

Doorking Around

Owning access control systems without touching a door

About Me

Name: Brett Chance

Work: Incident Response and AppSec

Hobbies: Security Research and Idling in IRC

Research: <https://brettchance.com>

Twitter: @rem1nd_



Intro

I've always found access control and telephone entry systems interesting. Like many people I enjoy learning and exploring the technology behind these systems to find out what makes them work. When I had some free time clear up in January of this year I dug a bit into these systems. This talk is based on my findings.

About Doorking

- Popular in the access control world
- Extremely common telephone entry systems that are used in apartment complexes and other buildings
- You've probably come in contact with one of their systems



Research Gameplan

- ~~Purchase a used entry system and dig in~~
 - Unable to find a working newer model for under \$2500
- Pour over the manuals and previous work done by other security researchers
- Don't be evil, be diligent and have fun

DKS Telephone Entry Systems

- Commonly installed in apartment complexes, businesses, plants, large homes, seaports and more
- Used to control access to doors, gates and elevators
- Provides access to users by
 - Keypad entry
 - Key FOB
 - Telephone Authorization (a user on the system buzzes you in)



Programming

- Programming of these systems can be done multiple ways.
 - System Keypad
 - Local Programming at the Panel
 - Remote Programming with DK Software
- Protocols and Services that can be used to program.
 - Modem to Modem
 - Serial Connection
 - USB Connection
 - Wireless Connection
 - TCP/IP Lan
 - **DKS Internet Modem or IM Server**
 - **DKS Cellular**

DK IM Server

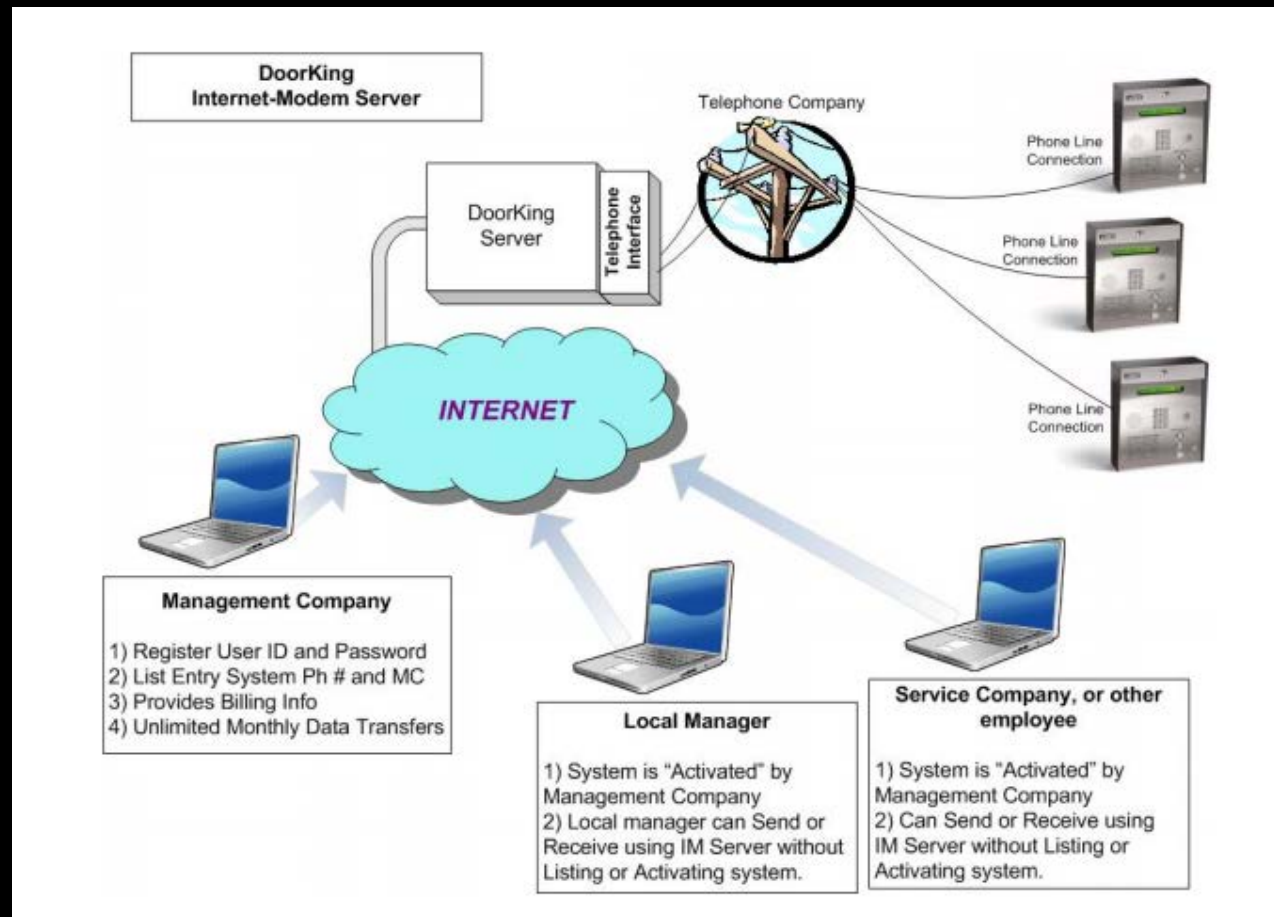
Advantage - DoorKing®

What is the DoorKing IM Server Modem™

- The DoorKing IM Server Modem is a subscription based website that will simplify programming connections between your PC and your Entry Systems
- Subscribing to the IM Server site combines the best of both worlds:
 - ✓ An Internet connection at the PC is the easiest and most cost effect method for data transfer at the PC.
 - ✓ A Modem connection at the Entry System is the easiest and most cost effect method for data transfer at the Entry System.
- The DoorKing IM Server links your computers Internet connection to the Modem inside the entry system
- This offers a simple, reliable and easy to use method to Send and Receive data from your systems





IM Server Connection



DKS Registration


After reading a few manuals that customers who wish to use the remote account manager software are asked to register on Doorking's registration system.

Registration is required if the customer will be using DKS Cellular or IM Server services.

		DKS Registration					
<p>Register your DoorKing Account Manager software to receive update notifications and other benefits, and to enable Internet programming via the IM Server or the DKS Cellular service.</p> <p>If you have already registered, you can log in here.</p> <div><div>Live Chat Offline Email us</div></div> <p>live chat mac</p>		Choose your Registration Type. <p>Various types of registration are available through this site.</p> <p>Click the IM / DKS VoIP button below to register for an IM Server Modem subscription, an IM Server VoIP subscription, or as a person who only programs existing systems, including via direct modem.</p> <p>To register for voice and data plans using our DKS Cellular devices, click the DKS Cellular button below.</p> <table border="1"><thead><tr><th>IM / DKS VoIP</th><th>DKS Cellular</th></tr></thead><tbody><tr><td><p>Choose this option to activate any of the following registrations:</p><p>DKS VoIP: Utilize the DKS Voice-Over-IP telephone service, and program your entry systems using our Plug & Play™ networking.</p><ul style="list-style-type: none">• Voice and Data Service For 1830 Series entry systems.• Voice Only Service For all DoorKing entry systems.<p>DKS Data over IP: Plug & Play Internet programming.</p><ul style="list-style-type: none">• Data over IP Service (formerly IM Server Client). For 1830 Series entry systems with an existing phone line.<p>IM Server Modem: Program your entry systems over the internet from your PC using the existing telephone line connected to the entry system.</p><p>Data Entry: For those programming entry systems that already have an active subscription. Or if you program your entry system using a direct connection or your own PC modem.</p></td><td><p>Choose this option to activate your DKS Cellular plans for DoorKing Cellular compatible entry systems. The following Service Types are available:</p><ul style="list-style-type: none">• Voice and Data Service.• Data Only Service.• Voice Only Service.</td></tr></tbody></table>		IM / DKS VoIP	DKS Cellular	<p>Choose this option to activate any of the following registrations:</p> <p>DKS VoIP: Utilize the DKS Voice-Over-IP telephone service, and program your entry systems using our Plug & Play™ networking.</p> <ul style="list-style-type: none">• Voice and Data Service For 1830 Series entry systems.• Voice Only Service For all DoorKing entry systems. <p>DKS Data over IP: Plug & Play Internet programming.</p> <ul style="list-style-type: none">• Data over IP Service (formerly IM Server Client). For 1830 Series entry systems with an existing phone line. <p>IM Server Modem: Program your entry systems over the internet from your PC using the existing telephone line connected to the entry system.</p> <p>Data Entry: For those programming entry systems that already have an active subscription. Or if you program your entry system using a direct connection or your own PC modem.</p>	<p>Choose this option to activate your DKS Cellular plans for DoorKing Cellular compatible entry systems. The following Service Types are available:</p> <ul style="list-style-type: none">• Voice and Data Service.• Data Only Service.• Voice Only Service.
IM / DKS VoIP	DKS Cellular						
<p>Choose this option to activate any of the following registrations:</p> <p>DKS VoIP: Utilize the DKS Voice-Over-IP telephone service, and program your entry systems using our Plug & Play™ networking.</p> <ul style="list-style-type: none">• Voice and Data Service For 1830 Series entry systems.• Voice Only Service For all DoorKing entry systems. <p>DKS Data over IP: Plug & Play Internet programming.</p> <ul style="list-style-type: none">• Data over IP Service (formerly IM Server Client). For 1830 Series entry systems with an existing phone line. <p>IM Server Modem: Program your entry systems over the internet from your PC using the existing telephone line connected to the entry system.</p> <p>Data Entry: For those programming entry systems that already have an active subscription. Or if you program your entry system using a direct connection or your own PC modem.</p>	<p>Choose this option to activate your DKS Cellular plans for DoorKing Cellular compatible entry systems. The following Service Types are available:</p> <ul style="list-style-type: none">• Voice and Data Service.• Data Only Service.• Voice Only Service.						

Being Curious

- I registered a test account and looked around the registration system
- Off the bat the look and feel of the application gave me the impression it was a bit dated
- I added an entry system to my account and noticed that the master code was displayed in plaintext.



Logged in as: [Log out](#)
[ted norman]
tednorman

Add, remove or edit entry systems.
[live chat mac](#)
Live Chat is available from 6:00 AM - 4:00 PM Pacific Time, Mon-Fri.
Messages left after hours will be replied to the next business day.

Subscription Rates
DK IM Server Modem

Tenants	Monthly	Annual
Up to 100	\$3.95	\$37.40
101 - 250	\$5.95	\$62.40
251 - 500	\$7.95	\$87.40
501 up	\$10.95	\$125.40

1st month free for new phones.


Entry System Management


[Profile](#)[Entry Systems](#)[Billing](#)[Help & Info](#)


Your Current Entry Systems - Click to Edit or Remove

Name	Phone Number	MC	Service	Est	Actual
Ted Norman Account	555 555 5554	1298	IM Server	500	---

Add an Entry System


Service Type: 
IM Server Modem


Phone Number: 

Account Name (optional): 

Estimated Annual Cost: \$87.40

Uses the IM Server Modem over a traditional land-line telephone for programming.

Master Code: 

Est. Resident Count: 
Optional...

Add

Cart contains: 1 new system. [Click here to start Checkout.](#)

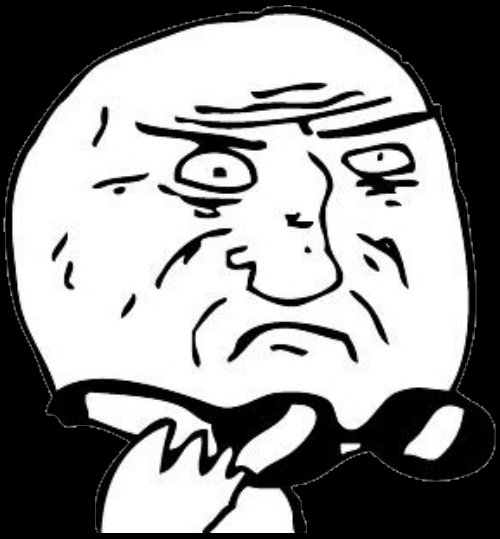
Digging In Deeper

- Although the master code is not a password it is all someone needs to dial or log into a machine. The lack of masking the master code in some way made me suspicious about the security practices of this application as a whole.
- Naturally I'm interested here and much more curious about how the site is handling this data and account authentication. I decided to run Telerik's Fiddler and take a peak under the hood of this application.

Session Management

Here's the raw GET request to navigate to the Profile tab on the registration system.

```
1 GET https://dksdb.dksoftware.com/UserAccount.aspx
2 Host: dksdb.dksoftware.com
3 Connection: keep-alive
4 Upgrade-Insecure-Requests: 1
5 User-Agent: Mozilla/5.0 (Windows NT 6.2; WOW64) AppleWebKit/537.36 (KHTML, like
6 Gecko) Chrome/55.0.2883.87 Safari/537.36
7 Accept: text/html,application/xhtml+xml,application/xml;q=0.9,image/webp,*/*;q=0.8
8 Referer: https://dksdb.dksoftware.com/
9 Accept-Encoding: gzip, deflate, sdch, br
1 Accept-Language: en-US,en;q=0.8
0 Cookie: Credits=User:tednorman
```



Cookie: Credits=User:tednorman

The Problem

- The only information telling the application what account anyone is logged into is the cookie `Credits=User:$user`. There are no authorization parameters or special headers that would verify in my case that tednorman is actually tednorman.
- To verify my findings I created a second account and while logged into the second account modified the cookie to the first account's userid. I reloaded the page and I was viewing that account's information. This meant that anyone could modify their cookie to a different but valid userid and now be viewing that user's account information.

Impact

- Any user can gain access to an account by guessing an account's userid and modifying the credits cookie. Once that is done the following information would be viewable.
 - Full name
 - Physical and Email address
 - Phone number
 - Saved entry systems
 - Description of the system
 - Telephone number of the system
 - Master code of the system

Impact Cont.

- The following information would be modifiable
 - Profile information
 - Entry system information
 - Email address
 - Password on the account
- A malicious user would be able to lock an account holder out of his account and would force that user to contact Doorking to get access back to their account.

Deep Impact



- With the right configuration an attacker with the direct number to a telephone entry system and the master code for that system could connect and receive or send data to the system's panel
- This could be done by connecting to the system with a modem or using Doorking's remote access software
- Systems not programmable online could also be accessed by programming at the system's keypad

Weaponization

I like to get an idea of what could've happened if this issue would have been found and leveraged by a malicious actor. Here's a few steps that I'd suspect an attacker would take to weaponize this vulnerability.

- Create a script that makes a GET request to retrieve an account's profile information. Usernames and other common names would be run through the cookie.
- If there was an account on the system with a username check how many active entry systems are listed on the account by searching UserAccount.aspx for
`Entry systems 0.`
- If an account exists and had active entry systems the script would save the account, profile information and entry system information.

Scenarios



In the next few slides we're going to go on the scenario that someone has already checked for valid users and scraped information of active telephone entry systems.

Local Programming

- In this scenario we are going to assume that the profile information, system description and telephone number fetched from an account were enough to trace down the location of the entry system. With physical access to the system's keypad a malicious user could do the following and more.
 - Add pin, card, or fobs
 - Change master code
- To program these systems the master code switch needs to be switched on. For this to happen the enclosure needs to be opened.

One small hitch, there's a lock



DKS
DOORKING



To pick or not to pick

- These locks look like they can be picked
 - I have about two hours total time of picking locks so don't hold me to that
 - If you are terrible at lock picking like myself don't worry
- Purchase the key!



Remote Software Programming

- Once the entry system credentials are stored systems with remote access capability can be dialed into using Doorking's remote account manager software. Here's a few possibilities that a malicious user may try on the system
 - Add a new resident or employee to the system that would give access to the building.
 - Backup the current programming of the system with the Receive Data or Backup feature. This would give a list of the current users on the system with their phone numbers and entry codes.
 - Overwrite the programming on the system with the Send Data feature.

Quick Local Access with Tone Open Numbers













5.3.1 Connecting to the Telephone Entry System from a Remote Location

1. Call the telephone number that the entry system is installed on. The system will answer with a short tone (beep) after two rings.
 2. Press **★16** and enter the **four-digit MASTER CODE** _ _ _ _ (beep). The beep indicates system has accepted master code.
 3. Press the desired **tone open** number _ (beep).
- Note:** Refer to section 3.3.3 to determine which tone open features have been programmed, i.e. momentary open, hold open, release, hold open one hour and then release.
4. Hang up.

3.3.3 Tone Open Numbers



These steps will program the tone open numbers for Relays 1 and 2. You will need to enter a four-digit number (see chart below) to set the relay functions. **If a function is not desired, enter # in place of a number.**

Factory setting is: Relay 0 = ####, Relay 1 = 9876, Relay 2 = 5432.

1. Press    and enter your four-digit MASTER CODE     (beep).
2. Press   (beep) to set **Relay 1**, OR   (beep) to set **Relay 2** tone numbers.
3. Enter the **four-digit tone open number code**, then press  (beep).

(Example: If you want a relay to have a momentary activation function only, and you want that relay to momentary activate when the number 9 is pressed, enter 9 # # #. If a function is not desired, enter # in place of a number. Do not duplicate tone open numbers, Example: don't set relay 1 and 2 tone-open numbers both to 9.)

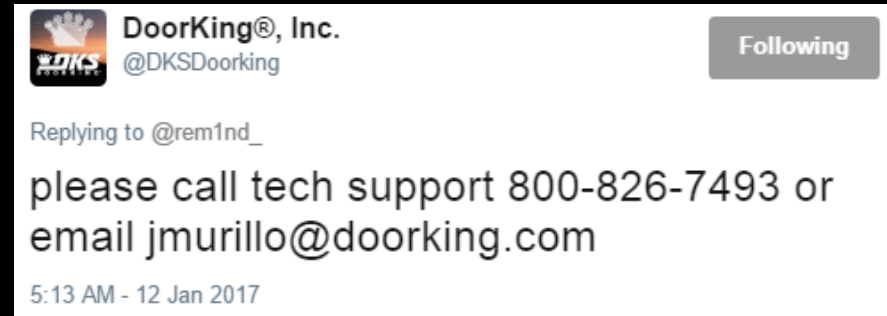
4-Digit Tone Open Number Code	Function
1st Digit	Momentary activation. Relay will activate for the programmed strike time (3.3.1).
2nd Digit	Relay hold. Relay will activate and remain activated until commanded to release.
3rd Digit	Relay release. Deactivates the relay hold command.
4th Digit	Relay hold 1-hour. Relay will activate for 1-hour and then will automatically deactivate itself.

4. Repeat steps 2 and 3 to set other relay tone open numbers.
5. Press   together to end this programming sequence (beeeeeep).

Note: Residents will only be able to activate the **Momentary activation** when using the entry system.

When Disclosure isn't Quick and Clean

- Initial contact on January 8th by email directed at two support emails on DK's website
- Responded to a DK tweet on January 11th asking to get in touch. They replied and directed me to their CEO's email and their tech support phone #.



- Never received a response from the CEO so I was left to call tech support.

...About your registration system

- Initial call summary
 - I managed to get a hold of tech support quickly and I described the issue that I found. It took a few attempts to convey exactly what I was speaking about but in the end the guy on the other end of the phone transferred me to someone who would be able to help.
 - But it went to voicemail :*(
- Over the next two weeks I tried to get a hold of this guy directly around 6 times but each time I got his voicemail.
- I began to think he was on an extended vacation so I called tech support and eventually was put in contact with someone who could help.

Disclosure Timeline

I reported this issue to Doorking on January 8th 2017. After three tweets, four emails, six voicemails and one interesting phone call I finally was able to get through to them and convey the seriousness of the issue. On January 31st I received an email from their VP of Engineering.

Thanks for your email concerning Doorking security.

I am the VP of engineering for Doorking. Unfortunately my expertise is not software but is on the hardware side. My engineers responsible for software and web development are on vacation. When they return, I will instruct them to look at the issues you have brought up.

I just want to assure you that Doorking takes seriously the security of the information our customers place on our servers. If there is a security problem, it will be fixed immediately.

Patrick Kochie
Doorking Inc.

Disclosure Timeline cont.

Three hours later I received an email from another member of Doorking's staff.

Not exactly immediately...

Hey Brett,
I thought I emailed you today about this issue but do not see in in my sent file folder.
Our Developers are out of town at the moment so it may be a few weeks before we get back to you on this issue. We will definitely look into this.
Which version of windows are you using?

Thanks
Allan Hearn
Doorking

On February 15th 2017 I received an email from Doorking stating they had implemented a fix. I published my findings three days later.

Length of Exposure

My best assessment is that this system was online from 2013 and likely earlier. This is based off videos on Doorking's youtube account that walk users through registering on the system as well as references to the registration system in manuals.

I can only assume that this hole was present through their system since 2013 and up until the second week of February 2017.

References

<http://www.doorking.com/sites/default/files/downloads/1834-065-B-10-14.pdf>

http://www.doorking.com/sites/default/files/downloads/1835-066-U-3-17_V63i.pdf

<http://www.doorking.com/sites/default/files/downloads/1835-065-T-7-12.pdf>

<https://www.youtube.com/watch?v=WO1uuv9v-P4>

<https://www.youtube.com/watch?v=MHZ2wAS95a0>

<http://www.doorking.com/imserver/>

http://www.doorking.com/sites/default/files/downloads/IM_Svr_Fee_Schedule_10.13.C.pdf

<https://dksdb.dksoftware.com>

Questions?