Bezpečnost mobilních telefonů

Ondřej Kollert

ČVUT FJFI

15.5.2014

Osnova prezentace

Osnova prezentace

Úvodní povídání

- Mobilní telefony jsou součástí našeho běžného života.

Úvodní povídání

- Mobilní telefony jsou součástí našeho běžného života.
- Od roku 1990 vzrostl počet mobilů z 12,4 milionů na 6 miliard v roce 2011.

Úvodní povídání

- Mobilní telefony jsou součástí našeho běžného života.
- Od roku 1990 vzrostl počet mobilů z 12,4 milionů na 6 miliard v roce 2011.
- Dnes existuje mnoho potenciálních hrozeb pro uživatele.

Osnova prezentace

Mobilní pravěk

- Zpočátku byla hlavní bezpečnost při mobilních hovorech.

Nokia Cityman

Váha: 760 g
Rozměry: 183x43x79 mm
Baterie: 1000 mAh, NiCD
Pohotovostní režim: 14 h
Doba hovoru: 50 min

1G

- První technologie pro mobilní komunikaci v Evropě byla NMT (Nordic Mobile Telephone) v roce 1981.
- Na našem území byla zavedena v 90. letech.
- Technologie 1. generace, která podporovala více souběžných hovorů než předchůdci 0. generace.
- Analogový signál, který navíc zpočátku nebyl šifrovaný.
- Pozdější verze již komunikaci šifrovali pomocí tzv. scramblerů.

1G

- První technologie pro mobilní komunikaci v Evropě byla NMT (Nordic Mobile Telephone) v roce 1981.
- Na našem území byla zavedena v 90. letech.
- Technologie 1. generace, která podporovala více souběžných hovorů než předchůdci 0. generace.
- Analogový signál, který navíc zpočátku nebyl šifrovaný.
- Pozdější verze již komunikaci šifrovali pomocí tzv. scramblerů.

1G

- První technologie pro mobilní komunikaci v Evropě byla NMT (Nordic Mobile Telephone) v roce 1981.
- Na našem území byla zavedena v 90. letech.
- Technologie 1. generace, která podporovala více souběžných hovorů než předchůdci 0. generace.
- Analogový signál, který navíc zpočátku nebyl šifrovaný.
- Pozdější verze již komunikaci šifrovali pomocí tzv. scramblerů.

1G

- První technologie pro mobilní komunikaci v Evropě byla NMT (Nordic Mobile Telephone) v roce 1981.
- Na našem území byla zavedena v 90. letech.
- Technologie 1. generace, která podporovala více souběžných hovorů než předchůdci 0. generace.
- Analogový signál, který navíc zpočátku nebyl šifrovaný.
- Pozdější verze již komunikaci šifrovali pomocí tzv. scramblerů.

1G

- První technologie pro mobilní komunikaci v Evropě byla NMT (Nordic Mobile Telephone) v roce 1981.
- Na našem území byla zavedena v 90. letech.
- Technologie 1. generace, která podporovala více souběžných hovorů než předchůdci 0. generace.
- Analogový signál, který navíc zpočátku nebyl šifrovaný.
- Pozdější verze již komunikaci šifrovali pomocí tzv. scramblerů.

2G

- Mobilní komunikace druhé generace spuštěna v roce 1991.
- Založená na standardu GSM (Global System for Mobile Communication).
- Technologie digitální, šifrovaná pomocí algoritmů ozn. jako A5.
- První šifry byly A5/1 a slabší verze A5/2, přičemž se jedná o šifry proudové.
- Nejdříve byly utajené, ale později se zjistilo, jak fungují.
- Bylo odhaleno několik závažných chyb a dnes jsou šifry prolomitelné.

2G

- Mobilní komunikace druhé generace spuštěna v roce 1991.
- Založená na standardu GSM (Global System for Mobile Communication).
- Technologie digitální, šifrovaná pomocí algoritmů ozn. jako A5.
- První šifry byly A5/1 a slabší verze A5/2, přičemž se jedná o šifry proudové.
- Nejdříve byly utajené, ale později se zjistilo, jak fungují.
- Bylo odhaleno několik závažných chyb a dnes jsou šifry prolomitelné.

2G

- Mobilní komunikace druhé generace spuštěna v roce 1991.
- Založená na standardu GSM (Global System for Mobile Communication).
- Technologie digitální, šifrovaná pomocí algoritmů ozn. jako A5.
- První šifry byly A5/1 a slabší verze A5/2, přičemž se jedná o šifry proudové.
- Nejdříve byly utajené, ale později se zjistilo, jak fungují.
- Bylo odhaleno několik závažných chyb a dnes jsou šifry prolomitelné.

2G

- Mobilní komunikace druhé generace spuštěna v roce 1991.
- Založená na standardu GSM (Global System for Mobile Communication).
- Technologie digitální, šifrovaná pomocí algoritmů ozn. jako A5.
- První šifry byly A5/1 a slabší verze A5/2, přičemž se jedná o šifry proudové.
- Nejdříve byly utajené, ale později se zjistilo, jak fungují.
- Bylo odhaleno několik závažných chyb a dnes jsou šifry prolomitelné.

2G

- Mobilní komunikace druhé generace spuštěna v roce 1991.
- Založená na standardu GSM (Global System for Mobile Communication).
- Technologie digitální, šifrovaná pomocí algoritmů ozn. jako A5.
- První šifry byly A5/1 a slabší verze A5/2, přičemž se jedná o šifry proudové.
- Nejdříve byly utajené, ale později se zjistilo, jak fungují.
- Bylo odhaleno několik závažných chyb a dnes jsou šifry prolomitelné.

2G

- Mobilní komunikace druhé generace spuštěna v roce 1991.
- Založená na standardu GSM (Global System for Mobile Communication).
- Technologie digitální, šifrovaná pomocí algoritmů ozn. jako A5.
- První šifry byly A5/1 a slabší verze A5/2, přičemž se jedná o šifry proudové.
- Nejdříve byly utajené, ale později se zjistilo, jak fungují.
- Bylo odhaleno několik závažných chyb a dnes jsou šifry prolomitelné.

KASUMI

- Novější šifry skupiny A5 jsou ozn. jako A5/3, A5/4 nebo také KASUMI.
- Jedná se o šifry blokové používané zprvu pro GSM.
- Šifry v roce 2010 (Dunkleman, Keller, Shamir) prolomeny metodou related key attack.
- Nejedná se o původní šifru, ale upravenou MISTY1.
- Naopak útok typu related key není na MISTY1 účinný.

KASUMI

- Novější šifry skupiny A5 jsou ozn. jako A5/3, A5/4 nebo také KASUMI.
- Jedná se o šifry blokové používané zprvu pro GSM.
- Šifry v roce 2010 (Dunkleman, Keller, Shamir) prolomeny metodou related key attack.
- Nejedná se o původní šifru, ale upravenou MISTY1.
- Naopak útok typu related key není na MISTY1 účinný.

KASUMI

- Novější šifry skupiny A5 jsou ozn. jako A5/3, A5/4 nebo také KASUMI.
- Jedná se o šifry blokové používané zprvu pro GSM.
- Šifry v roce 2010 (Dunkleman, Keller, Shamir) prolomeny metodou related key attack.
- Nejedná se o původní šifru, ale upravenou MISTY1.
- Naopak útok typu related key není na MISTY1 účinný.

KASUMI

- Novější šifry skupiny A5 jsou ozn. jako A5/3, A5/4 nebo také KASUMI.
- Jedná se o šifry blokové používané zprvu pro GSM.
- Šifry v roce 2010 (Dunkleman, Keller, Shamir) prolomeny metodou related key attack.
- Nejedná se o původní šifru, ale upravenou MISTY1.
- Naopak útok typu related key není na MISTY1 účinný.

KASUMI

- Novější šifry skupiny A5 jsou ozn. jako A5/3, A5/4 nebo také KASUMI.
- Jedná se o šifry blokové používané zprvu pro GSM.
- Šifry v roce 2010 (Dunkleman, Keller, Shamir) prolomeny metodou related key attack.
- Nejedná se o původní šifru, ale upravenou MISTY1.
- Naopak útok typu related key není na MISTY1 účinný.

3G

- Třetí generace, založená na standardu W-CMDA (Wideband - Code Division Multiple Access), byla spuštěna v roce 2001.
- Šifrování komunikace nejdříve pomocí KASUMI, později algoritmem SNOW 3G.
- Tento algoritmus použit zatím také pro 4G LTE.

3G

- Třetí generace, založená na standardu W-CMDA (Wideband - Code Division Multiple Access), byla spuštěna v roce 2001.
- Šifrování komunikace nejdříve pomocí KASUMI, později algoritmem SNOW 3G.
- Tento algoritmus použit zatím také pro 4G LTE.

3G

- Třetí generace, založená na standardu W-CMDA (Wideband - Code Division Multiple Access), byla spuštěna v roce 2001.
- Šifrování komunikace nejdříve pomocí KASUMI, později algoritmem SNOW 3G.
- Tento algoritmus použit zatím také pro 4G LTE.

Osnova prezentace

Wi-Fi (Wireless Fidelity)

- Původně ochrana zajišťována pomocí WEP (Wired Equivalent Privacy).
- Dnes je zabezpečení pomocí WPA (Wi-Fi Protected Access) - Dynamické generování klíče.
- WEP a WPA používají proudové šifry RC4.
- Nástupcem WPA je protokol WPA2, který používá blokovou šifru AES (Advanced Encryption Standard).

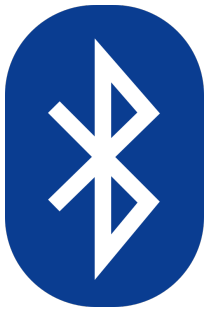
Wi-Fi (Wireless Fidelity)

- Původně ochrana zajišťována pomocí WEP (Wired Equivalent Privacy).
- Dnes je zabezpečení pomocí WPA (Wi-Fi Protected Access) - Dynamické generování klíče.
- WEP a WPA používají proudové šifry RC4.
- Nástupcem WPA je protokol WPA2, který používá blokovou šifru AES (Advanced Encryption Standard).

Wi-Fi (Wireless Fidelity)

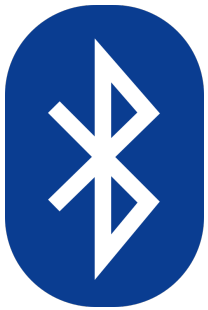
- Původně ochrana zajišťována pomocí WEP (Wired Equivalent Privacy).
- Dnes je zabezpečení pomocí WPA (Wi-Fi Protected Access) - Dynamické generování klíče.
- WEP a WPA používají proudové šifry RC4.
- Nástupcem WPA je protokol WPA2, který používá blokovou šifru AES (Advanced Encryption Standard).

Bluetooth



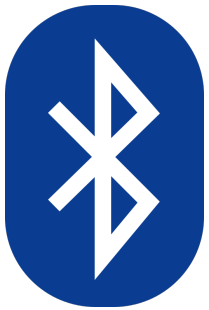
- Sdílený klíč je generován pomocí algoritmu založeném na blokových šifrách SAFER+ (Secure and Fast Encryption Routine).
- Posílaná data jsou šifrována proudové šifře E0.
- Útoky skrze Bluetooth se nazývají bluesnarfing, bluejacking a bluebugging.
- Útočník může získat přístup k datům nebo vzdáleně ovládat telefon.

Bluetooth



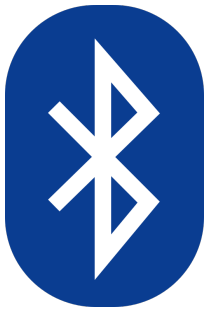
- Sdílený klíč je generován pomocí algoritmu založeném na blokových šifrách SAFER+ (Secure and Fast Encryption Routine).
- Posílaná data jsou šifrována proudové šifře E0.
- Útoky skrze Bluetooth se nazývají bluesnarfing, bluejacking a bluebugging.
- Útočník může získat přístup k datům nebo vzdáleně ovládat telefon.

Bluetooth



- Sdílený klíč je generován pomocí algoritmu založeném na blokových šifrách SAFER+ (Secure and Fast Encryption Routine).
- Posílaná data jsou šifrována proudové šifře E0.
- Útoky skrze Bluetooth se nazývají bluesnarfing, bluejacking a bluebugging.
- Útočník může získat přístup k datům nebo vzdáleně ovládat telefon.

Bluetooth



- Sdílený klíč je generován pomocí algoritmu založeném na blokových šifrách SAFER+ (Secure and Fast Encryption Routine).
- Posílaná data jsou šifrována proudové šifře E0.
- Útoky skrze Bluetooth se nazývají bluesnarfing, bluejacking a bluebugging.
- Útočník může získat přístup k datům nebo vzdáleně ovládat telefon.

Osnova prezentace

Slabiny OS a webových prohlížečů

- Hrozby obdobné těm při používání PC.
- Např. u iPhonu s firmwarem 1.1.1 bylo možné se do smartphonu nabourat skrze webový prohlížeč.
- Podobná slabina byla v roce 2008 zjištěna i u operačního systému Android.

Slabiny OS a webových prohlížečů

- Hrozby obdobné těm při používání PC.
- Např. u iPhonu s firmwarem 1.1.1 bylo možné se do smartphonu nabourat skrze webový prohlížeč.
- Podobná slabina byla v roce 2008 zjištěna i u operačního systému Android.

Slabiny OS a webových prohlížečů

- Hrozby obdobné těm při používání PC.
- Např. u iPhonu s firmwarem 1.1.1 bylo možné se do smartphonu nabourat skrze webový prohlížeč.
- Podobná slabina byla v roce 2008 zjištěna i u operačního systému Android.

Mobilní malware

- Při prohlížení webu se do smartphonu může dostat malware.

Mobilní malware

- Při prohlížení webu se do smartphonu může dostat malware.
- Nejčastěji jsou to trojani, viry a červi.

Mobilní malware

- Při prohlížení webu se do smartphonu může dostat malware.
- Nejčastěji jsou to trojani, viry a červi.
- Příklady mobilního malwaru:
  - Cabir (2004) - první červ napadající mobilní telefony.
  - Commwarrior (2005) - červ působící skrze MMS přes Bluetooth.
  - Phage, RedBrowser, CardTrap

Děkuji za pozornost.)