Wildix

SECURITY IN UCC:
Is It Possible to Be "Secure by Design?"

CONTENTS

Wildix EE OÜ

Narva mnt 7-339A,
10117 Tallinn - Estonia
VAT ID: EE101984698

www.wildix.com
info@wildix.com
+ 372 (66) 01842

THE NEED FOR SECURITY

In all parts of IT, security is utterly vital. Although this applies to both consumer and business contexts, **the need for protection against cyberattacks is astronomically higher in an enterprise setting** due to the increased impact such attacks necessarily have.

THIS IS DUE TO TWO PRIMARY FACTORS:

1. **Suffering a cyberattack severely damages a company's reputation,** causing business partners and customers alike to question if they can trust their personal data with the unsecured company.

2. **Company servers hold significantly more data, financial or otherwise, for cybercriminals to exploit compared to the consumer space.**

The significance of these factors only increases as we consider just how frequently cyberattacks are launched against businesses.

- From January 2005 through March 2020, there have been 11,556 information security breaches, exposing a total of **1.663 trillion records**[1]
- Cyberattacks cost the world **$3 trillion USD in 2015**, and will cost the world **$6 trillion USD in 2021**
- Worldwide spending on information security exceeded **$114 billion USD in 2018**, and will grow to **$170.4 billion USD in in 2022**
- **92%** of North American companies experienced a distributed denial of service (DDoS) attack in 2018. These attacks cost US businesses a total exceeding **$10 billion USD per year**
- **28%** of small businesses have experienced a cyberattack. **As a result:**

69%

have gone temporarily offline

37%

have experienced a financial loss

25%

have filed for bankruptcy

Citing sources are listed on p.15

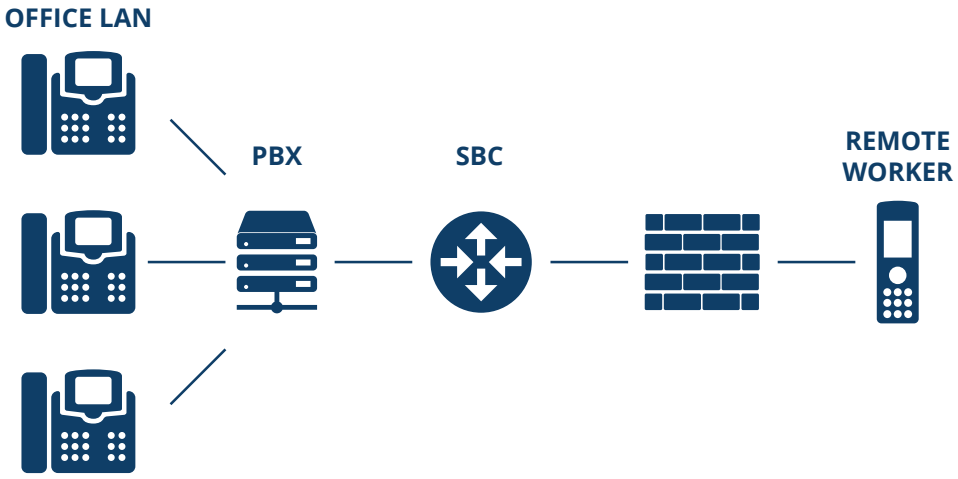
SUBSTANDARD OPTIONS

As a result of these substantial threats to reputation and even direct financial holdings, **businesses have a clear and pressing need to continue investing in IT security.**

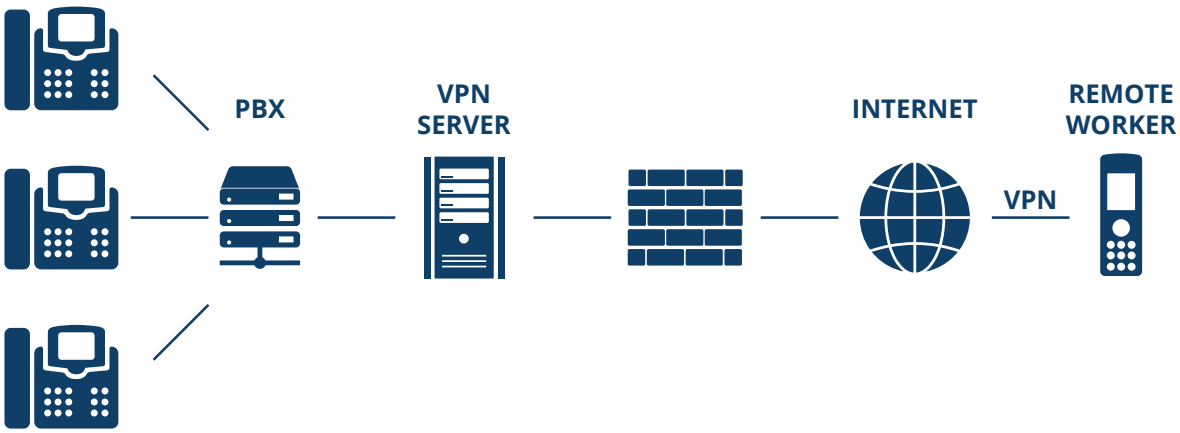
This extends to the space of Unified Communications, where the exchange of confidential information internally or externally can make chats, voice calls, and video a lucrative target for cybercriminals.

To combat threats, companies often make use of one or both of the following common security measures:

- **SBCs (Session Border Controllers):** A device deployed on an internet connection to establish security during sessions (i.e., a single instance of communication between two parties over the network). These function as metaphorical gateways that police data traffic flowing into and out from a VoIP network, ideally keeping out malicious agents such as hackers in the process. Usually, SBCs are an element built into the network router or somewhere else external of the UCC platform itself.



- **VPNs (Virtual Private Networks):** A virtual network established within a public connection. Effectively, these connections create a metaphorical "tunnel" inside an existing network, as well as typically encrypting data so that it cannot be read by unauthorized users. VPNs must be logged into to be accessed, meaning that, theoretically, their connection is accessible only to approved personnel.



SUBSTANDARD OPTIONS

However, **NUMEROUS PROBLEMS EXIST WITHIN THESE TWO COMMON SETUPS.**

- Because VPNs require an additional login, it creates **an additional space where hackers can gain access to secure networks.** There is also an **increased risk of user error**, as employees may refuse to use it during communication sessions.
- **VPNs typically take up additional bandwidth,** with some codecs such as G.729 taking up to double regular network use.
- Relying on an SBC for security means that **if the SBC is breached, there are no additional security measures to stop the intrusion,** and a successful attack can quickly spread across an entire corporate server.
- External VPNs and SBCs must be managed in addition to the UCC solution itself, **increasing the cost of cybersecurity maintenance and the labor associated with it. This also increases the risk of user error or device failure,** as if technicians or end-users make a mistake with the security measure, or such measures have a vulnerability, it will create additional ways cybercriminals can enter the network.

PREFERABLE ALTERNATIVES

To avoid the issues created by these inherent vulnerabilities and user error – as well as reduce the costs of security in UC overall – **it is preferable to implement UC architecture that is "secure by design."**

This axiom refers to an **implementation of security measures directly within the PBX and on every one of its associated devices:** the network, all connected phones, the UC software itself, and each individual software license.

If each and every element within a UC platform were to have its own security measures, the security of the network overall would increase significantly. To begin with, **the network itself would be better protected** due to the more robust and complete security protocols safeguarding it. Additionally, in the event the network is breached, **such an intrusion would be slower to spread,** as further security measures implemented across individual devices and software instances would block the attack rather than being wholly susceptible to it.

Further security would be achieved by the fact that, were security measures fully integrated into the inherent design of the platform, **there would be no need for regular maintenance from IT personnel or training employees against improper usage.** Consequently, user error and its associated risks would dramatically decrease.

It is also worth considering that **this approach to security would also decrease associated costs,** as there would be no fees or payments for a separately deployed security protocol.

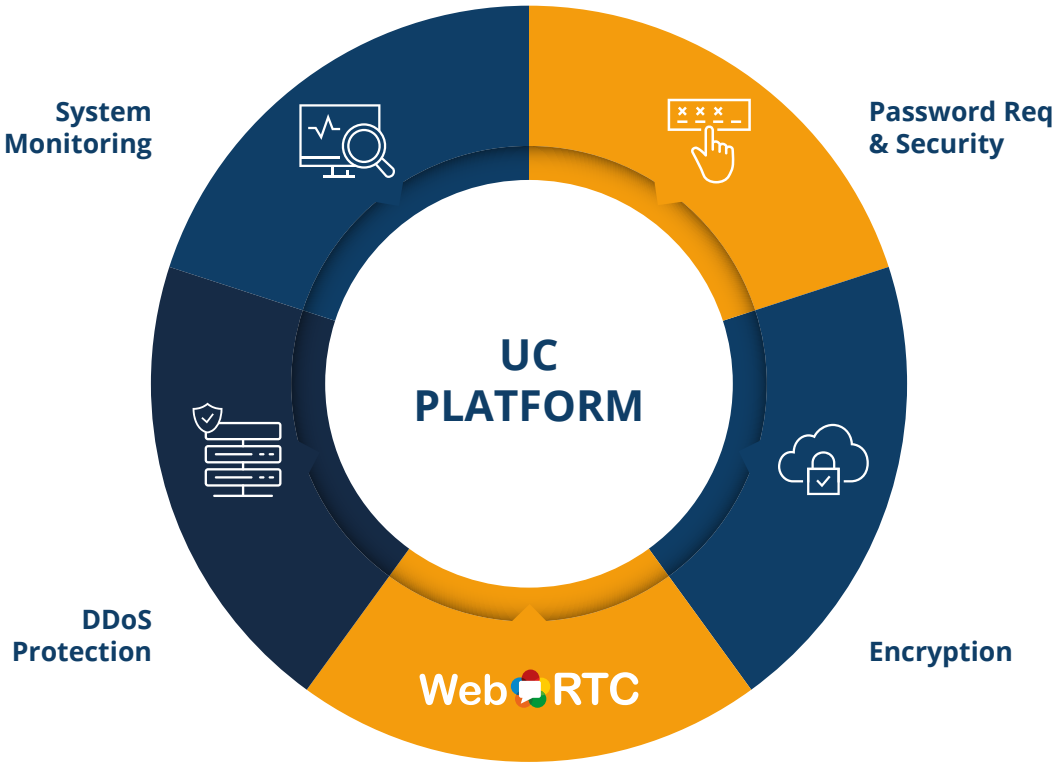
Wildix EE OÜ

Narva mnt 7-339A,
10117 Tallinn - Estonia
VAT ID: EE101984698

www.wildix.com
info@wildix.com
+ 372 (66) 01842

ELEMENTS OF
A "SECURE-BY-DESIGN" PLATFORM

Practically speaking, the implementation of a UC platform that has effective measures built into its design would make use of the following protective elements:



WebRTC Architecture

THESE ELEMENTS WILL BE DISCUSSED IN MORE DETAIL IN THE FOLLOWING PAGES.

PASSWORD REQUIREMENTS & SECURITY

In any given aspect of cybersecurity, passwords are an essential element. However, this means that **the protected element can only be as secure as the password is.** Hackers can easily guess or deduce common, uncomplex passwords ("abc123," "password," etc.) and as such, poor passwords leave a UC platform highly susceptible to attack.

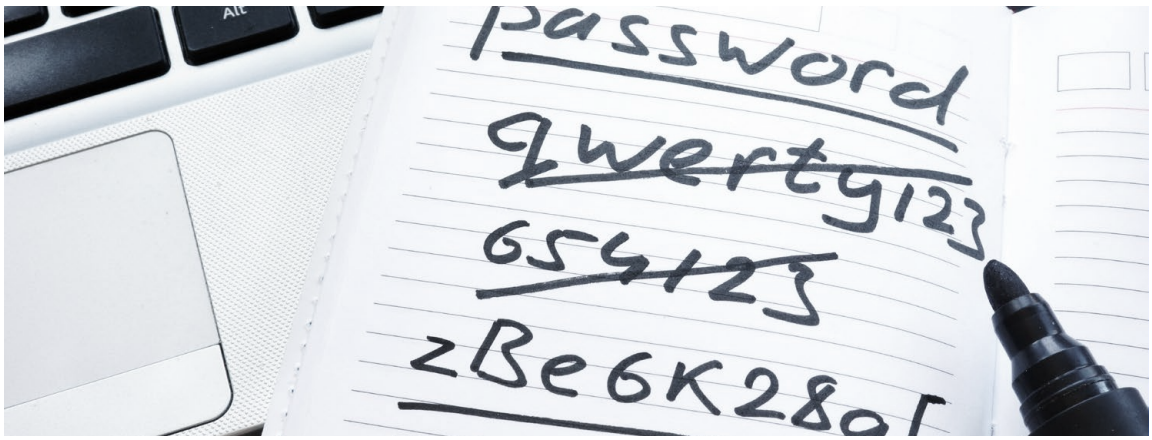
To close this security loophole, **effective security must include a requirement for strong passwords.** Because many users will ignore security standards and try to create an easy-to-remember (yet highly unsecured) password, **the requirement for a strong password must be enforced by the system:** when setting up an account, the system itself should ask users to create a password with multiple character cases, numbers, and unique symbols ("@", "^", etc.), and actively reject any passwords that do not meet complexity standards.

Additionally, **passwords will have to be saved in a secure, encrypted way so as to ensure that they are unusable in the event their server is illicitly accessed.** This can be done quickly and effectively by using the SHA512 algorithm and salt cryptography, two encryption methods that effectively randomize input data in such a way that only the internal server can unscramble them.

Beyond this protection, **the system must protect against "brute force" access attempts,** in which intruders cycle through characters randomly and make multiple login attempts. This can be done effectively by setting up the system to **deny access to any IP addresses that make an excessive number of failed attempts within a short period of time.** Such instances and their related IP addresses should also be logged by the system for review by an admin.

For even further access security, the system would also include the option for **2-factor authentication (2FA),** where in addition to inputting a password, users must also enter a one-time, randomly generated code delivered either to their email or on their personal device. This additional requirement dramatically reduces the risk of accounts becoming compromised, as it requires a hacker to have access to email or the user's specific instance of code-generating software for access.

Alternatively, a way to reduce the risk of user error in password protection is the implementation of **a single sign-on** protocol. Under this process, users could simply log into their PBX account by entering the username and password for a different account, such as their Gmail login or Microsoft account. The procedure **increases security due to its practicality in implementation;** when users are required to remember numerous complex passwords, it increases the risk that they will leave passwords out in the open (such as on paper) for fear of forgetting them. As a result, **it is more realistically secure to allow users to remember just one highly secure password.** The single sign-on procedure should also be able to be used in conjunction with 2FA for stricter security.



ENCRYPTION

Because many hackers and cyberattacks operate by effectively eavesdropping on ongoing communications, rather than simply accessing accounts, it is essential that such communications be encrypted. This achieves much the same purpose as a VPN: **even if unauthorized parties gain access to transmitted data, it is in a state where they cannot make use of it.**

By default, **the system should use Transport Layer Security (TLS) to encrypt data between users,** which functions by sharing a decryption method only between direct users and using a third-party certificate authenticator (CA) to verify identity of both users. In other words, **using TLS, data is encrypted via a cypher known only to the involved users, rendering it impossible for non-authorized users to decipher it.** In an ideal setup, TLS would be used for voice, video, screensharing, messages, and any other communications initiated through the PBX.

The system should also utilize Secure Real-Time Protocol (SRTP), which is a standard of relaying data over the web with further encryption and authentication. Similar to TLS, **it turns communications into coded data, then identifies the right user to give the decoding keys to.** One especially effective way of implementing this protocol is through the SDES-AES 128 key and the DTLS-SRTP key (which works directly in conjunction with TLS) for further encryption of all communications.

To reiterate, although an encryption process alone cannot prevent unauthorized agents from eavesdropping on communications, it is nevertheless a crucial part of creating a "secure-by-design" platform. Implemented correctly, **encryption ensures that even those attackers who do gain access to the inner workings of the system are unable to make practical use of the uncovered data;** this creates a powerful layer of security inherent to the design of the system.

Wildix Collaboration

DDOS PROTECTION

As discussed earlier, **DDoS attacks are of prime concern to the security infrastructure of any business.** Such attacks occur when a purposefully excessive amount of web traffic is directed at a single web server for the purpose of overloading it and causing it to crash; as they can also be directed at UC servers, a proper security setup must implement safeguards against them.

This protection would already be carried out in part by the previously considered element of brute force entry protection, wherein too many failed password attempts would lock out access from an IP address. This safeguard would already ensure that an attacker cannot overload the system by forcing it to process an excess of failed password attempts.

However, further protection should be taken as well. The system itself must also feature **a protocol that policies traffic coming into the system** (both internal and externally) in order to ensure that the data does not overload the system through voice calls, videoconferences, instant messaging, or any other capability built into the system.

Similar to brute force entry protection, this could easily be manifested as a **provision that outright blocks traffic from an IP if the data is in such an amount that it threatens to overload the server.** In fact, considering the reality and severity of the risk posed by DDoS attacks, such a provision is not an option; it's very much required for a fully secure UC system, especially one that can claim to have security built into its very foundational architecture.

Wildix UC system – security built into its very foundational architecture.

Wildix EE OÜ

Narva mnt 7-339A,
10117 Tallinn - Estonia
VAT ID: EE101984698

www.wildix.com
info@wildix.com
+ 372 (66) 01842

A less obvious source of web security within UC comes from **WebRTC** (Web Real-Time Communication), an internet communications framework that arrives built into the majority of modern web browsers. An Open Source project based on HTML 5 and JavaScript and started by Google in 2011, the technology is a series of protocols and interfaces that enable instant and secure communications between compatible web browsers.

From a security standpoint, **WebRTC provides numerous key benefits over other communications protocols,** both in terms of active security and preventing user error.

To begin with, **WebRTC does not function through external plugins or software, but internally through a browser.** As a result, **WebRTC is updated quickly and automatically, and does not rely on user input to be changed to the latest version.** This ensures that user error does not result in using the system with an unpatched vulnerability.

Additionally, because WebRTC operates through the browser rather than through a separate plugin, **the protocol is unaffected by infections or security vulnerabilities that may exist elsewhere on an individual user's device.** If, for instance, a user's work laptop has been unknowingly infected by spyware, there is no way for the program to reach the instance of WebRTC, as it does not truly "exist" on the laptop in such a way that it could be infected. Consequently, users are guaranteed safe browsing even if they use personal (and potentially compromised) devices.

WebRTC also implements the following specific security measures:

- **Requires explicit permission from the user to use webcam or mic,** and actively displays to user when those devices are in use, meaning there is no way for hackers or programs to hijack webcam or mic through the tech
- **Offers full end-to-end encryption through DTLS and SRTP,** which are never decrypted during the connection — in other words, even if communications were intercepted by a third party, they would not be decipherable by the interceptor
- **WebRTC connections are made directly from browser to browser,** without intermediaries, obviating the possibility of interception

Furthermore, because these elements of WebRTC are inherently built into the browser, **implementing them could easily be an automatic process.** This again would ensure that security for the UC system is an inherent aspect of the platform rather than something to be externally managed.

SYSTEM MONITORING

Finally, **it is vital that admins have a thorough ability to monitor the UC system,** as even the most secure platforms carry a risk of intrusion and should therefore have means to detect such instances in detail.

As such, an effective UC security platform (particularly one with inherent security) must also include **automatic alerts for system intrusions across all devices managed by the PBX,** as well as alerts for any attacks that originate within the system (e.g., an authorized user's account being used for a DDoS attack).

For additional, optional insight, **the system should also feature integration with external monitoring software, such as Zabbix.** This would allow security personnel to better detail and report any detected attacks or vulnerabilities in the system.

Wildix EE OÜ

Narva mnt 7-339A,
10117 Tallinn - Estonia
VAT ID: EE101984698

www.wildix.com
info@wildix.com
+ 372 (66) 01842

USE CASES

To more practically illustrate the combined benefit of these various elements, this section will now list a number of hypothetical instances of their implementation. For a fuller picture of their purpose and value, each case will indicate a scenario unfolding **with and without the specific security element.**

1. A DDoS attack hits a system through multiple login attempts

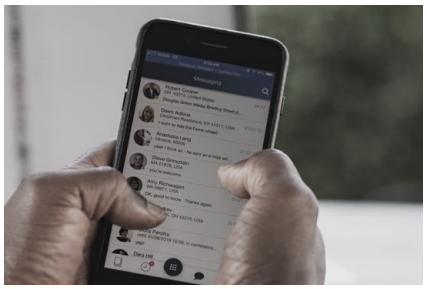
NOT SECURE BY DESIGN: The system is overloaded and **everyone is locked out** anywhere from half an hour to multiple hours.

SECURE BY DESIGN: After a limited number of login attempts, **the attacker is locked out.** The attack is logged in the system for an admin to review and defend against.

2. An end-user is setting up an account on a PBX. Disregarding company protocol, he decides to create a short, simple password, under the pretense that it will be easy to remember

NOT SECURE BY DESIGN: The user is allowed to create the basic password. Soon after, **a hacker who has access to the user's username quickly guesses the simple password** and locks the user out of his account.

SECURE BY DESIGN: The system actively prevents the user from creating the easy password and forces him to create a complex one. Although the user is frustrated that he has to use a complex password, he then discovers the single sign-on feature, which allows him to log in with a complex password he already has memorized.



3. Adam wants to send a quick message to his colleague, Brenda, to ask about finances

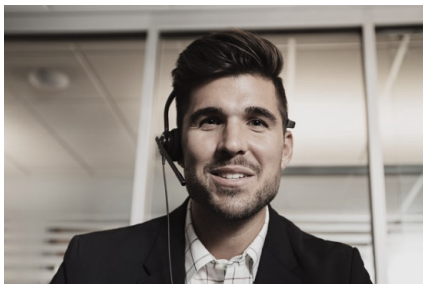
NOT SECURE BY DESIGN: The UC system is protected by a VPN that Adam is expected to log into for all communications. However, since it's such a quick message, Adam decides logging into the VPN is too much hassle, and sends the message without VPN protection. As the message is sent, however, the unencrypted data is then stolen by a hacker who was aware of the VPN's use and waiting for a flaw.

SECURE BY DESIGN: Adam is not required to log into a VPN to send this one message. Instead, it is encrypted automatically, meaning even if there were a hacker watching the network, they would be unable to read the communications.

4. An end-user must communicate with this team immediately over a vital project that concerns numerous internal details. The need to collaborate is so pressing that he does not have time for updates to his PBX.

NOT SECURE BY DESIGN: The end-user logs into the PBX without downloading a firmware update for their SBC. Because this update contained a patch for a vulnerability with the SBC, the end-user's communications are now open to hackers.

SECURE BY DESIGN: WebRTC has been updated automatically, and is already patched to the latest, most secure version immediately as the end-user logs in. He communicates with his team quickly and securely.



5. A customer calls into a company to interact with a call agent. They discuss many of the customer's private details, including her company website login info and bank information.

NOT SECURE BY DESIGN: The conversation takes place over a VPN or SBC; however, the connection is unsecured on the customer's end. This results in any hackers who have been tracking the customer being able to access her data directly.

SECURE BY DESIGN: The conversation takes place over WebRTC, which is conducted directly from the call agent to the customer and cannot be intercepted. The conversation also is encrypted for further protection.

Wildix EE OÜ

Narva mnt 7-339A,
10117 Tallinn - Estonia
VAT ID: EE101984698

www.wildix.com
info@wildix.com
+ 372 (66) 01842

VALUE GAINED

By implementing these security measures, businesses become able to achieve **an idealized balance between security and usability.** On the one hand, they will have **a system that is uniquely positioned to remain guarded against attacks,** shielding them from blows to their reputation caused by breaches and the direct financial costs such attacks deal.

At the same time, users will have access to **a system that remains easy to implement in their everyday business,** or, put simply, a system that is not weighed down by the security put in place.

In fact, it is worth considering that this latter point on usability itself increases system security. As illustrated by use cases, **if an end-user finds security measures cumbersome or otherwise an impediment to their work, they will typically find a way to circumvent those protocols.** It is therefore preferential to have security enforced seamlessly within the inherent design of the platform, as illustrated in the principles outlined previously.

Additionally, **such a system would almost certainly lead to money saved on the part of businesses** even in the event that cyberattacks do not occur, as with a security system that does not rely on external programs, there would necessarily be less time and money spent on maintenance and upkeep.

A "secure-by-design" system as described previously would, in short, achieve **more security, more usability, and less expenses issued by a company in the process.**

Given this wealth of benefits, particularly when compared to other leading options on the market, **such a system is unquestionably a crucial element that any business should be seeking out in their UC platform.**

Citing sources:

bit.ly/Security-in-UCC

bit.ly/Security-in-UCC-2

bit.ly/Security-in-UCC-3

bit.ly/Security-in-UCC-4

bit.ly/Security-in-UCC-5


T-Mobile
9:31 AM
91%
Messaging
Robert Cooper
OH 43065, United States
08:47
Douglas Green Media Briefing Sheet.d...
Dawn Adkins
Cincinnati Roadshow, KY 41011, USA
31.07.19
I want to ride the Ferris wheel!
Anastasia Lang
Ukraine, 65000
31.07.19
yeah I think so - he sent an e-mail wit...
Steve Grinsztein
MA 01879, USA
31.07.19
you're welcome
Amy Richwagen
WA 98671, USA
31.07.19
OK, good to know. Thanks again.
Philip Turkov
Cincinnati RS, OH 43215, USA
31.07.19
thanks!
Giulia Perotta
08005 Barcelona, Spain
yep!
Dara Hill
Ukraine, 65000

Wildix