Gracies Dinnertime Theatre

Volume 32, Issue 1, Bughouse
www.hellskitchen.org/gdt

Member of
Hell's Kitchen
www.hellskitchen.org

Download this issue at http://www.hellskitchen.org/gdt/pdf/Volume32/01.BugHouse.pdf

Welcome

by The GDT Staff

To returning students, welcome back! We know you're excited to start another academic year at everybody's favorite college!

To freshmen, we at Gracies Dinnertime Theatre would like to welcome you to our beloved Brick City. Learn your way around, remember to actually attend an occasional class, and prepare to enjoy the most expensive four, five, or n years of your life.

I'm going to try something different for this year's intro article. I'm going to keep it short, and oddly lacking in negative (or whiny, or bitchy) statements about RIT.

No, I haven't turned a new leaf. No, I haven't realized how much I love my alma mater and put the insults behind me. I just know that you will soon be hit on all sides by the truths about RIT... and I don't mean in FYE.

So before you continue reading this wonderful magazine you hold before you, I'd like to leave you with some advice, which you can go ahead and disregard as I know you will. Get out of your dorm room every once in a while. Keep your dorm door open and actually become friends with your floormates. Unless you send your RIT bills to Daddy and Mommy, learn to enjoy the taste of Ramen and Campbell's soup, because eventually, RIT will decide that you're old enough to decide how you want to spend your money, and will no longer force you to overpay for a mealplan (but you're big enough boys and girls to decide to spend that $20k!) Go to your math classes. Learn to buy your textbooks (at least the necessary ones) online to save the awkward looks you will receive in class from sitting funny after visiting an unnamed on-campus bookstore. And of course, read GDT, send us email (gdt@hellskitchen.org), write an article and submit it to GDT, draw a pretty (or not-so-pretty) picture and submit it to GDT, and come to folding[1]!

[1] Help us fold this magazine, every Wednesday at 8PM in Crossroads!

PARRINELLO

Talk English good.

Insecurity @ RIT

Editor's Note: The information contained in this article is for informational purposes only. Gracies Dinnertime Theatre does not condone or advocate doing any of the activities mentioned in this article. In fact, personally, we think that you'd have to be fairly stupid to do any of this, considering how RIT would surely be pretty unhappy with you. We do though, feel that if you, as an RIT student, are forced to carry your RIT ID Card with you at times, that it is your right to know exactly what data is stored in and on that piece of plastic in your wallet. You should know the implications and security risks of having and possibly losing this card. Remember, use good judgement. Don't do any of the stuff in this article, or you're on your own. Don't be stupid.

Alright alright, let's get into breaking stuff. RIT gives students/faculty/staff an ID card. There are a few technologies that we care about on this ID: the bar code on the front, the 2 magnetic stripes on the back, and the picture on the front[1].

Stuff you need to understand, your Social Security Number and student ID are referred to as the same thing. They™ have been in talks to change your student ID to something besides your Social. Rumors say this will happen around Christmas. Regardless, all this information is still relevant. The only thing that will change is hard core identity theft will be more difficult, which is a good thing to fix. Each card has a version number. Under the barcode on your card, there are 5 numbers: the last 4 digits of your Social appended with your version number. If this is your first ID, the version should be 0. If you lose your ID and you get it replaced, the version number will be incremented to prevent the old (unmodified) one from working. If you return your ID for a new one, the version will not be incremented.

Barcode

The barcode has been discussed before in GDT[2], so it's not like I'm breaking any ground here[3]. The format is called "code 3 of 9," or "code 39"[4]. This means there are 9 elements to each character, 4 spaces (white bars) and 5 lines (black bars). Three of these bars are wide, the rest are narrow. Between characters there is a narrow white bar. There is a start and end character referred to as the asterisk. This is why you will notice your friend's ID starts and ends the same as yours. Code 3 of 9 can contain a checksum character but the RIT ID doesn't contain this. Encoded on this barcode is your Social Security Number and the version number of your card. I know of the barcode being used at the library to check out books, and as a time keeping system at certain campus jobs. Anyway, if you are good enough, you could remember the 10 characters (numbers 0-9) and theoretically be able to read anyone's Social and version with your eyes, right off their card. This would allow you to fully clone their card. The barcode above is 3 of 9 encoding "*1234567890*".

Barcode Exploits

A malicious person could generate a barcode from the information it contains (if they knew someone's Social and version), or by taking a picture of the barcode and decoding the Social and version, which could also be done with a neutered CueCat. After acquiring a new barcode, an attacker could print it out on a sticker and place it over theirs on their card. They would have to put some thought into this, so that people handling the ID wouldn't notice the sticker. It could possibly be printed on a glossy sticker and maybe can be laminated on the front somehow so there wouldn't be any rough edges. This doesn't even matter if a malicious person was cloning it for checking in/out to an automated scanner and could even be on a piece of paper. Of course, they can checkout books as someone else. This isn't exactly amazing but an exploit nonetheless.

Magstripe

Here's the good stuff. Flip your card over and notice there are two magstripes. The thinner one is darker than the thicker one. This is because the thinner one (library stripe) is HiCo, whereas the thicker stripe is LoCo. HiCo (high coercivity) refers to the density of the magnetic particles on the stripe, measured in Oersted (Oe). HiCo can have ten times the Oe of LoCo. Over your head? Simply, HiCo requires a much stronger magnetic field to be erased/rewritten than LoCo. This is why stores that use anti-theft devices that must be rubbed over rare earth magnets have a sign saying "don't place credit cards on pad." One important note is that any reader can read both cards. HiCo and LoCo "put out" the same strength magnetic field, one is just harder to change than the other.

[1] Comes into play later when we try to get a new ID for free

[2] See GDT, Volume 13, Issue 2, "Dass a NO!" http://hellskitchen.org/gdt/pdf/Volume14/02.DassANo.pdf -TS

[3] If you haven't read it, it's new to you

[4] Code 3 of 9 with a barcode generator: http://www.spatula.net/proc/b arcode/code39.src

Magnetic cards can contain up to 3 tracks per stripe[5] (in numerical order from top to bottom when the stripe is at the top of the card). The thicker LoCo stripe contains tracks 1 and 2. There is nothing on track 1 of the LoCo stripe. Track 2 contains your Social Security, version number, and facility code. Take out all the cards you have in your wallet and overlap them. You can see the difference if one has 3 tracks compared to the RIT LoCo stripe.

Example track 2: a card contains ";123456789=1047?" where ";" is the start sentinel, "?" is the end sentinel, and, I would guess, "=" is a field separator. In this example "123456789" would be the Social. The "1" after the equals would be the version number. And I am told by what I believe is a reliable source that "047" is the facility code, meaning all RIT cards would contain this to work at RIT. Initially I thought it was your class (student/faculty/staff) but I have scanned a staff member's card and it was the same. However, I have not tested special cards such as the ones to operate registers, or any professors.

Now for the thin HiCo stripe. Look at the stripe and rotate your card 180 degrees so the thin stripe is at the top of the card. This is a single track, track 2 when swiping it upside down. To my knowledge, this is only used inside the library for printing/copying, because 30k just doesn't cover paper and ink anymore. One very important thing to notice is everywhere you use this stripe your card is sucked into the machine. This is because the actual monetary amount is written to the card, this is also why it's HiCo (if it's erased it's gone). You should also notice when you try to eject your card it moves your card slightly out then back in before it ejects it. This is because it is re-writing the card. You can buy a card from the library for 1 dollar with a single HiCo track 2 stripe if you don't want it stored on your ID.

Magstripe Exploits

An easy way an attacker could clone a card is either reading the barcode (discussed above), or finding a lost card and incrementing the version number which will take place once the person reports it. An easy way to test if they have reported it yet is to write a card with the new version and test the card in a vending machine. That way, the attacker doesn't have to deal with people and doesn't have to come up with an excuse if it doesn't work.

Clone someone's LoCo track 2 and that will allow a malicious person to gain access to all areas the card owner has access to, and use their debit/tiger bucks/meals (your classmates do have laundry to do right?). "This kid I know" was on coop and wanted to use the gym. Well, RIT makes you pay if you are not a full time student. So "This kid I know" re-wrote his second ID's magstripe to contain his friend's info who was a full time student. Since the gym doesn't track people currently inside the gym (you don't scan out) this worked great. Also if they did scan people out you could always use the excuse that you used another exit last time. If you go with the friend whose card you cloned and you get crap, you could always say you went in the gym, realized they dropped/left their keys outside the scan area and went back for them, hence having to scan in twice in a short time. Come on, it's not hard to social engineer these idiots.

Now the safest exploit and most useful to some people will be the cloning of the HiCo library stripe. Since it doesn't look up your Social in a database to see how much money you have, by cloning a card one would get the exact amount of money from that card. They could buy an extra card for 1 dollar (or read on to get a free one) and add $2 to the card, then continue to clone that $2 card to their real ID when they need to print/copy. The major obstacle they throw in is the track contains non-standard data. So there is no start/end sentinel. Because magstripes are not exact, and this is storing a monetary value, I assume that there is a checksum so being off by a bit or two might be ok. I have not figured out the encoding to make a $100 card or something, although this would save card cloners the initial investment of $3 or so for the original/source card, unless they are cloning a friend's card. For example, this would get one some money (hex).

```
7FFB8B00CE13BFFFFFFFFFA
```

When ejecting the card, the library readers/writers stick the card out just a little bit then suck it back in. Although I have not tried this a dedicated attacker might be able to rip their card out of the library writer when it first sticks its head out. If the magnetic stripe is at the bottom of the card, the track is read/written from left to right. If they were able to pull the card out using pliers or something before it sucks it back in, the writer might not have a chance to re-write the card with the new/smaller monetary amount. They would probably use one of those dollar cards you buy from the info desk, so if it breaks in half or jams the machine they could walk away. The most vulnerable reader/writer location I know if is the copier on the first floor past the info desk on the right. There's

[5] Some tech specs on magcards: http://www.cyberd.co.uk/support/technotes/isocards.htm

a little cut-in space where the view is blocked from most people, specifically the back copier against the wall.

Getting A Free ID

If your ID stops working in RIT's readers you can get a free ID if you return your undamaged card, this will not increment the version number. But what if you want a second card with your picture to clone info to, or maybe you broke your card? Well "this kid I know" was able to get a free ID with a little social engineering. His original goal was to get a card with his picture and a different name, but first needed to know what information they verified when giving cards. If you don't have practice at this, you must evaluate your audience, and use little social engineering tricks like requesting something that they are allowed to give you before asking for the sensitive information/request. Go ask a psych major why this works - I couldn't tell you. So here's how it went for "this kid I know" known as "tkik", the clerk will be known as "gina".

Tkik: Hi, I lost my wallet. How can I get a new ID? [acting really sad]
Gina: So you don't have anything with your name on it?
Tkik: No
Gina: Do you have any money?
Tkik: My parents sent a check but it won't be here for a few days, but without my card I can't eat on campus.
Gina: Ok I want to help you, hold on. [I'm golden!] What's your Social?
Tkik: [answer]
Gina: And your name?
Tkik: [answer] [I tried to get in a better position to view the monitor but she moved it away]
Gina: And your birthday?
Tkik: [answer]
Gina: And your home address?
Tkik: [answer]
Gina: [to other clerk] Verify his picture on the computer

That last line is critical, and I was impressed that they at least took security serious here. They store your last picture in the computer, so when they need to re-issue a card to someone without knowing who they are, they can make sure they aren't giving someone's info to an attacker by checking the picture. I'm so old, I can't remember specifically how I got my first card but maybe there's a way to mess with them if they don't have a stored picture. Come up with your own stories. I'm sure there are many ways to get a free ID. The above method isn't going to work when 25 people a day try it.

How To Fix This Crap

Now that I'm probably facing expulsion and a pissed off RIT, let me tell you and them how they could fix this. The major technology they still have control over is the cards (it's hard to find a 2 track LoCo and 1 track HiCo on the same card), and the printing process. There is a thin film that is actually printed onto. Now I'm sure it wouldn't be too hard to print these cards if you had the right printer, but I'm no photo/printing major[6]. So the one thing they can verify against is those 5 numbers under the barcode. If I can't print a card with my picture, then I need to re-write the magstripe on my legit card. Well, when this happens they could catch the fake by checking the Social on the magstripe against the 5 numbers printed on the card. Good stores do this with credit cards, they scan the card then have to type in the last 4 digits of the card. For this to be a system without more exploits they should use a more complex printer (black light ink/holograms?), and stamp the numbers in the card, credit card style.

Also scrap the barcode all together, only a few systems still use it and upgrading them wouldn't hurt. This would prevent people using a cell phone camera from capturing your info. As for vending machines, it's tricky. Unless you sucked in the card, scanned the surface and recorded the time etc you could still use a cloned card. I have not seen a good solution to this problem. Maybe implement a system somewhat like a credit limit, if you go over it you have to show up in person somewhere to verify your identity and reset the limit. They could also implement biometrics. This would be much harder to use cloned cards and solve many problems. The problem with biometrics is the inability to reset the private data. If you lose your credit card they can cancel the account, if someone takes the data from your fingerprint you can never change that.

Scrap the version number. This is one level away from retarded. A lost card should be useless once reported, and provide no usable info besides name (printed in plain text) and picture. When switching to student numbers, use a large number, and when the card is lost re-issue a new and random student number[7]. Student numbers must also not be sequential. If this is not an option use a version

[6] Or am I?

[7] Or another possibility is to have the ID number on the card be randomly generated and have no association to the Student ID, which is probably used in many systems outside of ID Cards and thus would be difficult to reassign. -Ed

number of at least 6 digits and when it is lost use a new random version number. This way the finder of a card can't know what the new version number will be. If they make it 3 digits or less, I'll kill something, 99 possibilities are way to few to be effective. "This kid I know" could write 20 cards at a time and go to the vending machine until one worked if he was determined.

I'm not sure how the cat5 line connection works from vending machines/registers to the central database[8], but make sure that unplugging these at anytime wouldn't yield free items. Generally they only accept money once unplugged. Also it seems like taping this line would be relatively easy, it should use strong encryption over the lines to the database server. The cat5 wiring from the power supply looking box in the laundry buildings should also be more secure and use encryption, so even if tapped it will provide little to no information.

Physical security also needs to be taken regarding the special cards and readers. It has been reported that attackers have implanted an extra reader in some ATM, capturing every card that is inserted to the machine. This might also be possible to do to one of the hundreds of door access readers/vending machines/registers on campus. Employees should be trained to verify that there is only one read head inside the reader and that the casing hasn't been disassembled to tap into the read head. It is very easy to record data by attaching a small MP3 player with recording capability to the read head[9]. I have personally seen a special register access card left on the register when no employee was within 25 feet of the register. Access to these cards must be controlled, and the data on the cards should be changed often.

"Remember… if an officer asks to search you, he doesn't have the right to" - PSA from "don't talk to cops"

[8] I hear it's serial, so splice into it and check it out

[9] For more information on this, see 2600 Magazine, Volume 22, Number 1, Spring '05, "Magnetic Stripe Reading" by Redbird -Ed

An August Proposition Or A Final Solution to the Activist Question

by Katsunori Matsushita

The questions and concerns raised by PETA and other such activist organizations about the validity of testing medical, pharmaceutical, and biotechnological products and procedures upon animals, wherein said products and procedures are ultimately meant for human use, have resulted in great conflict between these groups and the scientific community which toils to improve the lot of humanity. I therefore would ask of people their indulgence to entertain the solution to this problem that I shall now outline.

Given that PETA and their allies believe that the testing of biomedical products and procedures meant for humans on animals is invalid, I would like to posit that a solution exists to allow for the testing of these new and valuable medicines. The testing of pharmaceutical products upon humans is currently considered to be the final stage of testing before a product can be released onto the market. If the testing upon humans were to be effected from the very first battery of tests, then there would be no need to test upon other animals, for the very being for which these products are meant is now undergoing the testing process. Animals which were originally bred for only medical experimentation could then be relocated.

This methodology, used extensively by Unit 731 of the Imperial Japanese Army during World War 2, is ideal for the testing of products aimed at human beings. As the products will be tested upon humans first, researchers will receive immediate results and feedback as to the effectiveness of their product. By directly applying the products in question to humans, the lengthy years of tests which were originally done on animals before finally being allowed to be tested on humans can be cut out and reduced. This will serve to not only allow for better and more effective treatments and medicines, but it will allow them to come to those in need that much faster. Corporations will also see their profits soar as the millions spent in the long years of tests and in the upkeep for animals could be eliminated, with volunteer human subjects being returned to their original families for final disposal.

And so it is to the members of PETA and other animal rights groups that I make this appeal: volunteer yourselves for medical testing, so that a lab mouse may live. Offer your bodies and minds to science and medicine, so that experimentation on animals will no longer be required. If, however, you feel that your own life is needed to continue the work of protecting animals, then I urge you to offer up some relative: a parent, spouse, sibling, or even your own child. With your sacrifice, an animal life shall be spared, and a new medicine shall come one step closer to realization. With your participation, a final solution can be had.

Poetry.

Joanna Licata

Shafted

Are you fucking happy now?
Now that you’ve left me falling apart
At a time when I needed someone the most
All the lies that you told me
Are falling apart now that you’re with her
But that doesn’t matter
You’re happy
Bringing new life into the world with her
While I sit and stare
At the one who I was shafted for

Falling

What would it be like
To fall off the face of the Earth
And fly through space?
Would another star finally catch you?
Or would you die first,
A lifeless body falling through eternity.

A Little Too Late

when I met you
I never thought it would turn out like this
friendship into passion
who could resist?
but I am being robbed of our time
as you have to go
this will probably never happen again
and the sinking feeling in my stomach confirms this so
am I sorry that it happened?
no, it was great
it just happened
a little too late

Beware the mighty SPORK!

SUBMIT

gdt@hellskitchen.org

Gracies Dinnertime Theatre™

DRAMATIS PERSONÆ

Publisher: C. Diablo

Editors:
Peter C. Gravelle
Pete Lazarski
Tom Samstag
Ray Wallace

Sponsors:
Contact us!

Writers:
Joanna Licata

Printer Daemons:
Katsunori Matsushita