When Good Ninjas Turn Bad: Preventing Your Students from Becoming the Threat

Thomas Cook, Gregory Conti, and David Raymond, *United Stated Military Academy*

Abstract – Information security programs teach dangerous skills to their students. Despite our best efforts as instructors and mentors, some students will use these skills in inappropriate, and sometimes illegal, ways. As a result, students jeopardize their careers, hurt others, and put their institution's entire information security program at risk. In this article, we present results from interviews with information security instructors from academic and government information security education programs. This article includes analysis of real-world incidents where students crossed the line in using their skills, and suggests best practices for deterring student misbehavior as well as techniques for mitigating damage and maximizing learning when an incident does occur.

Index terms – information security education, ethics, insider threat, security violation, hacking, incident handling

I. INTRODUCTION

You are sitting in your office and in walks a student carrying a Mr. Potato Head toy dangling a USB cable. The student is very enthusiastic about his project and plugs Mr. Potato Head into a laptop to demonstrate. "What does it do?" you ask. "Oh, it sniffs the college's wireless network and performs a Man in the Middle Attack to view the traffic" (Fig. 1). Choking on your lunch, you quickly ask the student to stop. This is a true story, and many information security instructors have faced similar situations, although perhaps not involving Mr. Potato Head as the perpetrator, and wondered what to do next

In information security education, we teach skills to our students that are potentially dangerous. This is by necessity. Cyber security experts are in high demand, but critically short supply [1]. Some of the most important lessons in information security come from studying and applying the techniques, tactics, and methodologies of attackers; to do otherwise would leave large gaps in the knowledge base of graduates [2,3]. However, including dangerous content in our programs incurs the risk that students my experiment with these techniques in inappropriate, and sometimes illegal, ways.

This article studies the problem of misuse of the information security skills we teach our students, provides detail of real-world incidents involving students, proposes best practices for handling incidents when they do occur, and importantly, suggests techniques for preventing incidents from occurring in the first place.

As part of our research, we conducted interviews with information security instructors from eight diverse institutions, at the undergraduate and graduate level as well as from government. The incidents we present actually happened, but we have deliberately anonymized specific individuals and institutions.

Misuse of information security expertise is serious business and could result in criminal prosecution, bad publicity, personal injury, cyberbullying, suicide, and termination of educational programs, among numerous other negative outcomes. To create vibrant programs we must inspire students to dive deeply into their personal learning, and the edgy nature of hacking is an incredibly powerful motivator. The problem of skill misuse is not specific to information security. Other communities, including those of martial artists, soldiers, locksmiths, biologists, psychologists, chemists, electrical engineers, nuclear engineers, and even accountants and interface designers, all possess skills that can be dangerous if misused [4].

Student misbehavior is a dirty little secret in the information security education community and rarely discussed publicly. We found that most instructors have wrestled with student misbehavior and sought to direct student exploration in positive directions, set appropriate limits, and create a healthy culture, with varying degrees of success. The instructors' goal is to foster long-term responsible behavior and internalization of ethical practices in students, all while maintaining an inspirational learning environment and setting a positive

Thomas Cook is an senior research scientist and assistant professor in West Point's Department of Electrical Engineering and Computer Science (email: thomas.cook@usma.edu).
Gregory Conti is an associate professor in West Point's Department of Electrical Engineering and Computer Science (email: gregory.conti@usma.edu).
David Raymond is an assistant professor in West Point's Department of Electrical Engineering and Computer Science (email: david.raymond@usma.edu).

ISBN 1-933510-95-1/$15.00

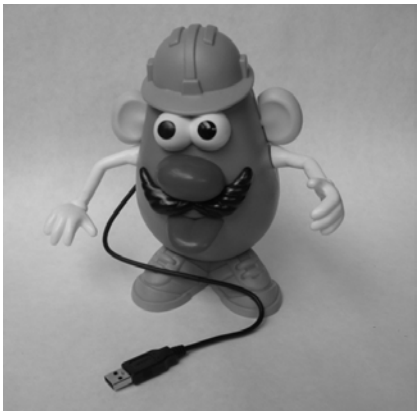

Fig. 1. One unauthorized student project involved a Mr. Potato Head toy modified to sniff campus network traffic.

course for the students' future. Students, of course, may have different goals.

II. Instructor Interview Methodology

Our interviews typically lasted thirty minutes and included discussion on type and frequency of incidents, incident handling, and deterrence. When possible, we conducted interviews face to face, but when necessary, via telephone. We used the following questions to guide the discussions.

- How long have you taught information security education courses?
- Does your program have a hands-on component and does it teach tools and techniques that could be used for offensive purposes?
- How do you seek to prevent incidents of students misusing their information security skills?
- Did your program have any incidents? If so, please describe.
- In each case, who first reported the incident?
- How did you respond to each incident?
- What was the ultimate resolution of each incident?
- After each incident, did you change your curriculum and practices and if so, how?
- May we publish these incidents in an anonymized form?

This non-scientific survey is not meant to provide statistically significant results showing numbers or types of potentially malicious student behavior. It was designed to augment our own experiences with those of a range of educators in circumstances similar to ours in order to provide a broader range of incidents and tested coping mechanisms to examine in this discussion. Future work may involve a scientific survey designed to measure rates of malicious incidents among cyber security students and the effectiveness of the mitigation measures examined here.

III. Reported Incidents

During the course of our interviews, instructors described 24 incidents. We've highlighted representative examples below. Depending on severity, instructors informally addressed some incidents, while others went through formal reporting and investigative procedures. Fig. 2 shows the technical difficulty versus the degree of malicious intent for several incidents based on the facts of each case. As you examine the figure, note that most incidents required relatively low technical expertise, but spanned a broad range of malicious intent.

A. Full Incidents

Phishing Attack Back - One interesting incident occurred when a college administrator sent out phishing emails as part of a security awareness campaign. The student body was unaware that these emails were only a test. In response to the test, several students collaborated and developed scripts to deliberately pollute the "phisher's" database. The students were successful. On the surface, this sort of response may seem innocuous and perhaps even justified. However, a vigilante-style reverse attack can have unintended consequences when executed without proper authority and without fully considering the potential outcomes. In this case, the value of the administrator's test was reduced because of the polluted data.

Spoofed Email - Several instructors reported the use of spoofed emails, but the intent behind these emails varied significantly. At one end of the spectrum, a student sent what we characterized as a fraternity prank and at the other end, a student sent an email containing fraudulent medical test results diagnosing a serious medical condition. The prank email resulted in verbal counseling. The medical test email resulted in a formal investigation.

Cross Site Scripting - Shortly after learning web application security penetration testing techniques, a student used a cross site scripting attack on a collegiate course evaluation system which caused an alert box to appear every time the page was viewed. The institutional administrators of the system chose to recruit the student to perform an authorized penetration test of the system rather than pursue administrative or legal action.

Keystroke Logger - As part of a legitimate computer security competition, a student purchased a keystroke logger and inadvertently placed it on an off-limits, official-use terminal rather than an authorized classroom

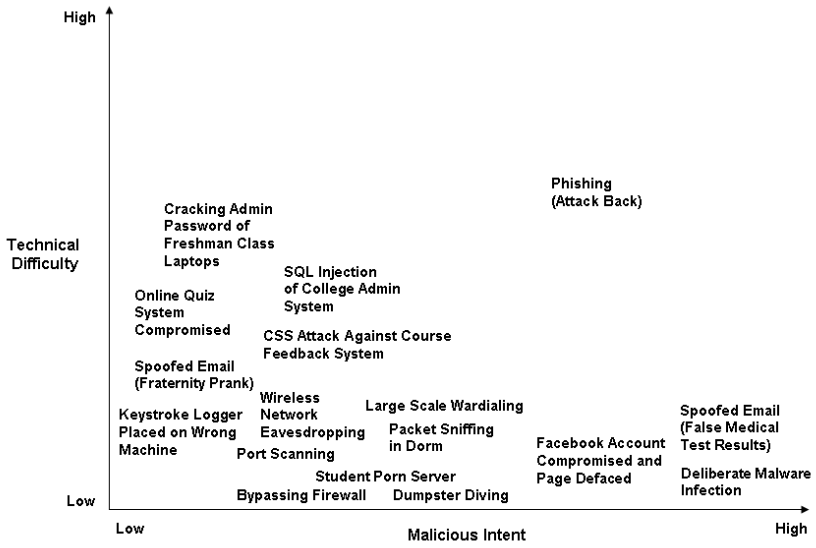

Fig. 2. Plot of incidents reported during instructor interviews. Note that the majority of the incidents required limited technical expertise, but range from little malicious intent to significant malicious intent.

terminal. The keystroke logger captured logon credentials of faculty members and students not associated with the course. The student was verbally reprimanded and affected faculty and students were advised to change their passwords.

Password Cracking - In this case, an institution provided laptops to all incoming freshman. To aid administration, each laptop was configured with a single, centralized administrative password. A student noticed the unfamiliar account on his laptop and cracked the password hash found on his hard drive, effectively giving himself administrative privileges on every freshman laptop.

SQL Injection - A student performed SQL injection on a web-based administrative system. He was successful in approving an (non-malicious) administrative action normally restricted to college officials. He immediately reported the vulnerability to appropriate administrators.

Online Grading System Compromised - An instructor used an online quiz system offered by his course textbook's publisher. A talented student immediately subverted the system and gave himself a perfect score on the quiz. The student then informed his instructor of the vulnerability.

Facebook Account Credentials Stolen and Page Defaced - Shortly after being taught the use of the Firesheep, the Firefox browser extension that automates collection of social networking site credentials, a student's Facebook account was compromised and webpage defaced.

There isn't space in this article to describe all incidents in full detail, but other examples include a student who deliberately gave a malware infected disk to an ex-girlfriend, dumpster diving for sensitive documents, students caught bypassing firewall safeguards, and packet sniffing of dormitory networks, and port scanning of university servers.

B. Near Incidents

The following are examples of situations that may have led to full incidents, but were prevented due to instructor or student intervention.

Large-scale Wardialing - If you are going to cross the line, think big. Students approached their instructor with a desire to perform large-scale wardialing. The students had already built and tested their system and asked for instructor assistance in purchasing a calling card to proceed with the project. The instructor dissuaded the students and clearly explained the potential negative consequences of the students' proposal.

Threats to Hack Facebook Account - A student in a dispute with her boyfriend threatened to deface his Facebook page, and possessed the skills to do it. Peers from her computer security class convinced her that she should not proceed.

C. A Curious Lack of Incidents

One surprise we encountered was that two schools reported no incidents at all, despite having programs that existed for many years. Faculty members at these schools

speculated that the reasons might include their program's selectivity, their no-tolerance policies for malicious hacking, or their honor codes. However, even though these schools had not encountered an incident, instructors were still concerned that a serious incident could still occur, and actively worked to prevent such an event.

As you consider the above examples, it is important to note that these incidents were only those that came to the attention of the instructors we interviewed. There are likely other incidents that were not discovered, as well as incidents that occurred after students departed their programs, but these additional incidents are beyond the scope of this article.

IV. Preventing an Incident

Ultimately, it is up to the students to make responsible choices when deciding when and where to use skills learned in the classroom, but it is up to their instructors and institution to help provide the proper tools, environment, and culture to develop maturity and facilitate correct choices. We derived the practices we suggest below from our interviews, and they represent the wisdom of many hard learned lessons.

A. Provide Appropriate Context and Ethical Tone

A program that deters inappropriate behavior must provide a climate and culture where instructors, staff, and students all work together to prevent misconduct. Most instructors regularly briefed students on the ethical use of tools and techniques at the start and end of each course, as well as immediately before teaching particularly dangerous material, such as the Metasploit penetration testing framework, wireless security, and web application security. Instructors also deliberately and frequently provided context for students as to why they were learning dangerous material. They encouraged responsibility, teamwork, and mature decision-making. However, all warnings are not created equal. One instructor reported that, over time, he sensed students were becoming desensitized to his warnings, so he invited another well-respected instructor to visit his class and reinforce his warnings. The timing of warnings may also be important. Locasto and Sinclair placed warnings at the end of their two-week seminar and laboratory course in order to foster informed debate that would leave a lasting impression, rather than at the beginning when students were less well informed [5].

B. Explain the Downsides of Inappropriate Behavior

Students must possess a clear understanding of the serious and long-term implications of their actions. Beyond merely failing an assignment or even failing a course, students have much to lose. Students risk expulsion, criminal prosecution, and could threaten the existence of their institution's information security education program. Future employment is another concern. For example, students wishing to pursue positions requiring a security clearance might be in for a rude awakening. Several instructors reported that former students with relatively minor hacking indiscretions were unable to acquire a security clearance or pass a required polygraph exam, eliminating significant job opportunities.

Instructors tried differing approaches to communicate these downsides to their students. One instructor suggested sharing previous student misbehavior cases or having a different student each week lead a discussion about a recent malicious hacking incident in the news. After having informed her students of the standards of proper behavior, another instructor tells her students, with a serious smile, that she would be happy to testify against them in a court of law, if necessary. The balance here is to instill in the students a healthy respect for the downsides of any puerile or malicious behavior, but not go as far as damping healthy enthusiasm. However, deterrence is only part of the solution and must be buttressed with other techniques. For one viewpoint, see the work of Hu et al. for analysis of relevant criminological theories and their relationship to deterring security policy abuse [6].

C. Policies Should be Unambiguous, Enforced, and Legally Defensible

Students should also possess a clear understanding of the boundary between appropriate and inappropriate behavior, including knowledge of local, federal, and international law. One instructor we interviewed summarized this point as "drawing a line and showing the students where it is." Take care however, the location of the line is subjective and depends on who you ask. A related lesson includes understanding the institution's policies and online use agreement. Additional supporting material should be included in course syllabus and grading procedures. Some institutions reinforced their warnings by having students review and sign a contract, pledge, or non-disclosure agreement that stated expected behaviors. Some instructors prepared these documents without legal review, although others suggested that a legal review would be prudent, particularly if the agreement would be used to prove due diligence on part of the institution to avoid culpability and liability. As policy and law may change without warning it is important for instructors to continually track these changes and ensure updates are understood by their peers and students. Similarly, instructors should regularly evaluate their own policies and classroom climate, making changes when necessary. One school reported only a single hacking event over more than five years, and

attributed part of their success to their meting out quick and firm justice in the one incident that did occur.

D. Encourage Students to Pause and Reflect Before Acting

Depending on level of maturity, many incidents occur due to a single impulsive act. Simply pausing and reflecting before acting leaves opportunity for students to make better decisions and seek out mature guidance. Self-restraint and good judgment are difficult topics to teach, particularly with younger students, but can be developed over time by a consistent message communicated effectively through instructors, peers, and the program's culture, both inside and outside the classroom.

E. Avoid Stupid Mistakes

It is important to avoid simple mistakes when attempting to prevent mishaps. Tools and techniques should be introduced at an appropriate point in a student's academic career so they understand how to properly employ and control their tools. For example, a lack of understanding could result in unintentionally port scanning an entire college network, instead of checking the security of a single authorized target server. Several institutions saved offensive techniques until very late in their programs to give time for students to mature and better understand the power of the tools they taught. Students should know the right way to use their knowledge, always acquire permission, and understand that, even if authorized, ethical hacking activities could cause unforeseen disruption.

F. Provide an Ethics Lesson Early in Your Program

Several instructors suggested adding a dedicated lesson on ethics early in their program. For example, one institution included ethical aspects annually as part of its mandatory seminar program, another chose to weave ethics learning objectives throughout its curriculum. One suggested approach was to use misuse scenarios to drive discussion and help students understand appropriate behavior, as well as analyze the implications of improper behavior. If your institution has an honor code, discussion could include the relationship between the honor code and malicious hacking.

G. Tell the Positive Story of Your Program Before Something Bad Happens

Student misbehavior should be an aberration and not a common occurrence. Use the many positive aspects of your program to build a trusted relationship with faculty, staff, and management *before* a negative instance occurs. By doing so, you will set in their minds a longstanding, positive view of what your program seeks to accomplish and provide breathing room if an incident occurs. Those we surveyed validated this belief. For example, an academic institution's Information Technology support division may be the first to notice something amiss. It is far better if the IT division reached out to the program or instructor first, rather than immediately contacting security officials.

H. Make Students Part of the Process

Students can be the enemy or allies. It is in everyone's best interest to make students part of the solution. Several institutions have partnered with students outside the classroom to tap their expertise, enthusiasm, and available time to create educational opportunities that also serve organizational best interests. For example, Dartmouth College created their Cyber Security Initiative (CSI), which allows vetted students to perform security assessments. CSI students have helped secure Dartmouth's wireless network, evaluated authentication systems, and performed security reviews of proposed technologies [7]. Another institution selected students with an advanced skill level, ability to pass a qualification exam, and appropriate level of maturity to serve as system administrators within their advanced computing center. The students were given the responsibility of setting up and configuring information assurance and information technology classrooms and performing system administration duties on a number of virtual systems. A third institution's program provided increased student responsibility over time and elevated students through leadership positions as they progressed through the program.

I. Provide Safe Environments for Exploration and Experimentation

A very powerful technique is to provide students with environments that allow healthy and safe exploration of dangerous techniques. This support could be via specialized classrooms (ideally accessible 24/7) that are on isolated networks or by providing properly configured networks of virtual machines on stand-alone hardware. Instructors can encourage students to participate in cyber defense, capture the flag, and similar competitions. The key here is to help fill the need of students to explore and experiment without requiring them to learn on production systems or the open Internet.

J. Provide Leadership, Mentorship and Role Models

Proper leadership and mentorship, as well as exposure to positive role models, such as guest speakers, are effective means of preventing incidents. If confronted with an ethical dilemma or challenging interpersonal problem, students will often seek out a trusted peer, instructor, or mentor. The operant word here is *trust.* These

relationships aren't built overnight; the development of trust requires time and interaction, particularly outside of the classroom. Instructors must know their students well, particularly new people, supervise actively, and deliberately seek out at-risk students. Sometimes instructors would assign senior students to work one-on-one with at-risk students. Face-to-face interaction always outweighs attempts at leadership via email. These techniques prevented several incidents at ideation rather than action. A healthy leadership environment encourages students to take ownership of their program and to regulate their collective behavior, performing interventions when necessary in order to not let their leaders, peers, and program down. During one incident, a Department Head brought in her seniors and chastised them for not preventing an incident they knew was in progress stating, "You should have known better and intervened." Some instructors encouraged students to perform outreach work, such as teaching cyber security at local elementary and middle schools, as a means of developing student maturity and helping to build a positive reputation for their programs.

Leaders, mentors and role models must always set an example and avoid subtle approval of inappropriate behavior. One of the most damaging challenges to proper student behavior is the tacit approval of inappropriate behavior by a respected instructor. An instructor's casual joke about their own hacking activities could easily be interpreted as a wink and a nod to students that they should do the same.

K. Don't Crush the Enthusiasm of Your Students

Perhaps the most important lesson of all is to not crush the enthusiasm of your students in an overzealous attempt to prevent misbehavior. Students shouldn't be so concerned about living in a zero-tolerance, police state that they forget to learn.

The above practices won't eliminate every possibility of student misbehavior, but will help greatly reduce the occurrence of incidents. In addition, for those interested in curriculum issues surrounding ethical hacking, we recommend the work of Logan and Clarkson [8].

V. COPING WITH AN INCIDENT

As an instructor, coping with an incident is a stressful experience, but one that results in significant learning for both the instructor and the student. The following is a list of best practices derived from our interviews of instructors who had firsthand experience in handling student incidents.

Know Your Legal Limits: To handle an incident you must know which actions are legally in bounds and what are out of bounds. In this section, we provide some general guidelines on how to handle an incident of student misconduct, but please consult your organization's legal counsel to confirm your own legal boundaries. We recommend reaching out to your legal counsel before, during, and after an incident occurs to make sure you stay on track.

Find out What Happened: Our instructors initially found out about incidents from students, other instructors, or staff. Despite your initial, and likely emotional, response, avoid overreacting and jumping to conclusions. Guilt is hard to determine. Most instructors would seek out additional information to perform an initial assessment of the situation. One instructor emphasized the importance of not jumping to conclusions, as "there are always two sides to any story."

Know When to go Formal: Some incidents clearly demand immediate initiation of formal legal and law enforcement procedures; some incidents do not. The trick is the large gray area in between clear-cut cases. Every case is different, but it is often better to handle minor infractions informally, even if sterner measures are available. Exceptional learning occurs when you have a student's attention, and being caught in misconduct clearly provides you the student's attention. Several instructors reported waiting 24 hours or longer to carefully consider alternatives in order to choose the best possible course of action, one that minimizes harm and maximizes learning. During this time, instructors would discuss incidents informally with trusted colleagues and sometimes informed management or sought legal advice.

Communicate Effectively: When an incident does occur it is important to communicate effectively and appropriately. Many minor incidents are best handled at the lowest level possible in an informal fashion. However, in the case of severe incidents, make sure you keep your management well informed and reach out for legal assistance as necessary. Bad news doesn't get better with age. If you believe the incident will receive media attention, work with your institution's public affairs office to frame the key points and message you wish to present in advance of an interview. Note that the attention span of the media is typically short; reporters will move on very quickly to the next big story that will inevitably occur. The attention of your management will not move on so quickly. However, if you've made a point of highlighting successes over the past years, are following institutional policy and procedures, and make appropriate changes to prevent future incidents, you should be well on your way to putting the incident behind you. How much information you share with students varies, but incidents are frequently teachable moments that can be used to reinforce the positive ethical culture and tone you've been trying to create.

Remediation: Formal proceedings typically include specific, and often severe, punishments and rehabilitation measures. However, the instructor may have an opportunity to provide recommendations to key decision makers. If so, carefully consider the many facets of each case, such as age, maturity, severity of the incident, malicious intent, previous student performance, and future potential before making a recommendation. Remediation decision making should also include thought on how to best deter future incidents. In cases that were handled informally, many instructors used group sit-downs as well as private discussions with responsible students and affected parties (but always with another faculty member present), reminding students of the implications of their actions, that everyone loses when one misbehaves. Again, face-to-face interactions always trump bulk emails. Fight the urge to write-off offending students completely. If a given student remains in your program there is a requirement to remain engaged in their development. Oftentimes, students mature significantly and change their ways. Regardless of what you decide, make no mistake; other students are watching your actions carefully. Make every effort to be firm, fair, and consistent.

VI. Conclusions

Incidents of student misbehavior do occur, are always an unsettling experience for the instructor, and are rarely as cut and dried as they might appear at first glance. Despite these challenges, dangerous knowledge is a critical part of an information security program. Some people object to ethical hacking and we are all concerned that the skills that we teach will be misused, but incidents can be deterred by a healthy environment, clear understanding of the downsides of inappropriate behavior, well-understood policies, positive leadership, and co-opting students to become part of the solution. However, despite these efforts, incidents will sometimes still occur. Incidents that do occur must be acted on swiftly and fairly. Instructors must keep their management, peers, and students appropriately informed, and use incidents to help students learn and help mature their policies, procedures, and programs. The best practice is a thoughtful program of prevention, reinforced over time. Exceptional learning often occurs near the line, we must be certain our students do not cross it.

VII. Acknowledgements

We would like to thank the instructors who candidly shared their challenges, techniques, and insights. The views in this article are the authors' and don't reflect the official policy or position of the US Military Academy, the Department of the Army, the Department of Defense, or the US Government.

VIII. References

[1] M. Schwartz, "Cybersecurity Expert Shortage Puts U.S. At Risk," 21 July 2010. [Online]. Available: http://www.informationweek.com/. [Accessed 20 Jan. 2012].

[2] G. Ledin, "The Growing Harm of Not Teaching Malware," *Communications of the ACM,* vol. 54, no. 2, pp. 32-34, Feb. 2011.

[3] S. Brutus, A. Shubina and M. Locasto, "Teaching Principles of the Hacker Curriculum to Undergraduates," in *Special Interest Group on Computer Science Education Symposium (SIGCSE),* Milwaukee, WI, March 2010.

[4] G. Conti and E. Sobiesk, "Malicious Interface Design: Exploiting the User," in *International World Wide Web Conference (WWW),* Raleigh, NC, April 2010.

[5] M. Locasto and S. Sinclair, "An Experience Report on Undergraduate Cyber-Security Education and Outreach," in *Annual Conference on Education in Information Security (ACEIS),* Feb. 2009.

[6] Q. Hu, Z. Xu, T. Diney and H. Link, "Does Deterrence Work in Reducing Information Security Policy Abuses," *Communications of the ACM,* vol. 54, no. 6, pp. 54-60, June 2011.

[7] A. Goldstein and D. Bucciero, "The Dartmouth Cyber Security Initiative," *IEEE Security and Privacy,* pp. 72-74, November/Dec. 2009.

[8] P. Logan and A. Clarkson, "Teaching Students to Hack: Curriculum Issues in Information Security," in *Special Interest Group on Computer Science Education Symposium (SIGCSE),* St. Louis, MO, Feb. 2005.