Bezpečnost mobilní komunikace

Tomáš Vávra

UKRY

9. května 2011

Obsah

Obsah

Obsah

Obsah

Obsah

Útoky

Možné typy útoků:

- operátor;
- pasivní odposlech dat - nutnost prolomení šifry;
- IMSI catching - není třeba lámat šifru;
- Flexispy;
- reálný odposlech;

Útoky

Možné typy útoků:

- operátor;
- pasivní odposlech dat - nutnost prolomení šifry;
- IMSI catching - není třeba lámat šifru;
- Flexispy;
- reálný odposlech;

Útoky

Možné typy útoků:

- operátor;
- pasivní odposlech dat - nutnost prolomení šifry;
- IMSI catching - není třeba lámat šifru;
- Flexispy;
- reálný odposlech;

Útoky

Možné typy útoků:

- operátor;
- pasivní odposlech dat - nutnost prolomení šifry;
- IMSI catching - není třeba lámat šifru;
- Flexispy;
- reálný odposlech;

Útoky

Možné typy útoků:

- operátor;
- pasivní odposlech dat - nutnost prolomení šifry;
- IMSI catching - není třeba lámat šifru;
- Flexispy;
- reálný odposlech;

A5/1 - šifra 2G sítě (prolomitelná)

A5/2 - zeslabená varianta A5/1 pro export

A5/3 (KASUMI) - šifra 3G sítě (2010, Dunkleman, Keller and Shamir - prolomení)

¡ Při přechodu 2G→3G nejsou vygenerovány nové klíče!

A5/1 - šifra 2G sítě (prolomitelná)

A5/2 - zeslabená varianta A5/1 pro export

A5/3 (KASUMI) - šifra 3G sítě (2010, Dunkleman, Keller and Shamir - prolomení)

¡ Při přechodu 2G→3G nejsou vygenerovány nové klíče!

A5/1 - šifra 2G sítě (prolomitelná)

A5/2 - zeslabená varianta A5/1 pro export

A5/3 (KASUMI) - šifra 3G sítě (2010, Dunkleman, Keller and Shamir - prolomení)

¡ Při přechodu 2G→3G nejsou vygenerovány nové klíče!

A5/1 - šifra 2G sítě (prolomitelná)

A5/2 - zeslabená varianta A5/1 pro export

A5/3 (KASUMI) - šifra 3G sítě (2010, Dunkleman, Keller and Shamir - prolomení)

¡ Při přechodu 2G→3G nejsou vygenerovány nové klíče!

Obrana

Hardwarová řešení - vyžaduje speciální telefon/sd kartu/přídavné zařízení, ¡klíč od výrobce!

Softwarová řešení - běžné telefony, ale možné problémy s kompatibilitou, latencí...

Hybridní řešení - běžný telefon s vlastním firmwarem/systémem

Obrana

Hardwarová řešení - vyžaduje speciální telefon/sd kartu/přídavné zařízení, ¡klíč od výrobce!

Softwarová řešení - běžné telefony, ale možné problémy s kompatibilitou, latencí...

Hybridní řešení - běžný telefon s vlastním firmwarem/systémem

Obrana

Hardwarová řešení - vyžaduje speciální telefon/sd kartu/přídavné zařízení, ¡klíč od výrobce!

Softwarová řešení - běžné telefony, ale možné problémy s kompatibilitou, latencí...

Hybridní řešení - běžný telefon s vlastním firmwarem/systémem

Cryptocult

Cryptocult je software od české firmy, který umožňuje komunikovat šifrovaně přes mobilní telefony (hovory, zprávy, email);

- Funguje na telefonech se systémem Symbian;
- Náhodná data jsou sbírána z kamery. Kontroluje se dostatečná rozdílnost snímků (např. ve tmě se téměř nic nenasnímá);
- Zprávy - "stálý"klíč, používá se PGP pro instant-messaging a email (resp. AES pro SMS);
- Hovory - jednorázový klíč, ZRTP protokol (mj. výměna klíčů pomocí Diffie-Hellman), AES-256;

Cryptocult

Cryptocult je software od české firmy, který umožňuje komunikovat šifrovaně přes mobilní telefony (hovory, zprávy, email);

- Funguje na telefonech se systémem Symbian;
- Náhodná data jsou sbírána z kamery. Kontroluje se dostatečná rozdílnost snímků (např. ve tmě se téměř nic nenasnímá);
- Zprávy - "stálý"klíč, používá se PGP pro instant-messaging a email (resp. AES pro SMS);
- Hovory - jednorázový klíč, ZRTP protokol (mj. výměna klíčů pomocí Diffie-Hellman), AES-256;

Cryptocult

Cryptocult je software od české firmy, který umožňuje komunikovat šifrovaně přes mobilní telefony (hovory, zprávy, email);

- Funguje na telefonech se systémem Symbian;
- Náhodná data jsou sbírána z kamery. Kontroluje se dostatečná rozdílnost snímků (např. ve tmě se téměř nic nenasnímá);
- Zprávy - "stálý"klíč, používá se PGP pro instant-messaging a email (resp. AES pro SMS);
- Hovory - jednorázový klíč, ZRTP protokol (mj. výměna klíčů pomocí Diffie-Hellman), AES-256;

Cryptocult

Cryptocult je software od české firmy, který umožňuje komunikovat šifrovaně přes mobilní telefony (hovory, zprávy, email);

- Funguje na telefonech se systémem Symbian;
- Náhodná data jsou sbírána z kamery. Kontroluje se dostatečná rozdílnost snímků (např. ve tmě se téměř nic nenasnímá);
- Zprávy - "stálý"klíč, používá se PGP pro instant-messaging a email (resp. AES pro SMS);
- Hovory - jednorázový klíč, ZRTP protokol (mj. výměna klíčů pomocí Diffie-Hellman), AES-256;

Cryptocult

Cryptocult je software od české firmy, který umožňuje komunikovat šifrovaně přes mobilní telefony (hovory, zprávy, email);

- Funguje na telefonech se systémem Symbian;
- Náhodná data jsou sbírána z kamery. Kontroluje se dostatečná rozdílnost snímků (např. ve tmě se téměř nic nenasnímá);
- Zprávy - "stálý"klíč, používá se PGP pro instant-messaging a email (resp. AES pro SMS);
- Hovory - jednorázový klíč, ZRTP protokol (mj. výměna klíčů pomocí Diffie-Hellman), AES-256;

Cryptocult

Cryptocult je software od české firmy, který umožňuje komunikovat šifrovaně přes mobilní telefony (hovory, zprávy, email);

- Funguje na telefonech se systémem Symbian;
- Náhodná data jsou sbírána z kamery. Kontroluje se dostatečná rozdílnost snímků (např. ve tmě se téměř nic nenasnímá);
- Zprávy - "stálý"klíč, používá se PGP pro instant-messaging a email (resp. AES pro SMS);
- Hovory - jednorázový klíč, ZRTP protokol (mj. výměna klíčů pomocí Diffie-Hellman), AES-256;

- Pre-shared secret - metoda proti man-in-the-middle útoku, šance $\frac{1}{2^{16}}$;
- Po skončení hovoru se klíč zahazuje;
- Software má vlastní grafické rozhraní;

- Pre-shared secret - metoda proti man-in-the-middle útoku, šance $\frac{1}{2^{16}}$;
- Po skončení hovoru se klíč zahazuje;
- Software má vlastní grafické rozhraní;

Realita

Teorie je jedna věc, ale v praxi se můžete potýkat s problémy:

- Uzavřenost mobilních platforem, certifikace přístupů k citlivým věcem;
- spotřeba baterie (nutnost být připojen na internet);
- kvůli certifikátům vznikla potřeba oddělit jádro aplikace od voice-serveru -> vznikly problémy;
- jedno vlákno může utlačit ostatní;
- wifi přechízí po 100ms do úsporného režimu;

Realita

Teorie je jedna věc, ale v praxi se můžete potýkat s problémy:

- Uzavřenost mobilních platforem, certifikace přístupů k citlivým věcem;
- spotřeba baterie (nutnost být připojen na internet);
- kvůli certifikátům vznikla potřeba oddělit jádro aplikace od voice-serveru -> vznikly problémy;
- jedno vlákno může utlačit ostatní;
- wifi přechízí po 100ms do úsporného režimu;

Realita

Teorie je jedna věc, ale v praxi se můžete potýkat s problémy:

- Uzavřenost mobilních platforem, certifikace přístupů k citlivým věcem;
- spotřeba baterie (nutnost být připojen na internet);
- kvůli certifikátům vznikla potřeba oddělit jádro aplikace od voice-serveru -> vznikly problémy;
- jedno vlákno může utlačit ostatní;
- wifi přechízí po 100ms do úsporného režimu;

Realita

Teorie je jedna věc, ale v praxi se můžete potýkat s problémy:

- Uzavřenost mobilních platforem, certifikace přístupů k citlivým věcem;
- spotřeba baterie (nutnost být připojen na internet);
- kvůli certifikátům vznikla potřeba oddělit jádro aplikace od voice-serveru -> vznikly problémy;
- jedno vlákno může utlačit ostatní;
- wifi přechízí po 100ms do úsporného režimu;

Realita

Teorie je jedna věc, ale v praxi se můžete potýkat s problémy:

- Uzavřenost mobilních platforem, certifikace přístupů k citlivým věcem;
- spotřeba baterie (nutnost být připojen na internet);
- kvůli certifikátům vznikla potřeba oddělit jádro aplikace od voice-serveru -> vznikly problémy;
- jedno vlákno může utlačit ostatní;
- wifi přechízí po 100ms do úsporného režimu;

- fragmentace paměti a zpomalení aplikace;
- neobjasnitelné rozdílné chování různých kusů téhož modelu telefonu;

- fragmentace paměti a zpomalení aplikace;
- neobjasnitelné rozdílné chování různých kusů téhož modelu telefonu;

- fragmentace paměti a zpomalení aplikace;
- neobjasnitelné rozdílné chování různých kusů téhož modelu telefonu;

Další věci k ochraně

Znemožnit/znepříjemnit triangulaci;

Anonymizace komunikace;

Další věci k ochraně

Znemožnit/znepříjemnit triangulaci;

Anonymizace komunikace;