender) games where the nodes in the net-
work are regarded as a single entity (or a central de-
defender). For example, Lye and Wing [2002] look at
the interactions between an attacker and the (system)
administrator using a two-player stochastic game. Re-
cent work uses a Stackelberg game model in which the
defender (or leader) commits to a mixed strategy to
allocate resources to defend a set of nodes in the net-
work, and the follower (or attacker) optimally allocates
resources to attack a set of “targets” in the network
given the leader’s commitment [Jain et al., 2011, Kiek-
intveld et al., 2009, Korzhyy et al., 2010, 2011a,b].

Other recent work strive to understand the motiva-
tion of the attackers. For example, Liu [2003] focus
on understanding the attacker’s intent, objectives, and
strategies and derive a (two-player) game-theoretical
model based on these, while Cremonini and Nizovtsev
[2006] use cost-benefit analysis (of attackers) to ad-
dress the issue of the optimal amount of security (of
the nodes in the network).

Our Contribution. We adapt the standard non-
cooperative framework of IDS games to settings in
which the source of the risk is the result of a deliber-
ate, strategic decision by an external attacker. In par-
ticular, we design and propose interdependent defense
(IDD) games, a new class of games that, in contrast
to standard IDS games, model the attacker explicitly,
while maintaining a core component of IDS systems:
the potential transferability of the risk resulting from
an attack. We note that the explicit modeling of risk
transfer is an aspect of our model that has not been
a focus of previous game-theoretic attacker-defender
models of security discussed earlier.

We formally define and study IDD games in depth in
Section 3. We present several results that fully char-
acterize their NE. 2 2 We also provide a polynomial-time
algorithm to compute all MSNE for the important
subclass of IDD games in which there is only one at-
tack, the defender nodes are fully transfer-vulnerable
(i.e., investing in security does nothing to reduce their
external/transfer risk) and transfers are one-hop. 3

We note that considering a single attacker is a typical
assumption in security settings (see previous work dis-
cussed earlier). It is also reasonable: We can view
many attackers as a single attacker. Allowing at
most one attack prevents immediate representational
and computational intractability problems because the
number of the attacker’s (pure) strategies grows ex-
ponentially with the number of attacks. Finally, because
the attacker has no fixed target, it is ineffective for
the attacker to consider or go beyond plans of attacks
involving multiple (> 2) transfers: such plans are com-
plex, time consuming and costly.

Our computational results are significant and surpris-
ing because computing all NE in general IDS games is

2Due to space limitation, we omit proofs of our main
technical results and instead refer the reader to the sup-
plementary document for details [Chan et al., 2012].

3We note that the original IDS games were also fully
transfer-vulnerable and assume one-hop transfers.