Název přednášky: „SIM karty a bezpečnost v mobilních sítích“

SIM karty vydávané telekomunikačními operátory má každý z nás v mobilním telefonu. Zkratka SIM znamená „Subscriber Identity Module“ a vychází ze základní funkce SIM, kterou je identifikace účastníků v mobilní síti. Možnosti SIM karet se postupným vývojem neustále rozšiřují. Operátoři na karty umisťují aplikace napsané v jazyce JavaCard, které umožňují zákazníkům zjistit aktuální předpověď počasí, jízdní řád či například obsluhovat bankovní účet. Především u bankovních aplikací jsou kladeny pochopitelné nároky na bezpečnost a spolehlivost prováděných operací.
Cílem přednášky je poodhalit posluchačům základními technické vlastnosti SIM karet, jejich současné možnosti a omezení. Hlavní funkcí SIM je, a do budoucna zřejmě stále bude, identifikace a autentizace účastníků; v přednášce budou proto ukázány autentizační protokoly a algoritmy používané v GSM a uvedeny jejich známé slabé stránky a vylepšení, která oproti GSM přináší modernější systém UMTS. Dále budou představeny možnosti, které pro vývoj mobilních aplikací poskytuje jazyk JavaCard a jeho rozšíření SIM Toolkit pro vývoj uživatelského rozhraní, provádění kryptografických operací a navázání zabezpečené komunikace se servery operátora pomocí šifrovaných a digitálně podepsaných SMS zpráv. Na závěr bude ukázáno, jak lze tyto možnosti využít v aplikacích mobilního bankovnictví.
Přednáška se snaží být přístupným náčrtem toho, co umí SIM karty vložené v mobilních telefonech posluchačů, proto u nich nepředpokládá žádné speciální znalosti z oboru telekomunikací nebo čipových karet.